

ATTACK

在攻与防的对立统一中
寻求技术突破

黑客攻防 从入门到精通

Web技术实战篇

明月工作室 王栋◎编著

超值赠送

黑客攻防全能视频+计算机硬件管理超级手册+Windows文件管理高级手册+Linux命令应用大全

以下人群请勿翻阅本书:

1. 自以为很牛，对黑客不屑一顾的人
2. 心存侥幸，认为黑客离自己很远的人
3. 习惯黑客攻击，总是折腾他人的人
4. 号太多，习惯被盗号的人
5. 不差钱，不怕被盗刷的人
6. 我不是Boss，对交易安全漠不关心的人

DEFENSE



北京大学出版社
PEKING UNIVERSITY PRESS

黑客攻防

从入门到精通

Web技术实战篇

明月工作室 王栋◎编著



北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

本书由浅入深、图文并茂地再现了计算机安全相关的多方面知识。

全书共18章,主要讲了什么是Web安全,Web应用程序的安全剖析,对Web应用程序进行入侵及防范技术,利用验证机制漏洞入侵Web及防范技术,利用访问控制漏洞入侵Web及防范技术,利用会话管理漏洞入侵Web及防范技术,利用编程方式进行Web入侵及防范技术,实现数据存储区的入侵及防范技术,实现数据库入侵及防范技术,利用Cookies攻击及防范技术,利用文件上传漏洞的攻击及防范技术,实现XSS(跨站脚本攻击)及防范技术,实现攻击Web服务器及防范技术,实现Web入侵及防范技术,Web框架安全,时下最新技术安全解析——HTML5安全,Web安全新领域——Wi-Fi安全攻防,企业Web应用安全计划——全计划。

本书语言简洁、流畅,内容丰富全面,适用于计算机初、中级用户,计算机维护人员,IT从业人员以及对黑客攻防与网络安全维护感兴趣的计算机中级用户,各大计算机培训班也可以将其作为辅导用书。

图书在版编目(CIP)数据

黑客攻防从入门到精通 Web技术实战篇 / 王栋编著. — 北京:北京大学出版社, 2017.2
ISBN 978-7-301-27903-8

I. ①黑… II. ①王… III. ①黑客 - 网络防御 IV. ①TP393.081

中国版本图书馆CIP数据核字(2016)第313913号

书 名: 黑客攻防从入门到精通 (Web技术实战篇)

HEIKE GONGFANG CONG RUMEN DAO JINGTONG

著作责任者: 明月工作室 王栋 编著

责任编辑: 尹 毅

标准书号: ISBN 978-7-301-27903-8

出版发行: 北京大学出版社

地 址: 北京市海淀区成府路205号 100871

网 址: <http://www.pup.cn> 新浪微博: @北京大学出版社

电子信箱: pup7@pup.cn

电 话: 邮购部62752015 发行部62750672 编辑部62580653

印 刷 者: 三河市博文印刷有限公司

经 销 者: 新华书店

787毫米×1092毫米 16开本 33.25印张 728千字

2017年2月第1版 2017年2月第1次印刷

印 数: 1-3000册

定 价: 69.00元

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

举报电话: 010-62752024 电子信箱: fd@pupku.edu.cn

图书如有印装质量问题,请与出版部联系,电话: 010-62756370



从2003年起，中国互联网逐渐找到了适合国情的商业模式和发展道路，互联网应用呈现多元化局面，电子商务、网络游戏、视频网站、社交娱乐等百花齐放。计算机技术及通信技术的进一步发展，持续催动中国互联网新一轮的高速增长，截至2008年，我国网民数量已经达到2.53亿户，首次超过美国，跃居世界首位。

2009年开始，移动互联网兴起；互联网与移动互联网共同营造了当前双网互联的盛世。网络已经成为个人生活与工作中获取信息的重要手段，网络购物也已经成为民众重要的消费渠道。当前，“互联网+”的战略布局与工业4.0的深入发展，使得国家经济发展、民众工作生活，都与网络休戚相关，一个安全的网络环境是必不可少的。

当前面临的最大问题是广大用户对网络相关软硬件技术的掌握程度远远不够，这就为不法分子提供了大量的机会，借助于计算机网络滋生的各种网络病毒、木马、流氓软件、间谍软件，给广大网络用户的个人信息及财产带来了非常大的威胁。

为提升广大民众对于计算机网络安全知识的掌握程度，做好个人信息财产安全的防护，我们编著了这套“黑客攻防从入门到精通”丛书，本书为其中的《黑客攻防从入门到精通（Web技术实战篇）》分册。

丛书书目

黑客攻防从入门到精通（全新升级版）

黑客攻防从入门到精通（Web技术实战篇）

黑客攻防从入门到精通（Web脚本编程篇·全新升级版）

黑客攻防从入门到精通（黑客与反黑工具篇·全新升级版）

黑客攻防从入门到精通（加密与解密篇）

黑客攻防从入门到精通（手机安全篇·全新升级版）

黑客攻防从入门到精通（应用大全篇·全新升级版）

黑客攻防从入门到精通（命令实战篇·全新升级版）

黑客攻防从入门到精通 (社会工程学篇)

本书特点

- 内容全面：涵盖了从计算机黑客攻防入门，到专业级的Web 技术安全知识，适合各个层面、不同基础的读者阅读。
- 与时俱进：本书主要适用于Windows 7 及更高版本的操作系统用户阅读。尽管本书中的许多工具、案例等可以在Windows XP 等系统下运行或使用，但为了能够顺利学习本书全部的内容，强烈建议广大读者安装Windows 7 及更高版本的操作系统。
- 任务驱动：本书理论和实例相结合，在介绍完相关知识点以后，即以案例的形式对该知识点进行运用，加深读者对该知识点的理解和认知能力，力争彻底掌握该知识点。
- 适合阅读：本书摒弃了大量枯燥文字叙述的编写方式，而是采用了图文并茂的方式进行编排，以大量的插图进行讲解，可以让读者的学习过程更加轻松。
- 深入浅出：本书内容从零起步，步步深入，通俗易懂，由浅入深地讲解，使初学者和具有一定基础的用户的计算机操作能力都能得到逐步提高。

读者对象

- 计算机初、中级用户。
- 网店店主、网店管理及开发人员。
- 计算机爱好者、提高者。
- 各行各业需要网络防护的人员、中小企业的网络管理员。
- Web 前、后端的开发及管理人员。
- 无线网络相关行业的从业人员。
- 计算机及网络相关的培训机构。
- 大中专院校相关学生。

本书结构及内容

本书一共有18章内容。内容由浅入深，循序渐进，前后衔接紧密，逻辑性较强。

第1章 什么是Web 安全

第2章 Web 应用程序的安全剖析

第3章 对Web 应用程序入侵及防范技术

第4章 利用验证机制漏洞入侵Web 及防范技术

第5章 利用访问控制漏洞入侵Web 及防范技术

- 第6章 利用会话管理漏洞入侵 Web 及防范技术
- 第7章 利用编程方式进行 Web 入侵及防范技术
- 第8章 数据存储区的入侵及防范技术
- 第9章 数据库入侵及防范技术
- 第10章 利用 Cookies 攻击及防范技术
- 第11章 利用文件上传漏洞的攻击及防范技术
- 第12章 实现 XSS (跨站脚本攻击) 及防范技术
- 第13章 攻击 Web 服务器及防范技术
- 第14章 Web 入侵及防范技术
- 第15章 Web 框架安全
- 第16章 时下最新技术安全解析——HTML5 安全
- 第17章 Web 安全新领域——Wi-Fi 安全攻防
- 第18章 企业 Web 应用安全计划——全计划



超值赠送资源

1. 黑客攻防全能视频

为了读者能全面地了解黑客方面的知识从而有效地防御黑客的不法入侵行为,本书特赠送黑客攻防全能教学视频,视频内容包括社会工程学、黑客攻防入门、信息的扫描与嗅探、木马与病毒的防范、系统漏洞防范、远程控制术、加密与解密、数据备份与恢复、移动网络安全等内容。

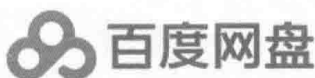
2. 其他赠送资源

- Windows 系统安全与维护手册
- 计算机硬件管理超级手册
- Windows 文件管理高级手册
- (140个) Windows 系统常用快捷键大全
- (157个) Linux 基础命令手册
- (136个) Linux 系统管理与维护命令手册
- (58个) Linux 网络与服务器命令手册
- 黑客攻防命令手册

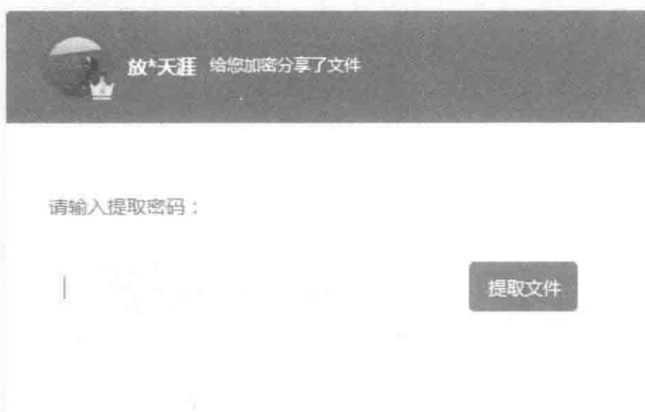
我们已将赠送内容上传百度网盘,在浏览器中输入下载链接,打开链接后,在如下图所示的文本框中输入提取码便可下载赠送资源。下载链接: <http://pan.baidu.com/s/1eSfvxDK>,提取码: ez6a。

提示

读者也可加入QQ群，在群文件中下载“资源下载地址列表”文档，直接复制链接和密码，下载多媒体视频。（注意：我们会在群文件中共享一些赠送资源，如百度网盘链接失效，请加入QQ群下载资源。）



“百度网盘，享你所想”



后续服务

本书由王栋编著，胡华、栾铭斌、宗立波、马琳、赵玉萍、闫珊珊等老师也参加了本书部分内容的编写和统稿工作，在此一并表示感谢！在本书的编写过程中，我们竭尽所能地为您呈现最好、最全的实用功能，但仍难免有疏漏和不妥之处，敬请广大读者不吝指正。若您在学习过程中产生疑问或有任何建议，可以通过E-mail或QQ群与我们联系。

投稿邮箱：pup7@pup.cn

读者信箱：2751801073@qq.com

读者交流群：218192911（办公之家）、99839857

郑重声明

本丛书对大量计算机及移动端的攻击行为进行了曝光，是为广大读者做好安全防范工作。请广大本丛书读者注意：根据国家有关法律规定，任何利用黑客技术攻击他人的行为都是违法的！



第 1 章 什么是 Web 安全	1
1.1 Web 安全的发展历程.....	2
1.1.1 Web 安全概念的提出与发展.....	2
1.1.2 中国 Web 安全的发展历程.....	3
1.1.3 当前 Web 安全的发展现状.....	5
1.2 Web 应用程序中存在的风险及预防.....	9
1.2.1 Web 应用程序的安全套接层 (SSL) 应用.....	9
1.2.2 Web 应用程序安全的核心问题.....	12
1.2.3 Web 应用程序中存在的安全风险.....	16
1.2.4 Web 应用程序安全的预防及发展趋势.....	18
1.3 小结.....	21
技巧与问答.....	22
第 2 章 Web 应用程序的安全剖析	23
2.1 Web 应用程序使用的通信协议——HTTP 协议.....	24
2.1.1 什么是超文本传输协议 HTTP.....	24
2.1.2 统一资源定位器——URL.....	25
2.1.3 HTTP 请求.....	25
2.1.4 HTTP 响应.....	28
2.1.5 HTTP 消息报头.....	31
2.1.6 利用 Telnet 观察 HTTP 协议的通信过程.....	35
2.1.7 HTTP 协议相关技术补充.....	37
2.2 Web 功能及使用技术.....	39

2.2.1	Web 服务器端功能	39
2.2.2	Web 客户端功能	45
2.2.3	会话与状态	49
2.3	Web 应用程序的内容与功能	49
2.3.1	抓取站点内容——网络爬虫介绍	49
2.3.2	Wireshark 抓包步骤详解	51
2.3.3	Web 应用程序的传递参数解析	54
2.4	小结	56
	技巧与问答	56

第 3 章 对 Web 应用程序入侵及防范技术 60

3.1	轻而易举实现的 Web 攻击——Metasploit 攻击	61
3.1.1	Metasploit 环境的搭建与安装	61
3.1.2	Metasploit 使用教程详解	65
3.2	让用户自动上钩的 Web 攻击——欺骗攻击	67
3.2.1	常见的欺骗攻击解析	67
3.2.2	经典欺骗攻击解析——网络钓鱼攻击	72
3.2.3	网络钓鱼攻击技术详解	73
3.2.4	网络钓鱼攻击的日常防范	74
3.3	Web 攻击的“隐形外衣”——日志逃避	75
3.4	应用于 Web 应用程序的防范技术	77
3.4.1	适用于任何应用程序的防范技术	77
3.4.2	应用于 IIS 的防范技术	78
3.4.3	应用于 Apache 的防范技术	82
3.4.4	应用于 PHP 的防范技术	85
3.5	小结	89
	技巧与问答	89

第 4 章 利用验证机制漏洞入侵 Web 及防范技术 92

4.1	Web 验证机制实现技术——SSL 身份验证	93
-----	------------------------------	----

4.1.1	SSL 身份验证产生背景	93
4.1.2	SSL 身份验证协议安全机制	93
4.1.3	利用非对称密钥算法保证密钥本身的安全	96
4.1.4	利用 PKI 保证公钥的真实性	96
4.1.5	SSL 验证协议工作过程	97
4.1.6	Web 应用程序应用 SSL 验证机制	100
4.2	Web 验证机制存在的漏洞	101
4.2.1	用户名和密码可以进行预测	101
4.2.2	重置密码和忘记密码漏洞	102
4.2.3	对验证登录的暴力破解攻击	106
4.2.4	对用户密码强度不进行控制	106
4.2.5	对网络安全证书进行攻击	109
4.3	对验证机制漏洞进行防范	111
4.3.1	设置安全可靠的证书	112
4.3.2	对密码重置和忘记密码功能进行控制	113
4.3.3	对密码设置强度进行控制	114
4.3.4	采用多重安全机制实现多因素验证	116
4.4	小结	118
	技巧与问答	118

第 5 章 利用访问控制漏洞入侵 Web 及防范技术..... 121

5.1	访问控制模型有哪些	122
5.1.1	自主访问控制模型	124
5.1.2	强制访问控制模型	125
5.1.3	基于角色的访问控制模型	128
5.1.4	基于任务的访问控制模型	130
5.1.5	基于对象的访问控制模型	132
5.1.6	信息流模型	133
5.2	如何实现访问控制机制	134
5.2.1	访问控制的实现机制	134
5.2.2	访问控制表	134
5.2.3	访问控制矩阵	135

5.2.4	访问控制能力列表	135
5.2.5	访问控制标签列表	136
5.2.6	访问控制实现的具体类别	137
5.3	访问控制的授权与审计	137
5.3.1	授权行为	137
5.3.2	信任模型	138
5.3.3	信任管理系统	140
5.3.4	审计跟踪概述	141
5.3.5	审计内容	141
5.4	对访问控制的攻击方法	142
5.4.1	使用其他账户访问应用程序	142
5.4.2	直接访问服务器 API 端方法的请求	143
5.4.3	URL 直接访问 Web 程序中的静态资源	143
5.4.4	利用 HTTP 平台级控制的漏洞进行入侵	143
5.5	对访问控制进行安全防范	144
5.5.1	制定安全策略	144
5.5.2	安全级别与访问控制	146
5.6	小结	147
	技巧与问答	148

第 6 章 利用会话管理漏洞入侵 Web 及防范技术..... 150

6.1	Web 应用程序会话状态	151
6.2	生成会话令牌过程中的漏洞	155
6.2.1	结构化令牌的组成存在漏洞	155
6.2.2	令牌含义的可预测性	156
6.2.3	对令牌的算法存在漏洞	158
6.3	处理会话令牌过程中的漏洞	163
6.3.1	日志记录导致的令牌泄露	163
6.3.2	网络传送导致的令牌泄露	164
6.3.3	会话管理机制存在各种漏洞	167
6.3.4	不能提供有效会话终止功能	167

6.3.5 向应用程序客户端用户发动攻击	169
6.4 对会话管理进行安全防范	169
6.4.1 设置最有效的令牌生成机制	170
6.4.2 保障令牌使用过程中的安全	171
6.4.3 使用日志、监控等辅助功能	173
6.5 小结	173
技巧与问答	174
第 7 章 利用编程方式进行 Web 入侵及防范技术	178
7.1 什么是木马	179
7.1.1 木马的工作原理	179
7.1.2 木马的发展演变	179
7.1.3 木马的组成与分类	180
7.2 木马编写的两种实现方法	182
7.2.1 基于 ICMP 的木马编写步骤详解	182
7.2.2 基于 Delphi 的木马编写步骤详解	185
7.3 常见的木马伪装方式	190
7.3.1 解析木马的伪装方式	190
7.3.2 CHM 木马伪装方式	191
7.3.3 EXE 捆绑机伪装方式	195
7.3.4 自解压捆绑木马伪装方式	199
7.4 Web 安全双刃剑——计算机扫描技术	201
7.4.1 实现文件目录扫描的方法	201
7.4.2 实现进程扫描的方法	203
7.4.3 实现主机的端口状态扫描的方法	204
7.5 使用木马清除软件进行安全防范	205
7.5.1 在“Windows 进程管理器”中管理进程	205
7.5.2 使用“木马清道夫”清除木马	207
7.5.3 使用“木马清除专家”清除木马	210
7.6 小结	213
技巧与问答	213

第 8 章 数据存储区的入侵及防范技术 217

8.1	什么是 SQL 注入攻击.....	218
8.1.1	实现 SQL 注入攻击的基本条件.....	219
8.1.2	注入攻击的突破口——寻找攻击入口	222
8.1.3	决定提交变量参数——SQL 注入点类型.....	223
8.1.4	决定注入攻击方式——目标数据库类型.....	224
8.2	常见的注入工具.....	226
8.2.1	Domain (明小子) 注入工具使用详解.....	226
8.2.2	NBSI 注入工具使用详解	229
8.2.3	啊 D 注入工具使用详解.....	231
8.3	XPath 注入攻击	233
8.3.1	什么是 XPath.....	233
8.3.2	保存用户信息的 XML	235
8.3.3	实现 XPath 注入的 JAVA 登录验证源代码	236
8.3.4	简单模拟攻击	237
8.4	LDAP 注入攻击.....	237
8.4.1	LDAP 注入攻击介绍.....	237
8.4.2	LDAP 注入攻击中的 AND 注入	238
8.4.3	LDAP 注入攻击中的 OR 注入.....	239
8.5	mongodb 注入攻击	239
8.5.1	什么是 mongodb 注入	239
8.5.2	注入攻击步骤详解.....	241
8.5.3	注入攻击经典案例解析.....	245
8.6	SQL 注入攻击的防范.....	247
8.7	小结.....	249
	技巧与问答	249

第 9 章 数据库入侵及防范技术 251

9.1	Web 数据库漏洞类型.....	252
9.1.1	脚本漏洞的头号撒手锏——数据库下载漏洞.....	252
9.1.2	瞬杀——暴库漏洞.....	253

9.2 什么是数据库技术.....	254
9.2.1 动态服务器页面与 ActiveX 数据对象介绍.....	254
9.2.2 存取数据库的实现——ADO 对象.....	256
9.2.3 如何通过编程实现数据库连接.....	257
9.3 数据库下载漏洞的攻击详解.....	258
9.3.1 Web 网站的搭建步骤.....	258
9.3.2 数据库下载漏洞的攻击流程.....	260
9.3.3 Web 网站数据库的下载流程.....	263
9.3.4 数据库下载漏洞的防范技术.....	264
9.4 暴库漏洞的攻击详解.....	266
9.4.1 conn.asp 暴库法介绍.....	266
9.4.2 暴库漏洞——%5c 暴库法.....	267
9.4.3 暴库攻击的防范技术.....	273
9.5 小结.....	274
技巧与问答.....	275

第 10 章 利用 Cookies 攻击及防范技术..... 278

10.1 Cookies 技术详解.....	279
10.1.1 Cookies 基础知识.....	279
10.1.2 Cookies 高级知识.....	281
10.1.3 Cookies 最佳实践.....	283
10.2 Cookies 欺骗攻击.....	290
10.2.1 Cookies 信息存在的漏洞.....	290
10.2.2 搜索目标计算机中的 Cookies 信息——IECookiesView 工具.....	292
10.2.3 如何利用 Cookies 欺骗入侵网站.....	293
10.3 案例详解——Cookies 欺骗入侵网站.....	296
10.4 如何利用 Cookies 欺骗实现上传病毒文件.....	299
10.4.1 “L-Blog” 中的 Cookies 欺骗漏洞分析.....	299
10.4.2 防范 Cookies 欺骗技术详解.....	303
10.5 Cookies 欺骗的防范措施与技术.....	303
10.5.1 删除 Cookies 记录.....	303
10.5.2 更改 Cookies 文件的保存位置.....	305

10.6 小结.....	306
技巧与问答	306

第 11 章 利用文件上传漏洞的攻击及防范技术 309

11.1 什么是文件上传漏洞	310
11.1.1 文件上传漏洞的基本原理	310
11.1.2 如何实现文件上传漏洞攻击	311
11.1.3 如何实现绕过文件上传检查功能	313
11.2 文件上传功能中存在的漏洞.....	313
11.2.1 IIS 文件解析问题	313
11.2.2 Apache 文件解析问题	314
11.2.3 PHP CGI 路径解析问题	315
11.2.4 如何利用上传文件实现“钓鱼”	315
11.3 上传漏洞与目录遍历攻击	316
11.3.1 文件上传漏洞	317
11.3.2 文件下载漏洞 (目录遍历攻击).....	319
11.4 文件上传漏洞防御	320
11.4.1 系统开发阶段的防御.....	321
11.4.2 系统运行阶段的防御.....	321
11.4.3 安全设备的防御	321
11.5 小结.....	322
技巧与问答	322

第 12 章 实现 XSS (跨站脚本攻击) 及防范技术 326

12.1 XSS 攻击的 3 种类型	327
12.1.1 什么是反射型 XSS 攻击	328
12.1.2 什么是存储型 XSS 攻击	328
12.1.3 基于 DOM 的 XSS 攻击	330
12.2 XSS 攻击实例详解	331
12.2.1 XSS 攻击的主要途径	331

12.2.2	XSS攻击传送机制类型	332
12.2.3	XSS跨站脚本攻击过程	334
12.3	XSS漏洞利用	337
12.3.1	窃取Cookies	337
12.3.2	渗透路由器	338
12.3.3	读取本地文件	339
12.3.4	Hacking Home Page	339
12.3.5	跨站中的“溢出攻击”	340
12.3.6	XSS Worm	340
12.3.7	DDOS攻击	340
12.4	实现XSS防范技术	341
12.4.1	XSS漏洞的查找与检测	341
12.4.2	HttpOnly防止劫取Cookies	343
12.4.3	输入检查	344
12.4.4	输出检查	344
12.4.5	处理富文体	346
12.4.6	防御DOM Based XSS	346
12.4.7	网站如何应对XSS攻击	347
12.5	小结	348
	技巧与问答	348

第13章 攻击Web服务器及防范技术..... 351

13.1	Web服务器面临的攻击	352
13.1.1	缓冲区溢出	352
13.1.2	目录遍历	353
13.1.3	脚本权限	353
13.1.4	目录浏览	354
13.1.5	默认示例	355
13.1.6	其他服务	355
13.2	Web服务器隐藏漏洞	355
13.2.1	Web服务器常见的8种安全漏洞	356
13.2.2	IIS 5.x/6.0/7.0解析漏洞	357

13.2.3	IIS 8 服务器上的隐藏漏洞.....	358
13.2.4	Nginx 服务器畸形解析漏洞.....	359
13.2.5	Apache 解析漏洞.....	360
13.2.6	Web 服务器其他漏洞.....	361
13.3	Web 服务器常用防护工具.....	362
13.3.1	第三方安全产品.....	362
13.3.2	Web 服务器漏洞扫描工具.....	363
13.4	Web 服务器安全措施.....	366
13.4.1	Web 服务器安全机制.....	367
13.4.2	Web 服务器维护人员守则.....	367
13.4.3	Web 服务器的加固.....	368
13.4.4	保护公开 Web 服务器.....	368
13.4.5	保护 Web 服务器的 6 点计划及其他细节.....	371
13.5	企业级 Web 服务器安全主动防御措施.....	374
13.5.1	在编写代码时就要进行漏洞测试.....	374
13.5.2	对 Web 服务器进行持续的监控.....	375
13.5.3	设置蜜罐——将攻击者引向错误的方向.....	375
13.5.4	专人对 Web 服务器的安全性进行测试.....	376
13.6	小结.....	376
	技巧与问答.....	377

第 14 章 Web 入侵及防范技术..... 379

14.1	Web 入侵技术.....	380
14.1.1	SQL 注入漏洞的入侵.....	380
14.1.2	ASP 上传漏洞技术.....	381
14.1.3	网站旁注入侵技术.....	381
14.1.4	提交一句话木马的入侵方式.....	381
14.1.5	论坛漏洞利用入侵方式.....	381
14.1.6	Google HACKing 技术.....	382
14.1.7	Web 入侵实例.....	383
14.2	利用手动的方式来防范基于 Web 的入侵.....	383
14.2.1	安装补丁/安装杀毒软件.....	383