TURING 图灵程序设计丛书 网络安全系列

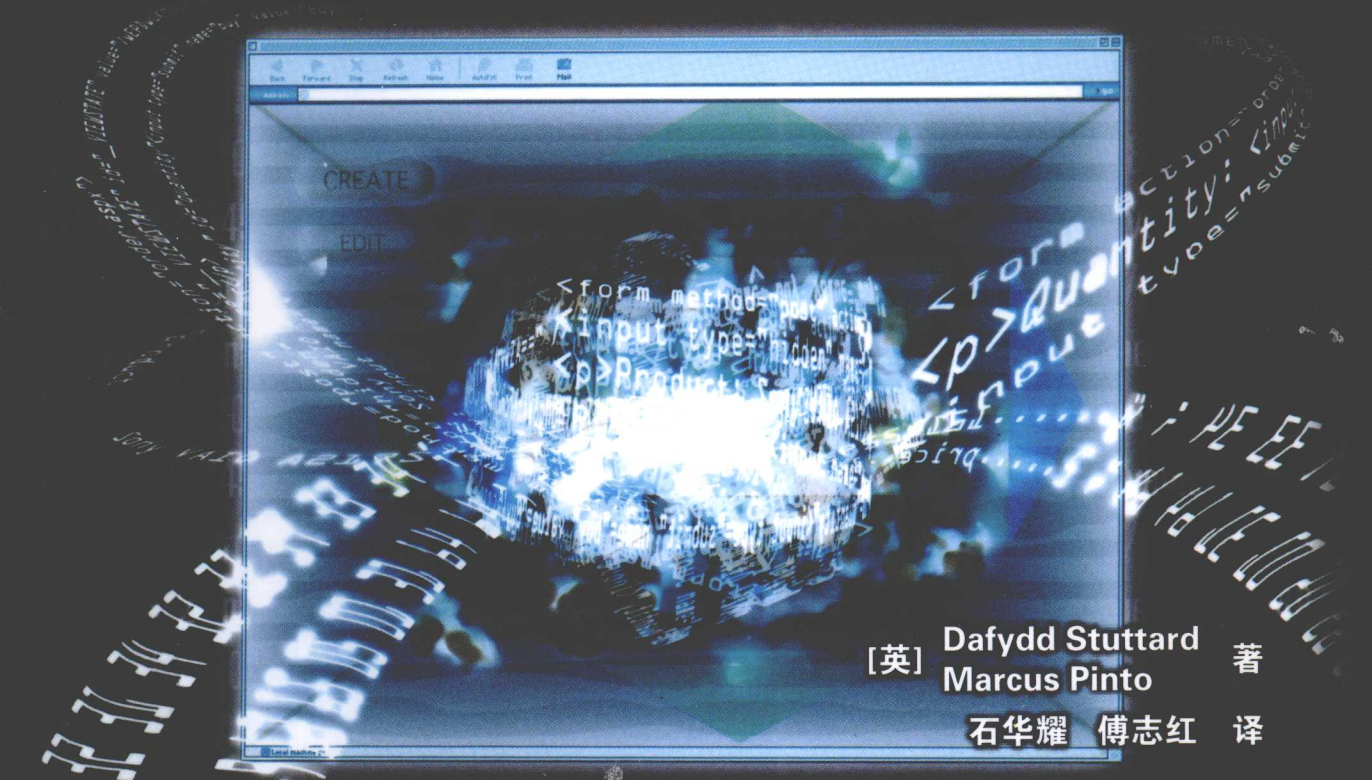
WILEY

The Web Application Hacker's Handbook

Finding and Exploiting Security Flaws Second Edition

黑客攻防技术宝典

Web实战篇（第2版）



[英] Dafydd Stuttard
Marcus Pinto 著
石华耀 傅志红 译

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书 网络安全系列

The Web Application Hacker's Handbook

Finding and Exploiting Security Flaws Second Edition

黑客攻防技术宝典

Web实战篇（第2版）

[英] Dafydd Stuttard
Marcus Pinto 著
志红 译

人民邮电出版社
北京

图书在版编目（CIP）数据

黑客攻防技术宝典 : 第2版. Web实战篇 / (英) 斯图塔德 (Stuttard,D.), (英) 平托 (Pinto,M.) 著 ; 石华耀, 傅志红译. -- 北京 : 人民邮电出版社, 2012.7
（图灵程序设计丛书）
书名原文: The Web Application Hacker's Handbook:Finding and Exploiting Security Flaws Second Edition
ISBN 978-7-115-28392-4

Ⅰ. ①黑… Ⅱ. ①斯… ②平… ③石… ④傅… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第113416号

内 容 提 要

本书是探索和研究 Web 应用程序安全漏洞的实践指南。作者利用大量的实际案例和示例代码，详细介绍了各类 Web 应用程序的弱点，并深入阐述了如何针对 Web 应用程序进行具体的渗透测试。本书从介绍当前 Web 应用程序安全概况开始，重点讨论渗透测试时使用的详细步骤和技巧，最后总结书中涵盖的主题。每章后还附有习题，便于读者巩固所学内容。

第 2 版新增了 Web 应用程序安全领域近年来的发展变化新情况，并以尝试访问的链接形式提供了几百个互动式“漏洞实验室”，便于读者迅速掌握各种攻防知识与技能。

本书适合各层次计算机安全人士和 Web 开发与管理领域的技术人员阅读。

图灵程序设计丛书

黑客攻防技术宝典：Web实战篇（第2版）

◆ 著 [英] Dafydd Stuttard Marcus Pinto
译 石华耀 傅志红
责任编辑 毛倩倩
执行编辑 刘美英

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京天宇星印刷厂印刷

◆ 开本：800×1000 1/16
印张：40.5
字数：957千字 2012年7月第1版
印数：1－5 000册 2012年7月北京第1次印刷

著作权合同登记号 图字：01-2012-2174号

ISBN 978-7-115-28392-4

定价：99.00元

读者服务热线：(010)51095186转604 印装质量热线：(010)67129223

反盗版热线：(010)67171154

版权声明

译 者 序

自本书第1版出版以来，Web安全状态发生了很大变化，虽然随着人们安全意识的提高，一些漏洞已经得到修复，但随着各种新技术不断涌现，特别是Web 2.0、HTML5、无线互联网以及云服务的推出，Web应用程序的安全将面临更大的挑战。为帮助用户应对这些挑战，本书的两位作者对第1版的内容进行了修订，新增了约30%的内容，主要介绍Web安全领域的新趋势及大量新近出现的漏洞。

从第1版的读者反响来看，大多数读者认为本书内容较深，不太适合初学者学习。诚然，两位作者都是Web安全领域的资深专家，本书更是他们多年职业生涯的智慧结晶。因此，建议读者更多关注书中介绍的基本理论及作者考虑问题的角度，而不是具体的渗透测试方法。

应一些读者的要求，我们推出了书中问题答案的中文版，感兴趣的读者可以访问译者的博客（http://blog.sina.com.cn/s/blog_545eb7860101379s.html）或图灵社区本书页面（http://www.ituring.com.cn/book/885）。

由于本书涉及内容非常广泛，加之译者水平所限，书中难免存在疏漏甚至错误，译者在此恳请读者谅解并指正。

最后，向朱巍、刘美英等诸位编辑表示感谢，谢谢你们的无私帮助。还要感谢我的家人，感谢你们的默默支持。

石华耀

2012年5月20日

前　言

本书是发现并利用Web应用程序安全漏洞的实用指南。这里的“Web应用程序”是指通过使用Web浏览器与Web服务器进行通信，从而加以访问的应用程序。本书不仅分析了大量各种各样的技术，如数据库、文件系统与Web服务器，而且讨论了它们在Web应用程序中的使用情况。

如果你想了解如何运行端口扫描、攻击防火墙或以其他方式对服务器进行渗透测试，我们建议你阅读其他图书。但是，如果你希望了解渗透测试员如何攻击Web应用程序、窃取敏感数据、执行未授权操作，那么本书可以满足你的需要。本书将就以上主题展开全面而翔实的讨论。

本书概述

本书极其注重实用性。虽然我们提供了足够的背景信息与理论知识，以帮助读者了解Web应用程序中包含的漏洞；但是，渗透测试员在攻击Web应用程序时所需要实施的步骤及采用的技巧，才是我们讨论的重点所在。本书详细阐述了探查每一种漏洞所需采用的特定步骤，以及如何利用它执行未授权操作。我们还根据多年的工作经验，列出大量实例，说明在当今Web应用程序中存在的各种安全漏洞。

另一方面，安全意识就像一把双刃剑。开发者能够从了解攻击者所使用的方法中受益；相反，黑客也可以通过了解应用程序的防御机制而窥探它的受攻击面。除介绍安全漏洞与攻击技巧外，我们还将详细介绍应用程序为抵御攻击者而采取的应对措施。同时，Web应用程序渗透测试员还可以从本书中获得大量实用的建议，以帮助应用程序所有者强化他们的应用程序。

本书目标读者

本书的目标读者是Web应用程序渗透测试员，以及负责开发和管理Web应用程序的人，因为了解你的敌人有助于对他们进行有效防御。

我们希望读者熟悉核心安全概念，如登录和访问控制；并希望读者掌握基本的核心Web技术，如浏览器、Web服务器和HTTP。通过阅读本书提供的解释说明或其他参考资料，可以迅速弥补当前读者在这些领域的知识欠缺。

在介绍各种安全漏洞的过程中，我们将提供代码片断，说明应用程序为何易受攻击。这些示例都非常简单，不需要事先了解编写代码的语言就能够理解它们，但是，具备阅读或编写代码的基础知识就再好不过了。

本书结构

总体而言，本书根据不同主题之间的依赖关系将内容组织在一起。如果你还不了解黑客是如何攻击Web应用程序的，应该从头至尾读完本书，以了解在后续有关章节中需要用到的背景信息和技巧。如果你在这方面已经拥有一定的经验，可以直接跳到特别感兴趣的任何章节或部分。必要时，我们将提供其他章节的交叉参考，以帮助你弥补理解上的欠缺。

本书前3章介绍一些背景信息，描述当前Web应用程序的安全状况，说明它将来的发展趋势。然后将介绍影响Web应用程序的核心安全问题，以及应用程序为解决这些问题所采取的防御机制。同时还将介绍当前Web应用程序所使用的关键技术。

本书的主要部分重点讨论核心主题——渗透测试员在攻击Web应用程序时使用的技巧。我们根据实施全面攻击所需要完成的关键任务组织材料，这些任务依次为：解析应用程序的功能，检查和攻击它的核心防御机制，探查特殊类型的安全漏洞。

最后3章对本书涵盖的各种主题进行简要总结：描述如何在应用程序源代码中查找漏洞；回顾能够帮助渗透测试员攻击Web应用程序的工具；详细介绍攻击方法论，说明渗透测试员如何对一个目标应用程序实施全面而深入的攻击。

第1章描述当前在因特网上运行的Web应用程序的安全状况。尽管软件商常常保证Web应用程序是安全的，但绝大多数的应用程序并不真正安全，只要掌握一些技巧，就能够攻破它们。Web应用程序中的漏洞源于一个核心问题：用户可提交任意输入。这一章将分析造成当今应用程序安全状况不佳的关键因素，并说明Web应用程序中存在的缺陷如何导致组织庞大的技术基础架构非常易于受到攻击。

第2章描述Web应用程序为解决“所有用户输入都不可信”这个基本问题而采用的核心安全机制。应用程序通过这些机制管理用户访问、控制用户输入、抵御攻击者。这些机制还为管理员提供各种功能，帮助他们管理和监控应用程序自身。应用程序的核心安全机制还是它的主要受攻击面，在对它们实施有效攻击前，渗透测试员必须了解这些机制的工作原理。

第3章简要介绍渗透测试员在攻击Web应用程序时可能遇到的关键技术，包括相关HTTP协议、客户端与服务器端常用的技术以及各种数据编码方案。已经熟悉主要Web技术的读者可以跳过本章。

第4章描述渗透测试员在攻击一个新的应用程序时所需采取的第一步，即尽可能多地收集与应用程序有关的信息，以确定它的受攻击面，制订攻击计划。渗透测试员需要搜索并探查应用程序，枚举它的全部内容与功能，确定所有用户输入进入点并查明它所使用的技术。

第5章描述了存在漏洞的第一个区域。如果一个应用程序依靠在客户端实现的控件来保护它的安全，就可能造成这种漏洞。这种保护应用程序的方法往往存在缺陷，因为攻击者可轻易避开任何客户端控件。应用程序易于受到攻击的原因有两个：(1) 通过客户端传送数据，认为这些数据不会被修改；(2) 依赖客户端对用户输入进行检查。这一章将介绍一系列有用的技术，包括HTML、HTTP与JavaScript所采用的轻量级控件，以及使用Java applet、ActiveX控件、Silverlight和Flash对象的重量级控件。

第6～8章将主要介绍Web应用程序中最重要的防御机制——负责控制用户访问的机制。第6章描述应用程序确认用户身份的各种功能，包括主登录功能和更加外围的与验证有关的功能，如用户注册、密码修改和账户恢复功能。验证机制在设计和执行方面都包含大量漏洞，攻击者能够利用它们获得未授权访问。这些漏洞包括明显的缺陷，如保密性不强的密码和易于受到蛮力攻击，以及验证逻辑中存在的更微妙的问题。这一章还将详细分析许多安全性至关重要的应用程序所采用的多阶段登录机制，并描述这些机制中频繁出现的新型漏洞。

第7章介绍会话管理机制。大多数应用程序通过有状态会话这个概念补充无状态的HTTP协议，帮助它们在不同的请求中确定每个用户的身份。当Web应用程序受攻击时，这个机制是一个主要的攻击目标；因为如果能够攻破它，就能够有效避开登录机制，伪装成其他用户，而不必知道他们的证书。这一章还将分析生成和传送会话令牌过程中存在的各种常见漏洞，并描述发现和利用这些漏洞所需采取的步骤。

第8章说明应用程序如何实施访问控制。应用程序主要依靠验证与会话管理机制来完成这项任务。本章将介绍各种破坏访问控制的技巧，以及探查和利用这些弱点的方法。

第9章和第10章介绍大量相关漏洞。如果应用程序以不安全的方式在解释型代码中插入用户输入，就会造成这些漏洞。第9章首先详细介绍SQL注入漏洞，讨论各种攻击方法，从最明显、最简单的方法到一系列高级攻击技巧（如带外通道、推断和时间延迟）。对于每一种漏洞和攻击技巧，我们将描述3种常用数据库（MS-SQL、Oracle和MySQL）之间的相关差异，然后介绍一系列针对其他数据存储（包括NoSQL、XPath和LDAP）的类似攻击。

第10章介绍几种其他类型的注入漏洞，包括注入操作系统命令，注入Web脚本语言，文件路径遍历攻击，文件包含漏洞，注入XML、SOAP、后端HTTP请求和电子邮件服务。

第11章将介绍应用程序受攻击面的一个重要的、常被人们忽略的区域——实现其功能的内部逻辑。应用程序逻辑中的漏洞各不相同，它们比SQL注入与跨站点脚本之类的常见漏洞更难以辨别。为此，我们将列举一系列实例，其中存在的逻辑缺陷导致应用程序易于受到攻击，借此说明应用程序设计者与开发者所做出的各种错误假设。根据这些各不相同的缺陷，我们将进行一系列特殊测试，以确定许多常常难以探测的逻辑缺陷。

第12章和第13章介绍一类广泛存在且广受关注的相关漏洞，即应用程序的恶意用户利用Web应用程序中的缺陷攻击其他用户，并以各种方式攻破这些用户。第12章介绍这其中最主要的漏洞——一种影响因特网上的绝大多数Web应用程序的广泛存在的漏洞。我们将详细分析各种类型的XSS漏洞，并介绍检测和利用即使是最难以察觉的XSS漏洞的有效方法。

第13章介绍针对其他用户的几种其他类型的攻击，包括通过请求伪造和UI伪装诱使用户执行操作、使用各种客户端技术跨域获取数据、各种针对同源策略的攻击、HTTP消息头注入、cookie注入和会话固定、开放式重定向、客户端SQL注入、本地隐私攻击以及利用ActiveX控件中的漏洞。最后，我们将讨论一系列不依赖任何特定Web应用程序中的漏洞、但可以通过任何恶意Web站点或处于适当位置的攻击者实施的针对用户的攻击。

第14章并不介绍任何新的漏洞，而是描述一种渗透测试员攻击Web应用程序时需要掌握的技巧。由于每种应用程序都各不相同，大多数攻击都经过某种方式的定制（或自定义），以针对应

用程序的特殊行为，以及发现对攻击有利的操纵方法。这些攻击还要求提出大量相似的请求，并监控应用程序的响应。手动执行这些请求非常费力，而且容易出错。要成为真正熟练的Web应用程序黑客，必须尽可能自动实施攻击步骤，使定制攻击更加简单、快捷而高效。本章将详细描述一种行之有效的方法，以完成这项任务。我们还将讨论在使用自动化技巧时遇到的各种障碍，包括防御性的会话处理机制和CAPTCHA控件。此外，我们还将介绍可用于克服这些障碍的工具和技巧。

第15章分析应用程序如何在遭受攻击时泄露信息。当实施本书描述的其他各种攻击时，渗透测试员应该始终监控应用程序，以确定其他可供利用的信息泄露来源。我们将介绍如何分析应用程序的反常行为与错误消息，以深入了解应用程序的内部工作机制，并细化攻击。我们还将介绍如何利用存在缺陷的错误处理机制，从应用程序中获取敏感信息。

第16章介绍在以C和C++等本地代码语言编写的应用程序中存在的一些重要漏洞。这些漏洞包括缓冲区溢出、整数漏洞和格式化字符串漏洞。这个主题涉及的内容非常广泛，我们将重点讨论如何在Web应用程序中探查这些漏洞，并分析一些实例，了解造成这些漏洞的原因，以及如何对它们加以利用。

第17章介绍一个常被忽略的Web应用程序安全领域。许多应用程序采用一种分层架构，无法恰当地隔离这些层面可能会导致应用程序易于受到攻击，导致攻击者能够利用在其中一个组件中发现的漏洞迅速攻破整个应用程序。共享托管环境带来另外一些严重的威胁，有时，攻击者可以利用一个应用程序中存在的缺陷或恶意代码攻破整个环境及其中运行的其他应用程序。本章还会介绍一种众所周知的共享托管环境“云计算”中出现的各种威胁。

第18章描述各种攻击技巧，说明如何通过攻击Web服务器进而攻击其中运行的Web应用程序。Web 服务器中存在的漏洞主要包括服务器配置方面的漏洞以及Web服务器软件中的安全漏洞。这个主题属于本书的讨论范围，因为严格来讲，Web服务器是技术栈的另一个组件。但是，大多数Web服务器都与在它们之中运行的Web应用程序关系密切。因此，本书介绍针对Web服务器的攻击，因为攻击者常常可以利用它们直接攻破一个应用程序，而不是首先间接攻破基础主机，然后再攻击Web应用程序。

第19章描述另外一种查找安全漏洞的方法。这种方法与本书其他章节讨论的方法截然不同。许多时候，我们都可以对应用程序的源代码进行审查，并且不必得到应用程序所有者的协助。通常，审查应用程序的源代码可以迅速确定一些漏洞，但在运行的应用程序中探查这些漏洞可能极其困难，或者需要耗费许多时间。我们将介绍一种代码审查方法，并简要说明如何对以各种语言编写的代码进行审查，以帮助读者在编程经验不足的情况下进行有效的代码审查。

第20章详细介绍本书描述的各种工具。笔者在攻击真实的Web应用程序时使用的就是这些工具。我们将分析这些工具的主要功能，并详细描述充分运用这些工具的工作流类型。另外，讨论一些全自动工具能否有效地发现Web应用程序中存在的漏洞，并提供一些提示和建议，说明如何充分利用工具包。

第21章综合介绍本书描述的所有攻击步骤与技巧。我们将根据渗透测试员在实施攻击时所需完成的任务之间的逻辑依赖关系来组织这些步骤与技巧，并对它们进行排序。如果你已经阅读并

理解书中描述的各种漏洞和攻击技巧，就可以把这个方法当作一个完整的清单和工作计划，对Web应用程序实施渗透测试。

新增内容简介

第1版出版4年以来，许多事情发生了改变，而许多事情仍保持原状。当然，新技术继续高速发展，这引发了各种新型漏洞和攻击。同时，黑客们还开发出了新的攻击技术，设计了利用旧有漏洞的新方法。但是，这些技术或人为因素都不可能引发革命。今天应用程序采用的技术早在许多年前就已经确立，现今的先进攻击技术所蕴涵的基本概念也早在高效应用这些技术的许多研究人员出生之前就已经成形。Web应用程序安全是一个动态且充满活力的研究领域，但多年来，人类积累的智慧也在缓慢进化，因此，当前的技术状况与10年或更久以前的情况截然不同。

第2版并不是对第1版的彻底改写，第1版的大部分内容，现在仍然适用。第2版约30%的内容为新增内容或改动很大，剩余70%的内容仅有小幅改动或未作任何修改。如果读者购买了本书，但对这些改动感到失望，请不要放弃。如果你已经掌握了第1版中介绍的所有技巧，说明你已经学会所需的绝大部分技能和知识。这样的话，你就可以集中精力学习本书的新增内容，迅速了解Web应用程序安全领域近年来的发展变化情况。

第2版的一个显著特点是，在整本书中提供了所介绍的几乎所有漏洞的真实示例。读者可以使用“尝试访问”链接以交互方式在线运行书中讨论的示例，以确认可以发现并利用其中包含的漏洞。书中提供了几百个“示例实验室”，读者可以根据自己阅读本书的进度逐个访问这些“实验室”。访问这些在线“实验室”需要支付一定的订阅费用，这些费用主要用于管理和维护相关基础设施。

如果读者希望集中精力学习第2版中的新增内容，以下是对新增或改写内容的汇总。

第1章仅部分内容有所改动，将介绍Web应用程序的新应用、技术领域的一些显著趋势，以及组织的典型安全边界将如何继续发展变化。

第2章仅有小幅改动，新增内容将介绍几个用于避开输入确认防御的常规技巧示例。

第3章增加了几节新内容，主要介绍各种新技术及已在第1版中简要介绍的技术。新增的主题包括REST、Ruby on Rails、SQL、XML、Web服务、CSS、VBScript、文档对象模型、Ajax、JSON、同源策略和HTML5。

第4章仅有少量更新，以反映用于解析内容和功能的技术的发展趋势。

第5章进行了大幅改动。具体来说，基本上重新编写了有关浏览器扩展技术的几节内容，详细介绍了反编译和调试字节码的常规方法、如何处理常规格式的序列化数据，以及如何处理渗透测试过程中遇到的常见问题，包括不支持代理的客户端和SSL问题。本章还将介绍Silverlight技术。

第6章内容与现今情况保持一致，仅有小幅改动。

第7章新增内容主要介绍自动测试令牌随机性的新工具。本章还包含有关攻击加密令牌的新内容，包括如何在不了解所使用的加密算法或加密密钥的情况下篡改令牌的实用技巧。

第8章将介绍一些访问控制漏洞，包括由直接访问服务器端方法以及平台配置不当（将基于

HTTP的方法用于执行访问控制）导致的漏洞。本章还将介绍一些新工具和技巧，可在一定程度上自动完成测试访问控制的繁琐任务。

第9章和第10章的内容经过重组，因而变得更易于管理，其章节安排也更符合逻辑。第9章主要介绍针对其他数据存储技术的SQL注入和其他类似攻击。由于SQL注入漏洞已广为人知，并且在很大程度上得到了解决，因此，本章将着重介绍现在仍然可以发现SQL注入漏洞的实际情形。本章的其他内容也有小幅改动，将介绍当前的技术和攻击方法。同时，本章还新增了一节内容，用于说明如何使用自动化工具来利用SQL注入漏洞。有关LDAP注入的内容经过大幅改动，以更详细地介绍特定技术（Microsoft Active Directory和OpenLDAP），以及利用常见漏洞的新技巧。此外，本章还将介绍针对NoSQL的攻击。

第10章讨论以前在第1版第9章中介绍的其他类型的服务器端注入漏洞。新增内容主要介绍XML外部实体注入和注入后端HTTP请求，包括HTTP参数注入/污染和注入URL改写方案。

第11章将提供更多常见输入确认功能逻辑缺陷的示例。由于越来越多的应用程序采用加密来保护静态数据，本章还将介绍如何确定并利用加密提示来解密加密数据的示例。

第1版的第12章主要介绍针对其他应用程序用户的攻击。第2版将这一章内容放到了两章中，因为这些内容过于繁杂，不易管理。第12章主要讨论XSS，相关内容经过大幅改动。有关如何避开防御过滤以插入脚本代码的内容已完全重写，主要介绍一些新技术和新技巧，包括在当前浏览器中执行脚本代码的各种鲜为人知的方法。同时，本章还将更详细地介绍如何对脚本代码进行模糊处理，以避开常用的输入过滤的方法。本章还将介绍一些现实中新出现的XSS攻击示例。新增一节内容介绍了如何在充满挑战的情况下实施有效的XSS攻击，涵盖如何将攻击扩散到所有应用程序页面、如何通过cookie和`Referer`消息头利用XSS，以及如何在XML等非标准请求和响应内容中利用XSS。此外，本章还将分析浏览器的内置XSS过滤器，以及如何避开这些过滤器来实施攻击。新增几节还将讨论在Web邮件应用程序和上传文件中利用XSS的特定技巧。本章最后介绍可用于阻止XSS攻击的各种新的防御措施。

第13章为新增的一章，介绍“攻击用户”这一涉及广泛的主题的其他内容。有关跨站点请求伪造的主题经过更新，将介绍针对登录功能的攻击、反CSRF防御中的常见缺陷、UI伪装攻击，以及破坏框架防御中的常见缺陷。跨域捕获数据一节（13.2节）将介绍如何通过注入包含非脚本HTML和CSS的文本来窃取数据的技巧，以及各种使用JavaScript和E4X跨域捕获数据的技巧。新增一节更详细地介绍同源策略，包括其在不同浏览器扩展技术中的实施情况、HTML5带来的改变，以及通过代理服务应用程序跨域操作的方法。另设新增节介绍客户端cookie注入、SQL注入和HTTP请求污染。有关客户端隐私攻击的内容经过扩充，将介绍浏览器扩展技术和HTML5提供的存储机制。最后，另一个新增节将集中介绍不依赖任何特殊应用程序中的漏洞、针对Web用户的攻击。这些攻击可以由任何恶意或已被攻破的Web站点，或位于网络中的适当位置的攻击者实施。

第14章新增部分内容介绍自动化攻击过程中遇到的常见障碍，以及如何克服这些障碍。许多应用程序采用防御性的会话处理机制来终止会话，使用临时的反CSRF令牌，或使用多阶段过程来更新应用程序状态。本章将介绍一些处理这类机制的新工具，以便于继续应用自动化测试技巧。新增节将介绍CAPTCHA控件，以及一些通常能够加以利用来破解这些控件的常见漏洞。

第15章包含有关错误消息中的XSS及利用解密提示的新章节。

第16章未进行任何更新。

第17章中的新增节主要介绍基于云的体系架构中的漏洞，并更新了有关如何利用体系架构弱点的示例。

第18章包含在应用程序服务器和平台中发现的一些有趣的新漏洞示例。这些服务器和平台包括Jetty、JMX管理控制台、ASP.NET、Apple iDisk服务器、Ruby WEBrick Web服务器和Java Web服务器。另一个新增节介绍突破Web应用程序防火墙的实用方法。

第19章未进行任何更新。

第20章的更新内容将详细介绍基于代理的工具套件的最新功能。新增节将介绍如何传送不支持代理的客户端的流量，以及如何减少因使用拦截代理服务器而在浏览器和其他客户端中出现的SSL错误。本章还将详细介绍使用基于代理的工具套件进行测试时通常采用的工作流程。此外，本章还将讨论各种最新Web漏洞扫描器及在各种情况下使用这些扫描器的最佳方法。

第21章的更新内容将介绍在整本书中描述的新的方法论步骤。

需要的工具

本书着重讨论渗透测试员在攻击Web应用程序时所采用的实用技巧。阅读本书后，你将了解每项攻击任务的细节、它们涉及的技术以及它们为什么有助于探查和利用各种漏洞。下载某个工具，使用它攻击一个目标应用程序，并根据它的输出结果了解应用程序的安全状况，这些内容并不是本书讨论的重点。

也就是说，当实施我们描述的步骤与技巧时，你会发现一些有用、有时甚至是必不可少的工具。所有这些工具都可以在因特网上找到，建议你下载并试用本书介绍的每一个工具。

同步网站内容

本书的同步网站为http://mdsec.net/wahh，你还可以从www.wiley.com/go/webhackerze链接到本书的同步网站，其上提供一些掌握各种攻击技巧所需要的有用资源，你也可以利用这些资源攻击真实的应用程序。该网站主要包括以下内容：

- 本书列出的一些脚本的源代码；
- 本书讨论的所有工具和其他资源的链接；
- 攻击一个常见应用程序的步骤列表；
- 每章结束部分提出的问题的答案；
- 本书示例中使用的几百个互动式漏洞“实验室”，支付一定费用即可访问，可帮助你提升和改善攻击技巧。

其他说明

Web应用程序安全是一个有趣而流行的主题。对我们而言，撰写本书是一种享受，正如每天对应用程序进行渗透测试。我们希望，在学习本书描述的各种攻击技巧和了解如何防御这些攻击手段的过程中，你能够找到乐趣。

此外，我们在此提出严正警告。在许多国家，未经所有者许可而攻击他们的计算机系统的做法属非法行为。如果未经他人同意，执行我们描述的绝大多数技巧可能会触犯法律。

本书作者为专业的渗透测试员，他们代表客户端对Web应用程序实施攻击，以帮助强化应用程序的安全。近年来，许多安全专业人士与其他人由于未经许可而尝试或主动攻击计算机系统，从而犯罪，其职业生涯也因此结束。我们强烈要求你仅在法律许可的范围内使用本书提供的信息。

致谢名单

执行编辑
Carol Long

高级项目编辑
Adaobi Obi Tulton

技术编辑
Josh Pauli

制作编辑
Kathleen Wisor

文字编辑
Gayle Johnson

编辑经理
Mary Beth Wakefield

自由作家编辑经理
Rosemarie Graham

营销副总监
David Mayhew

营销经理
Ashley Zurcher

业务经理
Amy Knies

生产经理
Tim Tate

副总裁兼执行集团出版商
Richard Swadley

副总裁兼执行出版商
Neil Edde

合作出版商
Jim Minatel

项目协调员（封面）
Katie Crocker

校对
Sarah Kaikini, Word One
Sheilah Ledwidge, Word One

索引编写者
Robert Swanson

封面设计
Ryan Sneed

封面图像
Wiley InHouse Design

垂直网站项目经理
Laura Moss-Hollister

垂直网站项目经理助理
Jenny Swisher

垂直网站制作助理
Josh Frank
Shawn Patrick
Doug Kuhn
Marilyn Hummel

致　　谢

感谢Next Generation Security Software公司经理和其他同事，他们为我们提供了适当的环境，为撰写第1版提供了大力支持。除了他们，对于与我们共享观点和帮助我们了解当前面临的Web应用程序安全问题的更多研究员和专业人士，我们在此表示衷心感谢，是你们给了我们写作灵感。本书是一本实用手册，而非学术作品，因此我们尽量避免在书中过多引用讨论相关问题的重要论文、参考书和博客文章。一些作者在此并未提及，还望他们海涵。

感谢Wiley出版社的员工，特别感谢Carol Long在整个项目期间提供的热心支持；感谢Adaobi Obi Tulton帮助我们修订手稿和了解“美式英语”的怪癖；感谢Gayle Johnson所做的极其有益而细心的文字编辑工作；感谢Katie Wisor团队提供的一流制作。

尤其感谢我们的合作伙伴Becky和Amanda，感谢你们投入大量时间与精力帮助我们完成这本“大部头”作品。

对于引导我们从事这个行业的人们，我们在此表示感谢。

衷心感谢Martin Law，正是他首先教会我如何实施攻击，并鼓励我投入精力开发针对应用程序进行攻击测试的技巧与工具。

——Dafydd

衷心感谢我的父母，感谢他们为我付出的一切，也是他们让我对计算机产生兴趣，从此我就迷上了计算机。

——Marcus

目　录