Mc Graw Hill Education

“本书在致力于使Web变成一个更安全的商业环境方面做出了巨大贡献。”

——Mark Curphey，开放Web应用安全工程主席

Web Application Security Secrets & Solutions

Hacking Exposed™ Web Applications

Web应用黑客大曝光

Web应用安全机密与解决方案

【美】Joel Scambray, Mike Shema 著

田芳 陈红 译

Mc Graw Hill 清华大学出版社

Web 应用黑客大曝光

Web应用安全机密与解决方案

Hacking Exposed™ Web Applications

Web Application Security Secrets & Solutions

【美】 Joel Scambray Mike Shema 著

田芳 陈红 译

清华大学出版社

北京

Joel Scambray, Mike Shema
Hacking Exposed™ Web Applications:Web Application Security Secrets & Solutions
EISBN: 0-07-222438-X

图书在版编目（CIP）数据

Web 应用黑客大曝光/（美）斯坎布里（Scambray, J.），希曼（Shema, M.）著；田芳，陈红译. —北京：清华大学出版社，2003.10
书名原文：Hacking Exposed™ Web Applications
ISBN 7-302-07486-0

Ⅰ. W… Ⅱ. ①斯… ②希… ③田… ④陈… 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（2003）第 097013 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

组稿编辑：成昊
文稿编辑：朱起飞
封面设计：曹映红
版式设计：科海
印 刷 者：北京科普瑞印刷有限责任公司
发 行 者：新华书店总店北京发行所
开　　本：异 16　印张：23.625　字数：501 千字
版　　次：2003 年 11 月第 1 版　2003 年 11 月第 1 次印刷
书　　号：ISBN 7-302-07486-0/TP・5518
印　　数：1～4000
定　　价：39.00 元

内 容 提 要

在 Web 技术飞速演变、电子商务蓬勃发展的今天，在线安全风险达到了前所未有的高度。本书详细剖析了 Web 应用中的常见漏洞，并解释了当安全威胁到来时你应该如何正确行事。

本书分为 3 个部分：1. 侦察，备战网络大盗，罗列各种抗拒敌人的有用信息；2. 攻击，综合考虑所搜集的所有信息，针对获取 Web 应用非授权访问的企图，精心编制出应对方法；3. 附录，是参考文献的集合（包括 Web 应用安全检查列表、Web 黑客工具和技术的列表、如何配置与安装 UrlScan，等等）。全书以 step-by-step 的方式教授你如何防御最新的基于 Web 的攻击，让你深入理解黑客的邪恶方法和思考过程。

本书是 Web 应用安全的宝典，是负责网络安全保障工作的网络管理员和系统管理员的必需品，电子商务从业者、网络爱好者及企业和组织的管理层也可以从中获益。

序

在最近 5 年里，一场静悄悄的但是具有革命性的变革很明显地改变了信息安全产业，同样也改变了黑客社会。随着人们逐渐掌握了利用防火墙、入侵检测系统以及主机硬化等技术来加强他们的网络和操作系统的安全性，这个世界便开始通过 WWW 的形式，在因特网上展示它的无穷魅力。Web 使得访问顾客和猎奇比以往所能想象的要容易得多。Sun、Microsoft 以及 Oracle 把宝都押在了将要在 21 世纪成为主要商务平台的 Web 上了。

不过，这一点与建筑工业非常类似：花费了多年心血来开发复杂而牢固的门和锁，但是在某一天早上醒来时却发现，原来那些玻璃能够被一眼看穿，同时又是脆弱的，很容易被不速之客破门而入。由于安全公司和专家们一直都在忙于帮助组织机构应对网络安全问题，所以曾经一度对于应用程序这一发展最快、应用最广的技术就很少关心了。两年前当我开始在 www.securityfocus.com 上修改 Web 应用安全邮件列表时，我敢说人们对于 Web 所面临的安全威胁是非常困惑的。大多数安全威胁是由于恶意的可移动代码以及基于 Web 的特洛伊木马的危险而造成的。这些用户端的小恶作剧与黑客们攻击 Web 应用所造成的严重破坏相比显得微不足道。航空公司被欺骗，几个美元就售出了去大西洋彼岸的机票；在线零售商们暴露了成千上万顾客的合法信用卡的细节；医院泄露了病人的记录，如此等等。一个 Web 应用攻击也许只需要点击一下鼠标就能够令一项业务陷于停顿。

最初的《黑客大曝光》系列揭露了躲在阴暗处的那些坏家伙所使用的一些技术，我相信《Web 应用黑客大曝光》和它们一样，对其关键技术也做了同样的工作。读者可以从书中的方法研究和适当的细节中得到启发、受到教育，要想在商务活动中把 Web 变成一个更为安全的地方，还需要走很长一段路。

——Mark Curphey

开放 Web 应用安全工程主席（http:// www.owasp.org），站点 securityfocus.com 的“webappsec”邮件列表的主持人。

前　言

我们已经织就一个混乱的 Web

3 年前，《黑客大曝光》的第一版引导了许多人看到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，但还是有大量的人们开始理解并采纳了防火墙、安全操作系统配置、及时打供应商提供的补丁，以及其他许多在以前看来都非常神秘的用于信息系统安全的基础设施。

不幸的是，由因特网带来的这种迅猛变化早已超出了人们的想象。防火墙、操作系统安全，以及最新的补丁都能够被一个简单的针对 Web 应用的攻击绕过去。虽然这些元素仍然是任何安全基础设施的关键部件，但是它们已经无力阻止新一代的攻击，而新型攻击现在每天都在快速地发展着。

我们不可能将因特网商务这匹马拉回厩，再关上门。没有别的出路，只有在沙地上划上一条线，保护由无数个组织机构和个人划分出的电脑空间。

对于任何组建了最基本的 Web 站点的人来说，这无疑是一项令人沮丧的工作。面对已有的协议所存在的安全限制，以及不断加速发展的新技术，如 WebDAV 和 XML Web 服务，设计并实现一个安全的 Web 应用绝对是一个非常艰巨的挑战。

迎接 Web 应用安全挑战

我们将向您展示如何迎接这一挑战——利用原有《黑客大曝光》中采用的双刃剑方法，现在已经出到第 3 版了。

首先，我们将你的 Web 应用可能面临的最严重威胁进行分类，并且会非常详细地解释它们的工作原理。我们是如何知道这些最严重的威胁的呢？因为我们是由世界上最大的公司雇用来进攻他们的 Web 应用，而且我们日常所用的就是这些威胁工具。我们进行这项工作已经有 3 年的时间了，在这期间我们不断地搜索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所认为的最有效的方法中去，这些方法能够渗透已有的、不安全的 Web 应用。

一旦你注意到这些威胁可能造成的危害，我们还会告诉你如何阻止每一种攻击。如果不掌握本书的内容就使用 Web 应用，就好比驾驶着一辆没有安全带的汽车——奔驰在光滑的路面上，要越过一条巨大的裂坑，没有刹车，将完全被扼杀在拥堵中。

本书是如何组织的

本书由 3 个部分组成，以下描述了各级内容的组织。

1. 侦察

备战网络大盗，以及如何抗拒你的敌人的有用信息。

2. 攻击

综合考虑所搜集的所有信息，针对获取 Web 应用非授权访问的企图，精心编制出应对方法。

3. 附录

附录是参考文献的集合，包括以下内容：一个 Web 应用安全检查列表（附录 A）；一个 Web 黑客工具和技术的详细列表（附录 B）；一个指导性的脚本样例，描述如何使用 HTTP 黑客工具 libwhisker（附录 C）；如何部署可靠的 IIS 安全过滤器 UrlScan（附录 D）；以及与本书有关的 Web 站点 www.webhackingexposed.com 的一个简介（附录 E）。

章节：Web 黑客大曝光的方法学

每一部分都由数章组成，本书的章节是按照明确的攻击计划进行划分的。这种攻击计划是恶意的黑客所采用的方法学，取自《黑客大曝光》：

- ▼ 剖析基础设施
- ■ 攻击 Web 服务器
- ■ 调查应用程序
- ■ 攻击认证机制
- ■ 攻击授权方案
- ■ 攻击会话状态管理
- ■ 输入验证攻击
- ■ 攻击 Web 数据存储
- ■ 攻击 XML Web 服务
- ■ 攻击 Web 应用管理
- ■ 攻击 Web 客户
- ▲ 案例分析

这种结构构成了本书的主要框架，因为如果没有一种方法学，这一切就会成为没有上下文联系和任何意义的信息的堆砌。这是我们贯穿本书的主线图。

模块化、组织和可读性

很显然，您可以从头到尾阅读本书，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，我们努力使得各个章节自成体系，这样的话，本书就可以被分成多个模块，以适应目标读者的各种不同需求。

另外，严格按照《黑客大曝光》的一贯风格，给读者以清晰、易读、简明的表述。我们知道你一定很忙，需要的是直奔目标，而不需要一大套无味的说教和无关紧要的行话。正如某一位《黑客大曝光》的读者所言，“读起来像小说，扣人心弦！”

如果你从头到尾一页一页地读，我们想你肯定会很满意，即使用其他的方法读，本书也会让你获益匪浅。

章节小结和参考文献以及进一步的阅读材料

为了进一步改善本书的组织结构，在每章的末尾增加了这样两个部分：“小结”和“参考文献以及进一步的阅读材料”。

顾名思义，“小结”是这一章所涉及的主要概念的一个简要大纲，并着重强调了对策。如果你阅读了每章的“小结”部分，就会知道针对各种攻击应如何保护 Web 应用。

“参考文献以及进一步的阅读材料”包括超级链接、ISBN 号，以及所有其他与本章中所涉及的内容有关的定位信息，包括销售商的安全公告和补丁、第三方的咨询、商业的和免费的工具、Web 黑客事件新闻，以及一般的背景阅读材料，这些材料可以扩展本章所涉及的信息。这样在一章中的正文部分你就会很少发现超级链接，如果你需要查找某些资料，可以到这一章的末尾，它们就在那里。我们希望将所有的参考资料汇集到一块，能够使你在阅读本书时全面享受。

基本构建模块：攻击和对策

与《黑客大曝光》系列书一样，本书的基本构建模块就是每一章所讨论的攻击和对策，并且，攻击在这里是着重强调的。

这是攻击图标

像这样着重强调的攻击名称可以便于标识特定的渗透测试工具和方法，并直指你所需要的信息，这些信息有助于您学习新的安全性。

每种攻击同样伴随有风险，这一点也与《黑客大曝光》的一贯风格一致：

流行度：在江湖上用于攻击实际目标的使用频繁度。1 为极少，10 为广泛使用。
容易度：执行攻击所必须的技巧。1 为很少或不需技巧，10 为老练的安全程序员。
影响力：攻击成功实施后导致的潜在损害。1 为目标的一些无关紧要的信息，10 为超级用户账户或类似的信息。
风险率：上述三者的平均值为基本的风险率，向上取整即为其值。

在对策方面我们也按照《黑客大曝光》的一贯风格，将对策紧跟在每种攻击或者相关的攻击系列之后。对策的图标保持原样：

这是对策图标

这种标记是为了让你的注意力集中在关键的修补对策上。

其他视觉上的帮助

我们还使用了更多的加强视觉效果的图标：

图标强调了一些细节，而这些细节通常很容易被忽略。

联机资源和工具

Web 应用安全是一门变化迅速的学科，我们也认识到印刷出来的文字通常并不能完全跟得上在这一领域中的最新研究结果。

因此，我们制作了一个 Web 站点，以跟踪与本书讨论的主题有关的最新信息、勘误表、公共域工具、脚本，以及我们在这本书中所涉及到的词汇。该站点的地址是：

http//www.webhackingexposed.com

该站点还提供了一个论坛，可以通过电子邮件与作者进行直接讨论：

joel@webhackingexposed.com
mike@wehhackingexposed.com

希望你在阅读本书的时候能够经常到这个站点上去，看看那些更新的资料，访问我们所提到的那些工具，另外还可以跟踪 Web 安全的最新动态。否则，在你能够武装起来以抵抗各种攻击之前，你永远不会知道有哪些新的发展可能危害你的应用程序。

最后致读者

这本书中蕴含着许多个不眠之夜和无数被磨损的鼠标垫，真诚地希望我们所有的研究和写作能够使你在保护 Web 应用的安全方面节省大量的时间。我们认为你做出这样的决定——将你的主张放到因特网上——是非常有勇气和前瞻性的。但是，在这本书中你会看到，当你的站点开始工作时，工作才刚刚开始。不要惊慌失措，开始阅读本书吧，当下一个巨大的 Web 安全灾难降临你的首页时，你会感到欣慰的是，你并不是一无所知。

——Joel&Mike

目 录

第1部分 侦 察

第2部分 攻 击

第3部分 附 录

第1部分

侦察

第1章

Web应用及其安全性导论