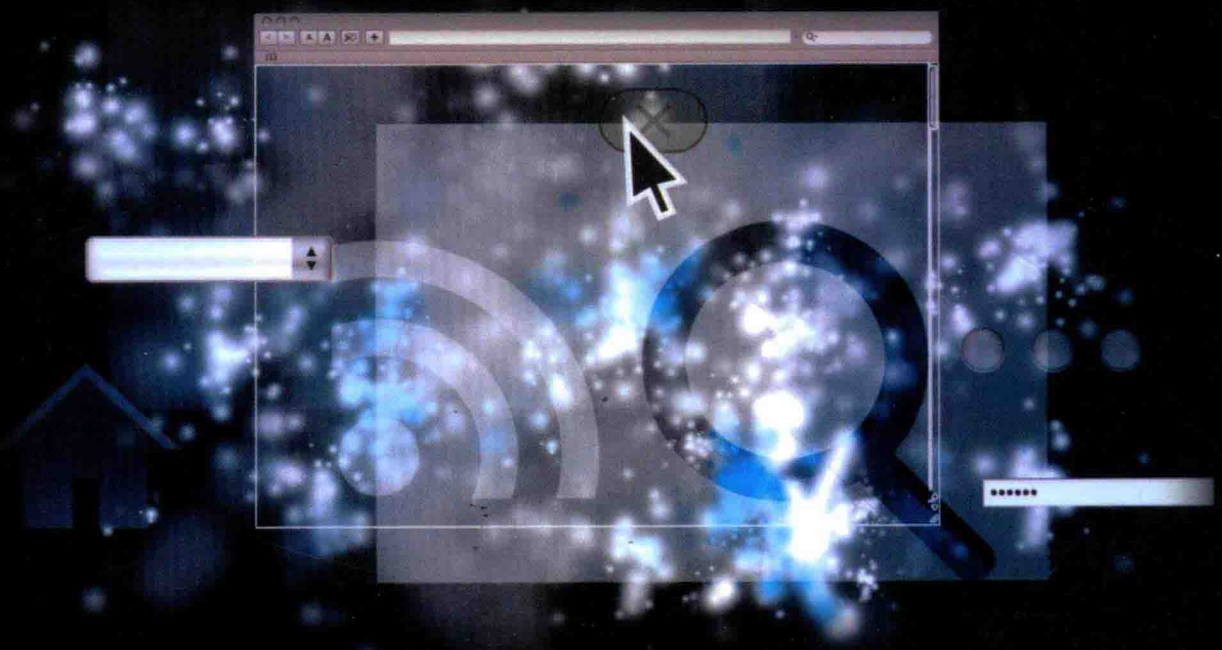
TURING 图灵程序设计丛书

The Browser Hacker's Handbook

黑客攻防技术宝典
浏览器实战篇

[澳] Wade Alcorn [美] Christian Frichot [意] Michele Orrù 著
奇舞团 译
0KEE TEAM 审校



中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

The Browser Hacker's Handbook

黑客攻防技术宝典
浏览器实战篇

[澳] Wade Alcorn [美] Christian Frichot [意] Michele Orrù 著
奇舞团 译
0KEE TEAM 审校

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. 浏览器实战篇 / （澳）瓦德·奥尔康（Wade Alcorn），（美）克里斯蒂安·弗里绍（Christian Frichot），（意）米凯莱·奥鲁著；奇舞团译. -- 北京：人民邮电出版社，2016.10
（图灵程序设计丛书）
ISBN 978-7-115-43394-7

Ⅰ. ①黑… Ⅱ. ①瓦… ②克… ③米… ④奇… 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(2016)第199197号

内 容 提 要

本书由世界顶尖级黑客打造，细致讲解了IE、Firefox、Chrome等主流浏览器及其扩展和应用上的安全问题和漏洞，介绍了大量的攻击和防御技术，具体内容主要包括：初始控制，持续控制，绕过同源策略，攻击用户、浏览器、扩展、插件、Web应用、网络，等等。这是你在实践中的必选参考指南，对实际开发具有重要指导作用，能够助你在浏览器安全领域有所作为。

本书适合计算机安全技术人员以及浏览器开发人员。

◆ 著　[澳] Wade Alcorn　[美] Christian Frichot
[意] Michele Orrù

译　奇舞团

审　校　0KEE TEAM

责任编辑　朱　巍

执行编辑　贺子娟　吴威娜

责任印制　彭志环

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路11号

邮编　100164　电子邮件　315@ptpress.com.cn

网址　http://www.ptpress.com.cn

三河市海波印务有限公司印刷

◆ 开本：800×1000　1/16

印张：31

字数：733千字　2016年10月第1版

印数：1－4 000册　2016年10月河北第1次印刷

著作权合同登记号　图字：01-2014-5455号

定价：109.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316

反盗版热线：(010)81055315

广告经营许可证：京东工商广字第8052号

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

站在巨人的肩上
Standing on Shoulders of Giants

iTuring.cn

版权声明

中文版推荐序

浏览器作为用户访问互联网的入口，其安全性至关重要。用户在浏览器中的任何一次不经意的点击，都可以成为噩梦的开始。攻击者利用浏览器的一些漏洞，仅需要用户点击一个链接：轻者可以窃取用户的cookie及身份信息，获得用户浏览记录等隐私；重者则导致用户电脑上的文件被窃取、篡改，甚至用户电脑会被安装后门，最终沦为攻击者的“囊中之物”。浏览器承载着万物互连和分享协作，因而保障浏览器的安全越来越重要。

今天，各家浏览器的发展如火如荼，特别是新的安全特性也层出不穷。比如，数据执行保护（DEP）、内存地址随机化（ASLR）、沙箱、隔离堆、延时释放、控制流防护（CFG）等，诸多安全特性的出现与应用折射出浏览器已然成为攻击者的目标。“道高一尺，魔高一丈”，新的安全特性必然会导致新的攻击方法的出现，只是攻击的难度和成本会越来越大，对攻击者技术的要求也越来越高。

未知攻，焉知防？本书是业界公认的最流行的浏览器利用工具BeEF的作者Wade等人结合自己亲身实践经验鼎力创作的，系统地介绍了浏览器的攻防技术。全书以BeFF工具为基础，将浏览器攻防分为初始化、持久化和攻击三大阶段，并在攻击阶段中从用户、浏览器核心、扩展、插件、Web应用和网络等多个方面去细化。全书一共分七个大类讲浏览器攻击方法：初始化、持久化、攻击用户和攻击浏览器、攻击扩展、攻击插件、攻击Web应用和攻击网络。每一章基本按攻击方法划分，作者对安全攻防的归类组织结构做到了一页不差，相关的技术点叙述得很清晰、很全面，并有基于BeEF等工具的实际演示，读者能很快理解和上手。很多技术点能从原理上阐述清楚，这很难能可贵。同时，攻击手段上的很多“奇技淫巧”深受广大黑客的喜爱。对爱好浏览器安全并打算详细了解和学习相关专业知识的人来说，这本书是最好不过的选择。本书是迄今为止介绍浏览器攻防实战的最详细之作。

最后特别感谢团队leader张鲁和团队成员为本书审校付出的心血！

奇虎360信息安全部 0KEE TEAM
李响
2016年8月

致　谢

如果没有两位重要人物，我这一生不会做出什么有价值的事情。非常感谢我美丽的妻子Carla，感谢她矢志不移的支持和不计其数的提醒。虽然在本书封面上看不到她的名字，但实际上本书中的每一个字都经过了她的润色。还要感谢我的英雄儿子Owen，如果不是他亲身实践在面对生活挑战时应该时刻面带笑容，我面对的每一个障碍都会更加难以逾越。

另外，能够与Rob Horton和Sherief Hammad共事将近十年对我而言也是一件幸事。正是他们源源不断的鼓励，造就了培养创造力和横向思维的支持性工作空间。当然，还要感谢Michele和Christian陪我一起进行这次写作之旅。

——Wade Alcorn

我在一家银行初次遇到她，当时恰逢系统崩溃。如果不是她无限耐心的支持，我想我是不可能参与写作这本书的。衷心地感谢我最心爱的妻子Tenille（还有在你肚子里成长的女儿），这本书就是为你而写（让你知道怎么对付小家伙）。我还要感谢我的其他家人。感谢老妈Julia和老爸Maurice，感谢你们给了我机会在信息安全领域发展。感谢我的妹妹Hélène、Justine和Amy，你们让我脑洞大开，你们的支持非常给力。感谢我的Asterisk Info Sec大家庭，感谢你们听我抱怨这事儿有多难，而且给我时间来做完它，非常感谢David Taylor、Steve Schupp、Cole Bergersen、Greg Roberts和Jarrod Burns。还得感谢澳大利亚和新西兰的黑客安全团队，感谢我在网上和会议上认识的所有朋友，非常高兴能够在这个社区里与你们为伍，共同进步。当然还有Wade和Michele，我必须感谢你们邀请我参与这个具有重大意义的任务，感谢你们的不厌其烦，感谢你们的毫无保留，感谢你们容忍我废话连篇！

——Christian Frichot

首先，我想感谢我心爱的Ewa，感谢她在我夜以继日地做研究和写作本书时给予我精神上的支持。向我的父母致敬，因为他们的支持，我才可能走上了研究和学习新事物的道路。非常感谢我的好朋友Wade Alcorn和Mario Heiderich，感谢他们对我研究的启发，以及跟我进行火花四射的讨论。如果没有他们，这本书就不会写得这么好。为所有相信Full Disclosure才是暴漏洞好方法的人喝彩。最后，感谢与我并肩战斗的好友及安全研究同事（你们知道我说的是谁），感谢你们与我分享漏洞利用技术以及会议后一起把酒言欢。

——Michele Orrù

本书是团队努力的结晶。首先，感谢两位特约作者Ryan Linn和Martin Murfitt。各大安全社区也让我们受益颇多，特别是这些年来为BeEF作出贡献的人们。正是他们多年的积累，最终汇聚成了这本书呈现在大家面前。

Wiley那些和蔼可亲的人以及本书的技术编辑也是我们必须重点感谢的。不能不提的是Mario Heiderich、Carol Long和Ed Connor，感谢他们的耐心、支持和专业技能。

感谢Krzysztof Kotowicz、Nick Freeman、Patroklos Argyroudis和Chariton Karamitas，感谢他们专家级的贡献。虽然我们不可能把每一位要感谢的人都一一列在这里，但还是要特别点出其中几位的姓名：Brendan Coles、Heather Pilkington、Giovanni Cattani、Tim Dillon、Bernardo Damele、Bart Leppens、George Nicolau、Eldar Marcussen、Oliver Reeves、Jean-Louis Huynen、Frederik Braun、David Taylor、Richard Brown、Roberto Suggi Liverani和Ty Miller。毫无疑问，还有其他重要的名字没有出现在这里。请相信我们，这绝非故意的。

——所有作者

前　言

内容介绍

看看你手中的这本书，它会让你了解我们每天都在用的Web浏览器可能遭受哪些攻击。当然，用这本书作为武器，也可以发起新的攻击。本书介绍的攻击技术围绕最主流的浏览器展开，偶尔也会提到几个非主流的。所谓主流浏览器，也就是Firefox、Chrome和Internet Explorer（以下简称“IE”）。必要的时候还会涉及现代移动浏览器，虽然移动浏览器不是我们的主要讨论对象，但书中涵盖的许多攻击技术有时候对它们同样适用。

攻击者和防御者都需要理解Web浏览器带给用户的危险。原因很简单：Web浏览器可能是21世纪迄今为止最重要的一种软件。它是人类访问网络空间最重要的门户。君不见，这个曾经笨拙的桌面软件，如今已经作为一个主要的应用程序进入了手机、游戏机，甚至不起眼的电视机里都有它的身影。Web浏览器堪称今日表现、检索和搜寻数据的“瑞士军刀”。自从Tim Berners-Lee爵士于1990年发明他的“可以做到的小Web浏览器”以来，这个软件的发展已经远远超过预期，成为当今世界最受世人关注的软件之一。

关于Web浏览器的全球用户数量，有各种各样的统计和说法。其实只要拿个烂笔头信手算算，就不难估计出这是一个多么庞大的数字。假如地球上有三分之一的人上网，那么浏览器用户基本就是23亿。再想一下，又会发现其中有一部分人还不止使用一个浏览器。他们在家里、单位和手机上都使用浏览器。就算没有史蒂芬·霍金的智商，也不难猜到这是多么惊人的数目。

既然Web浏览器的用户数量如此巨大，那么由此产生大量安全问题和漏洞利用机会也就不足为奇了。本书从黑客角度着眼，讲解如何攻击以及如何保护各种情形下的现代浏览器。

目标读者

如果你有技术背景，对浏览器面临的现实风险感兴趣，那你适合看这本书。可能你想保护你们的基础设施，也可能是想破坏客户的资产。或许你是一个系统管理员、开发者，甚至是一位信息安全专家。大概你跟我们很多人一样，对安全有着难以遏制的激情，正饥渴地寻找这方面的知识。

本书假设你每天都会用浏览器，出于某种原因想一探其背后的究竟。要看懂这本书，最好掌

握了基本的安全概念，或者额外花点时间补一补基础知识。比如客户端–服务器模型、HTTP协议和一些基本的安全概念，这些你都不应该陌生。

虽然编程经验不是必需的，但懂一点基本原理才能看懂书中的代码。书中大量的例子和演示全都源自一线实战，使用了多种语言，主要是JavaScript——毕竟浏览器里它是主宰。虽然听起来似乎不大可能，但即使你以前没有使用过JavaScript，其实关系也不大。每一段代码都有详细的解说。

本书内容

本书主要有10章，基本按攻击方法划分。必要时，每一章会按攻击点归类，但也不强求统一。作者本着有助于读者开展专业安全攻防的目的，组织了本书结构。

在任何安全攻防中，你都不大可能从头到尾一页不差地翻阅这本书，而是会跳着阅读，先看完前面的介绍性章节，然后再视情况跳到最相关的章节。另外，为了马上弄明白某个概念，你也可能会临时翻到某一节。为了让本书适应更多不同的使用情形，有的概念会在书中反复提及，但每次都会有不同的上下文，同时也贴近相应的主题。

每一章后面还设置了思考题。这些题目可以帮读者更加扎实地理解相应章节中介绍的核心概念。

第1章 浏览器安全概述

这一章是浏览器攻防之旅的首站。这里会让大家明确重要的浏览器概念，以及浏览器安全的一些核心问题。特别地，我们要探讨对今天的组织防御至关重要的“微防线”（micro perimeter）理念，同时反思一些广为流传却不安全的错误做法。

这一章还讨论发动浏览器攻击的方法、浏览器的攻击面，以及如何使其暴露以前隐蔽的资产。

第2章 初始控制

浏览器每一次连接到Web，都会请求要执行的指令。然后，浏览器会忠实地执行服务器发送给它的命令。不用说，限制总是有的，但浏览器仍然给攻击者留下了很大的攻击空间。

这一章带领读者领略浏览器攻防的第一阶段，告诉你如何在目标浏览器中执行自己的代码。你会看到XSS攻击、中间人攻击、社会工程，等等。

第3章 持续控制

此前介绍的初始控制技术只能让你执行一次指令。这一章介绍如何维持通信，持续控制目标，从而能够执行多轮命令。

在典型的攻击实战中，应该尽可能长时间地维持与浏览器的通信，而且可能的话，即使浏览器重新启动还要继续保持对它的控制。做不到这一点，那就只能停留在反复诱使目标进行连接的阶段。

这一章将介绍如何使用payload维持与浏览器的通信，从而达到发送多次命令的目的。这样就可以在至关重要的初始连接后，不浪费任何机会。掌握了这一章的知识，就为后面采取各种攻击

方法打下了基础。

第4章　绕过同源策略

本质上来说，同源策略（SOP）就是限制一个网站与另一个网站之间建立通信。因为SOP可以说是浏览器安全的一个最基本的概念，所以你可能会认为各种浏览器组件中的SOP都一样，而且预测常规操作的后果也不难。这一章会告诉你根本不是这么回事。

Web开发者常常被SOP所困扰。对浏览器、扩展和插件应用SOP的方法各不相同。而正是由于缺乏一致性造成的理解出入，给攻击者在边界条件下侵入系统提供了机会。

这一章讲解如何绕过浏览器中不同的SOP措施，甚至还会讨论拖放、界面伪装和时序攻击等问题。还会阐释一个足以令人惊讶的事实，就是在绕过SOP后，你可以把浏览器作为一个HTTP代理来使用。

第5章　攻击用户

人通常被认为是安全保障链条中最薄弱的一环。这一章主要讨论如何攻击毫无戒备心理的用户的湿件。有的攻击手段会利用第2章介绍的社会工程策略，另一些攻击手段会利用浏览器的功能，以及浏览器对接收的代码的信任。

这一章会涉及反匿名（de-anonymization）和隐蔽地启动Web摄像头，以及运行恶意可执行文件，这一切都不必通过用户。

第6章　攻击浏览器

虽然这一本书都在讲如何攻击浏览器，如何绕过它的安全部署，但这一章只关注所谓的核心浏览器，换句话说，就是没有任何扩展和插件的浏览器。

在这一章，我们会讨论直接攻击浏览器的过程。我们会探讨通过指纹识别区分厂商和版本，以及如何对运行浏览器的机器发动攻击。

第7章　攻击扩展

这一章探讨如何利用浏览器扩展的隐患。扩展就是给浏览器添加（或删除）功能的软件。扩展与插件不同，它不是独立的程序。LastPass、Firebug、AdBlock和NoScript都是常见的扩展。

扩展会在受信任区域以较高权限执行代码，但接收的输入则来自不那么受信任的区域，比如互联网。对于经验丰富的安全专家来说，这一点就足够引起重视的了。在实践当中，确实存在注入攻击的风险，而某些攻击则会导致远程代码执行。

这一章会剖析扩展攻击的方方面面，特别是会探讨提升权限以访问浏览器特权区域（chrome://），从而执行命令。

第8章　攻击插件

这一章关注攻击浏览器插件。插件是为浏览器增加特殊功能的软件。多数情况下，插件可以独立于浏览器运行。

流行的插件包括Acrobat Reader、Flash Player、Java、QuickTime、RealPlayer、Shockwave和Windows Media Player。其中一些插件是上网必需的，而另外一些则是为了实现公司的需求。比如，像YouTube这样的网站需要Flash播放视频（但会向HTML5迁移），而Java是WebEx实现功能所必需的插件。

插件一直是隐患的来源，也是攻击利用的主要突破口。稍后你会看到，插件是控制浏览器的最可靠的途径之一。

在这一章里，我们会探索使用流行、免费的工具分析和利用浏览器插件。我们会学习如何绕过“点击播放”之类的保护机制，利用插件中的漏洞取得浏览器的控制权。

第9章 攻击Web应用

浏览器虽然可以应对基于Web的强力攻击，但仍然要承担安全控件不利的风险。浏览器天生要通过HTTP与服务器通信。而这些HTTP机制很可能成为被利用的对象，甚至可以通过它们控制其他来源的目标。

这一章主要介绍在不违反SOP的前提下从浏览器发起攻击的方法，包括跨来源的资源指纹，甚至跨来源的常见Web应用隐患的识别技术。你会发现，在使用浏览器的时候，居然还能够利用跨来源的XSS和SQL注入。

在这一章最后，你会理解如何实现跨来源的远程代码执行，以及跨站点请求伪造攻击、基于时间的延迟枚举、攻击认证和拒绝服务攻击。

第10章 攻击网络

关于攻击的最后一章，将介绍如何通过端口扫描发现之前未知的主机，在内网中识别攻击面。接下来还会展示如NAT定位（NAT Pinning）这样的技术。

这一章还会介绍使用浏览器直接与非Web服务通信的攻击方式，以及如何使用内网协议利用技术在浏览器内网中俘获目标。

第11章 结语：最后的思考

本书到这里，已经向大家介绍了大量的攻击和防御技术，而前面所有章节现在都可以作为你将来实践的参考。希望你能够结合实际多加思考，在未来的浏览器安全领域有所作为。

在线资源

本书网站为https://browserhacker.com。Wiley上的本书主页为http://www.wiley.com/go/browserhackershandbook。在这两个网站上，读者可以找到本书的附加内容。尽管不能替代本书，但这些附加资源是本书中内容的有益补充。

网站上还包含可以复制粘贴的代码。这样可以你节省手工输入的时间，也希望能帮你避免攻击中的麻烦。此外，还有演示视频和每章后面问题的答案。

本书不可避免地会有这样或那样的错误，这一点我们都知道。很不幸，本书三位作者中有两位不靠谱（至于靠谱的是哪一位，至今我们三个还在激烈地争论）。如果你想知道现在我们是否有了结论，可以访问网站https://browserhacker.com，当然更重要的是，你也可以找到对其他读者发现的错误的修正。如果你也发现了错误，而且网站中还没有列出，请告诉我们。

备足弹药

本书会介绍可以用于攻击浏览器的各种工具，把这么多种工具收入工具箱，将来必有用武之地。

需要注意的是，本书旨在介绍如何在较低的级别上使用这些工具。随着你的技能越来越丰富，就会发现了解这些用法非常重要。我们的目标就是不仅让你知道怎么使用工具，还要理解它们，从而避免误用。

我们还希望你知道，所有工具都有自己的短处，你应该根据自己的知识选择它们。你的工具箱中最重要的工具，就是你的知识。本书作者的主要目标就是增长你的知识，而不是单纯地扩充你的软件库。

本书中有两个最常用的工具，一个是BeEF（Browser Exploitation Framework），另一个是Metasploit。当然，我们要介绍的工具不限于此，而且你还会了解所有工具的长处和短处。

本书作者就是BeEF项目的核心开发者，致力于让这个社区工具与本书描述的方法相契合。本书中的很多示例都选自BeEF的代码，而在这个工具中，大多数过程都已经实现了自动化。

免责声明

有必要在这里声明一下，作为安全专业人士，应该注意自我约束。本书所教授的任何方法，都不是为了鼓励读者去做违反法律的事情。

在实施黑客攻击行动之前，请确保得到了充分授权。这不仅适用于安全纪律，同样也适用于本书讨论的所有技术。

祝你好运

浏览器安全是互联网上升级最快的军备竞赛之一。对所有关注安全的人来说，它都是一个迷人而又有趣的领域。这个军备竞赛升级的步伐之所以慢不下来，主要是因为各种公司日益依赖浏览器去做越来越多的事。

我们注意到，大大小小的公司越来越认为不应该在桌面计算机中运行一个独立的软件。而任何预测浏览器将逐渐没落的人，都应该好好地清醒清醒，因为他们可能还在使用着隐患多多的Java插件呢！

浏览器军备竞赛和商业公司对它的广泛应用，使得浏览器的攻击面不断变化，而来自安全的挑战从未绝迹。现在，我们就准备大干一场，看看黑客如何攻击浏览器，而我们又应该如何加强防御！

目　录