Broadview
www.broadview.com.cn

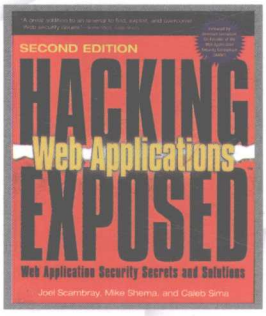
Mc Graw Hill
Osborne

安全技术大系

Hacking Exposed™ Web Applications，Second Edition

黑客大曝光
—Web应用安全
机密与解决方案（第2版）

【美】Joel Scambray，Mike Shema，Caleb Sima 著
王炜 文苗 罗代升 译



揭秘Web应用安全，
提供解决方案

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Mc Graw Hill
Osborne

安全技术大系

Hacking Exposed™ Web Applications，Second Edition

黑客大曝光
—Web应用安全
机密与解决方案（第2版）

【美】Joel Scambray，Mike Shema，Caleb Sima 著
王炜 文苗 罗代升 译

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

在网络技术和电子商务飞速发展的今天，Web 应用安全面临着前所未有的挑战。本书凝聚了作者们超过 30 年的 Web 安全从业经验，详细剖析了 Web 应用的安全漏洞，攻击手法和对抗措施，一步步的教授如何防御邪恶的攻击，并协助读者理解黑客的思考过程。

本书分为 13 章，书后带有附录和详细的英汉对照索引。本书是网络管理员、系统管理员的必备宝典，也是电子商务从业者、网络爱好者和企业管理者的参考书籍。

图书在版编目（CIP）数据

黑客大曝光：Web 应用安全机密与解决方案（第 2 版）/（美）斯卡姆布雷（Scambray,J.），（美）施玛（Shema,M.），（美）西玛（Sima,C.）著；王炜，文苗，罗代升译. —北京：电子工业出版社，2008.6
（安全技术大系）
书名原文：Hacking Exposed™ Web Applications, Second Edition
ISBN 978-7-121-06669-6

I. 黑… II. ①斯… ②施… ③王… ④文… ⑤罗… 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（2008）第 067332 号

责任编辑：许 艳
印 刷：北京市天竺颖华印刷厂
装 订：三河市金马印装有限公司
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：30.75 字数：512 千字
印 次：2008 年 6 月第 1 次印刷
定 价：65.00 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。

译 者 序

经过近一年的辛苦工作，《黑客大曝光——Web 应用安全机密与解决方案（第 2 版）》的翻译终于告一段落。看着厚厚的书稿，无疑有一些轻松的感觉。正是“纳清风台榭开怀，傍流水亭轩赏心。”

记得四年前，自己的第一本书《缓冲区溢出教程》出版时，漏洞满天飞，蠕虫肆虐，肉鸡成群。几年过去了，现在可喜地看到，政府、企业、网管的安全意识越来越强，安全措施越来越完善，安全技术也水涨船高，利用一个漏洞扫描器就可以忽悠单子的时代一去不复返了。不过，安全所处的大环境也急剧地变化，新型的网络应用越来越多，电子商务越来越发达；而另一方面，网络攻击正逐渐走向商业化，攻击者从追求名声转变成了追逐利益，黑客地下产业链悄然形成，安全面临的挑战非常严峻。而本书凝结了作者们超过 30 年的 Web 安全从业经验，无疑是 Web 应用安全领域的“圣经”。

自己看过本书第一版的中译版，恕我直言，翻译的效果实在不敢恭维，完全有理由相信，有些段落是由软件直接翻译得来的，简直浪费了一本经典好书！因此当文苗联系我说电子工业出版社正准备重译本书第二版，有没有时间参与时，自己毫不犹豫地答应了下来。

本书花费了自己这一年来所有的业余时间，不过可以阅读第一手原著，揣摩作者的思维，理解黑客的思考方式，非常物有所值。不仅进一步深入理解了自己已知的一些技术知识，也大大扩展了自己的知识面，最重要的是，拓宽了自己的思维结构。我想，凡是信息安全的相关人员，阅读本书都会受益匪浅的。

本书由自己和文苗亲译，全书由罗代升教授校阅。特别要感谢许艳编辑，对每句每词都进行了严格推敲和修订，工作量非常大，没有她的辛勤劳动，本书是不可能如此顺利译成的。

限于水平，不妥和错误之处在所难免，敬请广大读者批评指正。

另，在本书即将付印时，四川汶川爆发 8.0 级巨大地震，现在还不断感到阵阵余震传来……愿救援的人们平安，哀悼在灾难中遇难的同胞……

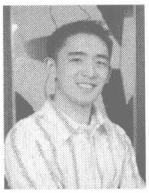
王　炜

于四川大学，成都

关于作者

Joel Scambray 拥有信息系统安全专家认证（CISSP），有 15 年的信息安全经验，包括：在微软和安永国际会计公司担任高级管理角色，与人创办 Foundstone 公司，担任“财富 500 强”企业的技术顾问，与人合著“黑客大曝光”（Hacking Exposed）系列畅销书。

Mike Shema 是 NT Objectives 的首席战略官（CSO），曾在多个安全会议上进行过 Web 应用安全的演讲。他研究了大量的广泛的 Web 技术，并开发出应用安全课程的培训教材。他是《反黑客工具包》（Anti-Hacker Toolkit）一书的合著者。



Caleb Sima 是 Web 应用安全产品公司 SPI Dynamics 的创办者之一和首席技术官，拥有超过 12 年的安全经验。他在 Web 安全方面的探索和专业知识对 Web 应用安全产业界确定产业发展的方向提供了极大的帮助。Caleb 是 *Associated Press* 著名的 Internet 攻击方面的时事评论员和专家。他也是各种杂志和在线专栏的作者。Caleb 是 ISSA（信息系统安全协会）成员，OASIS（结构化信息标准促进组织）中应用漏洞描述语言（Application Vulnerability Description Language）标准的发起者之一，也是 Web 应用安全联盟（Web Application Security Consortium，WASC）的发起成员。

关于技术编辑

Edward Tracy 持有信息系统安全专家认证（CISSP），他主要关注于应用安全，特别是 Web 应用安全。Tracy 先生在美国国家安全局（National Security Agency）开始了他的职业生涯，在那里他从事先进的计算机安全研究。后来，他与人合办了 Aspect Security 公司，该公司是一家从事应用程序安全的咨询公司。当在 Aspect Security 时，Tracy 先生负责渗透测试服务，进行代码和设计评审，提出在软件生命周期中的安全建议，并且在全美国讲授应用安全课程，包括在约翰·霍普金斯大学进行客座教学。

Tracy 先生是负责开放 Web 应用安全项目（Open Web Application Security Project，OWASP）的经理，也为 OWASP 的蜜罐 Web 应用程序 WebGoat 做出贡献。他也对应用程序扫描技术和静态代码分析进行研究和工程实现。Tracy 先生现在与 Booz Allen Hamilton 合作，通过公司的信息保证措施，继续提供应用程序安全服务。

关于丛书作者

Nishchal Bhalla “Security Compass”的创办者，是一个在产品、代码、Web 应用、主机和网络评审方面的专家。Nish 与人合著了《缓冲区溢出攻击——检测、剖析与预防》（Buffer Overflow Attacks: Detect Exploit & Prevent）一书，也是《Windows XP 安全专家》（Windows XP Professional Security），《黑客札记:: 网络安全手册》（HackNotes: Network Security）和《编写安全工具和利用代码》（Writing Security Tools and Exploits）的丛书作者。Nish 参与了开源项目，诸如 YASSP 和 OWASP，是 Toronto Chapter 的主席。他也为 SecurityFocus 撰写文章，也是紧急安全问题的时事评论员。

Samuel Bucholtz 是 Casaba Security 的创建成员，Casaba Security 是一家总部位于华盛顿西雅图的公司安全咨询公司。Samuel 擅长于测试应用程序、审查设计和实施系统/网络架构。在创办 Casaba Security 之前，Samuel 是 Foundstone 的一名安全顾问，为全球 1000 客户执行安全评审和渗透测试，管理超过一百个 Web 应用的测试，并且培训网络和 Web 应用安全方面的学生。在进入 Foundstone 之前，Samuel 是一名安全工程师，为一大型 Internet 咨询公司负责构建和运行拥有几百万用户的 Web 站点。Samuel 曾经在 Black Hat、CSI（Computer Security Institute，计算机安全协会）上发表过演讲，并对客户进行私人的指导。他拥有纽约大学计算机科学和经济专业学士学位，曾做过美国国防部网络安全的实习生。

David Wong 现在是安永国际会计公司攻击和渗透实践措施的经理。David 拥有超过 7 年的安全经验，为金融服务、能源、电信和软件产业公司进行过数百次渗透测试和攻击测试。在这之前，David 曾在一家金融服务公司担任应用安全主管，并在朗讯科技开始了他的安全研究职业生涯。David 持有信息系统安全专家认证（CISSP），并从库珀学会毕业获得工程学士学位。

Arian Evans 进入信息安全领域近 8 年时间。他关注的是应用安全和 IDS（入侵检测系统）。Arian 现在研究和开发了用于评估应用程序和数据库安全状态的新方法，除此之外，这种方法还能帮助客户设计、配置和防范他们的应用程序。Arian 就职于 FishNet Security，处理全世界范围内客户的应用安全问题，他也曾经为 Internet 安全中心（Center for Internet Security）、FBI，以及多家涉及 Web 应用安全和与攻击应急响应有关的商业组织工作过。

献给那些幕后的支持者们，你们支持我们不断追求生活、自由和快乐。谢谢你们！

——Joel

献给 Tera，如此吸引我并赋予我灵感。

——Mike

献给我的父母（谢谢你们对我的包容），我的兄弟 Jonathon，RJ 和 Andrew，我的姐姐 Emily。最后，献给 SPI 的所有人，你们改变了我的生活并帮助我创建了一家了不起的公司。

——Caleb

序

头脑让我的思维展翅翱翔。

——Harry Houdini

攻击一个 Web 应用程序就像表演一个魔术。如果你知道正确的技术和方法，你可以闯入任何在线银行、信用合作社、股票交易所、电子商务商店或者社会网络的 Web 站点。只需使用 Web 浏览器作为你的魔法棒，用你最快的速度说："芝麻开门！"，你就进去了。这正是本书的内容——安全产业顶级的 Web 应用专家们公开他们曾守口如瓶的 Web 攻击机密，这样大家可以据此实施一些防护措施来保护自己。即使是传奇魔术师哈里 霍迪尼也会铭记这些书页所描述的技术。

本书的作者，同样也是 Web 应用安全专家，他们考察 Web 站点的方式和大多数人有很大的不同。他们好像有某种神秘的力量，只是看一眼 URL，就可以确定操作系统、编程语言、Web 服务器版本甚至漏洞所处的位置。大部分专家也承认，当他们进行在线交易时，是痛苦有时也是诱人的体验。他们需要极力遏制自己的好奇心：在浏览器地址栏插入几个特殊字符会发生什么呢？你可以转储整个信用卡数据库吗？当购买确认 E-mail 到达时——我们可以简单地改变 URL 中的数字，就可以看见其他人的订单吗？答案很可能是：是的！因为如果你深入地分析，就会发现大多数 Web 站点都是可以被攻陷的。Web 应用安全常常是如此糟糕，以至于专家们偶尔会发现他们的手在不自觉地遮挡住地址栏，因为他们害怕在个人 Web 银行中发现漏洞。即使专家偶尔也会像鸵鸟主义者那样把头埋在沙堆里逃避现实，以叶障目，但这的确是真实的事情。

但是罪犯们一直在伺机行动。在过去，我们只担心爱开玩笑的黑客用几句精英语言（leet speak）篡改主页，在 Logo 的位置粘贴讨厌的 JPEG 图片，但这样的好时光已经过去了。恶意黑客们已经接管了整个世界，以娱乐为主的黑客时代一去不复返了。每天他们贪得无厌地盗窃信用卡号码、密码、生日、社会保险号码、银行账号以及任何他们可以用来牟利的信息。这些坏小子们是存心的，而且很狂热，他们已经在勒索商业活动，并已到了一个应该警惕的水平。成百上千桩的生意多多少少依赖于 Web，在这个地方忽略安全不是我们能够承担得起的。你曾经坐下来仔细考虑过如果一次入侵带来停工、罚款、法律责任，而且打击客户信心，使品牌信誉受损，真正的损失会是多少吗？

这些年来，入侵者的动机已经改变，但有一件事情保持不变——罪犯总是想选择可能遭遇最少抵抗的路径，这并不意外。当今这条路径是 Web 站点，或者更精确地说，是 Web

应用程序，因为 Web 应用十个中有八个带有严重的漏洞。这是非常严重的问题，会导致你拥有的所有敏感数据都丢失。同样，主流的产业界报告把 Web 攻击和发现的漏洞放在报告列表的顶端。这意味着大多数 Web 站点，即使不是所有的 Web 站点，都将会受到攻击。这只是攻击的时间、攻击者，以及在攻击成功前需要多长时间的问题。如果你的站点属于那80%不安全的 Web 站点，那么你只是在玩一个等待游戏，你的那个不祥数字终将出现。

这就是为什么只是有了 SSL，网络层防火墙和漂亮的证书标签就声称采取了严格安全措施的 Web 站点不让人放心的原因。这些都是 20 世纪的解决方案，它们被不加任何区别地用在防范 21 世纪的主流攻击中，诸如注入跨站脚本、SQL 注入和有漏洞的授权。显然，我们需要更高效的方法，有效地实现安全软件开发最佳实践、平台安全标准、应用层漏洞扫描和 Web 应用防火墙。当前的情况是，要使大多数 Web 站点的安全状态可以达到威慑甚至阻挠恶意攻击者的程度，我们还差得很远。幸运的是，对于那些真正希望安全的人——那些不希望成为下一个受害者或被列在明天媒体头条报道中的人——本书包含了你所需要的信息。

《黑客大曝光——Web 应用安全机密与解决方案（第 2 版）》的作者是知名的，备受尊敬的行业专家，他们都在数字战场上生活了多年。他们有十几年数百次 Web 应用的渗透测试的直接经验，他们知道什么可以起作用。他们都曾研究过几百份（可能数千份）技术白皮书、安全书籍、文章和漏洞公告。他们每个人在安全方面都已经发布了很多成果。他们将为你展示如何由内到外调查内在的 Web 应用程序，如何发现和利用薄弱点，以及最重要的，他们将描述会真正起到作用的安全方法。Joel，Mike 和 Caleb 已经做了非凡的工作，他们用一种通俗易懂而迷人的形式采集和展示技术材料。有一件事情是非常确定的：在你读完本书后，你绝不会再用同样的方式观察一个 Web 站点了。

—Jeremiah Grossman
WhiteHat Security 的创建者和首席技术官
Web 应用安全联盟（Web Application Security Consortium，WASC）的创建者之一
2006 年 3 月

致　　谢

如果没有很多人的支持、鼓励、建议和付出，就不会有本书的存在。我们希望在这里提到了所有的人，如果由于我们的疏忽而漏掉了某些人，在此也表示抱歉。

首先也是最重要的，我们非常感谢我们的亲人和朋友，感谢他们在我们需要研究和写作的这么多个月的时间里，一直对我们的支持。他们的理解和支持是我们完成本书的关键。我们希望我们可以补偿为了完成书籍项目而离开他们的时间（真的，这次我们一定！）。

其次，我们希望感谢我们的同事 Nish，Sam，David 和 Arian 对本书做出的重要的贡献。特别是要感谢 Ed Tracy，担任写作风格如此不同的手稿的技术编辑，他居然能够坚持下来。

当然，再次非常感谢为本书辛勤工作的 McGraw 产品小组，包括我们长期的特邀编辑 Jane Brownlow、出版协调员 Jenni Housh，他把书的制作进度安排得井井有条；我们也感谢项目编辑 Mark Karmendy，即使周末还要做书页校对，因为作者需要而使他的团队承受不公平的事情时，Mark 都能一直保持着冷静的头脑。

我们也感谢很多给本书各方面提供建议和指导的人，包括 SPI Dynamics 的 Brian Cohen，ModSecurity 和 Thinking Stone 的 Ivan Ristic，Google 的 Heather Adkins，Microsoft 的 J.D. Meier，Casaba 的全体 Late-Night Drinking 人员。

同样也感谢 Jeremiah Grossman 对书稿提出的意见，以及他在前言中的精彩评论。

和往常一样，我们对全世界敏锐创新的黑客们表示感谢，他们一直在创新，也一直在为“黑客大曝光”提供原始的资料，我们特别感谢那些定期交流的人。

最后，我们“感谢你”，“黑客大曝光”系列的所有读者，你们的一贯支持使得所有的辛苦都物有所值。

——Joel，Mike 和 Caleb

我想感谢 Mark Painter 和 George Hulme 对我糟糕文笔的帮助，感谢 Kevin Spett 所做的技术贡献，以及 Ashley Vandiver 对我一贯的推动。

——Caleb

前　言

回到 1999 年，《黑客大曝光（第 1 版）》让很多人看到了计算机网络和系统的脆弱性。虽然迄今为止仍然有很多人并没有意识到这一现实，但还是有大量的人开始了解到防火墙、安全的操作系统配置、厂商补丁维护，以及以前看来神秘的信息系统安全基础设施的必要性了。

遗憾的是，因特网带来的迅猛发展已经大大超过了人们的想象。防火墙、操作系统安全以及最新的补丁，都能被一个针对 Web 应用的简单攻击绕过。虽然这些元素仍是所有安全基础设施的重要部件，但它们已经无力阻止新一代的攻击，而这些攻击现在每天都在快速发展着。

这不是我们的一家之言，Gartner Group 报道说，75%的攻击都在 Web 应用层面上，而且对超过 300 个站点的审计表明 97%的站点都拥有会被攻击的脆弱点。恶意攻击的新闻头条现在是越来越常见了（例证：2005 年 CardSystems 电脑缺陷暴露了 4 千万客户的敏感信息），政府对伪电脑安全措施进行调查的情况也越来越多（一些关键的例子包括 BJ's Wholesale Club，美洲银行，花旗银行，Lexis-Nexis，ChoicePoint，微软的 Passport，Guess Inc 和美国礼来公司）

我们也不能因噎废食，从此放弃因特网商务。现在没有别的选择，只有在地上拉起一条警戒线，为无数的组织和个人的电脑空间保留一块净土。

哪怕只是组建过最简单的 Web 站点的人，都知道这是一项令人畏缩的任务。面对带有安全局限性的已有协议，诸如 HTTP，以及比任何时候都更迅猛的新技术的冲击，诸如 XMLWeb 服务，Ajax 和 RSS，要设计和实现一个安全的 Web 应用，简直就是一项“戈耳迪之结”样的难题！

应对 Web 应用安全的挑战

我们采用最初的“黑客大曝光”中的方法，分两方面向你展示如何应对这一挑战。

首先，我们为你的 Web 应用可能会面临的最严重的威胁进行分类，并且非常详细地解释它们的原理。我们是如何知道它们是最严重的威胁的呢？因为我们被不少世界上的大公司雇佣，来破解它们的 Web 应用程序，而我们同时也用这些 Web 程序完成日常工作。我们进行这项工作加起来有超过 30 年的时间了，在这期间，我们研究最新发布的黑客工具，

开发我们自己的工具和技术，并将它们集成到我们认为最有效的方法中，用来对已有 Web 应用的安全进行渗透测试。

一旦我们通过阐述那些攻击可能造成的损失吸引到了你的注意，我们还会告诉你如何防止每一种攻击。如果未理解本书中的信息就开始部署一个 Web 应用，那就好比驾驶着一辆没有安全带的汽车——在光滑的路上下滑，要越过一条巨大的裂坑——也没有刹车，最后必然会栽个大跟头的。

本书的结构

本书由若干章构成，每一章描述了“黑客大曝光”Web 应用攻击方法学的一个方面。该结构形成了本书的主线，因为如果没有方法学，许多内容不过是一堆空洞的没有意义的信息。下面是本书的导航图，它将为你展示出全书的纲要。

第 1 章　Web 应用攻击的基础知识

在本章中，我们对 Web 应用攻击工具和技术进行了综述，并用详细的例子进行了展示。系好你的安全带，Dorothy，因为就要和堪萨斯州说再见，开始我们的神奇之旅了！[①]

第 2 章　剖析

任何方法的第一步都是最重要的，剖析也不例外。该章展示了攻击一个 Web 应用及其架构之前的侦察流程。

第 3 章　攻击 Web 平台

如果建立在一个满身是安全漏洞的 Web 平台之上，那么没有任何应用程序会是安全的——该章描述了攻击、检测绕过技术，以及最流行 Web 平台的对抗措施，这些平台包括 IIS，Apache，PHP 和 ASP.NET。

第 4 章　攻击 Web 认证

该章涵盖了针对常见 Web 认证机制的攻击和对抗措施，这些认证机制包括基于密码的认证，多因素的认证（比如，SecureID，Passmark 和 CAPTCHA）和在线的认证服务，比如 Passport。

① 《绿野仙踪》中的句子——译者注。

第 5 章　攻击 Web 授权

通过先进的会话分析，会话劫持和会话定置技术，说明如何攻击到任意 Web 应用访问控制的核心。

第 6 章　输入验证攻击

从跨站脚本到 HTTP 响应头截断，大多数 Web 攻击的本质上是未曾预料到的应用输入引起的。在这一章中，我们回顾了经典类型的恶意输入，包括从超长输入（比如，缓冲区溢出）到转义攻击（比如，臭名昭著的../）。我们也揭露了应该永远作为怀疑对象的字符（包括尖括号、引号、单引号、双斜线、百分号、星号、下画线、换行符、连接符、管道符和分号）和隐形编码技术，以及输入验证/输出编码对抗措施。

第 7 章　攻击 Web 数据存储

SQL 注入被认为是最具有破坏性的 Web 应用攻击，因为它触及到了所有 Web 应用的核心——Web 应用所保存的宝贵的数据。该章描述了基本的 SQL 语法和常见的滥用方式，然后探讨了基本技术的高级变形，包括盲 SQL 注入，以及 MySQL 和 Oracle 平台的相关变量。

第 8 章　攻击 XML Web 服务

不要把 SOAP 遗漏了，因为这一章将揭密如何发现 Web 服务漏洞，并通过 WSDL 泄漏、输入数据注入、外部实体注入和 XPath 注入等技术来利用这些漏洞。

第 9 章　攻击 Web 应用管理

如果前门紧闭，那尝试后门吧！这一章揭示了针对远程服务器管理、Web 内容管理/创作、管理员错误配置和开发者造成的错误的最常见的 Web 应用管理攻击。

第 10 章　攻击 Web 客户端

你知道吗，你的 Web 浏览器其实是不速之客直接进入你家和你的办公室的方便之门。考察一下周围烦人的 Firefox 和 IE 的漏洞利用代码，然后遵循我们的“加固 Internet 安全体验的十步措施”（连同这一章列出的很多其他的对抗措施），这样的话，在你浏览网站时可以稍微放宽心了。

第 11 章　拒绝服务（Denial of Service）攻击

僵尸网络的出现将 DoS 攻击从无赖式攻击提升为一种高效的因特网勒索工具。另外，寻求投资 Web 分布性能的在线商业模型，都无一例外地暴露在分布式攻击，如点击欺骗攻击（click fraud）之下。在这一章中可以看到，DoS 攻击是如何地从传统类型（架构 DoS）

转变为新类型（应用层 DDoS）的。

第 12 章　充分认知分析（Full-knowledge Analysis）

在这一章中，我们从零知识/黑盒分析中暂时解脱出来，阐述完善的充分认知/白盒 Web 应用安全评估方法学的优势，充分认知分析包括威胁建模、代码评审、安全测试，以及如何将安全集成到 Web 应用开发生命周期中。

第 13 章　Web 应用安全扫描器

这一章面向大中型企业的 IT 操作人员和经理，他们需要将我们的 Web 应用评估方法自动化，使其可扩展，保持一致性，并且带来一定投资回报率（Return on Investment，ROI）。此章主要回顾了这一版书中介绍的可用的 Web 应用安全扫描工具。

最后同样也是重要的，我们在书的末尾附上了一系列实用的附录，包括一个完整的 Web 应用安全检查列表，Web 攻击工具和技术清单，“Web 服务器防火墙”——URLScan 和 ModSecurity 的手把手的安装指导，并且对本书配套站点 http://www.webhackingexposed.com 上可用资源进行了简短描述。

模块，组织和可及性

显然，本书可以从头到尾地阅读，以全面地认识 Web 应用渗透测试的各个方面。不过，秉承“黑客大曝光”的传统，我们努力让每一章都自成体系，这样本书可以被分解为多个模块，以满足目标读者的不同需求。

另外，我们严格按照“黑客大曝光”的一贯风格，给读者以清晰、易读、简明的描述。我们知道你很忙，而且知道你需要的是直奔目标，而不是一大堆说教和无用的行话。正如一位“黑客大曝光”读者所言：“就像读科幻小说，扣人心弦!”

如果你从头到尾一页一页地读，一定会觉得很满意；即使用其他的方法来阅读，本书也会让你开卷有益。

每章小结、参考和进一步阅读

在书中大多数章节的末尾有两个特色部分：一个是“小结”和另一个是“参考和进一步阅读”。

顾名思义，“小结”是对该章所涉及内容的简要总结，并强调对抗措施的重点。我们希望你读了每章的小结部分后，就知道如何保护 Web 应用以对抗任何形式的攻击。

每章中的“参考和进一步阅读”部分包括了超链接，参考书的 ISBN 号，和要找到这一章中参考内容所必需的信息，这包括了厂商安全通报和补丁、第三方公告、商业和免费工具、新闻报道的 Web 攻击事件，以及一般背景阅读材料以获取更多本章所涉及内容的信息。这样你在章节的正文中不会找到超链接——如果你需要查找某些东西，翻到该章的末尾，它们就在那里。我们希望将所有的参考资料汇集在一起，以改善你的阅读体验。

基本组成：攻击和对抗措施

与“黑客大曝光”系列的其他书一样，本书的基本组成是每章中所讨论的攻击和对抗措施。

在这里，着重强调了攻击，因为它们贯穿了“黑客大曝光”的整个系列。

这是攻击图标

像这样标注攻击，使你识别具体的渗透测试工具和方法时更容易，并将你直接指引到所需要的信息处，便于你学习新的安全知识。

每种攻击都提供了风险排名，和“黑客大曝光”其他书的打分方式一样，如下所示：

流行度：实际中攻击实际目标的频繁度，1 为极少被使用，10 为被广泛使用。

简单度：执行攻击所需要的技术，10 为很少或不需要技术，1 为只有老练的安全程序员才能实施这类攻击。

影响度：成功执行攻击后导致的潜在损害，1 意味着目标的一些无关紧要的信息将泄露；10 意味着超级用户账号或等价物可能被盗取。

风险度：根据上述三者的平均值给出全面的风险度评估，向上取整即为其值。

在对抗措施方面，我们也遵循“黑客大曝光”的风格，将对抗措施放在每种攻击或相关系列攻击之后。对抗措施的图标也保持不变：

这是对抗措施图标

该标记是为了让你注意到关键的修补信息。

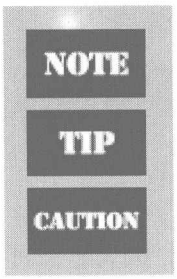
其他视觉辅助标记

我们也大量使用加强视觉效果的图标，以强调一些经常被忽略的细节。

注意：

提示：

警告（需要保持每章的一致性）



网上资源和工具

Web 应用安全是一门快速变化的学科，我们也认识到印刷出来的内容时常不能完全跟上这一领域中的最新研究成果。

因此，我们建立了一个 Web 站点，以跟踪与本书讨论相关的最新信息、勘误表、公共工具、脚本，以及本书中讲授过的技术。该站点的地址是：

```
http://www.webhackingexposed.com
```

该站点也提供了一个论坛，可以通过电子邮件直接与作者讨论：

```
joel@webhackingexposed.com
mike@webhackingexposed.com
caleb@webhackingexposed.com
```

关于站点上提供的内容的更多信息，请参见附录 D。我们希望你在阅读本书时能常访问该站点，看看更新的资料，方便地获取我们提到的工具，另外还可以跟上 Web 安全的最新变化。否则，你永远不会知道有哪些新的发展可能会危及到你的应用，因而无法防范它们。

最后致读者

在本书中凝聚了我们的心血、思想和各种经验。我们衷心地希望我们的努力能帮助你