HZ BOOKS
华章科技

Web安全领域的圣经级著作，唯一深度探索现代Web浏览器安全技术的专著，由来自Google Chrome浏览器团队的世界顶级黑客、国际一流信息安全专家撰写。

从浏览器设计角度深入剖析现代浏览器的技术原理、安全机制和设计上的安全缺陷，为Web安全工作者应对基于浏览器的各种安全隐患提供指南。

信息安全技术丛书

Web之困

现代Web应用安全指南

The Tangled Web

A Guide to Securing Modern Web Applications

[美] Michal Zalewski 著　朱筱丹 译　殷钧钧 审校

机械工业出版社
China Machine Press

Web之困

现代Web应用安全指南

The Tangled Web

A Guide to Securing Modern Web Applications

[美] Michal Zalewski 著　朱筱丹 译　殷钧钧 审校

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Web之困：现代Web应用安全指南 /（美）扎勒维斯基（Zalewski, M.）著；朱筱丹译. —北京：机械工业出版社，2013.10（2013.11重印）
（信息安全技术丛书）
书名原文：The Tangled Web: a Guide to Securing Modern Web Applications

ISBN 978-7-111-43946-2

Ⅰ. W… Ⅱ. ①扎… ②朱… Ⅲ. 浏览器－安全技术－研究 Ⅳ. TP393.092

中国版本图书馆CIP数据核字（2013）第211485号

本书在Web安全领域有“圣经”的美誉，在世界范围内被安全工作者和Web从业人员广为称道，由来自Google Chrome浏览器团队的世界顶级黑客、国际一流安全专家撰写，是目前唯一深度探索现代Web浏览器安全技术的专著。本书从浏览器设计的角度切入，以探讨浏览器的各主要特性和由此衍生出来的各种安全相关问题为主线，深入剖析了现代Web浏览器的技术原理、安全机制和设计上的安全缺陷，为Web安全工作者和开发工程师们应对各种基于浏览器的安全隐患提供了应对措施。

本书开篇回顾了Web的发展历程和安全风险的演化；第一部分解剖了现代浏览器的工作原理，包括URL、HTTP协议、HTML语言、CSS、文档格式、浏览器插件等内容；第二部分从浏览器的设计角度深入分析了各种现代Web浏览器（Firefox、Chrome、IE等）所引入的重点安全机制，例如同源策略、源的继承、窗口和框架的交互、安全边界、内容识别、应对恶意脚本、外围的网站特权等，并分析了这些机制存在的安全缺陷，同时为Web应用开发者提供了如何避免攻击和隐私泄露的应对措施；第三部分对浏览器安全机制的未来趋势进行了展望，包括新的浏览器特性与安全展望、其他值得注意的浏览器、常见的Web安全漏洞等。

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
北京市荣盛彩色印刷有限公司印刷
2013年11月第1版第2次印刷
186mm×240mm · 17.5印张
标准书号：ISBN 978-7-111-43946-2
定 价：69.00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 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

华章计算机
HZBOOKS | Computer Science and Technology

译 者 序

这是一本很特别的书。

在翻开本书之前，每位读者可能都曾阅读过一些 Web 安全相关的书籍。但本书的目标和写法，与常规的 Web 安全书籍大相径庭。套句江湖行话来说，这是一本修炼内功的秘籍，它并未传授什么具体的武功，不会手把手地教读者怎么练一门剑术或轻功，但它构建了一个完整的 Web 安全图景，为读者在这个庞杂领域里继续深入钻研打下稳固的技术根基，相信每位打开这本“秘籍”的读者都能从中获益良多。

所以如果读者打算找的是一本常规的“黑客手册”，那它可能不适合你。本书作者浸淫安全领域多年，无疑是圈内顶尖高手，甚至自己也开发了网站漏洞扫描程序 Skipfish。但在这本厚积薄发的技术书里，他却并没有告诉读者，要怎么去黑掉一个网站或有什么趁手工具可用，所以曾有国外读者玩笑似地抱怨本书写得不够“邪恶”。的确，全书的前三分之一，作者都在讨论貌似枯燥的各种 RFC 协议和规范的来龙去脉，解决什么问题，具体机制是什么，都潜藏了哪些漏洞或缺陷，以及这些问题的历史根源。这一部分涵盖了许多我们熟悉的 Web 相关内容，比如 URL、HTTP、HTML、JavaScript、CSS 和插件等最基本的 Web 组件。但作者探索程度之深之广，令人叹服（难怪 Joey 说这是 Web 安全的圣经）！在跟随作者展开这场 Web 安全之旅时，即使最资深的 Web 开发工程师和安全渗透工程师只怕也会觉得乱花渐欲迷人眼，而这些问题所带来的后果更时常令人弹眼落睛，怵目惊心——很多问题和陷阱，我们自己又何尝没吃过亏呢。

本书第二部分为全书核心，主题为浏览器安全机制，是作者更侧重的研究领域。作者在前言里开宗明义，提到本书源自他所维护的一个技术性维基站点“Google’s Browser Security Handbook”项目。作为走在浏览器安全领域技术潮流前端的人物，作者关注的问题不但全面而且深入。这一部分的重头戏是同源策略，围绕经典的同源策略应用，派生出不同场景里的微妙差异、各种继承关系以及跨域的解决方案，另外还涵盖了同源策略无法企及的一些犄角旮旯的方面。此外，作者还谈到了被广泛忽略的浏览器内容自动识别问题，以及一些外围的特权问题和恶意脚本的处理。对浏览器端的安全机制这一主题，可能是第一次有人进行如此全面深入的探讨。也许国内的安全工程师和开发人员往往更侧重服务器端的安全，但在当前的技术浪潮下，服务器端与浏览器端的界限已经越来越模糊，两者越来越紧密地相连，浏览器安全理应获得更多的关注，相信在全新的讨论领域里，读者

会受到许多启发。

作者在最后展望了一批属于未来的 Web 技术，以及它们对今后几年 Web 安全可能产生的影响，有助于读者了解前瞻性的技术动向。当然，由于本书写于两年前，可能其中有部分机制已经被业界采纳成为正式的规范。

在许多章的最后，作者都给出了“安全工程速查表”，内容是和本章主题相关的安全建议。这些整理得当的安全列表对网站和 Web 组件的开发者、架构设计师们想必都会有非常直接的帮助。但同时，这个速查表和本书的其他内容，也完全可以作为安全渗透人员的反向指标，为安全检测带来更多启发性的思路。尽管本书通常被归类为“黑客”书籍，但它也同样能为 Web 开发人员和 Web 防御工程人员带来实际的帮助。攻与防，在这里有机地结合到了一起。

本书另一个特别的地方是：它非常“扎实”！也就是说，干货很多很实在。原书只有不到 300 页篇幅，却涵盖了 Web 各组件、浏览器全部安全机制和未来技术展望，知识点异常密集！可想而知，作者的写法有多简洁明了，这给翻译带来了不小的困难。并且容我冒昧吐槽一句，由于作者本人非常聪明有才，往往不屑于把问题展开来阐述，所以一个非常复杂的知识点也经常被寥寥数语带过，对没有一定基础的读者来说，难免存在阅读和理解障碍。在此译者再啰嗦地提出几点阅读建议：

- 读慢些，反复读。本书绝对不是那种读一遍就能完全领会、流畅易懂的书籍，适合它的阅读方式应该是放在案头，时常翻阅，常读常新。
- 不要忽略文中带上标的注释。有些作者只写了几句话的地方，其实对应着一篇长达几十页的论文或很长的一篇网页文章！如果看不懂原文可试着阅读关联的注释内容或自行在搜索引擎里寻找答案。
- 作者本人的“Google's Browser Security Handbook”项目是个获取知识的宝库，涉及很多浏览器端安全相关内容。在阅读第二部分时，可配合阅读和实验。
- 译者水平有限，不能尽显原书之意，读者阅读时如觉理解困难，建议参考英文原文。

在本书的翻译过程中，得到了各位师友无私的帮助，特此鸣谢！感谢姚莉莉的建议，促使我接下本书的翻译，并在此后的翻译过程中给予了无数的帮助和监督；感谢编辑吴怡一直以来对我的耐心、宽容和信任；感谢 Joey（殷钧钧）对本书的推荐和审读，以及在翻译过程中提供的持续帮助；感谢贾洪峰老师和我的同事黄伟，他们对细节的关注，对技术的理解和对书稿的审阅，都使我获益良多；另外也要感谢 Xiaket（夏恺）、钱文芳对部分章节的审读。

本书是译者的第一本译作，水平有限，错误难免。只有诚挚地希望读者诸君在发现错误时请务必告知，我将建立一个勘误表，作为弥补之计。可使用电子邮件与我联系：danzhu@gmail.com，或新浪微博：medanzhu。

前　言

仅在 15 年前，互联网还是简单而无足轻重的：这套古怪的机制不过是让一群学生，还有一伙不太合群、住在地下室里的科学怪人，能访问彼此的个人主页而已，这些主页的内容可能是科学、他们的宠物或诗歌什么的。但到了今天，互联网已成为创建各种复杂交互应用的平台（这些应用包括从邮件客户端、图片编辑器到电脑游戏），它还是一种遍布全球、无数普通用户都能访问的大众媒体，同时它俨然已是重要的商业手段，以致 1999 ~ 2001 年第一次互联网泡沫破灭时，它正是导致经济倒退的主要原因。

即使以我们所处的信息化时代标准来衡量，互联网从默默无闻到无处不在，其发展速度也算异常惊人——但这种惊人的跃升速度也带来许多难以预计的问题。互联网在设计上的缺陷和实现上的漏洞与它的发展状况完全不相称，但我们并没有机会停下脚步回顾之前的错误。这些缺陷很快就导致今时今日许多严重又普遍的数据安全问题：人们发现，当年那个用在简单花哨个人主页上的互联网机制设计标准，已完全不适用于当下每年处理庞大信用卡交易的在线商店。

如果我们回顾过去 10 年，心里难免会略有失落：几乎每个如今值得说道的在线应用，都曾由于使用了那些早期贪图方便胡乱拼凑的互联网技术，导致以后付出了沉重的代价。以站点 xssed.com 为例，它仅仅收集了无数 Web 安全问题中很特定的一种，但在 3 年的运营时间里，已累计收集超过 5 万次攻击事件，真见鬼！然而，浏览器开发商还是颇为无动于衷，安全社区也未能就这些广泛存在的问题提出什么有见地的建议。与此相对的是安全专家正孜孜不倦地建造一套复杂而炫目的漏洞分类学，并对这种混乱景象的根本原因既习以为常又隐隐担忧绝望。

导致上述问题的部分原因，是由于这些所谓的专家长久以来对 Web 安全的整个混乱状态视而不见，对 Web 安全缺乏真正的了解。他们很利落地给网站漏洞贴上各种标签，比如“责任混淆”（confused deputy）问题[⊖]的各种体现，或者干脆用一些 30 年前商业期刊上惯常的抓眼球字眼。再说了，他们干嘛要费心去关注网络安全呢？一个关于宠物的无聊

⊖ 责任混淆问题（confused deputy problem）是信息安全领域里一个笼统的概念，指某一大类的设计和实现上的缺陷。这个术语描述的是攻击者通过欺骗程序，使其不当地使用“授权”（访问权限），得以某种意想不到的方式操纵资源——通常这种操纵有利于攻击者，这里姑且不论“有利”的具体含义。这个术语在学术界经常被安全专家提及，但从抽象层面来说，现实世界的所有安全问题几乎都可以用这个术语一言以蔽之，所以这个术语其实没多大意义。

个人主页上被加入了一段莫名其妙的注释代码哪能和传统的针对操作系统的漏洞攻击相提并论呢？

回顾过往，我确信我们中的大多数人都有过打落牙齿和血吞的感觉。不仅因为互联网的重要性已远超当初人们的预期，而且我们为了满足自己的心理舒适感，把一些重要的互联网基础特性置于不顾。结果导致即使设计最精良、经过最全面审核的网站应用，也往往比同样功能的非网站应用产生更多的问题。

我们过去搞砸了，现在到悔恨弥补的时候了。出于这个考虑，本书期望能在亟需解决的标准化问题上取得一点进展，除此以外，这也许还是第一本系统而全面地剖析当下 Web 应用安全问题的书籍。为达到这一目标，本书深入描述了我们日常面对的各种安全挑战的独特性，这里的“我们”包括安全专家、网站开发工程师和用户。

本书的章节安排以探讨浏览器的各主要特性和由此衍生出来的各种安全相关问题为主线。因为比起随便采用某种漏洞分类学来罗列问题（这是许多信息安全书籍通常采用的形式），希望这种方式能提供更丰富的信息和更直观的效果。我还希望，这样的安排能使本书更容易阅读。

为使读者便捷地获取答案，我会在每章的最后尽量附上一份“安全工程速查表”。这些速查表为网站应用设计中各种常见问题提供了一些合理的解决方向。此外，在本书的最后一章罗列了最常见的网站漏洞形式及其实现方式。

鸣谢

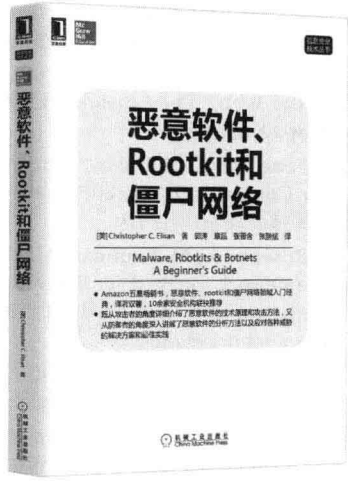
本书中的许多内容都源自 Google's Browser Security Handbook 项目，这是我从 2008 年开始维护整理的一个技术性维基站点，该站点以 Creative Commons 授权模式发布。你可以通过浏览以下网址：http://code.google.com/p/browsersec/ 获取相关的源码。我很幸运，因为这个项目不但获得公司的支持，而且能和一群出色的同事一起工作，使得 Browser Security Handbook 的内容能更有用、更准确。在此，我要特别感谢 Filipe Almeida、Drew Hintz、Mariu Schilder 和 Parisa Tabriz 的鼎力相助。

能站在巨人的肩膀上，对此我深感自豪。因为本书从安全社区成员对浏览器安全的广泛研究上获益良多，特别感谢 Adam Barth、Collin Jackson、Chris Evans、Jesse Ruderman、Billy Rios 和 Eduardo Vela Nava，他们极大地提高了我们对这个领域的理解，为这个领域作出了巨大贡献。

无限感激——各位大牛们，继续牛下去吧！

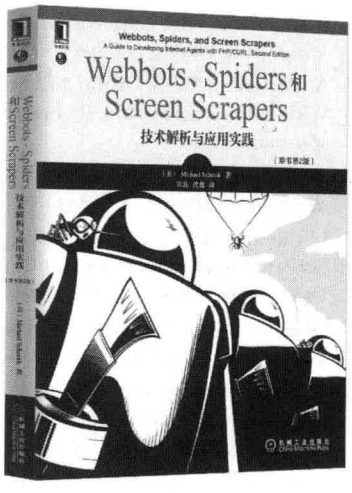
推荐阅读

本书是Metasploit渗透测试领域难得的佳作，由国内信息安全领域的布道者和资深Metasploit渗透测试专家领衔撰写，特色十足，必定会被奉为经典。



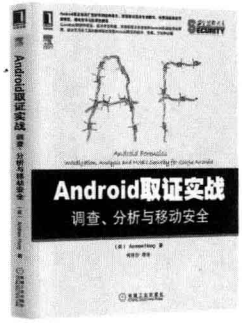
本书是恶意软件、Rootkit和僵尸网络领域的经典入门书，也被誉为是该领域最好的一本书，10余家安全机构联袂推荐，Amazon五星畅销书。

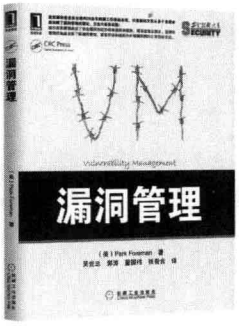
亚马逊五星级畅销书，资深计算机安全专家集大成之作，国内众多读者翘首以盼！首次从反取证角度，采用模块化示例、风趣的类比，形象解读rootkit的本质、检测和应对策略，以及各种防护工具的固有缺点和构建定制工具的方法和技术。

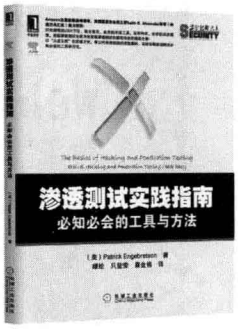


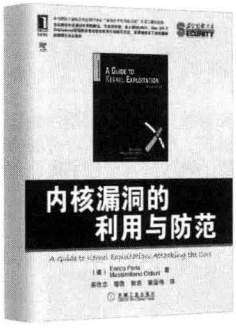
本书是Webbots（网络机器人）、Spiders（蜘蛛）、Screen Scrapers（抓屏器）领域的权威著作，在国际安全领域被广泛认可，是资深网络安全专家15年工作经验的结晶。

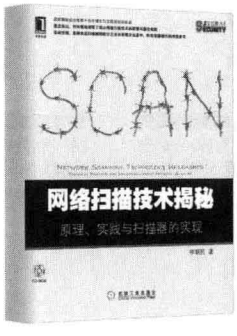
推荐阅读

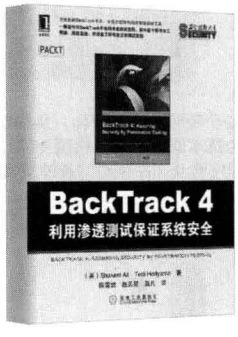












- **Android取证实战：调查、分析与移动安全**
  作者：Andrew hoog
  ISBN：978-7-111-42199-3
  定价：69.00元

- **漏洞管理**
  作者：Park Foreman
  ISBN：978-7-111-40137-7
  定价：69.00元

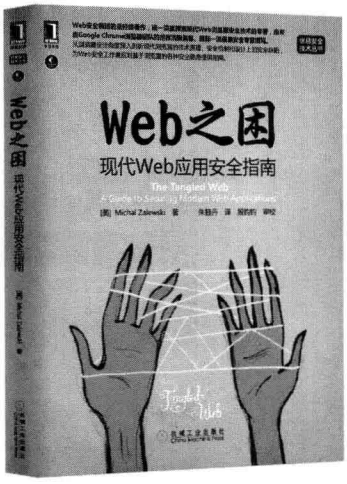
- **渗透测试实践指南：必知必会的工具与方法战**
  作者：Patrick Engebretson
  ISBN：978-7-111-40141-4
  定价：49.00元

- **内核漏洞的利用与防范**
  作者：Enrico Perla 等
  ISBN：978-7-111-37429-9
  定价：79.00元

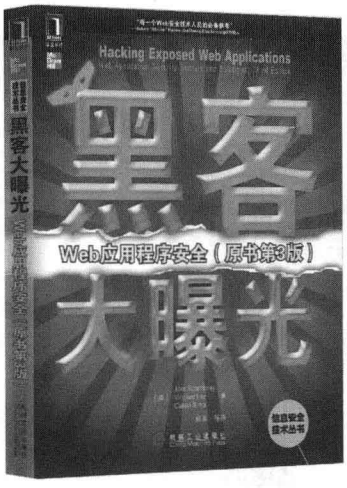
- **网络扫描技术揭秘：原理、实践与扫描器的实现**
  作者：李瑞民
  ISBN：978-7-111-36532-7
  定价：79.00元

- **BackTrack 4: 利用渗透测试保证系统安全**
  作者：Shakeel Ali
  ISBN：978-7-111-36643-0
  定价：59.00元

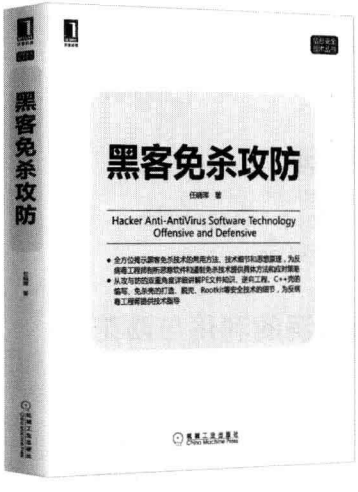
推荐阅读



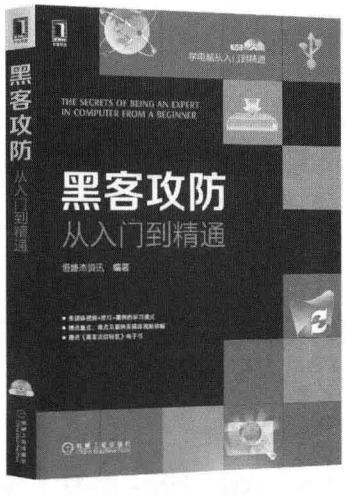
Web安全领域圣经级著作，从浏览器设计角度深入剖析现代浏览器的技术原理、安全机制和设计上的安全缺陷，为Web安全工作者应对基于浏览器的各种安全隐患提供应对措施。



本书覆盖新的网络渗透方法和对策，介绍如何增强验证和授权、弥补Firefox和IE中的漏洞、加强对注入攻击的防御以及加固Web 2.0安全，还介绍了如何将安全技术整合在Web开发以及更广泛的企业信息系统中。



从攻与防的双重角度详细讲解PE文件知识、逆向工程、C++壳的编写、免杀壳的打造、脱壳技术、Rootkit等安全技术的细节，为反病毒工程师提供技术指导。



本书逐层深入地将黑客入侵攻击演示以及防御黑客入侵的操作以图文结合的形式进行介绍，读者可以轻松掌握有关黑客入侵目标计算机和防御黑客入侵计算机的基础知识。

目　录

第1章

Web 应用安全

为了给本书后面的技术讨论提供必要的背景知识，我们首先解释清楚安全领域涵盖哪些方面，以及为什么在这个早已被研究得很透彻的领域里，Web 应用的安全仍然值得引起额外的关注。那么，让我们开始吧？

1.1 信息安全速览

表面上看来，信息安全领域属于计算机科学里很成熟、明确且硕果累累的一个分支，自以为无所不知的专家们通过展现他们那分类清晰、数量庞大的安全漏洞集来标榜这一领域的重要性。至于那些漏洞的责任嘛，就全都归到那些“安全文盲”的程序员们头上好了，而理论家们则会从旁指点，说只要遵从今年最热门的某某安全方法学，早就能把这些问题都防患于未然了云云。安全问题更是带动了一个产业的繁荣，但对用户来讲，从普通计算机用户到庞大的国际公司等，其实并没有带来什么有效的安全保障。

从根本上来说，过去几十年，我们甚至没能构建出一个哪怕原始但至少还算可用的框架来理解和评估现代软件的安全性。除了几篇出色的论文和一些小范围内取得的经验，甚至无法拿出什么有说服力的真实的成功案例。现在的侧重点几乎都放在一些响应性质的、次要的安全方法上（如漏洞管理、恶意软件和攻击的检测、沙盒技术以及其他），要不就