

黑客攻防技术宝典



[黑客攻防技术宝典_下载链接1](#)

著者:[澳] Wade Alcorn

出版者:人民邮电出版社

出版时间:2016-10

装帧:平装

isbn:9787115433947

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。它是你在实践中的必读参考指南，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。

作者介绍:

作者简介:

Wade Alcorn

开源浏览器漏洞利用框架BeEF之父。

Christian Frichot

BeEF首席开发人员，Perth Open Web Application Security Project负责人。

Michele Orrù

BeEF核心开发人员，漏洞研究专家，社会工程专家。

译者简介:

本书译者均来自自由月影领衔的奇虎360最大前端团队——奇舞团（75team）。

李松峰

资深技术翻译，译有《JavaScript高级程序设计》《简约至上：交互式设计四策略》等数十部技术和设计书籍，现为奇舞团高级开发工程师、《奇舞周刊》总编、360公司W3C AC代表。

孟之杰

奇舞团高级开发工程师，热爱前端，热爱翻译，具有Geek精神，喜欢折腾各种有意思的东西。

审校者简介:

审校者均来自奇虎360 OKEE TEAM，即信息安全部Web攻防团队。该团队致力于保护360公司全线业务安全。

王珂

360Web攻防团队OKEE TEAM成员，具有多年攻防渗透经验，专注于研究浏览器与前端漏洞，是“360护心镜”的作者。

李响

360Web攻防团队OKEE TEAM成员，拥有多年攻防渗透经验，长期专注安全应急响应攻击溯源研究，具有丰富的甲方安全经验。

常春峰

360Web攻防团队OKEE

TEAM成员。曾就职360网站安全团队，担任过库带计划、网站安全检测等项目的安全工作，专注于安全攻防、漏洞挖掘以及自动化等领域，具有丰富的甲方和乙方的安全经验。

叶仁旭

360Web攻防团队0KEE

TEAM成员，多年信息安全领域研究经历，长期投身于自动化安全扫描技术、安全防御技术、安全体系建设等方面的研究，有丰富的实践积累，BlackHat 2016演讲者。

李福 (Darker)

360Web攻防团队0KEE

TEAM成员，知名白帽子，拥有多年安全实战经验，擅长渗透测试与漏洞挖掘，对各种漏洞利用及场景有独到见解，BlackHat 2016演讲者。

目录: 第1章 浏览器安全概述 1

- 1.1 首要问题 1
 - 1.2 揭密浏览器 3
 - 1.2.1 与Web应用休戚与共 3
 - 1.2.2 同源策略 3
 - 1.2.3 HTTP首部 4
 - 1.2.4 标记语言 4
 - 1.2.5 CSS 5
 - 1.2.6 脚本 5
 - 1.2.7 DOM 5
 - 1.2.8 渲染引擎 5
 - 1.2.9 Geolocation 6
 - 1.2.10 Web 存储 7
 - 1.2.11 跨域资源共享 7
 - 1.2.12 HTML5 8
 - 1.2.13 隐患 9
 - 1.3 发展的压力 9
 - 1.3.1 HTTP首部 9
 - 1.3.2 反射型XSS过滤 11
 - 1.3.3 沙箱 11
 - 1.3.4 反网络钓鱼和反恶意软件 12
 - 1.3.5 混入内容 12
 - 1.4 核心安全问题 12
 - 1.4.1 攻击面 13
 - 1.4.2 放弃控制 14
 - 1.4.3 TCP协议控制 15
 - 1.4.4 加密通信 15
 - 1.4.5 同源策略 15
 - 1.4.6 谬论 16
 - 1.5 浏览器攻防方法 16
 - 1.5.1 初始化 18
 - 1.5.2 持久化 18
 - 1.5.3 攻击 19
 - 1.6 小结 20
 - 1.7 问题 21
 - 1.8 注释 21
- 第2章 初始控制 23

2.1 理解控制初始化	23
2.2 实现初始控制	24
2.2.1 使用XSS攻击	24
2.2.2 使用有隐患的Web应用	34
2.2.3 使用广告网络	34
2.2.4 使用社会工程攻击	35
2.2.5 使用中间人攻击	45
2.3 小结	55
2.4 问题	55
2.5 注释	56
第3章 持续控制	58
3.1 理解控制持久化	58
3.2 通信技术	59
3.2.1 使用XMLHttpRequest轮询	60
3.2.2 使用跨域资源共享	63
3.2.3 使用WebSocket通信	63
3.2.4 使用消息传递通信	65
3.2.5 使用DNS隧道通信	67
3.3 持久化技术	73
3.3.1 使用内嵌框架	73
3.3.2 使用浏览器事件	75
3.3.3 使用底层弹出窗口	78
3.3.4 使用浏览器中间人攻击	80
3.4 躲避检测	84
3.4.1 使用编码躲避	85
3.4.2 使用模糊躲避	89
3.5 小结	96
3.6 问题	97
3.7 注释	98
第4章 绕过同源策略	100
4.1 理解同源策略	100
4.1.1 SOP与DOM	101
4.1.2 SOP与CORS	101
4.1.3 SOP与插件	102
4.1.4 通过界面伪装理解SOP	103
4.1.5 通过浏览器历史理解SOP	103
4.2 绕过SOP技术	103
4.2.1 在Java中绕过SOP	103
4.2.2 在Adobe Reader中绕过SOP	108
4.2.3 在Adobe Flash中绕过SOP	109
4.2.4 在Silverlight中绕过SOP	110
4.2.5 在IE中绕过SOP	110
4.2.6 在Safari中绕过SOP	110
4.2.7 在Firefox中绕过SOP	112
4.2.8 在Opera中绕过SOP	113
4.2.9 在云存储中绕过SOP	115
4.2.10 在CORS中绕过SOP	116
4.3 利用绕过SOP技术	117
4.3.1 代理请求	117
4.3.2 利用界面伪装攻击	119
4.3.3 利用浏览器历史	132
4.4 小结	139
4.5 问题	139
4.6 注释	140

- 第5章 攻击用户 143
 - 5.1 内容劫持 143
 - 5.2 捕获用户输入 146
 - 5.2.1 使用焦点事件 147
 - 5.2.2 使用键盘事件 148
 - 5.2.3 使用鼠标和指针事件 150
 - 5.2.4 使用表单事件 152
 - 5.2.5 使用IFrame按键记录 153
 - 5.3 社会工程学 154
 - 5.3.1 使用标签绑架 154
 - 5.3.2 使用全屏 155
 - 5.3.3 UI期望滥用 159
 - 5.3.4 使用经过签名的Java小程序 176
 - 5.4 隐私攻击 180
 - 5.4.1 不基于cookie的会话追踪 181
 - 5.4.2 绕过匿名机制 182
 - 5.4.3 攻击密码管理器 184
 - 5.4.4 控制摄像头和麦克风 186
 - 5.5 小结 192
 - 5.6 问题 192
 - 5.7 注释 193
- 第6章 攻击浏览器 195
 - 6.1 采集浏览器指纹 196
 - 6.1.1 使用HTTP首部 197
 - 6.1.2 使用DOM属性 199
 - 6.1.3 基于软件bug 204
 - 6.1.4 基于浏览器特有行为 204
 - 6.2 绕过cookie检测 205
 - 6.2.1 理解结构 206
 - 6.2.2 理解属性 207
 - 6.2.3 绕过路径属性的限制 209
 - 6.2.4 cookie存储区溢出 211
 - 6.2.5 使用cookie实现跟踪 214
 - 6.2.6 Sidejacking攻击 214
 - 6.3 绕过HTTPS 215
 - 6.3.1 把HTTPS降级为HTTP 215
 - 6.3.2 攻击证书 218
 - 6.3.3 攻击SSL/TLS层 219
 - 6.4 滥用URI模式 220
 - 6.4.1 滥用iOS 220
 - 6.4.2 滥用三星Galaxy 222
 - 6.5 攻击JavaScript 223
 - 6.5.1 攻击JavaScript加密 223
 - 6.5.2 JavaScript和堆利用 225
 - 6.6 使用Metasploit取得shell 231
 - 6.6.1 Metasploit起步 231
 - 6.6.2 选择利用 232
 - 6.6.3 仅执行一个利用 233
 - 6.6.4 使用Browser Autopwn 236
 - 6.6.5 结合使用BeEF和Metasploit 237
 - 6.7 小结 240
 - 6.8 问题 240
 - 6.9 注释 240
- 第7章 攻击扩展 244

7.1 理解扩展的结构	244
7.1.1 扩展与插件的区别	245
7.1.2 扩展与附加程序的区别	245
7.1.3 利用特权	245
7.1.4 理解Firefox扩展	246
7.1.5 理解Chrome扩展	251
7.1.6 IE扩展	258
7.2 采集扩展指纹	259
7.2.1 使用HTTP首部采集指纹	259
7.2.2 使用DOM采集指纹	260
7.2.3 使用清单文件采集指纹	262
7.3 攻击扩展	263
7.3.1 冒充扩展	263
7.3.2 跨上下文脚本攻击	265
7.3.3 执行操作系统命令	277
7.3.4 操作系统命令注入	280
7.4 小结	284
7.5 问题	284
7.6 注释	285
第8章 攻击插件	288
8.1 理解插件	288
8.1.1 插件与扩展的区别	289
8.1.2 插件与标准程序的区别	290
8.1.3 调用插件	290
8.1.4 插件是怎么被屏蔽的	292
8.2 采集插件指纹	292
8.2.1 检测插件	293
8.2.2 自动检测插件	295
8.2.3 用BeEF检测插件	295
8.3 攻击插件	297
8.3.1 绕过点击播放	297
8.3.2 攻击Java	302
8.3.3 攻击Flash	311
8.3.4 攻击ActiveX控件	314
8.3.5 攻击PDF阅读器	318
8.3.6 攻击媒体插件	319
8.4 小结	323
8.5 问题	324
8.6 注释	324
第9章 攻击Web应用	327
9.1 发送跨域请求	327
9.1.1 枚举跨域异常	327
9.1.2 前置请求	330
9.1.3 含义	330
9.2 跨域Web应用检测	330
9.2.1 发现内网设备IP地址	330
9.2.2 枚举内部域名	331
9.3 跨域Web应用指纹采集	333
9.4 跨域认证检测	339
9.5 利用跨站点请求伪造	342
9.5.1 理解跨站点请求伪造	343
9.5.2 通过XSRF攻击密码重置	345
9.5.3 使用CSRF token获得保护	346
9.6 跨域资源检测	347

9.7 跨域Web应用漏洞检测	350
9.7.1 SQL注入漏洞	350
9.7.2 检测XSS漏洞	363
9.8 通过浏览器代理	366
9.8.1 通过浏览器上网	369
9.8.2 通过浏览器Burp	373
9.8.3 通过浏览器Sqlmap	375
9.8.4 通过Flash代理请求	377
9.9 启动拒绝服务攻击	382
9.9.1 Web应用的痛点	382
9.9.2 使用多个勾连浏览器DDoS	383
9.10 发动Web应用利用	387
9.10.1 跨域DNS劫持	387
9.10.2 JBoss JMX跨域远程命令执行	388
9.10.3 GlassFish跨域远程命令执行	390
9.10.4 m0n0wall跨域远程命令执行	393
9.10.5 嵌入式设备跨域命令执行	395
9.11 小结	399
9.12 问题	400
9.13 注释	400
第10章 攻击网络	404
10.1 识别目标	404
10.1.1 识别勾连浏览器的内部IP	404
10.1.2 识别勾连浏览器的子网	409
10.2 ping sweep	412
10.2.1 使用XMLHttpRequest	412
10.2.2 使用Java	416
10.3 扫描端口	419
10.3.1 绕过端口封禁	420
10.3.2 使用IMG标签扫描端口	424
10.3.3 分布式端口扫描	426
10.4 采集非HTTP服务的指纹	428
10.5 攻击非HTTP服务	430
10.5.1 NAT Pinning	430
10.5.2 实现协议间通信	434
10.5.3 实现协议间利用	446
10.6 使用BeEF Bind控制shell	458
10.6.1 BeEF Bind Shellcode	458
10.6.2 在利用中使用BeEF Bind	463
10.6.3 把BeEF Bind作为Web shell	472
10.7 小结	475
10.8 问题	475
10.9 注释	476
第11章 结语：最后的思考	479
• • • • •	(收起)

[黑客攻防技术宝典_下载链接1](#)

标签

web安全

前端安全

黑客

网络安全

安全

计算机

信息安全

计算机安全

评论

没读下去

单纯了解一下

集大成者

[黑客攻防技术宝典 下载链接1](#)

书评

[黑客攻防技术宝典_下载链接1](#)