



Web渗透技术 及 实战案例解析

陈小兵 范渊 孙立伟 编著



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>



Web渗透技术 及 实战案例解析

陈小兵 范渊 孙立伟 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

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。

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做渗透。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 Google 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、ラ林ゼ等。

编 者

2011 年 10 月于北京

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	1.10 MD5 加密与解密	52
1.6.6 使用 GetHashes 获取系统 Hash 值技巧	34	1.10.1 有关 MD5 加解密知识	53
1.6.7 相关免费资源	34	1.10.2 通过 cmd5 网站生成 MD5 密码	53
1.7 使用 Saminside 获取系统密码	34	1.10.3 通过 cmd5 网站破解 MD5 密码	53
1.7.1 下载和使用 Saminside	34	1.10.4 在线 MD5 破解网站收费破解高难度的 MD5 密码值	54
1.7.2 使用 Scheduler 导入本地用户的 Hash 值	35	1.10.5 使用字典暴力破解 MD5 密码值	55
1.7.3 查看导入的 Hash 值	35	1.10.6 一次破解多个密码	57
1.7.4 导出系统用户的 Hash 值	35	1.10.7 MD5 变异加密方法破解	58
1.7.5 设置 Saminside 破解方式	36	1.11 Serv-U 密码破解	59
1.7.6 执行破解	37	1.11.1 获取 ServUDAemon.ini 文件	59
1.7.7 使用 Ophcrack 破解用户密码值	37	1.11.2 查看 ServUDAemon.ini 文件	59
1.8 使用 WinlogonHack 获取系统密码	38	1.11.3 破解 Serv-U 密码	61
1.8.1 远程终端技术 APP 和远程终端密码泄露分析	38	1.11.4 验证 Ftp	62
1.8.2 使用 WinlogonHack 工具软件截取密码原理	39	1.12 Access 数据库破解实战	63
1.8.3 使用 WinlogonHack 获取密码实例	40	1.12.1 Access 数据库的基本知识	63
1.8.4 攻击方法探讨	42	1.12.2 Access 数据库的主要特点	63
1.8.5 防范方法探讨	43	1.12.3 Access 数据库的缺点和局限性	64
1.9 使用 Ophcrack 破解系统 Hash 密码	43	1.12.4 Access 数据库版本	64
1.9.1 通过已有信息再次进行搜索和整理	44	1.12.5 Access 密码实战破解实例	64
1.9.2 安装 Ophcrack 软件	45	1.13 巧用 Cain 破解 MySQL 数据库密码	66
1.9.3 使用 Ophcrack 软件	46	1.13.1 MySQL 加密方式	67
1.9.4 下载彩虹表	46	1.13.2 MySQL 数据库文件结构	68
1.9.5 设置彩虹表	46	1.13.3 获取 MySQL 数据库用户密码加密字符串	68
1.9.6 准备破解材料	48	1.13.4 将 MySQL 用户密码字符串加入到 Cain 破解列表	69
1.9.7 开始破解	48	1.13.5 使用字典进行破解	70
1.9.8 彩虹表破解密码防范策略	51	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	2.3.1 AspxSpy 简介	116
1.15.2 添加 Shell	85	2.3.2 源代码简要分析	117
1.15.3 连接一句话后门	86	2.3.3 动手打造自己的 WebShell	118
1.15.4 执行文件操作	86	2.3.4 寻找他人的 WebShell	120
1.15.5 有关一句话后门的收集与整理	87	2.3.5 处理获取的 WebShell	121
1.16 远程终端的安装与使用	90	2.3.6 总结与探讨	125
1.16.1 Windows 2000 Server 开启远程 终端	90	2.4 用 phpWebShell 抓肉鸡	125
1.16.2 Windows XP 开启远程终端	90	2.4.1 使用搜索引擎查找 WebShell	126
1.16.3 Windows 2003 开启远程终端	93	2.4.2 进行相关信息收集	127
1.16.4 一些常见开启远程终端服务的 方法	95	2.4.3 获取 WebShell 与提权	127
1.16.5 开启远程终端控制案例	96	2.4.4 总结与探讨	132
1.16.6 命令行开启远程终端	98	2.5 利用 JFolder 后门渗透某网站	132
1.16.7 3389 实用技巧	98	2.5.1 JFolder 搜索与测试	132
第 2 章 Google ——爱你又恨你	109	2.5.2 Web 渗透测试	133
2.1 Google 批量注入	109	2.5.3 服务器提权	134
2.1.1 使用啊 D 注入工具搜索 SQL 注入点	109	2.5.4 其他信息获取	138
2.1.2 进行 SQL 注入测试	110	2.5.5 总结与探讨	139
2.1.3 总结与探讨	111	2.6 Public 权限渗透某 asp.net 网站	139
2.2 Google 搜索 WebShell 的实际处理 思路	112	2.6.1 寻找 SQL 注入点	140
2.2.1 通过 Google 搜索相应的 WebShell 关键字	112	2.6.2 使用工具进行信息收集和数 据猜测	140
2.2.2 处理搜索结果	112	2.6.3 获取 SQL 注入点	141
2.2.3 破解登录密码	113	2.6.4 猜解数据库中的表和数据	142
2.2.4 漏洞测试	113	2.6.5 扫描和获取后台地址	142
2.2.5 获取 WebShell	114	2.6.6 登录测试和验证	142
2.2.6 实施控制	115	2.6.7 寻找、测试和获取 WebShell	144
2.2.7 总结与探讨	116	2.6.8 尝试提权	146
2.3 从 Aspx 的 WebShell 到肉鸡	116	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	3.4 从 CuteEditor 漏洞利用到全面控制	
2.7.5 总结与探讨	161	服务器	181
第 3 章 都是文件上传惹的祸	162	3.4.1 漏洞扫描	181
3.1 利用 FCKeditor 漏洞渗透某 Linux		3.4.2 网站目录访问测试	182
服务器	162	3.4.3 使用社工进行登录测试	182
3.1.1 一个 Shell 引发的渗透	163	3.4.4 寻找突破点	182
3.1.2 验证 WebShell	163	3.4.5 修改管理员	183
3.1.3 分析 WebShell	164	3.4.6 获取该网站所在服务中的所有	
3.1.4 上传 WebShell	165	其他域名	184
3.1.5 测试上传的 WebShell	166	3.4.7 扫描漏洞	185
3.1.6 对 WebShell 所在服务器进行分析		3.4.8 SQL 注入手工测试	185
与信息收集	167	3.4.9 获取数据库类型	186
3.1.7 服务器提权	168	3.4.10 使用 Pangolin 进行 SQL 注入	
3.1.8 总结与探讨	171	测试	187
3.2 渗透某培训网站	171	3.4.11 通过 CuteEditor 上传而获得	
3.2.1 使用 Jsky 进行漏洞扫描	171	突破	187
3.2.2 SQL 注入获取管理员密码	171	3.4.12 提升权限	191
3.2.3 直接上传 WebShell	172	3.4.13 安全建议和总结	194
3.2.4 获取 WebShell	173	3.5 Dvbbs8.2 插件上传漏洞利用	195
3.2.5 服务器提权	173	3.5.1 使用 Google 搜索	196
3.2.6 登录服务器	173	3.5.2 注册用户	196
3.2.7 抓取系统密码并破解	174	3.5.3 修改样式	196
3.2.8 总结与探讨	174	3.5.4 无上传界面	197
3.3 利用 Flash 上传漏洞渗透国内某		3.5.5 成功上传文件	198
网站	175	3.5.6 使用一句话客户端进行连接	199
3.3.1 利用弱口令进入系统	175	3.5.7 获取网站的物理路径	199
3.3.2 寻找可利用漏洞	176	3.5.8 提权失败	200
3.3.3 获取 WebShell	177	3.5.9 查找并下载数据库	201
3.3.4 服务器提权	178	3.5.10 Dvbbs8.2 渗透思路与防范措施	201
3.3.5 获取管理员密码	179	3.6 利用 cfm 上传漏洞渗透某服务器	202
3.3.6 相邻服务器的渗透	180	3.6.1 手工查找和自动扫描漏洞	202
3.3.7 总结与探讨	180	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	3.9.7 获取 WebShell	221
3.6.5 关闭防火墙	204	3.9.8 获取管理员密码	222
3.6.6 成功登录 3389	205	3.9.9 下载数据库和源程序	224
3.6.7 收集其他信息	205	3.9.10 总结与探讨	224
3.6.8 渗透 mail 服务器	206		
3.6.9 总结与探讨	207	第 4 章 SQL 注入——渗透主乐章	226
3.7 EWebEditor 编辑器漏洞攻击案例	207	4.1 对某学校网站的安全检测和加固	227
3.7.1 发现网站使用 EWebEditor 编辑器	207	4.1.1 漏洞挖掘	227
3.7.2 下载 EWebEditor 默认数据库文件	208	4.1.2 提升权限	233
3.7.3 打开数据库并执行管理员密码 破解	208	4.1.3 内网渗透	235
3.7.4 进入样式管理	208	4.1.4 安全加固	238
3.7.5 修改样式管理中的运行上传类型	208	4.2 对某 CMS 一次安全检测和漏洞分析	242
3.7.6 上传网页木马文件	209	4.2.1 对某 CMS 的初步安全检查	242
3.7.7 实施控制	211	4.2.2 在本地进行安全测试	244
3.7.8 上传其他文件	211	4.2.3 挖掘并查找安全漏洞	245
3.7.9 获取信息和进一步控制	211	4.2.4 后台拿 WebShell	255
3.8 渗透某大学服务器	212	4.2.5 直接拿 WebShell	257
3.8.1 寻找并绕过后台登录验证	212	4.2.6 总结与探讨	259
3.8.2 成功进入后台	213	4.3 对某 SEO 公司网站的一次安全检测	259
3.8.3 寻找上传地址	213	4.3.1 常规检测	259
3.8.4 使用一句话后门客户端进行连接	214	4.3.2 网站安全性检测	261
3.8.5 获取服务器的基本信息	215	4.3.3 获取网站 WebShell	266
3.8.6 上传大的 WebShell	215	4.3.4 总结与探讨	266
3.8.7 通过数据库提权	215	4.4 对韩国某网站 CMS 界面的一次安全 检测	268
3.8.8 备份数据库和代码	216	4.4.1 服务器信息收集	268
3.9 密码绕过获取某站点 WebShell	217	4.4.2 Web 应用程序安全检测	272
3.9.1 获取 SQL 注入点	217	4.4.3 总结与探讨	285
3.9.2 进行 SQL 注入基本操作	217	4.5 对某公司站点的一次安全检查	285
3.9.3 数据库猜测	218	4.5.1 漏洞踩点	285
3.9.4 使用 Havij 进行 SQL 注入猜测	218	4.5.2 在线寻找漏洞信息	286
3.9.5 扫描网站管理员登录入口	219	4.5.3 数据库内容分析和获取	287
3.9.6 尝试密码绕过验证登录	220	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	4.8.8 成功创建 WebShell	318
4.5.6 登录后台并修改相应设置	291	4.8.9 成功获取并连接 WebShell	319
4.5.7 上传文件	292	4.8.10 提升权限	319
4.5.8 查看 WebShell 并进行控制	293	4.8.11 总结与探讨	320
4.5.9 安全评估结果和补救措施	293	4.9 对某游戏网站的安全检测	320
4.6 对某虚拟主机的一次安全渗透	294	4.9.1 基本信息收集	320
4.6.1 获取虚拟主机某一站点的 WebShell	294	4.9.2 Web 程序安全检测	321
4.6.2 使用 WebShell 中的“提权功能” 进行提权尝试	295	4.9.3 获得突破	323
4.6.3 查看可写目录	296	4.9.4 获取系统权限	326
4.6.4 渗透成功	298	4.9.5 总结与探讨	328
4.6.5 继续渗透内外网	300	4.10 对某手表网站的一次安全检测	328
4.6.6 总结与探讨	302	4.10.1 信息收集	330
4.7 对某职教网的一次安全渗透	302	4.10.2 寻找注入点	331
4.7.1 基本信息收集	302	4.10.3 尝试对其他站点进行渗透	332
4.7.2 口令检测	304	4.10.4 获取突破点	333
4.7.3 获取信息分析与利用	304	4.10.5 新的转机	336
4.7.4 获取 WebShell	305	4.10.6 安全防范措施	341
4.7.5 实施控制和渗透	306	4.10.7 总结与探讨	341
4.7.6 内网渗透和查看	308	4.11 对某软件公司网站的一次安全检测	342
4.7.7 简单的安全加固	312	4.11.1 安全检查原因	342
4.7.8 总结与探讨	312	4.11.2 信息收集	343
4.8 手工对某重点大学网站的一次安全 检测	313	4.11.3 弱口令扫描	344
4.8.1 获取出错信息	313	4.11.4 Ftp 扫描结果处理与应用	345
4.8.2 获取注射的长度	314	4.11.5 获取 WebShell 与提权	347
4.8.3 获取数据库配置文件路径	315	4.11.6 系统安全情况与安全加固	351
4.8.4 获取数据库密码	316	4.11.7 总结与探讨	354
4.8.5 查看 magic_quotes_gpc 参数的值	316	4.12 Access 注入获取 WebShell	354
4.8.6 使用 PhpMyadmin 来管理 MySQL 数据库	317	4.12.1 扫描漏洞	355
4.8.7 创建 WebShell 失败	317	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	4.16.5 获取管理员入口和进行登录 测试	399
4.13.1 基本信息探测与获取	359	4.16.6 获取漏洞的完整扫描结果以及 安全评估	401
4.13.2 手工判断是否存在 SQL 注入点 ...	360	4.16.7 总结与探讨	401
4.13.3 获取 MySQL 数据库版本	360	4.17 对某私服网站的一次渗透	403
4.13.4 Ftp 服务器测试以及利用	360	4.17.1 获取目标初步信息	403
4.13.5 获取 MySQL 数据库当前用户 的密码	362	4.17.2 SQL 注入安全检测	404
4.13.6 获取 phpMyadmin	362	4.17.3 获取突破	408
4.13.7 猜解管理员密码	363	4.17.4 陷阱	411
4.13.8 上传大马	364	4.17.5 尾声	413
4.13.9 进入服务器	364	4.18 对国外某站点的一次安全检测	414
4.13.10 总结与探讨	365	4.18.1 善用 Google 搜索	414
4.14 对杀毒软件网站的一次安全检测	365	4.18.2 手工进行注入点判断	415
4.14.1 基本信息收集	365	4.18.3 获取脚本错误提示	415
4.14.2 Web 程序安全检测	367	4.18.4 使用工具进行 SQL 注入测试	415
4.14.3 使用 Jsky 扫描系统漏洞	369	4.18.5 获取管理员密码	416
4.14.4 利用 Pangolin 进行渗透测试	370	4.18.6 扫描后台登录地址	417
4.14.5 获取网站后台管理地址	372	4.18.7 后台登录测试	417
4.14.6 登录某杀毒软件媒体联盟 管理系统	373	4.18.8 寻找上传地址	418
4.14.7 获取 WebShell 和提升权限	375	4.18.9 文件上传测试	418
4.14.8 总结与探讨	382	4.18.10 获取 WebShell	419
4.15 对某医科大网站的渗透检测	383	4.18.11 获取数据库密码	420
4.15.1 战前踩点	383	4.18.12 总结与探讨	421
4.15.2 实战提权和渗透	386		
4.15.3 同网段渗透	392	第 5 章 高级渗透技术	422
4.15.4 总结与探讨	396	5.1 社工入侵	422
4.16 安全检测易商科技类企业管理系统 ...	397	5.1.1 安全检测	423
4.16.1 使用 Jsky 扫描漏洞点	397	5.1.2 小遇周折, 提权成功	426
4.16.2 使用 Pangonlin 进行 SQL 注入探测	397	5.1.3 我也来社工	429
4.16.3 换一个工具进行检查	397	5.1.4 总结与探讨	433
4.16.4 检测表段和检测字段	398	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	5.8.2	使用 Havij SQL 注入攻击进行 自动检测	485
5.2.3	利用社会工程学进行反渗透	436	5.8.3	获得管理员账号和密码	485
5.2.4	总结与探讨	441	5.8.4	尝试读取 Linux 系统中的文件	486
5.3	顺藤摸瓜成功控制某大学投稿系统	441	5.8.5	构建和获取 WebShell	488
5.3.1	意外收获	441	5.8.6	提权以及下载数据库	490
5.3.2	服务器渗透之提权	443	5.9	巧用 G6FTPServer 账号渗透某服务器	492
5.3.3	渗透中的渗透	451	5.9.1	扫描漏洞	492
5.3.4	总结与探讨	451	5.9.2	SQL 注入漏洞实际测试	493
5.4	利用 IIS 写权限成功渗透西南某高校 OA 系统	452	5.9.3	获取 WebShell	493
5.4.1	IIS 写权限原理	452	5.9.4	渗透提权测试	497
5.4.2	实际渗透测试	453	5.9.5	总结与探讨	500
5.4.3	提升权限	456	5.10	对某网站的一次安全检查	500
5.4.4	安全防范与加固	458	5.10.1	关于新云网站管理系统漏洞	500
5.4.5	总结与探讨	459	5.10.2	偶遇目标站点	501
5.5	对某安全网站的一次渗透	460	5.10.3	从后台寻找关键信息	501
5.5.1	艰难的渗透之路	460	5.10.4	进行漏洞实际测试	503
5.5.2	服务器提权	462	5.10.5	获取数据库的实际地址, 下载 数据库文件	504
5.5.3	总结与探讨	469	5.10.6	登录后台并上传 asp 木马文件	504
5.6	对某贸易公司内网的一次安全检测	469	5.10.7	备份数据库得到 WebShell	505
5.6.1	内网渗透之信息收集	469	5.10.8	搜索漏洞关键字	506
5.6.2	利用已有漏洞实施渗透攻击	471	5.10.9	总结与探讨	508
5.6.3	社会工程学攻击	473	5.11	突破防篡改继续上传	509
5.6.4	总结与探讨	479	5.11.1	初遇防篡改	509
5.7	JBoss 获取 WebShell	479	5.11.2	突破上传	511
5.7.1	使用漏洞特征进行搜索	480	5.12	Tomcat 弱口令搞定某 Linux 服务器	512
5.7.2	访问网站并进行漏洞测试	480	5.12.1	使用 Apache Tomcat Crack 暴力 破解 Tomcat 口令	512
5.7.3	添加 WebShell 的 war 文件地址	480	5.12.2	对扫描结果进行测试	513
5.7.4	应用修改使设置生效	481	5.12.3	部署 war 格式的 WebShell	513
5.7.5	充实“武器库”	482	5.12.4	查看 Web 部署情况	514
5.7.6	获得 WebShell	483	5.12.5	获取 WebShell	515
5.8	对某 Linux 网站的一次渗透	484	5.12.6	查看用户权限	515
5.8.1	SQL 注入测试	484			

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

6.4.2 Citrix 的工作方式.....	577	6.7.12 总结与探讨.....	602
6.4.3 一个 Citrix 渗透实例.....	578	6.8 老 Y 文章管理系统 V2.2 注入漏洞分析 与利用.....	602
6.5 DZ7.1 and 7.2 远程代码执行漏洞 获取 WebShell	583	6.8.1 前期分析.....	602
6.5.1 漏洞形成原理分析.....	583	6.8.2 漏洞分析.....	602
6.5.2 漏洞的具体应用	585	6.8.3 网络实战.....	603
6.5.3 后记.....	590	6.8.4 实践体会.....	605
6.6 由 WordPress 获取 WebShell	590	6.9 使用 Discuz!NT3.5.2 文件编辑 0day 获取 WebShell	605
6.6.1 获取管理员用户名和密码.....	591	6.9.1 登录后台.....	605
6.6.2 寻找上传处.....	591	6.9.2 文件模板编辑 0day	605
6.6.3 浏览上传记录.....	592	6.9.3 利用模板文件编辑 0day	606
6.6.4 获取 WebShell 的直接地址	592	6.9.4 获取网站的真实路径.....	607
6.6.5 获取 WebShell	593	6.9.5 获取 WebShell	607
6.6.6 其他方法获取 WebShell 的探讨	593	6.9.6 还原原文件源代码.....	607
6.7 由 PHP168 任意文件下载 0day 到 服务器提权.....	594	6.9.7 数据库信息暴露 0day	608
6.7.1 使用 simplegoogle 工具搜索 使用 PHP168 系统的网站.....	594	6.9.8 备份网站数据库.....	608
6.7.2 使用转换工具进行 base64 地址 转换.....	594	6.9.9 压缩源代码程序.....	609
6.7.3 下载任意 PHP 文件.....	595	6.10 Discuz!6.0 管理员编辑模板文件 获取 WebShell	609
6.7.4 使用记事本编辑 adminlogin_ logs.php 文件	595	6.10.1 编辑板块.....	610
6.7.5 破解管理员的 MD5 密码值和登录 网站后台.....	596	6.10.2 模板编辑.....	610
6.7.6 获取网站系统的 WebShell	596	6.10.3 选择一种模板进行编辑.....	610
6.7.7 尝试提升系统权限.....	598	6.10.4 获取一句话后门.....	611
6.7.8 使用 udf 提升系统权限.....	599	6.11 Discuz!6.0 管理员权限插件导入 获取 WebShell	612
6.7.9 直接上传 PHP 大马.....	600	6.11.1 导入插件.....	612
6.7.10 查看系统开放端口和打开 3389 远程终端.....	600	6.11.2 查看导入的插件.....	612
6.7.11 使用端口转发程序成功进入该 服务器.....	601	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	7.3.5 总结与探讨	633
6.12.4 启用导入的插件 WebShell	616	7.4 Windows 2008 中 Magic Winmail Server 提权	633
6.12.5 查看 WebShell 地址	616	7.4.1 获取 Winmail 目录地址	633
6.12.6 获取 WebShell	617	7.4.2 执行 whoami 命令	633
第 7 章 Windows 提权与安全防范	618	7.4.3 添加用户到管理员组	634
7.1 Microsoft SQL Server 2005 提权	618	7.4.4 设置并登录远程终端服务器	636
7.1.1 查看数据库连接文件	618	7.4.5 Winmail 邮箱用户与口令	637
7.1.2 获取数据库用户和密码	619	7.4.6 进入邮箱	638
7.1.3 数据库连接设置	619	7.4.7 Winmail 服务器防范	638
7.1.4 查看连接信息	620	7.5 Pr 提权渗透国外某高速服务器	639
7.1.5 添加“xp_cmdshell”存储过程	620	7.5.1 分析 AWS 扫描结果	639
7.1.6 添加用户	621	7.5.2 获取直接文件上传地址	640
7.1.7 将普通用户添加到管理员组	622	7.5.3 直接上传网页木马测试	640
7.1.8 通过“XP_cmdshell exec”查看系统用户	622	7.5.4 创建并操作一句话后门	640
7.1.9 远程终端登录	623	7.5.5 上传大马进行管理	642
7.1.10 总结与探讨	623	7.5.6 查看网站服务器文件	642
7.2 MySQL 数据库提权	624	7.5.7 查询目标网站所在服务器下的所有域名	643
7.2.1 设置 MySQL 提权脚本文件	624	7.5.8 分析 site.mdb 数据库	644
7.2.2 进行连接测试	624	7.5.9 通过 Ftp 上传 WebShell	644
7.2.3 创建“Shell”函数	624	7.5.10 Pr 提权	645
7.2.4 查看用户	625	7.5.11 获取远程终端端口	647
7.2.5 创建具有管理员权限的用户	626	7.5.12 登录远程终端	648
7.2.6 提权成功	627	7.6 Jboss 信息查看获取 WebShell	648
7.2.7 总结与探讨	628	7.6.1 测试 Jboss 网页	648
7.3 Serv-U 提权	629	7.6.2 查看 Tomcat 状态	648
7.3.1 利用 WebShell 查看系统管理员用户组	629	7.6.3 执行命令测试	649
7.3.2 执行 SU Exp	630	7.6.4 下载 JspWebShell 的 txt 文件到本地	650
7.3.3 检查 Serv-U 提权情况	631	7.6.5 寻找可运行路径	651
7.3.4 远程终端登录测试	632	7.6.6 查看 Jboss 默认部署路径的文件和目录	651