

<<Web之困：现代Web应用安全指>>

图书基本信息

书名：<<Web之困：现代Web应用安全指南>>

13位ISBN编号：9787111439462

10位ISBN编号：7111439465

出版时间：2013-10

出版时间：机械工业出版社

作者：(美)Michal Zalewski

译者：朱筱丹

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：<http://www.tushu007.com>

<<Web之困：现代Web应用安全指>>

内容概要

《web之困：现代web应用安全指南》在web安全领域有“圣经”的美誉，在世界范围内被安全工作者和web从业人员广为称道，由来自google chrome浏览器团队的世界顶级黑客、国际一流安全专家撰写，是目前唯一深度探索现代web浏览器安全技术的专著。

本书从浏览器设计的角度切入，以探讨浏览器的各主要特性和由此衍生出来的各种安全相关问题为主线，深入剖析了现代web浏览器的技术原理、安全机制和设计上的安全缺陷，为web安全工作者和开发工程师们应对各种基于浏览器的安全隐患提供了应对措施。

作者简介

国际一流信息安全技术专家，被誉为IT安全领域最有影响力的11位黑客之一。曾发现过数以百计的网络安全漏洞，并发表了多篇具有重大影响的研究论文。对现代Web浏览器有非常深入的研究，目前就职于Google，基于其在Web安全方面的丰富经验帮助Google增强包括Chrome浏览器在内的一系列产品的安全性。此外，他还是一位开源软件贡献者，是著名开源软件p0f、skipfish、ratproxy等的开发者。

书籍目录

译者序

前言

第1章 web应用安全 / 1

1.1 信息安全速览 / 1

1.1.1 正统之道的尴尬 / 2

1.1.2 进入风险管理 / 4

1.1.3 分类学的启发 / 5

1.1.4 实际的解决之道 / 6

1.2 web的简明历史 / 7

1.2.1 史前时期的故事：1945 ~ 1994年 / 8

1.2.2 第一次浏览器大战：1995 ~ 1999年 / 10

1.2.3 平淡期：2000 ~ 2003年 / 11

1.2.4 web 2.0 和第二次浏览器大战：2004年之后 / 12

1.3 风险的演化 / 13

1.3.1 用户作为安全风险的一个环节 / 14

1.3.2 难以隔离的web运行环境 / 14

1.3.3 缺乏统一的格局 / 15

1.3.4 跨浏览器交互：失败的协同 / 16

1.3.5 客户端和服务端界限的日益模糊 / 17

第一部分 对web的解剖分析

第2章 一切从url开始 / 20

2.1 url的结构 / 21

2.1.1 协议名称 / 21

2.1.2 层级url的标记符号 / 22

2.1.3 访问资源的身份验证 / 22

2.1.4 服务器地址 / 23

2.1.5 服务器端口 / 24

2.1.6 层级的文件路径 / 24

2.1.7 查询字符串 / 25

2.1.8 片段id / 25

2.1.9 把所有的东西整合起来 / 26

2.2 保留字符和百分号编码 / 28

2.3 常见的url协议及功能 / 33

2.3.1 浏览器本身支持、与获取文档相关的协议 / 33

2.3.2 由第三方应用和插件支持的协议 / 33

2.3.3 未封装的伪协议 / 34

2.3.4 封装过的伪协议 / 34

2.3.5 关于协议检测部分的结语 / 35

2.4 相对url的解析 / 35

2.5 安全工程速查表 / 37

第3章 http协议 / 38

3.1 http 基本语法 / 39

3.1.1 支持http/0.9的恶果 / 40

3.1.2 换行处理带来的各种混乱 / 41

3.1.3 经过代理的http请求 / 42

- 3.1.4 对重复或有冲突的头域的解析 / 44
- 3.1.5 以分号作分隔符的头域值 / 45
- 3.1.6 头域里的字符集和编码策略 / 46
- 3.1.7 referer头域的表现 / 48
- 3.2 http 请求类型 / 48
 - 3.2.1 get / 49
 - 3.2.2 post / 49
 - 3.2.3 head / 49
 - 3.2.4 options / 50
 - 3.2.5 put / 50
 - 3.2.6 delete / 50
 - 3.2.7 trace / 50
 - 3.2.8 connect / 50
 - 3.2.9 其他 http 方法 / 51
- 3.3 服务器响应代码 / 51
- 3.4 持续会话 / 53
- 3.5 分段数据传输 / 55
- 3.6 缓存机制 / 55
- 3.7 http cookie 语义 / 57
- 3.8 http 认证 / 60
- 3.9 协议级别的加密和客户端证书 / 61
 - 3.9.1 扩展验证型证书 / 62
 - 3.9.2 出错处理的规则 / 63
- 3.10 安全工程速查表 / 64
- 第4章 html语言 / 65
 - 4.1 html文档背后的基本概念 / 66
 - 4.1.1 文档解析模式 / 67
 - 4.1.2 语义之争 / 68
 - 4.2 理解html解析器的行为 / 69
 - 4.2.1 多重标签之间的交互 / 70
 - 4.2.2 显式和隐式的条件判断 / 71
 - 4.2.3 html解析的生存建议 / 71
 - 4.3 html实体编码 / 72
 - 4.4 http/html 交互语义 / 73
 - 4.5 超链接和内容包含 / 75
 - 4.5.1 单纯的链接 / 75
 - 4.5.2 表单和表单触发的请求 / 75
 - 4.5.3 框架 / 77
 - 4.5.4 特定类型的内容包含 / 78
 - 4.5.5 关于跨站请求伪造 / 80
 - 4.6 安全工程速查表 / 81
- 第5章 层叠样式表 / 83
 - 5.1 css基本语法 / 84
 - 5.1.1 属性定义 / 85
 - 5.1.2 @ 指令和xml绑定 / 85
 - 5.1.3 与html的交互 / 86
 - 5.2 重新同步的风险 / 86

- 5.3 字符编码 / 87
- 5.4 安全工程速查表 / 89
- 第6章 浏览器端脚本 / 90
 - 6.1 javascript的基本特点 / 91
 - 6.1.1 脚本处理模型 / 92
 - 6.1.2 执行顺序的控制 / 95
 - 6.1.3 代码和对象检视功能 / 96
 - 6.1.4 修改运行环境 / 97
 - 6.1.5 javascript 对象表示法 (json) 和其他数据序列化 / 99
 - 6.1.6 e4x和其他语法扩展 / 101
 - 6.2 标准对象层级 / 102
 - 6.2.1 文档对象模型 / 104
 - 6.2.2 对其他文档的访问 / 106
 - 6.3 脚本字符编码 / 107
 - 6.4 代码包含模式和嵌入风险 / 108
 - 6.5 活死人：visual basic / 109
 - 6.6 安全工程速查表 / 110
- 第7章 非html类型文档 / 112
 - 7.1 纯文本文件 / 112
 - 7.2 位图图片 / 113
 - 7.3 音频与视频 / 114
 - 7.4 各种xml文件 / 114
 - 7.4.1 常规xml视图效果 / 115
 - 7.4.2 可缩放向量图片 / 116
 - 7.4.3 数学标记语言 / 117
 - 7.4.4 xml用户界面语言 / 117
 - 7.4.5 无线标记语言 / 118
 - 7.4.6 rss 和 atom订阅源 / 118
 - 7.5 关于不可显示的文件类型 / 119
 - 7.6 安全工程速查表 / 120
- 第8章 浏览器插件产生的内容 / 121
 - 8.1 对插件的调用 / 122
 - 8.2 文档显示帮助程序 / 124
 - 8.3 插件的各种应用框架 / 125
 - 8.3.1 adobe flash / 126
 - 8.3.2 microsoft silverlight / 128
 - 8.3.3 sun java / 129
 - 8.3.4 xml browser applications / 129
 - 8.4 activex controls / 130
 - 8.5 其他插件的情况 / 131
 - 8.6 安全工程速查表 / 132
- 第二部分 浏览器安全特性
- 第9章 内容隔离逻辑 / 134
 - 9.1 dom的同源策略 / 135
 - 9.1.1 document.domain / 136
 - 9.1.2 postmessage(...) / 137
 - 9.1.3 与浏览器身份验证的交互 / 138

- 9.2 xmlhttprequest的同源策略 / 139
- 9.3 web storage 的同源策略 / 141
- 9.4 cookies 的安全策略 / 142
 - 9.4.1 cookie对同源策略的影响 / 144
 - 9.4.2 域名限制带来的问题 / 145
 - 9.4.3 localhost带来的非一般风险 / 145
 - 9.4.4 cookie与“合法”dns劫持 / 146
- 9.5 插件的安全规则 / 147
 - 9.5.1 adobe flash / 148
 - 9.5.2 microsoft silverlight / 151
 - 9.5.3 java / 151
- 9.6 如何处理格式含糊或意想不到的源信息 / 152
 - 9.6.1 ip 地址 / 153
 - 9.6.2 主机名里有额外的点号 / 153
 - 9.6.3 不完整的主机名 / 153
 - 9.6.4 本地文件 / 154
 - 9.6.5 伪url / 155
 - 9.6.6 浏览器扩展和用户界面 / 155
- 9.7 源的其他应用 / 156
- 9.8 安全工程速查表 / 157
- 第10章 源的继承 / 158
 - 10.1 about:blank页面的源继承 / 158
 - 10.2 data: url的继承 / 160
 - 10.3 javascript:和vbscript: url对源的继承 / 162
 - 10.4 关于受限伪url的一些补充 / 163
 - 10.5 安全工程速查表 / 164
- 第11章 同源策略之外的世界 / 165
 - 11.1 窗口和框架的交互 / 166
 - 11.1.1 改变现有页面的地址 / 166
 - 11.1.2 不请自来的框架 / 170
 - 11.2 跨域内容包含 / 172
 - 11.3 与隐私相关的副作用 / 175
 - 11.4 其他的同源漏洞和应用 / 177
 - 11.5 安全工程速查表 / 178
- 第12章 其他的安全边界 / 179
 - 12.1 跳转到敏感协议 / 179
 - 12.2 访问内部网络 / 180
 - 12.3 禁用的端口 / 182
 - 12.4 对第三方cookie的限制 / 184
 - 12.5 安全工程速查表 / 186
- 第13章 内容识别机制 / 187
 - 13.1 文档类型检测的逻辑 / 188
 - 13.1.1 格式错误的mime type写法 / 189
 - 13.1.2 特殊的 content-type 值 / 189
 - 13.1.3 无法识别的content type类型 / 191
 - 13.1.4 防御性使用content-disposition / 193
 - 13.1.5 子资源的内容设置 / 194

- 13.1.6 文件下载和其他非http内容 / 194
- 13.2 字符集处理 / 196
 - 13.2.1 字节顺序标记 / 198
 - 13.2.2 字符集继承和覆盖 / 199
 - 13.2.3 通过html代码设置子资源字符集 / 199
 - 13.2.4 非http 文件的编码检测 / 201
- 13.3 安全工程速查表 / 202
- 第14章 应对恶意脚本 / 203
 - 14.1 拒绝服务攻击 / 204
 - 14.1.1 执行时间和内存使用的限制 / 205
 - 14.1.2 连接限制 / 205
 - 14.1.3 过滤弹出窗口 / 206
 - 14.1.4 对话框的使用限制 / 208
 - 14.2 窗口定位和外观问题 / 209
 - 14.3 用户界面的时差攻击 / 211
 - 14.4 安全工程速查表 / 214
- 第15章 外围的网站特权 / 215
 - 15.1 浏览器和托管插件的站点权限 / 216
 - 15.2 表单密码管理 / 217
 - 15.3 ie浏览器的区域模型 / 219
 - 15.4 安全工程速查表 / 222
- 第三部分 浏览器安全机制的未来趋势
- 第16章 新的浏览器安全特性与未来展望 / 224
 - 16.1 安全模型扩展框架 / 224
 - 16.1.1 跨域请求 / 225
 - 16.1.2 xdomainrequest / 228
 - 16.1.3 origin 请求头的其他应用 / 229
 - 16.2 安全模型限制框架 / 230
 - 16.2.1 内容安全策略 / 230
 - 16.2.2 沙盒框架 / 234
 - 16.2.3 严格传输安全 / 236
 - 16.2.4 隐私浏览模式 / 237
 - 16.3 其他的一些进展 / 237
 - 16.3.1 浏览器内置的html净化器 / 238
 - 16.3.2 xss 过滤 / 239
 - 16.4 安全工程速查表 / 240
- 第17章 其他值得注意的浏览器机制 / 241
 - 17.1 url级别和协议级别的提议 / 241
 - 17.2 内容相关的特性 / 243
 - 17.3 i/o接口 / 245
- 第18章 常见的web安全漏洞 / 246
 - 18.1 与web应用相关的漏洞 / 246
 - 18.2 web应用设计时应谨记的问题 / 248
 - 18.3 服务器端的常见问题 / 250
- 后记 / 252
- 注释 / 254

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:<http://www.tushu007.com>