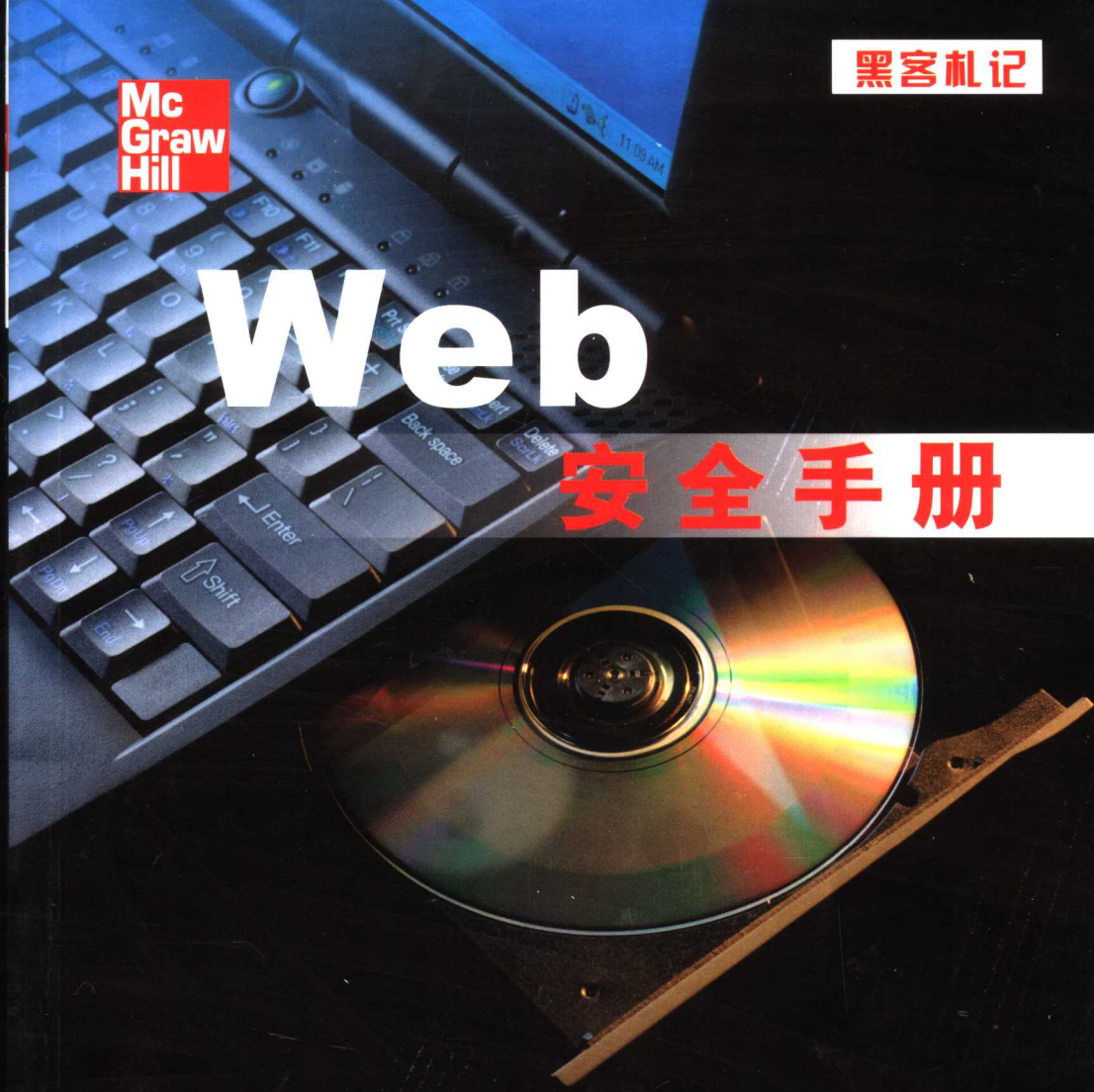
黑客札记



Web 安全手册

Mike Shema 著

谢文亮 马睿倩 译

清华大学出版社

黑客札记

Web安全手册

Mike Shema 著
谢文亮 马睿倩 译

清华大学出版社
北京

Mike Shema
HackNotes: Web Security Portable Reference
EISBN: 0-07-222784-2

图书在版编目(CIP)数据

黑客札记: Web 安全手册/(美)舍玛(Shema, M.)著; 谢文亮, 马睿倩译. —北京: 清华大学出版社, 2005.9
书名原文: HackNotes: Web Security Portable Reference
ISBN 7-302-11614-8

I. 黑… II. ①舍… ②谢… ③马… 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(2005)第 092527 号

出 版 者: 清华大学出版社 **地 址**: 北京清华大学学研大厦
http://www.tup.com.cn **邮 编**: 100084
社 总 机: 010-62770175 **客户服务**: 010-62776969
责任编辑: 常晓波
封面设计: 立日新
印 装 者: 北京嘉实印刷有限公司
发 行 者: 新华书店总店北京发行所
开 本: 150×230 **印张**: 13.75 **字数**: 212 千字
版 次: 2005 年 9 月第 1 版 2005 年 9 月第 1 次印刷
书 号: ISBN 7-302-11614-8/TP·7592
印 数: 1~3000
定 价: 28.00 元

译者序

《黑客札记》原版丛书是美国计算机安全类图书市场上极为畅销的经典之作。今天，译者有幸把这套优秀的书籍呈现给读者，备感荣幸，因为这是为广大计算机安全专业人士提高专业素质的良机。

安全问题如今已是信息技术领域刻不容缓的关键环节，不断浮出水面的漏洞，在网络上疯狂爬行的蠕虫、迅速扩散的冲击波，所有这一切都令人惶惶不可终日。这套丛书的目的就是帮助计算机用户尤其是安全界人士摆脱被动的局面，主动地扼杀威胁于襁褓之中。

这套丛书的特色不在于大而全，而是对流行的、重要的安全技术做出一针见血的分析，为读者提供恰到好处的参考和指南。丛书从攻与防两个角度来阐明安全漏洞的机理与修复措施。阅读本书后，不但可以了解如何抵御黑客的攻击，还能够从根本上杜绝此类攻击，真正做到防患于未然。更重要的是，本丛书还对相关内容进行了引申和拓展，对相关方法进行了归纳和总结，使读者不仅知其然，还知其所以然。值得一提的是，书中还附带了大量的参考资料，这些资料犹如黑暗中的盏盏明灯，为您应对各类攻击与漏洞指明了方向。本丛书还有一个特色便是轻便小巧，易于携带，相信读者一定会享受到这种贴心设计所带来的便利。

本书讨论的主要对象是 Web。如今，Web 的应用如火如荼，随之而来的安全问题也日益突出。人们一方面在享受着 Web 带来的好处，而另一方面却要忍受着不可预料的安全威胁。本书就是针对这种尴尬的现状，较为全面地介绍了 Web 中存在的各种漏洞和所面临的各种威胁，并给读者提供了完善的解决措施。读者在阅读本书后必定会恍然大悟，信心百倍地迎接任何与 Web 安全有关的挑战和威胁。

参加本书翻译工作的人员包括:谢文亮、马睿倩、张丽萍、梁金昆、潘彦斌、刘辉、杨仑、白白华、梁金仑、王玉成、张君伟、柴华等。谢文亮同志负责全书的校对和统稿工作。本书中的每字每句,都凝聚了他们的汗水,在此感谢他们的辛勤和努力!当然,只要广大读者能从书中汲取所需的知识,译者自是幸甚至哉!

作者简介

Mike Shema 是 Foundstone 公司的首席顾问，他为很多客户进行了几十项 Web 应用安全的评审，其中包括《财富》100 强公司、金融机构以及大型软件开发公司。Mike 有一套在大量 Web 应用平台上现场测试过的方法论，同时他还开发了一些自动化多方位测试的支持工具。Mike 发现了商务 Web 软件中的漏洞。Mike 还为 *Security Focus* 及 *DevX* 撰写 Web 服务器安全方面的技术专栏，他还作为合著者把自己的安全经验应用到 *Hacking Exposed: Web Applications and The Anti-Hacker Toolkit* 一书中。在空余时间，Mike 热衷于 RPG 游戏。Mike 获得了 Penn 州立大学的电子工程学及法语学学士学位。

Mike Shema 的联系方式是 mike@ webhackingexposed. com。

技术编辑简介

Yen-Ming Chen，亚洲区主管

Yen-Ming 擅长于无线网络安全、Web 应用评估、产品评审、入侵检测及渗透测试。Yen-Ming 有六年多的系统管理经验及 IT 安全经验，对于 Web 应用、无线联网、加密学、入侵检测与可存活性等领域有着广泛的认识。他的文章发行在 *SysAdmin*、*UnixReview*、*DevX*、*PCWeek* 等美国或中国台湾的多种技术类杂志上。Yen-Ming 是 Ultimate Hacking 课程的首席教员，他曾经做过 MISTI 及 Global Knowledge 的发言人。Yen-Ming 还是 *Hacking Exposed 3rd*、*Hacking Exposed for Web Application*、*Windows XP Professional Security* 等书的撰稿人。Yen-Ming 获得了中国台湾中央大学数学学科的学士学位，另外还获得了卡内基·梅隆大学信息联网学科的硕士学位。他还通过了多种专业认证，其中包括 CISSP 与 MCSE。

致谢

首先必须要感谢的是那些给 Web 应用安全无私地提供工具、技术、建议及观点的安全领域成员。然而很多人仍不知其名，下面只能列出一些曾经帮助过改善 Web 安全(至少指出了悲剧性的缺陷!)的人：Rain Forest Puppy、Mark Curphey 与他的 OWASP 小组、Georgi Guninski、Zenomorph、Chip Andrews、David Litchfield、Dave Aitel。这里还有更多的名字尚未列出。

我们要感谢“Con”小组，感谢他们热烈地讨论安全问题，以及更多有关远程电子邮件访问乐趣的讨论。同样也要感谢 Saumil Shah、J. D. Glaser、Shunns、Jason Glassberg 及组员，感谢他们使那些日子充满乐趣。

最后，在截稿期临近的那些夜晚，总有一点点流行文化让我们继续坚持了几个小时。因此，我要感谢 Type O Negative、Rasputina 以及其他乐队，它们让我在更适合睡觉的时候继续工作。

《黑客札记》丛书

McGraw-Hill/Osborne 为安全专业人士策划了一套全新的便携手册。这套速成书籍对页数进行了控制，使之成为真正的便携手册。

《黑客札记》丛书的目标是：

- 提供易懂易用、精简的安全参考信息。
- 教会大家如何保护网络或系统，展现黑客与犯罪分子如何利用知名手段闯入系统，阐述防御黑客攻击的最佳方式。
- 本套丛书能让那些新接触安全主题的人很快上手，并且能提供精练、直接的知识源泉。为此大家会发现自己需要不时地要参考本书。

这套丛书设计得易于携带，或者放在书包里也不会增加太多份量，并且使用时也不会引起不必要的注意。这套丛书尽可能地利用图表、表格与项目列表，只有在理解重点必须用到屏幕截图时，才会使用图例。更为重要的是，这套便携且轻巧的参考书不会用无关的空话烦人，也就不会让大家在繁忙工作之余还要费劲“啃”它们。我们保持了书写的清楚、精练与中肯。

不管是信息安全领域的新手(希望不用翻查 400 余页资料就能得到有用的基础知识与基本事实)，还是了解手册使用价值(手册相当于另一个大脑，它含有丰富的有用清单、表格及快速确认时所需的特定细节，或者说手册相当于一部安全话题的便携参考)的老练的专业人士。《黑客札记》丛书都能对你有所帮助。

丛书中的关键元素及图标

我们尽可能有条理地组织、展现本书。本书使用紧凑的形式，另外还放入页标签来标记主题。本书最后的“参考中心”包含了大家希望快速、容易访问到的信息及表格。

图标说明

本书中用到的图标使得导航非常容易。每种黑客技术或攻击都用一个特殊的利剑图标突出标示。

这种图标代表一种黑客技术或攻击

获得黑客用以闯入脆弱系统的各种技术/谋略的详细信息。

只要可能，每种黑客技术或攻击也会有一种防御手段，防御手段同样也有自己的特殊图标——盾牌。

这种图标代表对抗黑客技术/攻击的防御手段

获得如何防御所展现黑客技术或攻击的精练细节。

《黑客札记》丛书设计时还用到了其他特殊元素，其中有一些脱离于正文的信息小块，这是为了引起注意。

“i”图标代表一种信息提示，表明阅读该具体小节内容时应该记住这一点。

这种火焰图标代表一种热门事物或一个重要问题，要避免花样繁多的缺陷，就不应该忽视它们。

命令与代码清单

本书通篇都用黑体字显示用户命令输入以表示强调，比如：

```
[bash] # whoami
root
```

另外，正文中出现的常见 Linux 命令、Unix 命令和参数用一种等宽字体加以区分，比如：whoami。

倾听读者意见

我们衷心地感谢大家对本套丛书感兴趣。希望大家觉得本丛书既实用又有趣，我们欢迎任何有助于将来改进这些书的反馈。《黑客札记》丛书设计时特意考虑了大家的需要。有关该丛书的更多信息，请参见 http://www.hacknotes.com，大家也可以自由发送意见及想法至 feedback@hacknotes.com。

简介

濒临危境的 Web

万维网(World Wide Web)同时带来了信息、商机、个性化及其他东西。Web 上风行的应用反映了人们的愿望，不管他们是希望购物、销售、交易或仅仅是交谈。因此，Web 应用安全并不仅仅是站点使用 128 位加密保护了人们的信用卡。Web 安全要保护应用如何读取信用卡，如何把信用卡存放到数据库中，如何随后又从数据库取回信用卡。毕竟，如果恶意用户能进行一次 SQL 注入攻击，那时仅用网页浏览器就能窃取到数据库信息，于是 SSL 的使用毫无意义。

当然，保护财政数据并不是构建安全 Web 应用的惟一理由，信息同样需要保护。不管像家庭住址这样的个人信息，还是像论坛布告这样的公共信息，都不应该暴露在不安全的应用之下。人们可能会成为身份盗用的牺牲品，也可能成为人格毁损的目标。基于 Web 的应用处理的远不只是金钱，重要的是认识到任何应用漏洞都会有严重的后果。

本书应当成一本手册，希望能放在键盘旁边随手查阅。本书从很多安全站点收集了大量的信息，另外还介绍了新的技术与趋势，并把这两者综合起来，形成一种可信的方法论。因此，“参考中心”足以满足那些只需 URL 就能够发起攻击的有经验的黑客，另外也能满足那些对端口扫描器及现成缓冲区溢出工具之外安全层面感兴趣的人。每个 Web 应用都是不同的。本书将会介绍分析、拆解、保护任何应用的方法，但焦点却在于工具及技术上。

本书的组织形式

本书的每一章都只涉及了一个惟一的话题，这让大家可以方便地转到任何最需要的部分进行阅读。

组成部分

第一部分：黑客技术与防御

本书开始时给出了测试 Web 应用的详细方法论及技术，展示技术时从一般到特殊。第一步是枚举出各个应用的页面及变量。接着，这些章节说明了漏洞(如 SQL 注入、跨站点脚本、会话劫持等)的识别、验证及利用等技术。每种攻击都配有某种特定的防御对策。

第二部分：主机评估与安全性强化

本书的第二部分更关注于从头创造安全应用的技术，而不是修补应用的技术。这里给出了支持应用所需部署的平台及程序的清单。这几章并不是简单地重复像 Web 站点上所使用的那些步骤，而是给出了不同防御对策的详细理由和建议，目的在于提供一组能运用至 Web 应用各个部分的技术。

第三部分：专题

这部分给出了安全编码方面的更多信息，处理了负载平衡问题，而有时攻击成功需要这些“额外”知识。安全编码部分谈到了当今最流行的 Web 编程语言中发现的陷阱及对策。

参考中心

读者不会去寻找一份无用的端口号清单，因为只要查看系统上的/etc/services 文件就能得到它。相反，“参考中心”只给出了字符编

码清单、SQL 注入字符串清单以及一份综合的应用安全清单。这份综合的应用安全清单涉及了所有的内容，从搜寻站点直至检查会话状态机制。

黑客攻击与防御

本书阐述了防御大多数 Web 应用攻击时可利用的战术及战略对策。第 2 章主要介绍特定战术攻击及防御措施。因此，第 2 章中能找到我们所强调的大部分技术。

给读者最后的话

哪里有攻击，哪里就有防御。本书的目标是成为一本快速参考，不管大家是在进行应用的安全评审，还是仍在设计网站应用。本书的细节都应该以方法论为中心，足以让任何稍熟悉 HTML 与浏览器的人开始进行安全测试。另外，不管是对有经验的 Web 应用评审者，还是对那些想确信是否已解决了应用各方面安全性的人，“参考中心”都应该是一份便利的核对清单。多加利用！

目 录

第一部分 黑客技术与防御

第 1 章 Web 攻击和渗透方法论 …… 3

1.1 威胁和安全漏洞 …… 4

1.2 勾画平台轮廓 …… 5

1.3 勾画应用程序轮廓 …… 10

1.4 小结 …… 22

第 2 章 关键的黑客攻击与防御 …… 23

2.1 一般的输入验证 …… 25

2.1.1 常用途径 …… 26

2.1.2 源代码泄露 …… 28

2.2 字符编码 …… 29

2.2.1 URL 编码(转义字符) …… 29

2.2.2 Unicode …… 30

2.3 其他的请求方法 …… 32

2.4 SQL 注入 …… 33

2.4.1 Microsoft SQL Server …… 40

2.4.2 Oracle …… 43

2.4.3 MySQL …… 45

2.4.4 PostgreSQL …… 47

2.4.5 博采众家之长 …… 48

2.5 跨站脚本 …… 49

2.6 令牌分析 …… 51

2.6.1 查找令牌 …… 51
2.6.2 编码与加密 …… 52
2.6.3 模式分析 …… 56
2.7 会话攻击 …… 57
2.8 基于 XML 的服务 …… 64
2.9 应用程序的基本防范 …… 66
2.10 输入验证 …… 66
2.11 小结 …… 73

第二部分 主机评估及安全性强化

第 3 章 平台评估方法 …… 77
3.1 漏洞扫描器 …… 78
3.1.1 Whisker 及 LibWhisker …… 78
3.1.2 Nikto …… 80
3.1.3 Nessus …… 83
3.2 评估工具 …… 87
3.2.1 Achilles …… 88
3.2.2 WebProxy 2.1 …… 89
3.2.3 Curl …… 93
3.3 重播请求 …… 96
3.4 小结 …… 100
第 4 章 评估与加固核对表 …… 101
4.1 Web 服务器概述 …… 102
4.2 Apache …… 103
4.2.1 编译时选项 …… 104
4.2.2 配置文件：httpd.conf …… 109
4.3 IIS …… 112
4.3.1 Adsutil.vbs 及 Metabase …… 113
4.3.2 账户 …… 114
4.3.3 文件安全性 …… 115
4.3.4 日志记录 …… 118
4.3.5 IIS 锁定工具(iislockd.exe) …… 119

4.4 小结 …… 120

第三部分 专题

第5章 Web服务器安全与分析 …… 123
5.1 WEB服务器日志分析 …… 124
5.2 代理服务器 …… 131
5.3 负载均衡器 …… 133
5.4 攻击范围 …… 135
5.4.1 对文件系统进行的读取或写入访问 …… 135
5.4.2 执行任意命令 …… 135
5.5 小结 …… 141
第6章 安全编码 …… 143
6.1 安全程序设计 …… 144
6.2 和语言相关的问题 …… 148
6.2.1 Java …… 148
6.2.2 ASP …… 150
6.2.3 Perl …… 151
6.2.4 PHP …… 152
6.3 小结 …… 153

附 录

附录A 7位ASCII引用 …… 157
附录B WebGoat …… 165
B.1 安装WebGoat …… 166
B.2 使用WebGoat …… 167

参考中心

应用程序评估方法核对表 …… 173
HTTP协议说明 …… 179
输入验证测试 …… 182
常见Web端口和应用程序 …… 185
命令技术一览 …… 187