

# 《白帽子讲浏览器安全》

## 图书基本信息

书名：《白帽子讲浏览器安全》

13位ISBN编号：9787121281546

出版时间：2016-3

作者：钱文祥

页数：332

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu111.com](http://www.tushu111.com)

# 《白帽子讲浏览器安全》

## 内容概要

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《白帽子讲浏览器安全》中我们将给出解答，带你了解浏览器安全的方方面面。《白帽子讲浏览器安全》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。《白帽子讲浏览器安全》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。

# 《白帽子讲浏览器安全》

## 作者简介

钱文祥（常用ID：blast），专职浏览器安全研究。安徽理工大学毕业后就职于腾讯科技（北京）有限公司，专注于PC浏览器安全研究和安全相关功能的开发。活跃于多个漏洞报告平台，曾报告过数十个安全漏洞，涵盖IE、Chrome及国产定制浏览器。参与过多个浏览器安全相关以及漏洞挖掘的项目，维护有网马解密工具Redoce。

## 书籍目录

- 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 检证：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 调试工具的法 191
    - 8.1.1 调试符号 191
    - 8.1.2 WinDbg 的法 192
    - 8.1.3 IDA 的法 195
    - 8.1.4 OllyDbg 的法 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

# 《白帽子讲浏览器安全》

## 精彩短评

- 1、专门讲浏览器相关攻防的知识，讲的很透，从原理、调试，从web到二进制，说的都比较多。
- 2、内容还行，就是写的不怎么样。

# 《白帽子讲浏览器安全》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu111.com](http://www.tushu111.com)