

《Web渗透技术及实战案例解析》

图书基本信息

书名：《Web渗透技术及实战案例解析》

13位ISBN编号：9787121161810

10位ISBN编号：7121161818

出版时间：2012-4

出版社：电子工业出版社

作者：陈小兵

页数：698

译者：范渊,孙立伟

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Web渗透技术及实战案例解析》

内容概要

《Web渗透技术及实战案例解析》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。《Web渗透技术及实战案例解析》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《Web渗透技术及实战案例解析》可以快速掌握目前Web渗透的主流技术。《Web渗透技术及实战案例解析》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、Oday攻击和Windows提权与安全防范等。

《Web渗透技术及实战案例解析》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，Oday攻防，Windows提权与安全防范等。

书籍目录

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	ServU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ServU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 ServU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ServU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

章节摘录

版权页：插图：

《Web渗透技术及实战案例解析》

编辑推荐

《Web渗透技术及实战案例解析》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。

精彩短评

- 1、只是讲操作 没有讲原理
- 2、看后受益匪浅、推荐朋友们阅读、
- 3、应该说是文集
- 4、渗透经典
- 5、感觉不错，很喜欢
- 6、书一般，书中图片篇幅比较多，适合入门级别的人阅读
- 7、我很常后悔买这本书，原因这本书内容时老的，而且大多都是网上收集来的，进了他们安天365的群说了句这内容是网上收集来的，结果我被踢了，后来我问管理员为什么踢我，他说讨厌我，不行吗？面对我们弱势群体买本书还被骗 我对这个社会表示深深的无奈
- 8、使用中 我也不知道
- 9、新书，感觉不错
- 10、实战就是扫描？
- 11、适合网络渗透的初步进阶
- 12、网上有人推荐说适合作为安全入门.....可是我看为什么都是一大堆工具的使用，还有不少的默认密码登陆，案例讲来讲去就是那几个套路.....可能是我连入门的资格都没有吧？WTF.....
- 13、该书内容还算挺好的了

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com