HZ BOOKS
华章科技
Mc Graw Hill

"每一个Web安全技术人员的必备参考。" ——Robert "RSnake" Hansen,SecTheory的CEO和hackers.org的创始人

Hacking Exposed Web Applications
Web Application Security Secrets and Solutions, Third Edition

黑客大曝光

Web应用程序安全（原书第3版）

（美）Joel Scambray
Vincent Liu
Caleb Sima 著

姚军 等译

机械工业出版社
China Machine Press

信息安全技术丛书

Hacking Expose ons

Web Application Security Secrets and Solutions, Third Edition

黑客大曝光

Web应用程序安全（原书第3版）

（美）Joel Scambray
Vincent Liu
Caleb Sima 著

姚军 等译

机械工业出版社
China Machine Press

Joel Scambray, Vincent Liu, Caleb Sima
Hacking Exposed Web Applications: Web Application Security Secrets and Solutions, Third Edition
978-0-07-174064-7

图书在版编目（CIP）数据

黑客大曝光：Web 应用程序安全（原书第 3 版）/（美）斯坎布雷（Scambray, J.），（美）刘（Liu, V.），（美）西玛（Sima, C.）著；姚军等译 . —北京：机械工业出版社，2011.9
书名原文：Hacking Exposed Web Applications：Web Application Security Secrets and Solutions，Third Edition

ISBN 978-7-111-35662-2

I. 黑… II. ①斯… ②刘… ③西… ④姚… 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（2011）第 167720 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）
责任编辑：吴　怡
北京京北印刷有限公司印刷
2011 年 10 月第 1 版第 1 次印刷
186mm×240mm • 21.25 印张
标准书号：ISBN 978-7-111-35662-2
定价：65.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604

对本书的赞誉

“不管你是期望理解企业威胁的公司领导，还是为网站编写代码的工程师，或是识别和缓解对应用造成威胁的安全工程师，本书都是你的武器库中有价值的武器。”

——摘自 Chris Peterson 的序言
Zynga Game Network 应用安全高级主管
前 Microsoft 安全保障主管

“我认真品读了 Joel 的作品，这本书没有让我失望。人们常问，到哪里能找到在这个令人畏缩的行业里获得立足之地的高质量内容。这本书就是每个应用安全从业者所需要的案头参考。它将是我的珍藏书籍之一。”

——Robert“RSnake”Hansen　SecTheory CEO 及 ha.ckers.org 创始人

“作为了解当今 Web 应用安全形势的一个具有启发性的资源，本书研究了最新的漏洞以及攻击技术，以及用于对抗这些漏洞的手法。本书对于寻求进入 Web 应用安全世界、有抱负的工程师，以及紧跟最新技术发展、成熟的应用安全和渗透测试专家来说，都是值得一读的。”

——Chad Greene　eBay 全球信息安全主管

“由于我们的业务将更多的信息和商务通过 Web 应用推送给客户，这些业务的机密性和完整性是我们立足的根本，即使不是义务，也是责任。本书为担负这一责任的应用开发人员和安全人员提供了全面的信息。作者的研究、洞察力，以及 30 年以上信息安全专家的经历，都令本书成为应用和信息保护工具箱中宝贵的资源。这是本好书！”

——Ken Swanson　P&C 保险公司区域 IS 业务解决方案经理

“本书不仅是关于 Web 应用安全的权威入门书籍；它还是师从最著名的行业专家的一次机会，即使熟练的专业人员也应珍惜这一机会。”

——Andrew Stravitz, CISSP　Barnes & Noble.com 信息安全主管

“非常及时的参考书，随着云计算不断扩展到企业中，Web 安全成为了攻击者和防御者的新战场。这本全面的书籍是理解当代 Web 应用形势及对策的权威入门读物。特别值得一提的是书中对身份管理的详细论述，这本书第一次深入地审视并以如此容易理解的方式介绍了围绕身份验证的各种挑战。”

——Cem Paya　Google 安全团队

译 者 序

互联网确实是人类历史上伟大的发明之一，它彻底地改变了人们的生活，现在，可以毫不怀疑地说，人们日常生活的每个方面都已经和互联网息息相关。

那么，什么是互联网中最引人注目的部分呢？您一定能猜到，是各式各样的 Web 应用。Web 应用可以说是 IT 界的骄傲，它们使现实世界中形形色色的业务都搬到了网络上，使人们可以足不出户地购物、娱乐、处理各种日常事务。在这一刻，IT 人可以自豪地说：这么多年来，我们终于引领了业务，超越商业界创造了一种生产、销售、服务的新形式。

骄傲和危险总是相伴的，网络上巨大的商业机会也同样吸引着不法分子，既然可以在网络上从事各种商务活动，也就意味着，技术高超的黑客们不用荷枪实弹，就能洗劫一个商店，甚至偷走银行中的现金。使用电子商务的人不断激增，大部分人都不具备与黑客同样的技术背景，在与犯罪分子的斗争当中，人们已经落了下风。而搭建网上平台的企业，自然要承担起保护自身及客户财产和隐私安全的职责，企业的安全管理员们，肩上的责任也就更沉重了。

令人遗憾的是，近年来不断发展的平台技术，虽然在安全上有了巨大的进步，但是对于扩张如此迅速的 Web 应用所面对的越来越广泛的威胁仍然无能为力。网络架构本身的特点，决定了安全不再只是通过防火墙、防病毒软件和安全补丁就能完成的任务，而是涉及开发人员、安全管理人员以及整个企业的各个部门甚至网上所有客户的巨大项目，而黑客们所研究出来的各种攻击手段，则是五花八门，令人瞠目结舌。

和往常一样，《黑客大曝光》的作者们又一次走到了幕前，用他们在许多大型企业担当安全顾问的丰富经验，为我们呈现了安全工作中将要面对的各种威胁，丰富的实例解说、逼真的样板应用攻防，既让我们深深感受到黑客手段的可怕之处，又欣慰地看到，在开发和安全实施的很多时候，我们只要理解和运用书中所介绍的最佳实践，就能够很快地消除大部分的隐患，除了对各种威胁原理的详细解说之外，本书还为读者提供了一套十分好用的安全过程方法论，并且用实例讲解了如何将这些方法集成到 Web 应用产品生命期中，而这，正是安全工作者孜孜以求的。

这是我们第二次翻译《黑客大曝光》了，本书充实的内容使我们担心，因为自己的水平所限，不能百分之百地再现原作的精彩之处，我们为此倾注了很大心力，也真诚地向读者推荐这本书，希望它能成为你工作中的定海神针。

本书的翻译主要由姚军完成，徐锋、陈绍继、郑端、吴兰陟、施游、林起浪等人也为本书的翻译工作做出了贡献，在此也要感谢华章科技图书的编辑们对翻译工作提出的许多中肯意见，同时期待着广大读者朋友的批评指正。

序　言

不知彼不知己，每战必败。

——孙武《孙子兵法》

今天的商业活动依靠 Web 生存是无法回避的事实。从银行到书店，从拍卖到游戏，大部分公司都在 Web 上进行交易。例如，美国接近 50% 的音乐零售业务发生在网上，2010 年网络游戏中的虚拟交易市场将超过 15 亿美元。有人估计，美国成年人中超过 45% 的人专门使用互联网进行自己的银行业务。随着 Web 的智能手机的流行，现在大部分的网络商务活动对消费者来说在任何时间、任何地点都可以进行。不管如何估算，Web 上的业务都是经济的重要组成部分，并且正在快速发展。但是这种增长也带来了令人不快的现实——这部分商务活动的安全并没有齐头并进。

在现实世界里，企业所有者数十年来都在面对和学习缓解威胁，他们必须应付强行闯入、盗窃、持械抢劫、伪钞、支票诈骗以及各种骗局。但是现实世界里，企业的业务边界是有限而容易定义的。在大部分情况下，威胁的种类也在合理的限度内。随着时间的推移，他们已经学会应用越来越成熟的方法、工具和保安措施来对付这些威胁。而在 Web 上，情况就大不相同了。

Web 上的商务活动出现不足 20 年，在现实世界中积累的许多经验教训，在 Web 商务活动中才刚刚露出苗头。和现实世界中一样，只要有钱或者有价值的资产，总是会发现一些人为非作歹，企图利用这些资产。但是，电子商务和现实世界不同，企业面对令人眼花缭乱的技术和概念，大部分领导者都感觉这些技术和概念难以（甚至不可能）理解。除此之外，资产的边界常常没有得到很好的理解，潜在威胁可能横跨全球。虽然所有银行的高级主管对现实世界的安防都很在行，提高物理资产的访问管理，精细设计银行金库的安全性，钱柜里有染色包，大堂中加武装保安等，但是这些主管们常常困惑于跨站脚本、SQL 注入等技术对企业的影响。在许多情况下，即使这些公司雇用的建站“专家”、开发人员几乎也不知道这些威胁对网站的危害程度、他们所编写代码的脆弱性，或者那些打算获得系统访问权的攻击者的距离。

在电子商务和网络犯罪不对等的战场上，一些专家全心全意地将有关安全威胁的知识传授给企业，加强开发人员建立抗攻击代码的意识，并且不断地研究攻击者所采用的频繁变化的策略和工具。本书的作者代表着这个群体中最有经验和知识的专家，这本书是他们分享知识和经验的最新努力。

不管你是期望理解企业威胁的公司领导，还是为网站编写代码的工程师，或是期望识别和缓解对应用造成威胁的安全工程师，本书都是你的武器库中有价值的武器。正如孙子告诉我们的，这本书能让你更清楚地认识自己和你的敌人，最后你将有能力减少企业的风险。

——Chris Peterson，2010 年 8 月

Zynga Game Network 应用安全高级主管　前 Microsoft 安全保障主管

前　言

早在1999年，本书第1版就向读者介绍了计算机网络和系统多么容易闯入。尽管今天还有许多人没有意识到这个事实，但是很多人正在开始理解防火墙、安全操作系统配置、软件供应商补丁维护和许多其他以前觉得很神秘的信息系统安全的基础知识。

遗憾的是，互联网所带来的快速发展已经把“球门柱”推向了前场。防火墙、操作系统安全性和最新的补丁都可能被简单的Web攻击所绕过。尽管那些要素仍然是所有安全架构中的关键部件，但是对于越来越频繁而且不断成熟的新一代攻击来说明显无能为力。

这不是我的一家之言。Gartner集团指出，75%的网络攻击都在Web应用级别，而在300个经过审核的网站中，97%的网站都容易受到攻击。2009年秋季的WhiteHat网站安全统计报告称，83%的网站至少有一个严重的漏洞，64%的网站目前至少有一个漏洞，而漏洞解决率仅为61%，余留了8902个未解决的问题（样本大小：1364个网站）。毁灭性攻击的新闻现在已经很常见：身份盗窃资源中心（Identity Theft Resource Center，ITRC）称，在2010年上半年，至少有301个安全性缺口导致了超过820万份身份记录曝光。估计因为安全性缺口所引起的敏感数字记录侵害总数还会再攀新高：Verizon Business 2010数据破坏调查报告中称，6年来，仅查看900余种缺口样本就有超过9亿条记录受到侵害。

我们不能停止互联网商务的脚步，关上大门。我们除了划定一条底线，并保卫信息空间中无数的组织和个人所划定的阵地之外，别无选择。对于已经组建了最基本的网站的人来说，这是一个令人畏惧的任务。面对现有协议如HTTP的安全局限性，以及技术挑战（包括XML Web服务、AJAX、RSS、移动应用以及用户生成内容等）不断加速的脚步，设计和实现一个安全的Web应用可能成为一个戈尔地雅斯难结[⊖]。

面对Web应用安全挑战

本书为你展示如何使用书中提出的双管齐下的方法来应对这一挑战。

首先，我们把Web应用将要面对的最大威胁分类，并且非常详细地解释它们的工作原理。我们是如何知道这些最大的威胁的？因为我们受雇于世界上最大的公司，进入它们的Web应用，每天使用基于这些威胁的攻击来开展工作。我们几人做这项工作的时间加起来已经超过30年，我们研究最新出现的攻击，开发自己的工具和技术，并且将它们组合成为最有效方法，用于渗透现有的Web应用安全。

在你注意到我们展示的这些危险之后，我们告诉你如何避免所有这些攻击。在不理解本书

⊖ 戈尔地雅斯难结——希腊神话中的一个难题，神谕解开该结即为亚细亚国王。——译者注

中的信息的情况下开发 Web 应用，等同于开车时不系安全带，还开上光滑的路面，穿过大裂谷，没有刹车，并且把油门踩到最大。

本书的组织结构

本书由多个章节组成，每个章节描述攻击方法论的一个方面。这种结构组成了本书的主干，因为如果没有一种方法论，那么本书就仅仅是一堆没有上下文和意义的信息。以下是本书章节内容。

第 1 章　Web 应用入侵基础。这一章中，我们广泛地概述了 Web 应用入侵攻击和技术，同时展示了具体的实例。系上你的安全带，因为我们就要离开堪萨斯了。

第 2 章　剖析。任何方法论的第一步往往是最重要的，剖析也不例外。该章讲解了作为攻击 Web 应用及其相关基础设施前奏的侦查过程。

第 3 章　Web 平台入侵。如果建立在充满安全漏洞的 Web 平台之上，那么没有一个应用能够安全，该章描述了大部分流行的 Web 平台包括 IIS、Apache、PHP 和 ASP.NET 的攻击、检测躲避技术及其对策。

第 4 章　攻击 Web 验证。该章介绍常见 Web 验证机制的攻击和对策，包括基于密码、多因素（例如 CAPTCHA）以及 Windows Live ID 这样的在线验证服务。

第 5 章　攻击 Web 授权。了解通过高级会话分析、劫持和完成（Fixation）技术。

第 6 章　输入注入攻击。从跨站脚本到 SQL 注入，大部分 Web 攻击的实质是意外的应用输入。在该章中，我们回顾经典的恶意输入类别，从超长输入（像缓冲区溢出）到规范化攻击（像臭名昭著的 dot-dot-slash），并且揭示应该始终加以怀疑的元字符（包括角括号、引号、单引号、双破折号、百分号、星号、下划线、换行、&、管道符号和分号），从入门级到高级的 SQL 注入工具和技术，以及隐蔽编码技术和输入验证 / 输出编码对策。

第 7 章　攻击 XML Web 服务。不要遗漏了 SOAP，因为这一章将揭示如何通过包括 WSDL 暴露、输入注入、外部实体注入和 XPath 注入等技术发现和攻击 Web 服务漏洞。

第 8 章　攻击 Web 应用管理。如果前门上锁，就试试后门！该章揭示了大部分针对远程服务器管理、Web 内容管理 / 授权、管理员错误配置以及开发者造成错误的常见 Web 应用管理攻击。

第 9 章　入侵 Web 客户端。你可知道，浏览器实际上是不安全的东西直接进入你家里和办公室的一个有效的途径？来一次最危险的 Web 浏览器攻击之旅，然后遵循我们提出的“获得更安全的互联网体验 10 大步骤”（以及本章列出的许多附加对策），在浏览的时候就能更轻松地呼吸。

第 10 章　企业 Web 应用安全计划。在该章中，我们短暂地告别零知识 / 黑盒分析，解释一种健壮的全知识 / 白盒 Web 应用安全评估方法学的优点，包括威胁建模、代码评审、动态 Web 应用扫描、安全测试以及将安全集成到整个 Web 应用开发生命期和 IT 运作中。该章是针对中大型企业的 IT 运作和开发人员，他们需要实施我们的 Web 应用评估方法从而得到伸缩性、一致性和可接受的投资回报。

最后，我们添加了有用的附录，这并不代表这些内容不重要，具体包括："Web 安全检查列表"和"Web 黑客工具和技术快速参考"。

模块性、组织和易读性

很显然，本书可以从头到尾阅读，来得到 Web 应用渗透测试的全面描述。但是，我们尽力使每章独立，这样可以逐个模块地消化本书，适合时间紧张的目标读者。

而且，我们严格地坚持清晰、易于理解和简练的写作风格，这是读者对本书的总体印象。我们知道读者很忙，需要直接地得到第一手资料，而不是大量的空话和无谓的行话。正如本书以前版本的读者们所评论的："读起来像小说，如地狱般令人惊恐！"我们认为，从头到尾阅读和逐个章节阅读都能使你满意，本书的结构适合于任何一种阅读风格。

章节小结及参考与延伸阅读

本书每一章的结尾处都有两个特别部分："小结"和"参考与延伸阅读"。

"小结"顾名思义，是本章中介绍的主要概念的摘要，以及对各种对策的强调。我们希望，如果你阅读了每章的小结，就能知道如何加固 Web 应用来对付任何形式的攻击。

每章的"参考与延伸阅读"部分包含了该章正文介绍的每个条目所需的 URL、ISBN 号码和其他信息，这些条目包含供应商安全通告和补丁、第三方建议、商业和免费工具、新闻中的 Web 入侵事件以及关于正文的信息详细或者扩展读物。这样，如果你需要查找某些内容，可以翻到这一章的末尾去寻找。我们希望通过汇集附加的参考内容能够改进本书的整个阅读体验。

基本组成部分：攻击与对策

本书的基本组成部分是每一章所讨论的攻击和对策，因此我们使用了非常醒目的攻击与对策图标。

攻击图标

这个图标强调了各种攻击方法，使读者找到特定的渗透测试工具和方法很容易，并直接为你指出说服管理层投资新的安全倡议所需要的信息。

许多攻击附有危险等级，计分方法如下：

流行性：对活动目标的使用频度：1 表示最罕见，10 表示广泛使用。
难易度：执行这一攻击所需要的技能：10 表示很少或者完全不需要技能，1 表示成熟的安全编程人员。
影响力：成功执行这一攻击可能产生的破坏：1 表示暴露目标的没有价值的信息，10 表示超级用户账号侵入或者等价的破坏。

危险级：前三个值平均后向上取整得出总体危险等级。

伴随着每种或者每个系列的攻击，也有相应的对策，图标如下：

对策图标

这个标志应该会引起你对关键修复信息的注意。

其他辅助图标

我们还使用了很多视觉增强图标来突出显示那些经常被忽视的细节。

注意　　提示　　警告

在线资源和工具

Web 应用安全技术变化很快，我们承认书籍通常很难跟上这种急剧变化的研究领域。

因此，我们建立了一个网站，跟踪与本书讨论的主题相关的新信息、勘误表，以及书中介绍的公共工具、脚本和技术。网站地址为

http://www.webhackingexposed.com

网站还提供了论坛，可直接与作者通过以下邮件交流：

joel@webhackingexposed.com

我们希望读者在阅读本书各个章节时经常登录这个网站，查看更新的材料、获得我们提到的工具，并跟上 Web 安全技术的变化形势。否则，你永远无法在进行防御时预先得知哪些新的发展可能危及你的应用。

致读者的最后一段话

我们在本书中倾注了感情、才智和经验，我们真诚地希望所有的努力能为负责 Web 应用安全的读者节约大量的时间。我们认为你已经做出了一个有勇气和前瞻性的决策，希望在互联网上获得一席之地，但是，就像你将在本书中看到的那样，你的工作在网站启动的一刻才刚刚开始。不要惊慌，打开这本书，通过学习你会得到莫大的安慰：在下一个 Web 大灾难登上报纸头版时，你甚至连眼睛都不会眨一下。

作者简介

Joel Scambray

Joel Scambray 是一家战略安全资讯服务提供商 Consciere 的联合创始人和 CEO。他已经帮助从新兴公司到《财富》前 50 大公司在内的许多公司处理信息安全问题，历时超过 12 年。

他曾经担任过高管、技术顾问和企业家。他曾经是 Microsoft 公司的高级主管，在那里他领导 Microsoft 的在线服务安全工作三年多，然后加入 Windows 平台和服务部门，专门研究安全技术架构。Joel 还与他人共同创办了安全软件和服务公司 Foundstone，并获得了 McAfee 8600 万美元的投资。他先前还担任过 Ernst & Young 的经理，Microsoft TechNet 安全专栏作者，InfoWorld Magazine 的自由撰稿人，以及一家大型商业房地产公司的 IT 主管。

他是 1999 年首次出版的畅销世界的计算机安全书籍《Hacking Exposed: Network Security Secrets and Solutions》的合著者。他还是《Hacking Exposed Windows》和《Hacking Exposed Web Applications》的主要作者。

他在很多场合发表关于信息安全的演讲，包括 Black Hat、I-4、INTERFACE 以及亚欧会议（ASEM）等论坛，IANS、CERT、计算机安全学会（CSI）、ISSA、ISACA、SANS 等组织，私有公司以及韩国信息安全局（KISA）、FBI 和 RCMP 等政府机关。

他拥有加州大学戴维斯分校的学士学位，加州大学洛杉矶分校的硕士学位，他还是一位认证信息系统安全专家（CISSP）。

Vincent Liu

Vincent Liu（CISSP）是 Stach & Liu 的任事股东。在创办 Stach & Liu 之前，Vincent 在 Honeywell 国际公司领导全球安全单位的攻击与渗透及逆向工程团队。在此之前，他是 Ernst & Young 高级安全中心的顾问和美国国家安全局的分析师。Vincent 是广受欢迎的演说家，曾在 Black Hat、ToorCon 和 Microsoft BlueHat 等业界会议上介绍自己的研究成果。Vincent 拥有宾夕法尼亚大学的科学与工程学士学位，主修计算机科学与工程并选修心理学。

Caleb Sima

Caleb Sima 是以 Santa Clara 为基地的集成 Web 应用安全解决方案提供商 Armorize Technologies 的 CEO。他在 2000 年创立了 SPI Dynamics，并作为 CTO 目睹了堪称 Web 应用安全测试工具解决方案标杆的 WebInspect 的发展。2007 年

Hewlett-Packard（惠普公司）收购了 SPI Dynamics，Sima 成为了惠普公司的应用安全中心首席技术专家，在这里他指导并建立了该公司安全解决方案并且领导开发了基于云的安全服务。在这个位置上，他还管理一个训练有素的安全专家团队，成功地识别了新的安全威胁并且设计出先进的对策。在创办 SPI Dynamics 之前，他是 Internet Security Systems / IBM 精锐的 X-Force 研究和开发团队工作，推动了该公司的企业安全性评估。Sima 是一位 Web 应用安全领域的思想领袖和技术预言家，在 Web 安全技术上有五项专利并合著了这方面的多本书籍，他经常在媒体上投稿，并且定期地在主要的业界会议如 RSA 和 Black Hat 上演讲。他是 ISSA 的成员，OASIS 中的应用漏洞描述语言（AVDL）的创建者之一，还是 Web 应用安全协会（WASC）的创办会员。

对本书的贡献者

Hernan Ochoa 是具有 14 年专业经验的安全顾问和研究者。Hernan 于 1996 年随着 Virus Sentinel 的创立开始其职业生涯，Virus Sentinel 是一个基于特征码的文件 / 内存 /MBR/ 启动扇区检测 / 删除的防病毒应用程序，并且具备启发式检测多态病毒的能力。Hernan 还开发了一个详细的技术性病毒信息数据库和与之相伴的时讯报道。他在 1999 年加入 Core Security Technologies 并在那里供职 10 年，担任了多个职务，包括安全顾问和攻击程序编写者。作为攻击程序编写者，他进行了多种多样的安全评估，开发了多种方法论、外壳代码和安全工具，并对新的攻击方向提出了意见。他还为一种最终部署在某家金融机构的多 OS 安全系统设计和开发了多种低级 / 内核组件。Henan 已经发表了许多安全工具，包括 Universal Hooker（使用 Python 编写的动态处理例程的运行时工具），Pass-The-Hash Toolkit for Windows 和 WifiZoo。他目前在 Amplia Security 担任顾问 / 研究员，进行网络、无线和 Web 应用的渗透测试，独立 / 客户 - 服务器应用黑箱评估，源代码审核，逆向工程，漏洞分析，以及其他信息安全相关的服务。

Justin Hays 是 Stach & Liu 的一位高级安全顾问。在加入 Stach & Liu 之前，Justin 是 PTC 日本公司的企业支持工程师，负责调试、逆向工程以及缓解 PTC 的旗舰产品 Windchill 企业服务器 J2EE 软件缺陷。Justin 拥有肯塔基大学的学士学位，主修计算机科学，兼修数学。

Carl Livitt 是 Stach & Liu 的管理安全顾问。在加入 Stach & Liu 之前，Carl 领导一家广受尊敬的英国安全公司的网络安全服务组，这家公司为世界最大的许多制药公司提供网络安全咨询服务。Carl 还曾经与英国警察反恐怖单位合作，为执法部门人员举办安全技术讲座。

Rob Ragan 是 Stach & Liu 的一位高级安全顾问。在加入 Stach & Liu 之前，Rob 在惠普公司的应用安全中心任软件工程师，开发 Web 应用安全测试工具并且管理应用渗透测试。Rob 积极开展 Web 应用安全研究并在 Black Hat、Defcon、InfoSec World 和 Outerz0ne 等大会上加以展示。Rob 拥有宾夕法尼亚州大学的学士学位，主修信息科学与技术，主要关注系统开发。

本书的技术编辑

Robert Hensing 是 Microsoft 的高级顾问，他已经担任各种安全工作超过 12 年。Robert 以前在 Microsoft 安全响应中心（MSRC）工作，关注于提供安全漏洞的根源分析、鉴别缓解和变通方法，帮助客户免遭攻击。在 MSRC 工程团队工作之前，Robert 是客户支持服务安全团队的高级成员，帮助客户进行事故响应相关的研究。Robert 还是《Hacking Exposed Windows: Windows Security Secrets and Solutions, Third Edition》的作者。

致　谢

没有许多人的支持、鼓励、投入和贡献，本书就不可能出版。我们希望能够在这里提及所有这些人，如果因为我们的疏忽而忽略了某些人，请接受我们的歉意。

首先，要感谢我们的家人和朋友在这段繁忙的研究和写作时间里对我们的支持，他们的理解和支持对本书的完成至关重要，我们希望可以弥补这段离开他们完成又一个图书项目的日子（真的，这次我们保证！）。

其次，感谢我们的伙伴 Hernan Ochoa、Justin Hays、Carl Livitt 和 Rob Ragan 对本书的宝贵贡献。还要特别感谢 Robert Hensing 犀利的技术评审和许多重大的贡献。

特别感谢先前版本的主要作者对这个版本的巨大影响。Caleb Sima（第 1 版和第 3 版的合著者）在 Web 应用安全领域不断推出新发明，Mike Shema（第 1 版的合著者）坚持不懈地将书中的想法精炼为自动化的过程。

当然，要再次深深地感谢不知疲倦的 McGraw-Hill 制作团队，包括我们的组稿编辑 Megg Morin、黑客曝光系列“名誉编辑”Jane Brownlow、组稿协调员 Joya Anthony，感谢他们使一切工作井然有序，感谢制作顾问 Melinda Lytle 和项目编辑 LeeAnn Pickrel，他们即使面对周末交付的样稿和其他作者强加给他们的不公平的任务时都保持着负责任的心态。

我们还要感谢在本书许多主题上提供了意见和指导的很多人，包括 Consciere 的 Kevin Rich、Kevin Nassery、Tab Pierce、Mike DeLibero 和 Cyrus Gray。此外，我们还要衷心地感谢 Stach & Liu 的 Fran Brown、Liz Lagman、Steve Schwartz、Brenda Larcom、Shyama Rose 和 Dan 对我们工作的不懈支持。

还要感谢 Chris Peterson 对本书手稿的反馈意见以及序言中对本书的赞扬，感谢对我们的初稿提出意见的同事们：Chad Greene、Robert Hansen、Cem Paya、Andrew Stravitz 和 Ken Swanson。

我们要一如既往地向全世界许多敏锐而且有创造力的黑客们脱帽致敬，他们持续不断地创新并且为《黑客大曝光》提供原始素材，特别是那些经常与我们通信的人们。

最后，要对所有《黑客大曝光》的读者说声“谢谢”，你们的支持使得所有辛勤的工作都有了价值。

——Joel、Vinnie、Caleb

感谢 Jane 让《黑客大曝光》系列图书起飞，并且坚持了这么多年。

——Joel

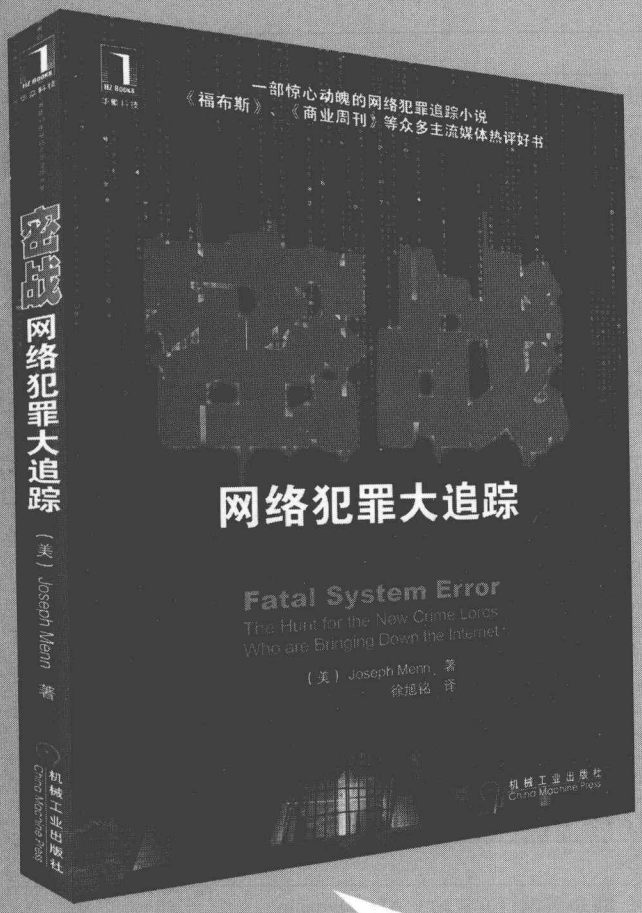
感谢 Heather 在本书整个写作过程中让我总是带着笑。

——Vinnie

感谢我的母亲和父亲（对我的宽容），我的哥哥 Jonathon、RJ 和 Andrew，以及我的姐姐 Emily。最后，感谢 SPI 的所有人，他们改变了我的生活并且帮助我建立了一个伟大的公司。

——Caleb

HZ BOOKS
华章科技



书号：978-7-111-33265-7
定价：39.00元

2004年的时候，加利福尼亚的计算机高手Barrett Lyon注意到一名多次攻击商业网站的黑客。在尽可能不引起对方警觉的情况下，他展开了一场跟踪调查，并发掘出一帮俄罗斯黑帮。计算机犯罪一直以来都在不断演化升级。它不再是过去那种小偷小摸的把戏，而是早就形成了严密的帮会组织。最初他们只会攻击一些公司的网站，但是现在正越来越多地开始偷取客户的商业数据，甚至政府的国防机密。

在Barrett调查这项高科技犯罪的时候，美国政府也正在迎头赶上。不过在英国，情况则完全不同。在1990年代末，女王亲自将安全的电子商务列为国家安全的头等大事。伦敦国家高科技犯罪小组的探员找到了Barrett，希望得到他的帮助。他们还派出了Andrew Crocker探长（他之前在威尔士当过拳击手）前往俄罗斯跟踪抓捕黑客，并设法找出他们究竟是在为谁工作。

《密战》揭露了俄罗斯网络暴徒和美国黑手党之间在互联网上爆发的大规模冲突。从旧金山到柯斯达黎加，再到伦敦和俄罗斯，本书引导读者深入了黑客阴暗的地下世界。通过前所未有的手段触及黑帮事务以及俄罗斯官方，展示了顶级罪犯是如何从俄罗斯政府那里获取庇护的，以及Barrett Lyon和Andrew Crocker是怎样步步接近这些之前从未有人成功接近的地下经济大鳄。这些故事将会告诉你计算机犯罪要远比你想象的更糟糕，以及为什么互联网有可能会无法生存。

机械工业出版社
China Machine Press

专业成就人生
立体服务大众

HZ BOOKS

www.hzbook.com

填写读者调查表　加入华章书友会
获赠精彩技术书　参与活动和抽奖

尊敬的读者：

感谢您选择华章图书。为了聆听您的意见，以便我们能够为您提供更优秀的图书产品，敬请您抽出宝贵的时间填写本表，并按底部的地址邮寄给我们（您也可通过www.hzbook.com填写本表）。您将加入我们的“华章书友会”，及时获得新书资讯，免费参加书友会活动。我们将定期选出若干名热心读者，免费赠送我们出版的图书。请一定填写书名书号并留全您的联系信息，以便我们联络您，谢谢！

书名：　　书号：7-111-(　　)

姓名：	性别：☐男　☐女	年龄：	职业：
通信地址：		E-mail：	
电话：	手机：	邮编：	

1. 您是如何获知本书的：

☐朋友推荐　☐书店　☐图书目录　☐杂志、报纸、网络等　☐其他

2. 您从哪里购买本书：

☐新华书店　☐计算机专业书店　☐网上书店　☐其他

3. 您对本书的评价是：

技术内容	☐很好	☐一般	☐较差	☐理由_____
文字质量	☐很好	☐一般	☐较差	☐理由_____
版式封面	☐很好	☐一般	☐较差	☐理由_____
印装质量	☐很好	☐一般	☐较差	☐理由_____
图书定价	☐太高	☐合适	☐较低	☐理由_____

4. 您希望我们的图书在哪些方面进行改进？

5. 您最希望我们出版哪方面的图书？如果有英文版请写出书名。

6. 您有没有写作或翻译技术图书的想法？

☐是，我的计划是_____　☐否

7. 您希望获取图书信息的形式：

☐邮件　☐信函　☐短信　☐其他_____

请寄：北京市西城区百万庄南街1号　机械工业出版社　华章公司　计算机图书策划部收
邮编：100037　电话：（010）88379512　传真：（010）68311602　E-mail: hzjsj@hzbook.com