

Web前端黑客技术揭秘



[Web前端黑客技术揭秘 下载链接1](#)

著者:钟晨鸣

出版者:电子工业出版社

出版时间:2013-1

装帧:平装

isbn:9787121192036

Web前端的黑客攻防技术是一门非常新颖且有趣的黑客技术，主要包含Web前端安全的跨站脚本（XSS）、跨站请求伪造（CSRF）、界面操作劫持这三大类，涉及的知识点涵盖信任与信任关系、Cookie安全、Flash安全、DOM渲染、字符集、跨域、原生态攻击、高级钓鱼、蠕虫思想等，这些都是研究前端安全的人必备的知识点。本书作者深入剖

析了许多经典的攻防技巧，并给出了许多独到的安全见解。

本书适合前端工程师阅读，同时也适合对Web前端各类安全问题或黑客攻防过程充满好奇的读者阅读，书中的内容可以让读者重新认识到Web的危险，并知道该如何去保护自己以免受黑客的攻击。

作者介绍:

钟晨鸣，毕业于北京化工大学，网名：余弦。国内著名Web安全团队xeye成员，除了爱好Web

Hacking外，还对宇宙学、人类学等保持着浓厚兴趣。2008年加入北京知道创宇信息技术有限公司，现任研究部总监，团队致力于Web安全与海量数据研究，并进行相关超酷平台的实现。如果大家想和我交流，可以私信我微博：weibo.com/evilcos，同时本书的最新动态也会发布在我的微博上。

徐少培，毕业于河北工业大学。网名：xisigr。国内著名Web安全团队xeye成员。2008年加入北京天融信公司，现任北京天融信资深安全专家，重点负责安全研究工作，主要研究领域包括：WEB安全、HTML5安全、浏览器安全、协议分析等。同时也是国内信息安全大会常见的演讲者。我的微博：weibo.com/xisigr，希望可以和大家交流。

目录: 第1章 Web安全的关键点 1

1.1 数据与指令 1

1.2 浏览器的同源策略 4

1.3 信任与信任关系 7

1.4 社会工程学的作用 9

1.5 攻防不单一 9

1.6 场景很重要 10

1.7 小结 11

第2章 前端基础 12

2.1 W3C的世界法则 12

2.2 URL 14

2.3 HTTP协议 15

2.4 松散的HTML世界 19

2.4.1 DOM树 20

2.4.2 iframe内嵌出一个开放的世界 21

2.4.3 HTML内嵌脚本执行 22

2.5 跨站之魂——JavaScript 23

2.5.1 DOM树操作 23

2.5.2 AJAX风险 25

2.5.3 模拟用户发起浏览器请求 30

2.5.4 Cookie安全 33

2.5.5 本地存储风险 43

2.5.6 E4X带来的混乱世界 48

2.5.7 JavaScript函数劫持 49

2.6 一个伪装出来的世界——CSS 51

2.6.1 CSS容错性 51

2.6.2 样式伪装 52

2.6.3 CSS伪类 52

2.6.4 CSS3的属性选择符 53

2.7 另一个幽灵——ActionScript 55

2.7.1 Flash安全沙箱 55

2.7.2 HTML嵌入Flash的安全相关配置 59

2.7.3 跨站Flash	61
2.7.4 参数传递	64
2.7.5 Flash里的内嵌HTML	65
2.7.6 与JavaScript通信	67
2.7.7 网络通信	71
2.7.8 其他安全问题	71
第3章 前端黑客之XSS	72
3.1 XSS概述	73
3.1.1 “跨站脚本”重要的是脚本	73
3.1.2 一个小例子	74
3.2 XSS类型	76
3.2.1 反射型XSS	76
3.2.2 存储型XSS	77
3.2.3 DOM XSS	78
3.3 哪里可以出现XSS攻击	80
3.4 有何危害	81
第4章 前端黑客之CSRF	83
4.1 CSRF概述	84
4.1.1 跨站点的请求	84
4.1.2 请求是伪造的	84
4.1.3 一个场景	84
4.2 CSRF类型	89
4.2.1 HTML CSRF攻击	89
4.2.2 JSON HiJacking攻击	90
4.2.3 Flash CSRF攻击	94
4.3 有何危害	96
第5章 前端黑客之界面操作劫持	97
5.1 界面操作劫持概述	97
5.1.1 点击劫持 (Clickjacking)	98
5.1.2 拖放劫持 (Drag&Dropjacking)	98
5.1.3 触屏劫持 (Tapjacking)	99
5.2 界面操作劫持技术原理分析	99
5.2.1 透明层+iframe	99
5.2.2 点击劫持技术的实现	100
5.2.3 拖放劫持技术的实现	101
5.2.4 触屏劫持技术的实现	103
5.3 界面操作劫持实例	106
5.3.1 点击劫持实例	106
5.3.2 拖放劫持实例	111
5.3.3 触屏劫持实例	119
5.4 有何危害	121
第6章 漏洞挖掘	123
6.1 普通XSS漏洞自动化挖掘思路	124
6.1.1 URL上的玄机	125
6.1.2 HTML中的玄机	127
6.1.3 请求中的玄机	134
6.1.4 关于存储型XSS挖掘	135
6.2 神奇的DOM渲染	135
6.2.1 HTML与JavaScript自解码机制	136
6.2.2 具备HtmlEncode功能的标签	140
6.2.3 URL编码差异	142
6.2.4 DOM修正式渲染	145
6.2.5 一种DOM fuzzing技巧	146
6.3 DOM XSS挖掘	150

- 6.3.1 静态方法 150
- 6.3.2 动态方法 151
- 6.4 Flash XSS挖掘 153
 - 6.4.1 XSF挖掘思路 153
 - 6.4.2 Google Flash XSS挖掘 156
- 6.5 字符集缺陷导致的XSS 159
 - 6.5.1 宽字节编码带来的安全问题 160
 - 6.5.2 UTF-7问题 161
 - 6.5.3 浏览器处理字符集编码BUG带来的安全问题 165
- 6.6 绕过浏览器XSS Filter 165
 - 6.6.1 响应头CRLF注入绕过 165
 - 6.6.2 针对同域的白名单 166
 - 6.6.3 场景依赖性高的绕过 167
- 6.7 混淆的代码 169
 - 6.7.1 浏览器的进制常识 169
 - 6.7.2 浏览器的编码常识 175
 - 6.7.3 HTML中的代码注入技巧 177
 - 6.7.4 CSS中的代码注入技巧 190
 - 6.7.5 JavaScript中的代码注入技巧 196
 - 6.7.6 突破URL过滤 201
 - 6.7.7 更多经典的混淆CheckList 202
- 6.8 其他案例分享——Gmail Cookie XSS 204
- 第7章 漏洞利用 206
 - 7.1 渗透前的准备 206
 - 7.2 偷取隐私数据 208
 - 7.2.1 XSS探针：xssprobe 208
 - 7.2.2 Referer惹的祸 214
 - 7.2.3 浏览器记住的明文密码 216
 - 7.2.4 键盘记录器 219
 - 7.2.5 偷取黑客隐私的一个小技巧 222
 - 7.3 内网渗透技术 223
 - 7.3.1 获取内网IP 223
 - 7.3.2 获取内网IP端口 224
 - 7.3.3 获取内网主机存活状态 225
 - 7.3.4 开启路由器的远程访问能力 226
 - 7.3.5 内网脆弱的Web应用控制 227
 - 7.4 基于CSRF的攻击技术 228
 - 7.5 浏览器劫持技术 230
 - 7.6 一些跨域操作技术 232
 - 7.6.1 IE res:协议跨域 232
 - 7.6.2 CSS String Injection跨域 233
 - 7.6.3 浏览器特权区域风险 235
 - 7.6.4 浏览器扩展风险 237
 - 7.6.5 跨子域：document.domain技巧 240
 - 7.6.6 更多经典的跨域索引 245
 - 7.7 XSS Proxy技术 246
 - 7.7.1 浏览器<script>请求 247
 - 7.7.2 浏览器跨域AJAX请求 248
 - 7.7.3 服务端WebSocket推送指令 249
 - 7.7.4 postMessage方式推送指令 251
 - 7.8 真实案例剖析 254
 - 7.8.1 高级钓鱼攻击之百度空间登录DIV层钓鱼 254
 - 7.8.2 高级钓鱼攻击之Gmail正常服务钓鱼 261

- 7.8.3 人人网跨子域盗取MSN号 265
- 7.8.4 跨站获取更高权限 267
- 7.8.5 大规模XSS攻击思想 275
- 7.9 关于XSS利用框架 276
- 第8章 HTML5安全 277
- 8.1 新标签和新属性绕过黑名单策略 278
- 8.1.1 跨站中的黑名单策略 278
- 8.1.2 新元素突破黑名单策略 280
- 8.2 History API中的新方法 282
- 8.2.1 pushState()和replaceState() 282
- 8.2.2 短地址+History新方法=完美隐藏URL恶意代码 283
- 8.2.3 伪造历史记录 284
- 8.3 HTML5下的僵尸网络 285
- 8.3.1 Web Worker的使用 286
- 8.3.2 CORS向任意网站发送跨域请求 287
- 8.3.3 一个HTML5僵尸网络实例 287
- 8.4 地理定位暴露你的位置 290
- 8.4.1 隐私保护机制 290
- 8.4.2 通过XSS盗取地理位置 292
- 第9章 Web蠕虫 293
- 9.1 Web蠕虫思想 294
- 9.2 XSS蠕虫 295
- 9.2.1 原理+一个故事 295
- 9.2.2 危害性 297
- 9.2.3 SNS社区XSS蠕虫 300
- 9.2.4 简约且原生态的蠕虫 304
- 9.2.5 蠕虫需要追求原生态 305
- 9.3 CSRF蠕虫 307
- 9.3.1 关于原理和危害性 307
- 9.3.2 译言CSRF蠕虫 308
- 9.3.3 饭否CSRF蠕虫——邪恶的Flash游戏 314
- 9.3.4 CSRF蠕虫存在的可能性分析 320
- 9.4 ClickJacking蠕虫 324
- 9.4.1 ClickJacking蠕虫的由来 325
- 9.4.2 ClickJacking蠕虫技术原理分析 325
- 9.4.3 Facebook的LikeJacking蠕虫 327
- 9.4.4 GoogleReader的ShareJacking蠕虫 327
- 9.4.5 ClickJacking蠕虫爆发的可能性 335
- 第10章 关于防御 336
- 10.1 浏览器厂商的防御 336
- 10.1.1 HTTP响应的X-头部 337
- 10.1.2 迟到的CSP策略 338
- 10.2 Web厂商的防御 341
- 10.2.1 域分离 341
- 10.2.2 安全传输 342
- 10.2.3 安全的Cookie 343
- 10.2.4 优秀的验证码 343
- 10.2.5 慎防第三方内容 344
- 10.2.6 XSS防御方案 345
- 10.2.7 CSRF防御方案 348
- 10.2.8 界面操作劫持防御 353
- 10.3 用户的防御 357
- 10.4 邪恶的SNS社区 359
- • • • • [\(收起\)](#)

[Web前端黑客技术揭秘_下载链接1_](#)

标签

安全

web

信息安全

黑客

前端

计算机

前端开发

计算机-安全

评论

干货颇多，不过我前端知识太那啥，所以吸收有限。另外有多处明显校对错误。

书架上放了一年,暂时标记看完了... 部分代码太长不看 _(:3」 ∠)_

很详细介绍了XSS CSRF
点击劫持等前端安全知识，感想是前端圈真乱，各种猥琐思想得以得逞。好在标准组织、浏览器厂商都在致力于规范化，相信不久后这些漏洞都能从根本上得到解决。

项目间隙翻了一遍，期望过高，略失望，xss的奇技淫巧实在太多，书中所列案例均为样板，巧劲全无，反倒不如去看些xss bypass的文章有意思。

Web 开发必读

还凑合，基本算是重温了一遍

读了不到两章就停了，跟不上作者思路

这种东西我一直想学~却一直无处下手。。所以至今看看这种书，当时了解一下吧

余弦的书，前有基础后有例子，还需再读

还要不断实践！

行间距为什么这么大

文字功底奇差…各种 0day 失效…唉。

行间距太大，另外就是不太深刻吧，这个揭秘，让人很是搞不清楚这本书的定位。

好多熟悉的id...

结构混乱，大段排版没法看的代码，挺难受的。其实本书定位不是很明确，至少在书名上应指出“以攻防实例为主”的属性。对入门者而言，前两章和最后一章比较有参考价值，中间的就很难下咽了。

自己基础有点薄弱，好多看不下去

对于XSS理解的做了一些笔记

所谓前端，也就是浏览器端，也就是挂马，跨站

对于前端安全的介绍还是比较详细，但在如何去做防御上或如何去自动化检测安全漏洞上分析的还不够。书中也有很多实战的例子，可以借鉴，也正如作者所说的，主要还是思想的问题。

所有用户输入都是邪恶的。

[Web前端黑客技术揭秘_下载链接1](#)

书评

这本书本身的写作我自己并不满意，包括排版，里面的内容我尝试点破很多“渔”的东西，由于各种原因有些并没点好，这种写作实在太拘谨了，我估计看这本书的人不一定能跟好节奏，如果有时间，我想出本属于我自己风格的这类书。
无论怎样，我相信这本书还是可以给国内的读者带去...

在Web技术飞速演变、电子商务蓬勃发展的今天，企业开发的很多新应用程序都是Web应用程序，而且Web服务也被越来越频繁地用于集成Web应用程序或与其进行交互，这些趋势带来的问题就是web应用系统的安全风险达到了前所未有的高度，在安全缺陷被利用时可能会出现灾难性后果。 SQL...

正准备买纸书支持一下余弦大神，看多看阅读上也出了这本，还特价，顺手就买下了。总的来说，这本书是对做 Web 安全的来说，算是极好的入门读物了。不过其实因为Web的发展也就是最近几年才如此疯长，对应的 web 安全问题，本来是许多年没什么发展的，到现在问题才变得尤为重...

跑赢职场前端开发学院——上海前端开发培训、上海JS培训、上海DIV+CSS培训、上海HTML5培训学校
培训宣言：如果您愿意努力，愿意奋斗，我们期待您加入跑赢职场，给自己一个争取10万年薪的机会！
培训保障：2016年上海最新最全的前端开发课程特惠价格13800元【就业薪资低于8000. ..

[Web前端黑客技术揭秘_下载链接1](#)