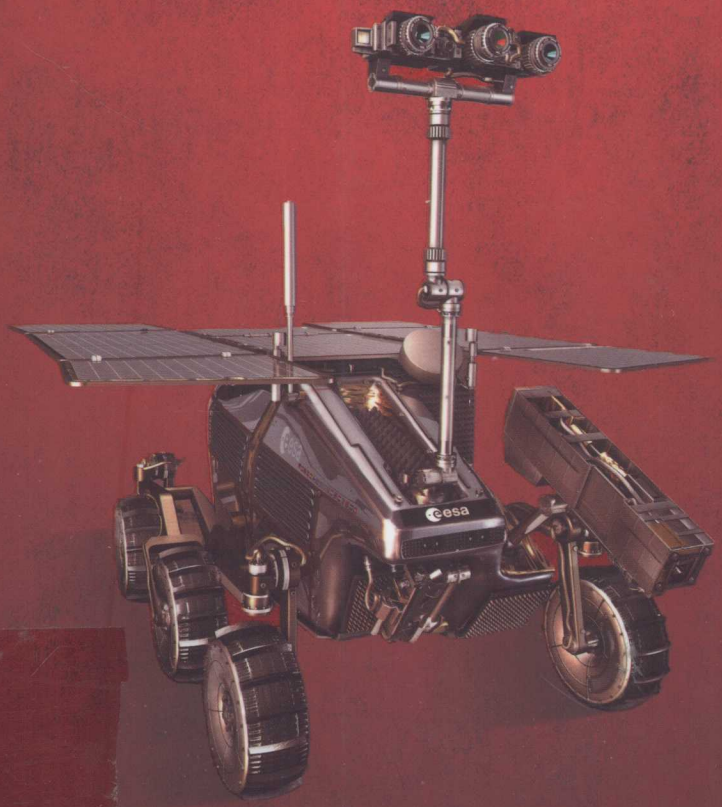
Broadview
www.broadview.com.cn

白帽子讲浏览器安全

钱文祥 著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

白帽子讲浏览器安全

钱文祥 著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

浏览器是重要的互联网入口，一旦受到漏洞攻击，将直接影响到用户的信息安全。作为攻击者有哪些攻击思路，作为用户有哪些应对手段？在本书中我们将给出解答，带你了解浏览器安全的方方面面。本书兼顾攻击者、研究者和使用者三个场景，对大部分攻击都提供了分析思路和防御方案。本书从攻击者常用技巧的“表象”深入介绍浏览器的具体实现方式，让你在知其然的情况下也知其所以然。

本书根据作者若干年实战与工作积累的丰富经验编写而成，深入地分析了浏览器从导航到页面展示的整个过程中可能会出现的安全问题，也对浏览器的部分实现细节有着详细和深入的介绍，对安全工作者有一定的参考意义。

图书在版编目（CIP）数据

白帽子讲浏览器安全/钱文祥著. 北京：电子工业出版社，2016.3
ISBN 978-7-121-28154-9

Ⅰ.①白… Ⅱ.①钱… Ⅲ.①浏览器－安全技术 Ⅳ.①TP393.092

中国版本图书馆 CIP 数据核字(2016)第 027318 号

策划编辑：张春雨
责任编辑：付　睿
印　　刷：北京京科印刷有限公司
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　印张：20.75　　字数：464.8 千字
版　　次：2016 年 3 月第 1 版
印　　次：2016 年 3 月第 1 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

序

人类第一次大规模的接触互联网，就是从 PC 上的浏览器开始的。从它的诞生开始，浏览器安全就成为一个极其重要的安全领域。浏览器内核、网页、钓鱼、XSS，包括让人又爱又恨的网银插件，这些都和浏览器安全息息相关。随着移动互联网和互联网＋时代的到来，浏览器已经变成了桌面端的互联网第一入口，而在移动端，虽然浏览器的入口地位受到了手机 APP 的分流，但依然是最重要的入口之一。浏览器安全问题，变得更加错综复杂。比如 iOS 越狱，用户只需要简单地访问一个特殊网页就能自动完成，也是利用了 iOS Safari 的安全漏洞。随着 HTML5 和 HTTP 2 标准的先后定稿，以微信、手机 QQ 为代表的开放平台迅猛发展，使得越来越多的 HTML5 内容在 APP 中的 WebView 里呈现。这些 APP 同样面临着广义的浏览器安全威胁。

无巧不成书，认识钱文祥也是缘于浏览器。2013 年，在乌云上偶然看到几个关于浏览器漏洞的报告后，我在 QQ 上联系了他。通过几次交谈，发现他是一个对安全技术尤其是浏览器安全技术非常痴迷并且有想法的人。所以，我邀请他来腾讯浏览器产品部工作，负责 PC 浏览器的安全工作。他在浏览器安全方面的经验，很好地保证了 QQ 浏览器的安全性，得到了团队的一致认可。此外，他还发现了 Microsoft IE 的和 Google Chrome 浏览器的一些漏洞，并得到了这两家公司认可。

当拿到书稿后，我不由地一震。他在工作之余，系统地总结和归纳了自己这些年在浏览器安全方面的一些知识，并深入浅出地呈现出来。这些知识可以给希望了解和学习浏览器安全的人提供一份有益的营养套餐。

浏览器安全，其实涵盖了客户端、web、server 等，给初学者一种雾蒙蒙的感觉，同时也给互联网罩上一层迷雾，就好似北京那令人百感交集的雾霾。希望《白帽子讲浏览器安全》一书，能像前几天的一场北风，吹走那迷雾，给读者带来一片清澈的蓝天。

边超，腾讯 T4 专家，PC 浏览器技术负责人

2015/12/8

前言

2015 年 3 月，我在乌云知识库中开始连载 IE 安全系列的文章（ID：blast）。博文视点的张春雨先生找到我，希望我写一本浏览器安全的书。

此时的浏览器市场已是一片红海——作为用户访问互联网的入口，无论是桌面还是移动端，各厂商争夺浏览器份额的形势，犹如多年前微软和网景的份额大战。这个过程中，他们留给互联网许多实用功能，制订了许多规范。

这些功能中，有一些也留下了不少安全隐患。我正好在从事浏览器安全工作，在日常问题处理中深知浏览器安全现有的资料非常分散，最大的问题便是不少人虽然兴趣浓厚，但是却不知道从哪里开始研究浏览器安全。

我的浏览器安全历程

1999 年接触计算机开始，我就对这个庞然大物产生了浓厚的兴趣。2001 年家中购买了电脑之后，由于最初的两年电脑没有联网，于是编程便成了我的另一个兴趣爱好。自学了几年编程之后，一直想做出一个有用的工具。

2007 年加入卡饭论坛开始的那段时间，应当是我和浏览器安全最长时期的接触，我一直活跃在病毒分析板块。由于当时网马猖獗，对病毒分析爱好的我编写了一个自动化网马解码分析工具 Redoce 并坚持更新了 6 年，这段经历让我认识了许多志同道合的朋友，也让我掌握了许多病毒以及漏洞的分析技能。

2010 年，我就读安徽理工大学信息安全专业，其间参阅了许多前辈的资料。2013 年是我第一次尝试由分析转为漏洞挖掘，之后我便沉浸于此，并最终以一个契机加入腾讯 QQ 浏览器部门。在腾讯，我依然从事浏览器安全研究工作。

浏览器的用户量数以百万、千万甚至于亿计，这样一款处处都会接受用户输入的软件，一旦出现漏洞，产品口碑和用户的信息安全都会深受其害，这是所有产品相关人员和安全研究人员都不想看到的。在对浏览器代码和应用的安全审查和测试过程中，我也总结了许多浏览器安全的“坑”和补救措施，这些内容将在本书内详细叙述。

本书结构

对有兴趣致力于浏览器安全的研究者来说，不知从哪里入手是研究热情的一个拦路虎。我将日常的经验和历史上的浏览器安全事件结合，编写了本书的 3 篇共 12 章的内容。希望能够为浏览器安全研究爱好者提供一些参考。

第 1 篇 探索浏览器安全介绍了从浏览器的用户界面以及浏览器展示网页的整个过程，针对过程中可能出现的问题进行了探讨，详细地介绍了浏览器的特性以及基础安全概念。浏览器的漏洞挖掘和 Fuzz 工具密不可分，本篇中我们也将介绍 Fuzzer 的基本理念并制作出一个可用的 Fuzzer。

本篇结合了 Web 安全与浏览器自身特性，就浏览器处理网页内容的原理及引发的安全问题展开讨论，希望能让读者对浏览器安全产生初步的印象，也打消从未涉及浏览器安全的读者的疑虑。

插件和扩展延伸了浏览器的功能，但是也带来了许多安全风险。

第 2 篇 实战网马与代码调试是过渡性的篇章，我们从插件和扩展安全说起，再通过几个网马的例子，将重点逐渐从 Web 向二进制调试转移。

插件部分将介绍逻辑漏洞的挖掘，以及在软件制作中规避风险的方法。网马部分则介绍恶意代码的混淆与加密方式，为恶意代码分析打好基础。代码调试部分则从二进制调试工具的用法开始，最后介绍 Shellcode 的调试。本章难度适中，希望能够带领读者探索浏览器中的二进制代码。

第 3 篇 深度探索浏览器漏洞对浏览器漏洞知识进行了更深入的挖掘和探讨。我们将从浏览器对网页元素的处理入手，分析网页元素在浏览器内存中创建时的过程并使用调试工具加以分析。我们还将从常见的漏洞入手，分析漏洞的成因并编写一个完整的浏览器漏洞利用程序。至此完成浏览器漏洞研究的最后一步。

编写历程

编写全书时工作繁忙，我每天只能够在业余时间抽出一至两个小时编写文章和调试代码。经历过后深知编写一本书的不易。在编写本书的过程中，我参考了大量资料。编写一本经验总结性质的书籍不仅仅是对自己过往的一个交待，更是为了促进对自己对浏览器认识的提高。如边超先生所言，通过将知识沉淀为文字，博文也好，书籍也好，都是一种重认识和再发现的过程。

在写一本介绍如此宽泛概念的书籍时，能够系统性地布局则是一大要事。在和乌云社区多个有兴趣研究浏览器安全的白帽子交流之后，最终我选择了本书这样一种先 Web 后底层深入的布局。但是，列大纲的时候我就发现，浏览器安全中每一部分都可以成为深入挖掘的方向，想在这一本薄薄的书中全部展现也是不切实际的。为了完整地涵盖安全的基础部分，本书挑选的更多是一些典型的例子，我希望通过这些典型例子起到抛砖引玉的作用——因为浏览器安全问题并不是单一因素引起的，更多的很可能是许多异常行为（也就是我们俗称的“BUG”）的组合。

相比于其他计算机科学相关的内容，浏览器安全研究的书籍资料并不多。但是互联网上仍然有许多专业研究人员提供了宝贵的数字资料，在遇到浏览器安全问题时，善用、勤用搜索引擎，是解决问题的一条捷径。

浏览器和浏览器标准的更新换代速度极快，在本书编写的过程中，就有许多新的浏览器标准和新的浏览器防御手段诞生。且本书编写时间仓促，又限于作者自身能力和水平的不足，书中不免会出现疏漏，烦请批评指正或留言宝贵意见。我提供了一个勘误表以及事件提单平台，本书的修订内容将在该平台上发布。平台的地址请见前言结尾的“联系方式”。

致谢

感谢我的公司腾讯科技有限公司和我的同事们，他们都愿意投入到浏览器中，以乐趣为出发点，在团队内部形成积极、友好讨论的氛围。

感谢边超先生为本书作序，边超先生在我开发和研究过程中细致耐心地提供了许多指导和帮助。

同时，也感谢边超、李普君、徐少培、张春雨等先生（排名不分先后）对本书章节布局的非常有建设性的建议。

协助本书内容审核的人员有：毛睿、关乃夫、丁川达、王连赢、李普君、周雨阳、梧桐雨（排名不分先后）等。毛睿先生是我在腾讯工作时的导师，感谢他为我提出了许多宝贵意见。

感谢我的家人，尤其是我的父母在编写本书的时候给予我的无尽的鼓励。

在编写本书时，同样受到了来自许多专家和前辈的指导和鼓励，无论列出与否，都由衷地感谢你们。

联系方式

邮箱：blastxiang@gmail.com

博客：http://nul.pw/

勘误表：http://nul.pw/issues.html

目录

第1篇

初探浏览器安全

- 漏洞与浏览器安全
- 浏览器中常见的安全概念
- 探索浏览器的导航过程
- 页面显示时的安全问题
- 浏览器扩展与插件的安全问题
- 移动端的浏览器安全