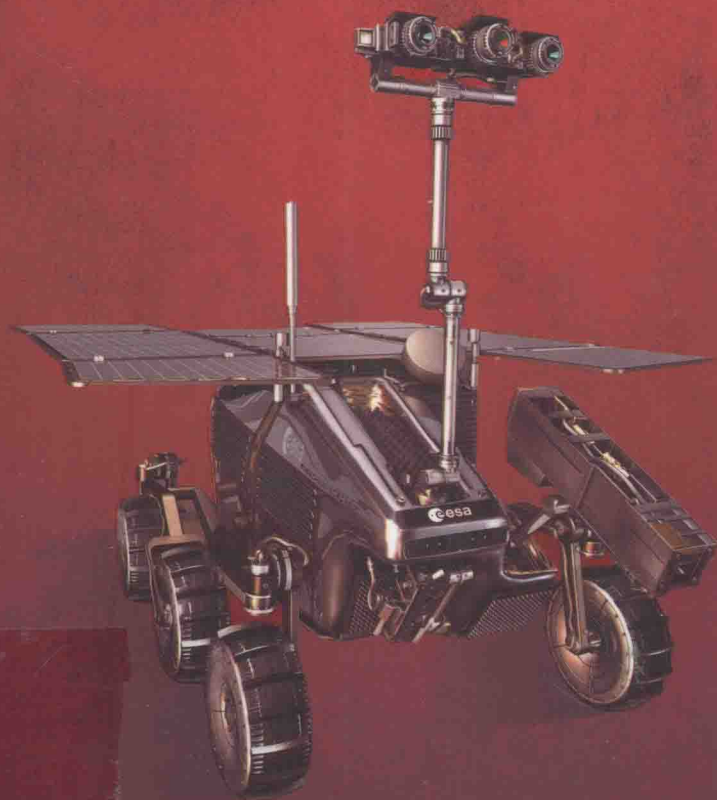


需要整本电子书，联系我QQ: [2667271557](#);
此处是样章，取的完整版的前面几页，和最后
面几页；完整版是带书签的，样章没带书签；
另外需要其他书，也可以找我。

白帽子讲 浏览器安全

钱文祥 著 | 🔍



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>



白帽子讲 浏览器安全

钱文祥 著 | 🔍

电子工业出版社

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。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

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 zltz@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 and 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	1
1 漏洞与浏览器安全	3
1.1 漏洞的三要素	3
1.2 漏洞的生命周期	4
1.3 浏览器安全概述	5
1.4 浏览器安全的现状	7
1.5 浏览器的应对策略	9
1.6 “白帽子”与浏览器厂商的联手协作	9
1.7 全书概览	10
1.8 本章小结	12
2 浏览器中常见的安全概念	13
2.1 URL	13
2.1.1 URL 的标准形式	15
2.1.2 IRI	16
2.1.3 URL 的“可视化”问题——字形欺骗钓鱼攻击	18
2.1.4 国际化域名字形欺骗攻击	19
2.1.5 自纠错与 Unicode 字符分解映射	20
2.1.6 登录信息钓鱼攻击	23
2.2 HTTP 协议	24
2.2.1 HTTP HEADER	25
2.2.2 发起 HTTP 请求	26
2.2.3 Cookie	28
2.2.4 收到响应	29

2.2.5	HTTP 协议自身的安全问题	31
2.2.6	注入响应头: CRLF 攻击	31
2.2.7	攻击响应: HTTP 401 钓鱼	32
2.3	浏览器信息安全的保障	33
2.3.1	源	33
2.3.2	同源准则	34
2.3.3	源的特殊处理	34
2.3.4	攻击同源准则: IE11 跨任意域脚本注入一例	35
2.4	特殊区域的安全限制	37
2.4.1	安全域	37
2.4.2	本地域	37
2.5	伪协议	38
2.5.1	data 伪协议	38
2.5.2	about 伪协议	40
2.5.3	javascript/vbscript 伪协议	41
2.5.4	伪协议逻辑出错: 某浏览器跨任意域脚本注入一例	42
2.6	本章小结	43
3	探索浏览器的导航过程	45
3.1	导航开始	45
3.1.1	浏览器的导航过程	46
3.1.2	DNS 请求	46
3.1.3	DNS 劫持和 DNS 污染	47
3.1.4	导航尚未开始时的状态同步问题	48
3.1.5	实例: 针对导航过程发起攻击	49
3.2	建立安全连接	50
3.2.1	HTTPS	50
3.2.2	HTTPS 请求中的 Cookie	51
3.3	响应数据的安全检查——XSS 过滤器	52
3.3.1	IE XSS Filter 的实现原理	53

3.3.2	Chrome XSSAuditor 的工作原理	55
3.4	文档的预处理	56
3.4.1	浏览器对 HTML 文档的标准化	56
3.4.2	设置兼容模式	57
3.5	处理脚本	59
3.5.1	脚本的编码	60
3.5.2	IE 的 CSS expression 的各种编码模式	62
3.5.3	浏览器的应对策略: CSP	63
3.5.4	“绕过”CSP: MIME Sniff	65
3.5.5	简单的 Fuzz: 混淆 CSS expression 表达式	68
3.6	攻击 HTML 标准化过程绕过 IE/Chrome 的 XSS Filter	71
3.7	本章小结	73
4	页面显示时的安全问题	75
4.1	点击劫持	76
4.1.1	点击劫持页面的构造	76
4.1.2	X-Frame-Options	78
4.2	HTML5 的安全问题	80
4.2.1	存储 API	81
4.2.2	跨域资源共享	83
4.2.3	基于 FullScreen 和 Notification API 的新型钓鱼攻击	84
4.2.4	组合 API 后可能导致的安全问题	87
4.2.5	引入新的 XSS 攻击向量	87
4.2.6	互联网威胁	89
4.3	HTTPS 与中间人攻击	92
4.3.1	HTTPS 的绿锁	92
4.3.2	HTTPS 有多安全?	94
4.3.3	HSTS	96
4.3.4	使用 SSLStrip 阻止 HTTP 升级 HTTPS	97
4.3.5	使用 Fiddler 对 PC 端快速进行中间人攻击测试	99

4.3.6 使用 Fiddler 脚本和 AutoResponse 自动发起中间人攻击.....	101
4.4 本章小结.....	103
5 浏览器扩展与插件的安全问题.....	105
5.1 插件.....	106
5.1.1 ActiveX.....	106
5.1.2 ActiveX 的安全问题.....	107
5.1.3 ActiveX 的逻辑漏洞.....	108
5.1.4 NPAPI、PPAPI.....	111
5.2 定制浏览器的扩展和插件的漏洞.....	113
5.2.1 特权 API 暴露.....	114
5.2.2 DOM 修改引入攻击向量.....	114
5.2.3 Windows 文件名相关的多个问题.....	115
5.2.4 NPAPI DLL 的问题.....	116
5.2.5 同源检查不完善.....	117
5.2.6 Content Script 劫持.....	118
5.2.7 权限隔离失败.....	118
5.2.8 配合切核策略+本地内部页 XSS 执行代码.....	118
5.2.9 下载服务器限制宽松.....	119
5.2.10 TLDs 判定问题.....	119
5.2.11 经典漏洞.....	120
5.2.12 中间人.....	120
5.3 Adobe Flash 插件与 Action Script.....	121
5.3.1 Flash 的语言——Action Script.....	121
5.3.2 Flash 文档的反编译、再编译与调试.....	122
5.3.3 SWF 的网络交互: URLLoader.....	124
5.3.4 crossdomain.xml 与 Flash 的“沙盒”.....	125
5.3.5 ExternalInterface.....	126
5.3.6 FLASH XSS.....	126
5.3.7 Microsoft Edge 中的 Flash ActiveX.....	130

5.4 浏览器的沙盒.....	131
5.4.1 受限令牌.....	132
5.4.2 完整性级别与 IE 的保护模式.....	133
5.4.3 任务对象.....	134
5.5 本章小结.....	135
6 移动端的浏览器安全.....	137
6.1 移动浏览器的安全状况.....	138
6.2 移动端的威胁.....	141
6.2.1 通用跨站脚本攻击.....	141
6.2.2 地址栏伪造.....	142
6.2.3 界面伪装.....	143
6.3 结合系统特性进行攻击.....	144
6.3.1 Android 一例漏洞：使用 Intent URL Scheme 绕过 Chrome SOP.....	144
6.3.2 iOS 的一例漏洞：自动拨号泄露隐私.....	146
6.3.3 Windows Phone 一例未修补漏洞：利用 Cortana 显示 IE 中已保存密码.....	147
6.4 本章小结.....	149

第 2 篇 实战网马与代码调试

7 实战浏览器恶意网页分析.....	153
7.1 恶意网站中“看得见的”攻防.....	153
7.2 恶意脚本的抓取和分析.....	155
7.2.1 发现含攻击代码的网址.....	156
7.2.2 使用 rDNS 扩大搜索结果.....	156
7.2.3 下载攻击代码.....	157
7.2.4 搭建测试环境.....	158
7.2.5 初识网马反混淆工具.....	158
7.2.6 恶意脚本中常见的编码方式.....	159
7.3 一个简单的挂马代码的处理.....	169
7.3.1 快速判断挂马.....	169

7.3.2	JS 代码的格式化	170
7.4	更为复杂的代码处理：对 Angler 网马工具包的反混淆	170
7.4.1	Angler EK 的特征	170
7.4.2	推理：找出代码中的“解密-执行”模式	172
7.4.3	验证：确定“解密-执行”模式的位置和方法	175
7.4.4	追踪：使用浏览器特性判断用户环境	179
7.4.5	利用漏洞 CVE-2014-6332 发起攻击	188
7.5	本章小结	190
8	调试工具与 Shellcode	191
8.1	调试工具的用法	191
8.1.1	调试符号	191
8.1.2	WinDbg 的用法	192
8.1.3	IDA 的用法	195
8.1.4	OllyDbg 的用法	199
8.2	与 Shellcode 的相关名词	201
8.2.1	机器指令	201
8.2.2	控制关键内存地址	203
8.2.3	NOP Slide	204
8.2.4	Magic Number 0x8123	205
8.3	Shellcode 的处理	205
8.3.1	实现通用的 Shellcode	206
8.3.2	调试网马中的 Shellcode	212
8.4	本章小结	218

第 3 篇 深度探索浏览器漏洞

9	漏洞的挖掘	221
9.1	挖 0day	221
9.1.1	ActiveX Fuzzer 的原理	221
9.1.2	使用 AxMan Fuzzer 来 Fuzz ActiveX 插件	222

9.1.3 现场复现.....	225
9.2 DOM Fuzzer 的搭建.....	229
9.2.1 搭建运行 Grinder 的环境.....	230
9.2.2 Fuzzer 的结构与修改.....	231
9.2.3 现场复现.....	232
9.3 崩溃分析.....	233
9.3.1 哪些典型崩溃不能称作浏览器漏洞.....	233
9.3.2 ActiveX 崩溃一例.....	236
9.3.3 IE11 崩溃一例.....	238
9.4 本章小结.....	244
10 网页的渲染.....	245
10.1 网页的渲染.....	245
10.1.1 渲染引擎.....	245
10.1.2 DOM 结构模型.....	247
10.1.3 IE 解析 HTML 的过程.....	249
10.1.4 IE 的 Tokenize.....	251
10.1.5 Chrome 解析 HTML 的过程.....	253
10.1.6 Chrome 的 Tokenize.....	254
10.2 元素的创建.....	256
10.2.1 IE 中元素的创建过程.....	256
10.2.2 Chrome 中元素的创建过程.....	257
10.2.3 元素的生成规律.....	258
10.3 实战：使用 WinDbg 跟踪元素的生成.....	260
10.4 实战：使用 WinDbg 跟踪元素的插入.....	263
10.5 实战：使用 WinDbg 跟踪元素的释放.....	264
10.6 本章小结.....	266
11 漏洞的分析.....	267
11.1 分析 IE 漏洞 CVE-2012-4969.....	267
11.1.1 崩溃分析.....	268

11.1.2	追根溯源	270
11.2	分析 JScript9 漏洞 CVE-2015-2425	271
11.2.1	跟踪漏洞	275
11.3	Hacking Team 的 Flash 漏洞 CVE-2015-5119 分析	276
11.3.1	静态阅读：成因分析	276
11.3.2	Vector 的覆盖过程	278
11.4	本章小结	279
12	漏洞的利用	281
12.1	ShellCode 的编写	281
12.2	CVE-2012-4969 的利用	284
12.2.1	DEP/ASLR 绕过	287
12.3	CVE-2015-5119 的 Vector	296
12.4	本章小结	301
附录	303
附录 A	IE (Edge) 的 URL 截断	303
附录 B	IE 的控制台截断	304
附录 C	表单中的 mailto: 外部协议	305
附录 D	危险的 regedit: 外部协议	306
附录 E	IE XSS Filter 的漏洞也会帮助执行 XSS	307
附录 F	更高级的策略保护——CSP Level 2	308
附录 G	更快的执行速度——JScript5 to Chakra	309
附录 H	Chakra 的整数存储	310
附录 I	安全实践	311
参考资料	315

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

漏洞与浏览器安全

1.1 漏洞的三要素

软件在设计、实现、配置运行过程中会存在缺陷，如果攻击者在未授权的情况下利用这些缺陷影响到用户的系统，就可以称这些缺陷为漏洞。那么，浏览器中出现了什么问题才可以真正算为漏洞呢？微软曾经给出了较为通俗的解释^①：仅当通过软件缺陷触发，而且有损完整性、可用性、机密性三者中至少一项时，这个问题才应当被考虑是漏洞。

- **完整性**：指对资源的可信程度。攻击者若是在未授权且无提示的情况下修改了资源，那便是破坏了其完整性。

引申到浏览器中，就是一个网页通过某种方式做了它正常情况下不应该做到的事情。如果浏览器对某些危险动作发出了明确的警告，而用户手动点了允许，这样则不应视为漏洞。如果浏览器的缺陷被利用，静默下载了木马程序，或是删除了用户计算机上的文件等，则应当被视为漏洞。

- **可用性**：指访问资源的能力。攻击者针对漏洞进行攻击时，如果能够控制产品不让用户访问资源，便破坏了其可用性。

有一个典型的例子：攻击者攻击 HTTP 服务器，使得其软件崩溃，导致其他用户无法访问该网站，这可以称作漏洞。但是如果攻击者通过 DDoS 来攻击 HTTP 服务器，虽然效果和前者一样，但是这不是漏洞。因为在前一种情况下，攻击者可以控制服务器程序的“生死”。而后者，虽然服务器运行缓慢或采取必要的限制流量措施，导致用户无法使用服务，但是程序执行的控制权依然在服务器手里。

^① <https://technet.microsoft.com/library/cc751383.aspx>

在浏览器中，一些无法利用的崩溃（unexploitable crash）虽然会导致网页无法访问，但是浏览器依然有控制权，浏览器可以在网页多次崩溃之后选择不再展示该网页，这表明代码的控制权依然在浏览器的手中。攻击者实际上仅做到了拒绝用户对该网站的访问，这与直接断开网站的服务器效果差别并不大。因此这样的代码归为缺陷比较合适，而不应当算作是浏览器漏洞。



图 1-1：IE 中网页一直崩溃后，IE 选择拒绝再次展示该网页

- **机密性**：机密性指对一些需要授权的信息的限制。如果攻击者通过漏洞获取到了一些不该由他来获取的内容，称作破坏了机密性。

举个例子，浏览器保存的密码，应当只能被保存它的用户和对应网站知道，如果攻击者通过浏览器缺陷知道了密码，这属于浏览器漏洞。如果一个人通过钓鱼骗到了密码，或是通过某种方式取得了用户的笔记本或手机，并偷看到用户保存的密码，这不属于浏览器漏洞。

前后二者的区别在于，前者信息泄露的载体是浏览器，诱因是浏览器的缺陷，所以应当被归为漏洞。而后者，用户已经丢失或主动让出了对数据的所有权，这种情况下，问题的载体为用户。

1.2 漏洞的生命周期

从漏洞的产生到漏洞消亡的这段时间称为漏洞的生命周期。从漏洞利用代码公开到漏洞补丁发布的这段时间称为 0day 期，攻击者可能会利用已经公开的 PoC 或对其稍加

修改，用来对目标进行攻击，此时由于无官方补丁，且并不是每个人都知道有这个漏洞，所以危害最大，攻击者最容易得手。

另一个攻击的好时机是官方补丁发布的第一天，许多用户还没来得及打上补丁，但是攻击者可以对补丁修改的文件进行差量分析，从而猜测漏洞的原理，并写出攻击代码，这称作 1day 漏洞，攻击成功后依然可以产生较大的危害。随着用户逐渐打上补丁和新漏洞的产生，旧漏洞的危害也逐渐变小，从而逐渐走向衰亡，直到漏洞生命终结。

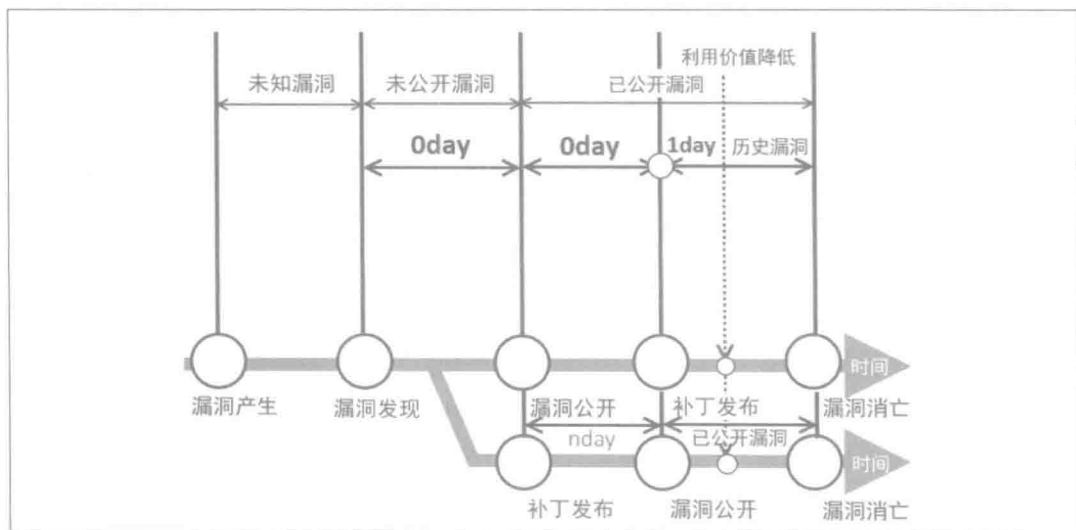


图 1-2: 漏洞的生命周期

随着用户的深入使用，系统中存在的漏洞会被不断暴露出来，这些早先被发现的漏洞也会不断被系统供应商发布的漏洞补丁修补，或在新版系统中得以纠正。同时，这也可能会引入一些新的漏洞和错误。随着时间的推移，旧的漏洞会不断消失，新的漏洞会不断出现。漏洞问题也会长期存在。

1.3 浏览器安全概述

作为用户与网络交互的最主要的一种平台，浏览器也日渐成为了网络攻击的目标，猖獗的地下 Oday 交易，以及简单、流程化的木马生成与发布程序都让浏览器安全问题影响变得广泛。

以浏览器最出名的漏洞之一 MS06-014 为例。这个漏洞曾被广泛利用于网马中，它

的利用代码简单，执行时几乎毫无声息。2006 年，某安全软件就拦截到总计 300 余万次来自它的攻击。更糟的是，当年许多用户没有安装补丁，所以 MS06-014 利用起来成功率相当高。在随后足足 5 年时间内，几乎所有的挂马工具包中都给 MS06-014 留有位置。直到被新漏洞取代之前，MS06-014 都是当之无愧的“挂马王”^①。在它爆发的几年中，预计有千万以上级别的计算机受到了影响。



图 1-3：傻瓜化的木马生成器

因何这样一个小小木马有如此大的威力？一个重要原因是当年的网站和服务器安全没有受到足够重视，因此给黑客们留有可乘之机。另一个原因则是由于黑客使用漏洞的门槛相当低。笔者找到了当年的一款“网马生成器”，从它的界面和程序内容就可以知道，这完全是“傻瓜式”操作。“网马生成器”造就了部分想要赚快钱的“脚本小子”。他们并不研究和了解漏洞，只会单纯地使用工具，动动手指就能把木马给布置妥当，然后坐等用户上钩。

作为安全研究人员，使浏览器变得安全则是我们的目标。从较为狭义的角度来解释的话，浏览器安全既指消除浏览器漏洞，又指浏览器程序能正确、安全地使用网络功能，还能够保护用户已经联网的数据不被泄露。

事实上，我们平时接触到的是更为广义的浏览器安全。许多问题只是利用了浏览器这个载体的特性。例如钓鱼网站，它没有利用任何浏览器漏洞，只不过这个问题发生的载体是浏览器，因此也被认为是浏览器安全的一部分。但它们并不一定要完全依靠浏览器解决，例如搜索引擎展示时可能就会给予用户明显的提示。

广义的浏览器安全包括所有可能会影响到用户信息安全的问题，例如页面伪造、钓鱼、下载文件病毒检查、广告弹窗、不良内容的过滤、用户设置保护等。

^① <http://it.sohu.com/20090409/n263288723.shtml>

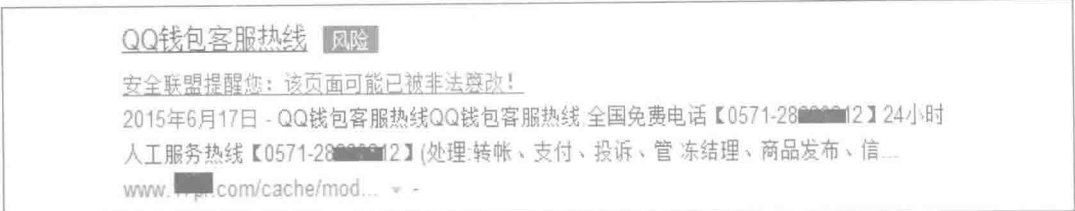


图 1-4: 对虚假信息、钓鱼网站的拦截也应被归为广义的浏览器安全

浏览器中数据和指令混杂（例如 HTML 代码既可能是数据又可能是指令），浏览器要处理的数据大部分又来自其他用户的输入，这就导致浏览器受到攻击时的内容更不可预测。将这些安全问题一个个击破，也正是研究浏览器安全的目标。

1.4 浏览器安全的现状

浏览器漏洞数量在不断增长，却并没有引起所有用户的重视。安全研究机构 Secunia 的研究报告称 2014 年浏览器漏洞数量同比增长了 42%，且大部分都是高危漏洞。此外，Secunia 扫描的用户中约 1/4 的用户并没有及时安装补丁。

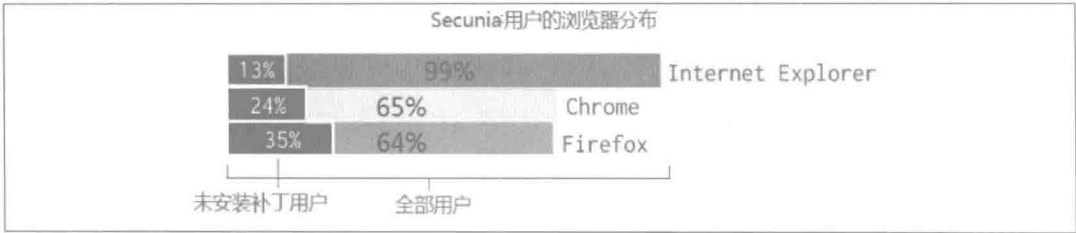


图 1-5: Secunia 对其企业用户调查的结果

而在移动端的情况也是一样。封闭的系统 iOS 和 Windows Phone 的更新瓶颈在于厂商，而 Android 则受限于平台过于开放和多样化。Android 4.4 中，Google 可以向设备推送一个小型补丁来修正浏览器漏洞。在 5.0 中，则是通过 Google Play 来发起更新。截至 2015 年 5 月，约一半的安卓设备在使用 4.3 以下的版本。Google 并不会针对 4.3 及以下版本的浏览器推送漏洞补丁。如果你仍然使用着安卓系统，那么建议及时更新系统或更换成其他第三方浏览器，这会减小由于补丁不及时推送而导致的各种安全风险。

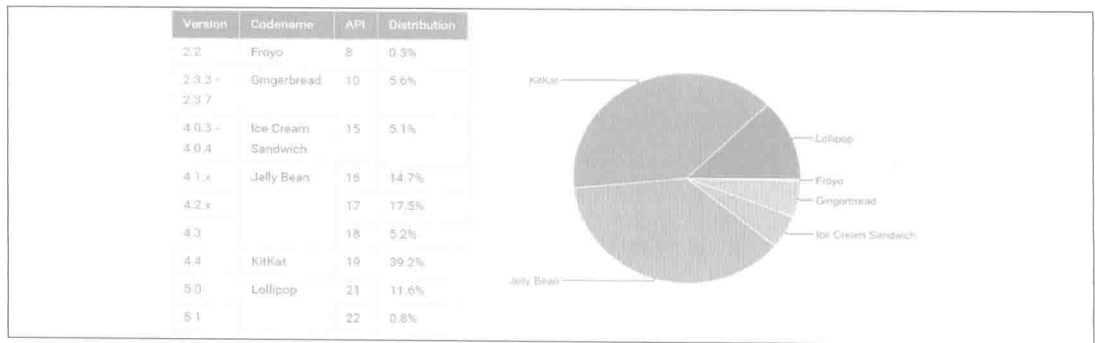


图 1-6：2015 年 5 月谷歌公布的安卓各版本所占比例

用户量和使用频率决定了一个软件是否容易受到攻击。2015 年 7 月 6 日，意大利舆情监控公司 Hacking Team 遭到攻击，攻击者公开了该公司用来销售的多个 0day 漏洞的利用代码。这个臭名昭著的工具的广告视频中，有一句宣传语特别刺眼——“要监视你的目标，你需要在他浏览网页时，黑掉他”。



图 1-7：Hacking Team 销售黑客工具达芬奇的广告

浏览器的应用非常广泛，不仅仅是我们日常使用的那个一眼就能认出来的浏览器，例如邮件客户端、RSS 阅读器、QQ 消息记录等软件中也会用到封装后的浏览器组件。浏览器有如此大的用户量，所以成为攻击者的首选目标也不足为奇。

黑客热衷于攻击浏览器的另一个重要原因是，攻击成本低但收益超高。杀毒软件公司 Sophos 研究表明，著名的漏洞工具包“黑洞”的完整服务版本每季度只需要 300 美元，提供挂马的服务每季度只需 1 500 美元。然而攻击者的收入很可能远高于这些服务费。从国内的报道中也可见端倪，一些盗号木马在短期内可以非法获利百万元。在这种利益的诱惑下，地下黑客以身试法，对浏览器发起攻击的事件层出不穷。

1.5 浏览器的应对策略

为了应对攻击，浏览器也增添了许多安全特性。例如，各浏览器都纷纷开启了数据执行保护（DEP）和地址空间分布随机化（ASLR）。同时，为了降低恶意代码运行时的权限，浏览器也在试图降低浏览器网页进程的权限，例如 IE 的保护模式和 Chrome 的沙箱。



图 1-8：Google Chrome 的恶意网站拦截功能

为了防止用户受到脚本注入的困扰，IE 和 Chrome 也各自添加了 XSS 过滤器。为了防止用户受到钓鱼网站或是恶意网站的干扰，浏览器也添加了形如 SmartScreen Filter、恶意网站拦截的功能。同时，浏览器也在兼容新的安全特性，例如 DNT（不要追踪，Do Not Track）和防止点击劫持的 HTTP 头、CSP 安全策略等。可以看得出来，浏览器在提升安全性上还是十分努力的。

由于网络复杂和不可预知的特性，浏览器的制作者既要保证产品遵循规范去使用网络资源，也要防止用户不当操作带来的风险。在与浏览器安全技术的对抗中，黑客们也形成了一套较为成熟的漏洞利用方法，例如我们常常能在攻击代码中看到成型的对“堆喷射”、返回导向编程攻击（ROP）的利用。而浏览器厂商则通过不断在产品中加入新的特性提升黑客攻击的门槛，提升自己产品的安全性。

1.6 “白帽子”与浏览器厂商的联手协作

虽然网络安全形式严峻，但是幸运的是有许多“白帽子”正在各种平台上努力提交浏览器的安全漏洞。2014 年 6 月至 2015 年 6 月间，乌云漏洞报告平台上就有 50 余名“白

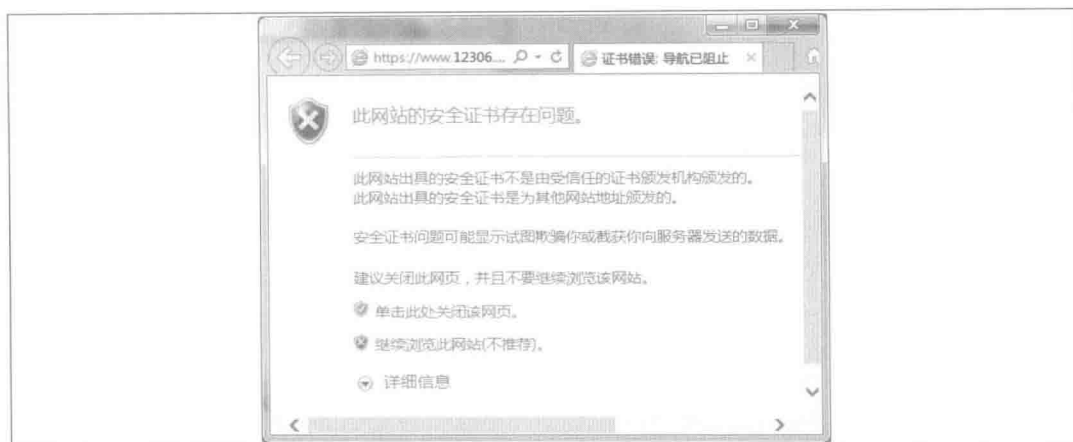


图 附-7: 充满安全术语的提示

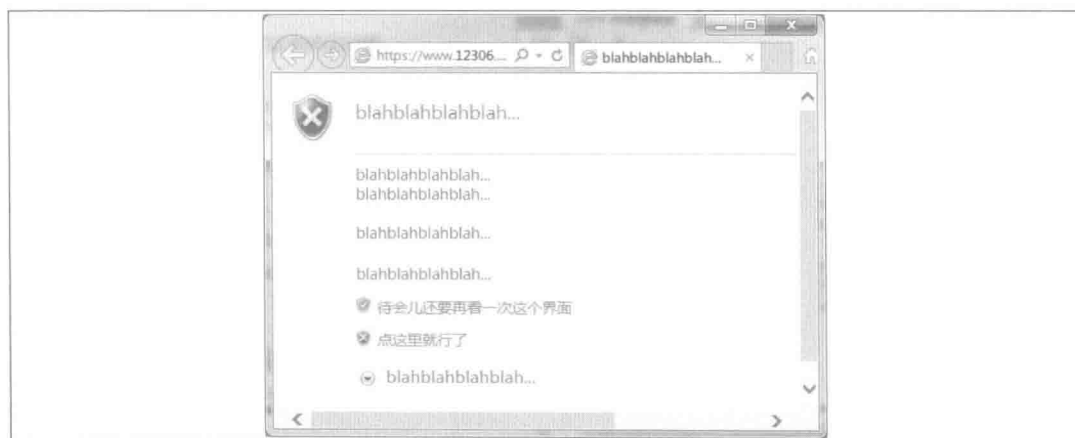


图 附-8: 在一般用户眼里的感觉

对于 12306 这样的“刚需”网站，用户可能并不会对安全提示买账，但是对于一些其他网站，证书错误提示可以优先显示简单的一句话“该网站的连接有问题，继续访问可能带来安全风险”，把技术细节隐藏起来，这样可以更好地让用户了解到如果继续访问，可能会给他带来的风险。

浏览器的安全是一个广阔且有魅力的方向，Web 和底层分析都可以走得很深很远，希望拙作可以让大家对浏览器安全有初步的认识，起到抛砖引玉的作用。感谢你为互联网安全所贡献的力量:))。

参考资料

- [1] 《The Death of the Internet》，Markus Jakobsson，2012，John Wiley & Sons, Inc.
- [2] 《软件漏洞分析技术》，吴世忠、郭涛等，2014，科学出版社。
- [3] 《Web 之困:现代 Web 应用安全指南》，Michal Zalewski，电子工业出版社
- [4] 《Web 前端黑客技术揭秘》，钟晨鸣，徐少培，2013，电子工业出版社
- [5] Secunia Vulnerability Review 2015，<http://secunia.com/confirmation/resources/reports/vr2015/>
- [6] How Browsers Work，<http://taligarsiel.com/Projects/howbrowserswork1.htm>
- [7] 《The Browser Hackers' Handbook》，Wade Alcorn、Christian Frichot，2014，Wiley
- [8] Internet Explorer Team Blog，<https://blogs.msdn.microsoft.com/ie/>
- [9] 《图解 HTTP》，上野宣，2014，人民邮电出版社
- [10] IEInternals，<http://blogs.msdn.com/b/ieinternals/>
- [11] Internet Explorer Architecture，[https://msdn.microsoft.com/en-us/library/aa741312\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa741312(v=vs.85).aspx)
- [12] 《WebKit 技术内幕》，朱永盛，2014，电子工业出版社
- [13] 《The Shellcoders' Handbook》，Chris Anley，2007，Wiley
- [14] Understanding the Attack Surface and Attack Resilience of Project Spartan's (Edge) New EdgeHTML Rendering Engine，<https://www.blackhat.com/docs/us-15/materials/us-15-Yason-Understanding-The-Attack-Surface-And-Attack-Resilience-Of-Project-Spartans-New-EdgeHTML-Rendering-Engine-wp.pdf>
- [15] Internet Explorer，<http://www.geoffchappell.com/studies/windows/ie/>
- [16] Advances in JavaScript Performance in IE10 and Windows 8，<http://blogs.msdn.com/b/ie/archive/2012/06/13/advances-in-javascript-performance-in-ie10-and-windows-8.aspx>
- [17] Bugzilla@Mozilla，<https://bugzilla.mozilla.org/>

- [18] Chromium Issues, <https://code.google.com/p/chromium/issues/list>
- [19] IE9 及高效互联网体验, <http://velocity.oreilly.com.cn/2010/ppts/velocityChina2010IE9.pdf>
- [20] 安全与隐私保护, <http://www.firefox.com.cn/desktop/security/>
- [21] 创建和管理受监管用户, <https://support.google.com/chrome/answer/3463947?hl=zh-Hans>
- [22] 《Windows 核心编程(第 5 版)》, Jeffrey Richter、Christophe Nasarre, 2008, 清华大学出版社
- [23] The Chromium Projects, <https://www.chromium.org/>
- [24] World Wide Web Consortium (W3C), <http://www.w3.org/>
- [25] Content Security Policy Level 2 介绍, <https://imququ.com/post/content-security-policy-level-2.html>
- [26] X-XSS-Nightmare: XSS Attacks Exploiting XSS Filter, <http://www.slideshare.net/masatokinugawa/xxn-en>
- [27] 《ActionScript 3.0 Bible, 2nd Edition》, Roger Braunstein, 2010, Wiley
- [28] Hosting and Reuse, [https://msdn.microsoft.com/en-us/library/aa752038\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa752038(v=vs.85).aspx)
- [29] MSHTML Reference, [https://msdn.microsoft.com/en-us/library/aa741317\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa741317(v=vs.85).aspx)
- [30] Introduction to Markup Services, [https://msdn.microsoft.com/en-us/library/bb508514\(VS.85\).aspx](https://msdn.microsoft.com/en-us/library/bb508514(VS.85).aspx)
- [31] Safe Initialization and Scripting for ActiveX Controls, [https://msdn.microsoft.com/en-us/library/aa751977\(VS.85\).aspx](https://msdn.microsoft.com/en-us/library/aa751977(VS.85).aspx)
- [32] PAVE:Initializing Aggregates, <https://msdn.microsoft.com/en-us/library/sdwe79a4.aspx>

浏览器上的安全是混乱的，W3C和WHATWG组织选择了——以标准化的形式使浏览器可以快速更新并增加新的安全策略——这样一种激进做法，来对抗浏览器上已有的和即将到来的安全风险。新的功能可以快速覆盖已有问题，但其带来的未知风险，或许更加可怕。我们必须从Web前端到浏览器底层全面了解浏览器安全技术，在面对浏览器上千变万化的威胁时，方能做到未雨绸缪。如何做到？请阅读本书，一定不会让你失望。

腾讯玄武实验室安全专家，《Web前端黑客技术揭秘》作者 徐少培

这本书很难得！从纯粹的Web前端安全玩法，到如何突破浏览器边界，都做了深度剖析，有许多独到见解。感谢作者能把自己的诸多实战经验分享出来。

知道创宇技术副总裁，《Web前端黑客技术揭秘》作者 余弦

这本书对浏览器规范层面、功能实现层面及渲染层出现的安全问题，都做了较为详细的描述。其中对各种现代浏览器的实例讲解，更是非常难得。作者似乎有这样一个意图：想从每个层面将读者带入一个个奇幻世界。无论如何，这是一本很完整的浏览器安全书籍，推荐想系统学习的道友从速入手。

双螺旋攻防实验室 李普君（长短短）

本书从应用层到系统层全面介绍了浏览器在各种场景下的安全防护及攻击思路，并且结合了很多乌云平台上的实际案例，是国内第一本全面介绍浏览器安全的书籍，对浏览器安全机制感兴趣的人员值得一读。

乌云知识库

和传统 Web 安全的书籍不同，本书着重围绕浏览器前端技术，并以案例形式讲解；覆盖基础知识及近几年出现的技术标准，其中不乏一些有趣的案例。如果对前端安全感兴趣，本书值得一读。

淘宝安全工程师 前端安全研究者 佳辰(EtherDream)

看过作者之前一些文章，发现他对浏览器安全有着非常专业的研究。由其将自己的相关经验整理成书，相信会是一本值得研究Web安全及浏览器安全从业人员阅读的好书。

万达电商资深安全经理 lion_00



博文视点Broadview



新浪微博

@博文视点Broadview



策划编辑：张春雨
责任编辑：付 睿
封面设计：侯士卿

上架建议：网络安全

ISBN 978-7-121-28154-9



9 787121 281549 >

定价：79.00元