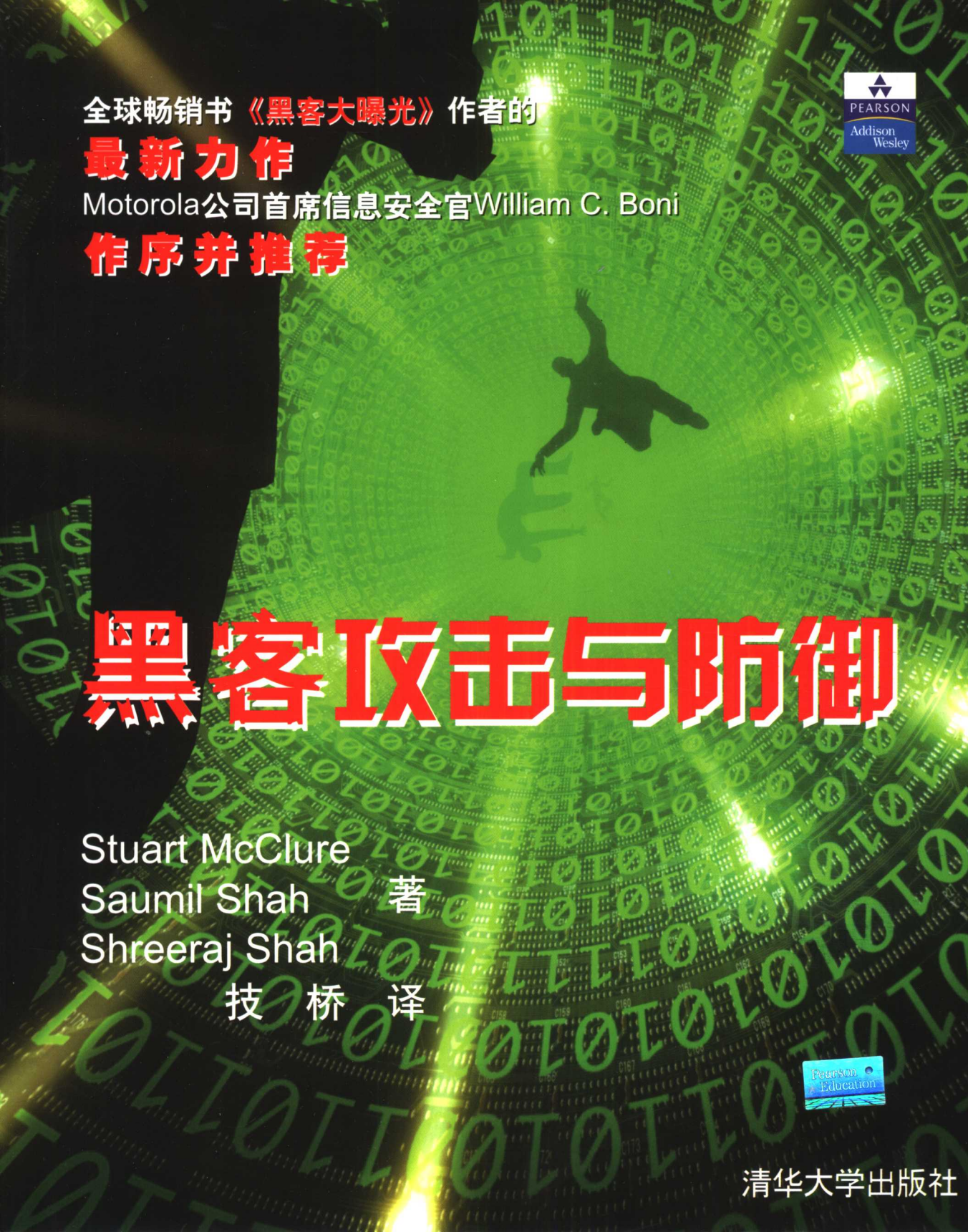
全球畅销书《黑客大曝光》作者的
最新力作
Motorola公司首席信息安全官William C. Boni
作序并推荐
PEARSON
Addison Wesley
黑客攻击与防御
Stuart McClure
Saumil Shah 著
Shreeraj Shah
技 桥 译
Pearson Education
清华大学出版社

黑客攻击与防御

Stuart McClure

Saumil Shah 著

Shreeraj Shah

技桥 译

清华大学出版社

北京

Simplified Chinese edition copyright©2004 by PEARSON EDUCATION ASIA LIMITED and TSINGHUA UNIVERSITY PRESS.
Original English language title from Proprietor's edition of the Work.

Original English language title: Web Hacking: Attacks and Defense, 1st by Stuart McClure, Saumil Shah & Shreeraj Shah, Copyright © 2003
EISBN: 0201761769
All Rights Reserved.

Published by arrangement with the original publisher, Pearson Education, Inc., Publishing as Addison-Wesley.

This edition is authorized for sale only in the People's Republic of China (excluding Hong Kong SAR, Macao SAR and Taiwan).
本书中文简体翻译版由 Addison-Wesley 授权给清华大学出版社在中国境内（不包括中国香港、澳门特别行政区和中国台湾地区）出版发行。

北京市版权局著作权合同登记号图字：01-2002-5751 号

版权所有，翻印必究。
本书封面贴有 Pearson Education（培生教育出版集团）激光防伪标签，无标签者不得销售。

图书在版编目（CIP）数据

黑客攻击与防御/麦克劳尔（McClure, S.），撒哈（Shah, S.）等著；技桥译. —北京：清华大学出版社，2004. 6
书名原文：Web Hacking
ISBN 7-302-08570-6

I. 黑… II. ①麦…②撒…③技… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2004）第 039172 号

出 版 者：清华大学出版社
http://www.tup.com.cn
社 总 机：010-62770175
地　　址：北京清华大学学研大厦
邮　　编：100084
客户服务：010-62776969
责任编辑：常晓波
封面设计：立日新
印 刷 者：北京四季青印刷厂
装 订 者：三河市金元装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×230　**印张**：22.75　**字数**：509 千字
版　　次：2004 年 6 月第 1 版　2004 年 6 月第 1 次印刷
书　　号：ISBN 7-302-08570-6/TP・6147
印　　数：1～4000
定　　价：40.00 元

本书如存在文字不清、漏印以及缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：（010）62770175-3103 或（010）62795704

序

Web 站点和电子商务系统是全球电子商业化的基础，本书则是保护这些日趋重要的 Web 站点和电子商务系统的基本指南。本书提供了一流的安全顾问提炼出的经验，以帮助受到围攻的安全和 IT 业人士扫平障碍，使他们得以避开电脑黑客的冲击（黑客们把 Internet 看作偷窃和攻击其他人的一种更快、效率更高的机制）。如果你学习和运用了本书提供的经验，那么 Internet 上经验最丰富的黑客也会由此而遭到挫败，因为他们那些最有效的诡计对你的站点也毫无作用。为了危及你的应用程序的安全，他们必须更有创造性，并且更努力地工作。本书饱含着知识和提炼出的经验，它们来自世界上最出色的白帽子黑客，他们是 Foundstone 公司的忠实顾问。

作者们讲述了在 Web 站点和应用程序入侵的领域中令人吃惊和眼花缭乱的内幕。本书讨论了一些最具破坏性的工具和技术，计算机领域的罪犯和黑客正是用它们来破坏全球范围内的 Web 站点。一开始的案例分析和章节中的示例极为详细地说明，如果没能理解和预料到“处于暗处的一方”可利用和使用中的众多方法所带来的后果。并且以实用的功效详述了为抗击这种破坏而必须采取的对策。为了击败黑客，本书帮助读者去认识他们何地、何时以及为何发起攻击，还有他们偏好的弱点。本书是针对这些技术的参考手册。

本书是技术方面的一部力作，对下列问题进行了颇有价值的描述：Web 站点的要素，遭到攻击的方式、时间、地点及原因。本书在精确、完整地讲解技术的同时，还将帮助技术方面知识不够渊博的读者掌握攻击的基本原理以及必要的防卫。

本书还将描述一个令人震惊的事实，那就是即使 Web 站点设计师和操作员受过良好的训练，在实现站点的工作中也经常会犯严重的错误。读了这本书之后，读者将了解 Web 站点受到攻击和操纵的多种方式。首先且最重要的一步是认识到对于 Web 站点的威胁是真实存在的，而且在不断地增加。在这种情况下，Internet 为入侵提供了理想的环境，而本书将帮助从事电子商务和在线交易的业内人士了解和提防这些普遍存在的危险。

本书给出了很多的示例，这些示例使人们理解了以往的经验教训：实际上，Internet 是商业运作的危险地带。当虚拟店面遇到了在电脑领域实施犯罪的真正罪犯时，甚至看似微小的错误（站点的编码方式和组件的链接方式）也能造成巨大的漏洞。Honeynet（www.honeynet.org）项目最近的研究证明，一个没有受到适当保护的站点在其出现在 Internet 上之后的数分钟内就会遭到攻击。更加糟糕的是，具有高风险这个弱点的商业 Web 站点可能会被无法识别的罪犯所利用，即使这些罪犯被发现了，他们也能完全置身于传统执法机构所能触及的范围之外。甚至非赢利性站点也可能被破坏外观或者用于为非法交易

（如密码保护已被破解的软件）提供在线存储。

在我们身处的这个时代中，适者生存是普遍的法则。当传统的法律手段不能有效地阻止攻击时，IT 管理人员和 Web 站点设计师、操作员就不能单纯依靠运气来保护其至关重要的电子商务环境。知识确实就是力量，所以要用世界各地最出色的遵守道德的计算机黑客所掌握的知识来武装自己和自己的团队。本书是一个虚拟的战斗计划，它能帮助你识别和消除因计算机领域的欺诈、毁损、未被授权的访问、修改或破坏而导致 Web 站点无法正常工作的威胁。你可以利用这些专业安全顾问所掌握的知识，从而在了解到你和你的组织正在为减少计算机犯罪的可能性尽自己的职责时，会更加安心。

William C. Boni
摩托罗拉公司首席信息安全官
2002 年 7 月

此为试读，需要完整PDF请访问：www.ertongbook.com

绪　论

真理只有一个，但错误却增生扩散。人们捕捉到它，把它分成小的部分，希望能把它转换成小粒度的真理。但是基本的微粒在本质上始终是错误的，是一个误算。

——René Daumal（1908—1944），法国诗人、评论家

“我们是安全的，我们拥有防火墙”

要是每当我们听到一个客户说这样的话时就有一枚硬币那该多好。我们现在也许不是在写这本书，而是正在某个白色的沙滩上喝着冰镇果汁朗姆酒，还……

如果你怀疑防火墙是否能使你高枕无忧，那么请记住这一点：据报道，65%以上的攻击都发生在 TCP 端口 80，这是传统的 Web 端口（http://www.incidents.org）。这真的是对 Web 的威胁吗？当然——这是千真万确的。

人非圣贤孰能无过

在回顾过去几十年众多安全问题的过程中，我们懂得了你将要了解的东西（如果你还不知道它的话）：没有什么是真正安全的。错误是所有安全漏洞的主要原因，正如那句谚语所说：人非圣贤孰能无过。防火墙、入侵检测系统（IDS）或反病毒软件都不能保证你的安全。用这种评论来介绍一本关于安全的书是不是使你觉得奇怪？其实并不奇怪，因为这是开始研究安全问题之前必须接受的残酷事实。

那么你应该做些什么？只是甩手不管、关掉计算机的电源，而且不理睬 Internet、调制解调器和计算机？你当然可以这么做，但是这种做法将使你孤立起来。Internet 和它提供的一切都是不可否认的：增加的通信和信息共享，毫无界限或限制地与所有种族、信仰、肤色、性别和智商的人互联。这些仅仅是家庭用户的获益。企业一天 24 小时、一周 7 天都要使用 Internet，一眨眼的瞬间即可赚钱和在全世界范围内传输资金。任何否认 Internet 普遍存在和持久力的人只是在欺骗他们自己。

灾祸将临的预兆

三年多以前，本书的一位作者写了一篇带有预感性的文章，预示着某些事情的到来。该文章发表于 1999 年 8 月 9 日，题目为“*Bane of e-commerce: We're secure: We allow only Web traffic through our firewall*（电子商务的毁灭：我们是安全的：我们只允许通过防火墙的 Web 传输）”（http://www.infoworld.com/articles/op/xml/99/08/09/990809opsecw- atch.xml）。该文章警告当时用于保证安全的防火墙存在缺点，但是没有人相信这一点，更没有人去讨论这一问题。所有人都好像被夸大的技术所吸引，例如：防火墙、IDS 和虚拟专用网络（VPN），或者从未成为主流的外围设备技术，如公钥基础结构（PKI）、分布式计算环境（DCE）和单点注册等。

那么现在为什么 Web 和其安全性引起了极大的兴趣？因为在当今互联的世界中，入侵事件经常发生。人们开始认识到 Web 应用程序的一个弱点是可以将整个公司的信息系统暴露给攻击者（如：红色代码和尼姆达蠕虫）。

本书结构

我们写这本书的目的是为了最大限度地吸收和理解，也就是说从介绍性的技术和概念到中级再到高级的技术和概念。为了实现这一目标，我们将本书分成 4 部分，其中包括 17 章，还有附录。

各个部分

- 第一部分——电子商务的天地
- 第二部分——解读 URL
- 第三部分——他们是如何做到的？
- 第四部分——高级 Web 技巧

每一部分在内容和讲解方式上都有所提高，从简单的 Web 语言介绍（第 1 章）到发现和利用自己的缓冲区溢出（第 14 章）。但是不要因加快阅读速度而影响循序渐进的学习过程。如果你遗漏了一些东西，可以回过头去补上，或者在有些情况下，可以在继续深入学习的过程中获得这些知识。

第一部分和第二部分是对万维网初级和中级的介绍。在“电子商务的天地”中展现了 Web 如何运作——包括语言、应用程序、数据库、协议和语法。“解读 URL”深入研究了 URL 的含义，对于攻击者来说什么是重点，以及可见的代码如何帮助攻击者；还展示了映

射的 Web 站点对于攻击者的全部技能来说是如何的至关重要。

第三部分阐明了 Web 入侵的技术，它的实现方法，以及在开发阶段如何采用简单的步骤消除大部分威胁。到目前为止，这部分所呈现的信息是比较发人深思的一部分，该部分常常提供关于计算机黑客如何实施其行为的最好的线索。每章都给出了对于入侵的详细分析，在结尾部分还给出了对策以帮助阻止入侵。

第四部分讨论一些高级的 Web 入侵概念、方法和工具，读者千万不能错过这些内容。

最后，本书的结尾是附录，其中包括 Internet 上的公共 Web 端口列表、用于远程命令执行的速查页和源代码解密技术，还有其他一些有用的信息。

各章

第一部分，“电子商务的天地”，包含 5 章。

第 1 章 Web 语言：21 世纪的巴比伦——讨论当今 Internet 上使用的所有主要的 Web 语言。

第 2 章 Web 和数据库服务器——讨论 Web 背后的技术和它们如何引入了安全漏洞。

第 3 章 购物车和支付网关——讨论在线购物车和网上电子商务站点背后的技术。

第 4 章 HTTP 和 HTTPS：用于破解的协议——讨论用于在 Internet 上指引 Web 和电子商务传输的两个主要协议。

第 5 章 URL：Web 黑客之剑——讨论仅仅通过理解 URL 来了解一个 Web 站点的方方面面。

第二部分，“解读 URL”，包含 3 章。

第 6 章 Web 的工作原理——讨论一个完整的 Web 应用程序的细节，包括其全部组件和附属物。

第 7 章 体会言外之意 —— 讨论如何从 Web 浏览器或其他接口中找出源代码的杰出技术。

第 8 章 站点链接分析——讨论攻击者如何编制 Web 站点的详细目录以便从总体上理解应用程序以及如何攻击它。

第三部分，“他们是如何做到的？”，包含 6 章。

第 9 章 计算机涂改——讨论攻击者如何破坏 Web 站点的外观、他们的技术和诡计。

第 10 章 电子商店盗窃行为——讨论攻击者如何通过欺骗应用程序以较低的价格卖给他们商品来实施在线入店行窃。

第 11 章 数据库访问——讨论攻击者如何通过数据库来入侵 Web 应用程序。

第 12 章 Java：远程命令执行——讨论攻击者如何利用 Java 来入侵系统。

第 13 章 假冒——讨论攻击者如何假冒另一个用户的身份。

第 14 章 缓冲区溢出：动态方式——讨论攻击者如何在应用程序中识别和引起溢出。

第四部分，“高级 Web 技巧”，包含最后 3 章。

第 15 章 Web 攻击：自动化工具——讨论计算机黑客以自动化的方式实施其诡计所使用的工具和技术。

第 16 章 蠕虫——讨论致命的蠕虫及其如何制造、传播和除掉。

第 17 章 击败 IDS——讨论 IDS 如何帮助和妨碍寻找攻击者。

结束语

本书初步介绍了入侵，并详细观察了网络黑客的世界。同时特意提高了可读性，使你不会感到枯燥乏味。学习本书的理想方式是从前向后阅读。但是，如果你已经掌握了关于安全的基础知识和 Web 技术，完全可以直接跳到第二部分（解读 URL）和第三部分（他们是如何做到的？）。

任何环境都会存在漏洞，但我们希望使用 Web 和 Internet 的人清醒过来、振奋精神，改正其误解和错误。因为如果人们不这么做，黑客就会趁虚而入。

致 谢

许多因素帮助我们完成整本书的工作。首先，也是最重要的，我们要感谢 Addison-Wesley 公司的全体编辑人员。他们从始至终的指导和耐心值得称赞。我们还要向 Foundstone 公司的专家表示诚挚的尊敬和感激。该公司成立的联合智囊团给人留下了深刻的印象，使人大为惊奇。

我们要称赞业界的安全研究员，我们为能与他们并肩作战而感到非常荣幸。我们还要感谢印度 Net-Square 的朋友们，感谢他们帮助我们进行研究，并就本书的许多问题进行合作。

最后，特别要感谢 Barnaby Jack 对本书所做的贡献。

贡献者

Barnaby Jack 是 Foundstone 公司的研发工程师，专门进行漏洞研究和对非法利用的开发。在加入 Foundstone 之前，他是 Network Associates 公司中 COVERT 研究组的一位工程师。

他对操作系统的内部已经进行了多年的深入研究，主要集中于 Windows NT 和其派生系统。他已经在 Windows 非法利用方法的领域做了大量的研究，后来，许多主要的安全出版物都参考了他的工作和论文。

目　录

第一部分　电子商务的天地

第 1 章　Web 语言：21 世纪的巴比伦 8
引言 8
Web 语言 9
HTML 9
动态 HTML（DHTML） 11
XML 11
XHTML 13
Perl 13
PHP 16
ColdFusion 18
ASP 20
CGI 25
Java 28
小结 38

第 2 章　Web 和数据库服务器 39
引言 39
Web 服务器 39
Apache 39
Microsoft IIS 44
数据库服务器 51
Microsoft SQL Server 52
Oracle 58
小结 66

第 3 章　购物车和支付网关 67
引言 67

此为试读，需要完整PDF请访问：www.ertongbook.com

商店的演变 68
电子购物 70
购物车系统 71
电子购物车的功能和存在时间 71
收集、分析和比较所选商品 72
留意总成本 72
改变主意 72
处理购买 72
购物车应用程序的实现 73
产品目录 74
会话管理 74
数据库接口连接 75
与支付网关的集成 75
拙劣实现的购物车示例 75
Carello 购物车 75
DCShop 购物车 75
Hassan Consulting 的购物车 76
Cart32 和其他几种购物车 76
处理付款 76
确定订单 76
付款方式 77
验证和欺骗保护 77
执行订单和生成发票 77
付款处理系统概述 77
克服信用卡欺骗的新方法 77
订单确认页面 79
支付网关接口 79
交易数据库接口 80
与支付网关接口——一个示例 80
付款系统实现问题 83
集成 83
临时信息 83
SSL 83
存储用户简介 83
购物车和支付网关的低效集成造成的安全漏洞 84

PayPal——使个人接受电子付款 84
小结 85

第 4 章 HTTP 和 HTTPS：用于破解的协议 86
引言 86
Web 协议 86
HTTP 87
HTTPS（建立在 SSL 技术之上的 HTTP） 93
小结 96

第 5 章 URL：Web 黑客之剑 97
引言 97
URL 结构 98
Web 黑客哲学 99
URL 和参数传递 100
URL 编码 101
元字符 102
元字符和输入验证 103
在 URL 串中指定特殊字符 103
Unicode 编码 104
Acme Art 公司，破解 104
滥用 URL 编码 105
Unicode 编码和红色代码的 Shell 代码 105
Unicode 的漏洞 106
双解码或者多余解码漏洞 107
HTML 表单 109
剖析 HTML 表单 110
输入元素 111
通过 GET 和 POST 的参数传递 112
小结 117

第二部分 解读 URL

第 6 章 Web 的工作原理 121
引言 121

Web 应用程序的组成部分 121
前端 Web 服务器 123
Web 应用程序执行环境 124
数据库服务器 124
编写组件 125
本地应用程序处理环境 125
Web 服务器 API 和插件程序 126
URL 映射和内部代理 126
使用后端应用程序服务器代理 126
示例 127
与数据库的连接 130
最巧妙的破解 130
使用本地数据库 API 132
示例 132
使用 ODBC 133
使用 JDBC 134
专用 Web 应用程序服务器 134
从 URL 中识别 Web 应用程序组件 134
技术识别基础 135
示例 136
更多示例 138
技术识别的高级技巧 140
示例 140
识别数据库服务器 141
对策 144
规则 1：使 HTTP 报头中的信息泄露减到最少 144
规则 2：防止错误信息发往浏览器 144
小结 144

第 7 章 体会言外之意 145
引言 145
通过 HTML 的信息泄露 146
浏览器不会显示的内容 146
Netscape Navigator—View|Page Source 146
Internet Explorer—查看|源文件 148

应寻找的线索 149
HTML 注释 149
修改历史 150
开发者或作者的详细情况 150
对应用程序其他区域的交叉引用 150
提示和占位符 150
Web 应用程序服务器插入的注释 151
添加注释标签使其不起作用的老代码 152
内部和外部超链接 152
电子邮件地址和用户名 153
UBE、UCE、垃圾邮件和广告邮件 153
关键字和 Meta 标签 154
隐藏字段 154
客户端脚本 155
自动源代码过滤技术 156
使用 wget 156
使用 grep 159
Sam Spade、Black Widow 和 Teleport Pro 160
小结 161

第 8 章 站点链接分析 162
引言 162
HTML 和站点链接分析 162
站点链接分析方法论 163
第一步：爬行 Web 站点 164
人工爬行站点 164
HTTP 响应报头详解 164
一些用于站点链接分析的常用工具 165
第一步结束 168
爬行程序和重定向 169
第二步：在应用程序结构中创建逻辑组 170
第二步结束 172
第三步：分析每种 Web 资源 173
1. 扩展名分析 173
2. URL 路径分析 174

3．会话分析 174
4．表单确定 175
5．Applet 和对象识别 175
6．客户端脚本评价 176
7．注释和电子邮件地址分析 176
第三步结束 176
第四步：编制 Web 资源目录 177
小结 178

第三部分 他们是如何做到的？

第 9 章 计算机涂改 181
引言 181
涂改 Acme 旅游公司的 Web 站点 181
映射目标网络 184
反向访问代理服务器 185
暴力破解 HTTP 身份验证 188
目录浏览 191
上传涂改过的页面 194
哪里出差错了呢？ 197
HTTP 暴力破解工具 198
Brutus 198
WebCracker 4.0 199
针对 Acme 旅游公司攻击的对策 201
关闭反向代理 201
采用更强有力的 HTTP 身份验证密码 202
关闭目录浏览 202
小结 203

第 10 章 电子商店盗窃行为 204
引言 204
构建电子商店 205
商店前端 206
购物车 206
收款台 206

数据库 206
放在一起 206
电子商店的发展 207
抢劫 Acme Fashions 公司 208
建立 Acme 的电子商店 208
找出问题 209
避开客户端验证 215
使用搜索引擎寻找隐藏字段 215
彻底修改 www.acme-fashions.com 220
修改后的系统面临一个新的问题 220
事后的调查分析和进一步的对策 225
带有远程命令执行的购物车 225
小结 226

第 11 章 数据库访问 228
引言 228
直接的 SQL 攻击 228
一个二手汽车经销商被入侵 230
输入验证 231
对策 236
小结 236

第 12 章 Java：远程命令执行 237
引言 237
Java 驱动的技术 238
Java 应用程序服务器的体系结构 239
攻击 Java Web 服务器 240
识别 Java 应用程序服务器的漏洞 241
示例：在线商店交易门户 241
调用 FileServlet 244
对策 252
加固 Java Web 服务器 252
其他概念上的应对措施 253
小结 254

此为试读，需要完整PDF请访问：www.ertongbook.com