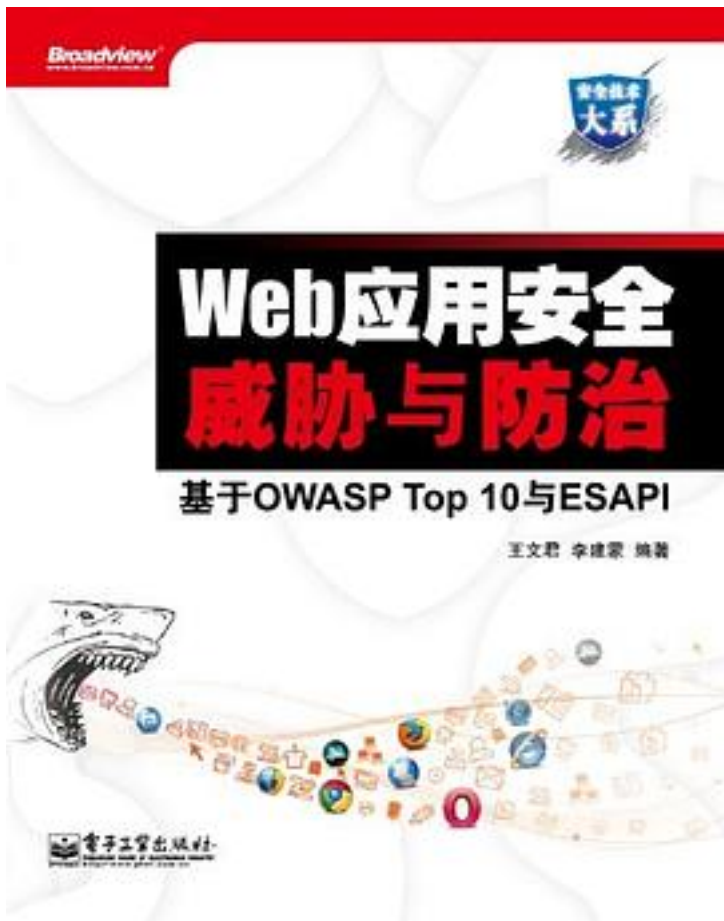


Web应用安全威胁与防治



[Web应用安全威胁与防治_下载链接1](#)

著者:王文君

出版者:电子工业出版社

出版时间:2013-1

装帧:平装

isbn:9787121188572

本书是一本讲解Web应用中最常见的安全风险以及解决方案的实用教材。它以当今公认的安全权威机构OWASP（Open Web Application Security Project）制定的OWASP Top 10为蓝本，介绍了十项最严重的Web应用程序安全风险，并利用ESAPI（Enterprise Security

API) 提出了解决方案。本书共有五篇, 第1篇通过几个故事引领读者进入安全的世界; 第2篇是基础知识篇, 读者可以了解基本的Web应用安全的技术和知识; 第3篇介绍了常用的安全测试和扫描工具; 第4篇介绍了各种威胁以及测试和解决方案; 第5篇在前几篇的基础上, 总结在设计和编码过程中的安全原则。

本书各章以一个生动的小故事或者实例开头, 让读者快速了解其中的安全问题, 然后分析其产生的原因和测试方法并提出有效的解决方案, 最后列出处理相关问题的检查列表, 帮助读者在以后的工作和学习中更好地理解 and 处理类似的问题。读完本书之后, 相信读者可以将学过的内容应用到Web应用安全设计、开发、测试中, 提高Web应用程序的安全, 也可以很有信心地向客户熟练地讲解Web应用安全威胁和攻防, 并在自己的事业发展中有更多的收获。

本书适用于Web开发人员、设计人员、测试人员、架构师、项目经理、安全咨询顾问等。本书也可以作为对Web应用安全有兴趣的高校学生的教材, 是一本实用的讲解Web应用安全的教材和使用手册。

作者介绍:

王文君, 2007年加入惠普软件从事软件开发、软件安全分析以及手机开发等工作。现为OWASP中国上海地区负责人之一, 并于2011年被OWASP邀请参加OWASP亚洲峰会, 作为演讲嘉宾和培训讲师, 拥有CISSP、PMP、ITIL认证, 2012年被评为HP Global Software Star。王文君于2002年毕业于上海交通大学, 拥有电力工程硕士学位以及电力工程和涉外会计双学士学位。

李建蒙, 2004年从日本回国之后。加入华为技术有限公司。开发移动通信平台。2006年加入思科, 从事在线应用产品的后台开发和应用安全领域的工作, 有丰富的多平台多语言开发、渗透测试和安全开发经验。曾于2011年被OWASP邀请作为OWASP亚洲峰会的演讲嘉宾和培训讲师。

目录: 第1篇 引子

故事一: 家有一IT, 如有一宝 2

故事二: 微博上的蠕虫 3

故事三: 明文密码 5

故事四: IT青年VS禅师 5

第2篇 基础篇

第1章 Web应用技术 8

1.1 HTTP简介 8

1.2 HTTPS简介 10

1.3 URI 11

1.3.1 URL 11

1.3.2 URI/URL/URN 12

1.3.3 URI比较 13

1.4 HTTP消息 13

1.4.1 HTTP方法 14

1.4.2 HTTP状态码 19

1.5 HTTP Cookie 20

1.5.1 HTTP Cookie的作用 22

1.5.2 HTTP Cookie的缺点 23

1.6 HTTP session 23

1.7 HTTP的安全 24

第2章 OWASP 27

2.1 OWASP简介	27
2.2 OWASP风险评估方法	28
2.3 OWASP Top 10	34
2.4 ESAPI (Enterprise Security API)	35
第3篇 工具篇	
第3章 Web服务器工具简介	38
3.1 Apache	38
3.2 其他Web服务器	39
第4章 Web浏览器以及调试工具	42
4.1 浏览器简介	42
4.1.1 基本功能	42
4.1.2 主流浏览器	43
4.1.3 浏览器内核	44
4.2 开发调试工具	45
第5章 渗透测试工具	47
5.1 Fiddler	47
5.1.1 工作原理	47
5.1.2 如何捕捉HTTPS会话	48
5.1.3 Fiddler功能介绍	49
5.1.4 Fiddler扩展功能	56
5.1.5 Fiddler第三方扩展功能	56
5.2 ZAP	58
5.2.1 断点调试	60
5.2.2 编码/解码	61
5.2.3 主动扫描	62
5.2.4 Spider	63
5.2.5 暴力破解	64
5.2.6 端口扫描	65
5.2.7 Fuzzer	66
5.2.8 API	66
5.3 WebScrab	67
5.3.1 HTTP代理	67
5.3.2 Manual Request	69
5.3.3 Spider	70
5.3.4 Session ID分析	71
5.3.5 Bean Shell的支持	71
5.3.6 Web编码和解码	73
第6章 扫描工具简介	74
6.1 万能的扫描工具——WebInspect	74
6.1.1 引言	74
6.1.2 WebInspect特性	74
6.1.3 环境准备	74
6.1.4 HP WebInspect总览	76
6.1.5 Web网站测试	79
6.1.6 企业测试	86
6.1.7 生成报告	88
6.2 开源扫描工具——w3af	91
6.2.1 w3af概述	91
6.2.2 w3af环境配置	92
6.2.3 w3af使用示例	93
6.3 被动扫描的利器——Ratproxy	94
6.3.1 Ratproxy概述	94
6.3.2 Ratproxy环境配置	95
6.3.3 Ratproxy运行	96

第7章 漏洞学习网站	98
7.1 WebGoat	98
7.2 DVWA	99
7.3 其他的漏洞学习网站	99
第4篇 攻防篇	
第8章 代码注入	102
8.1 注入的分类	104
8.1.1 OS命令注入	104
8.1.2 XPath注入	109
8.1.3 LDAP注入	114
8.1.4 SQL注入	118
8.1.5 JSON注入	131
8.1.6 URL参数注入	133
8.2 OWASP ESAPI与注入问题的预防	135
8.2.1 命令注入的ESAPI预防	135
8.2.2 XPath注入的ESAPI预防	138
8.2.3 LDAP注入的ESAPI预防	138
8.2.4 SQL注入的ESAPI预防	141
8.2.5 其他注入的ESAPI预防	143
8.3 注入预防检查列表	143
8.4 小结	144
第9章 跨站脚本 (XSS)	146
9.1 XSS简介	146
9.2 XSS分类	146
9.2.1 反射式XSS	146
9.2.2 存储式XSS	148
9.2.3 基于DOM的XSS	149
9.2.4 XSS另一种分类法	151
9.3 XSS危害	154
9.4 XSS检测	156
9.4.1 手动检测	156
9.4.2 半自动检测	158
9.4.3 全自动检测	158
9.5 XSS的预防	159
9.5.1 一刀切	159
9.5.2 在服务器端预防	160
9.5.3 在客户端预防	168
9.5.4 富文本框的XSS预防措施	170
9.5.5 CSS	172
9.5.6 FreeMarker	174
9.5.7 OWASP ESAPI与XSS的预防	177
9.6 XSS检查列表	183
9.7 小结	184
第10章 失效的身份认证和会话管理	185
10.1 身份认证和会话管理简介	185
10.2 谁动了我的琴弦——会话劫持	186
10.3 请君入瓮——会话固定	188
10.4 我很含蓄——非直接会话攻击	191
10.5 如何测试	199
10.5.1 会话固定测试	199
10.5.2 用Web Scraper分析会话ID	200
10.6 如何预防会话攻击	202
10.6.1 如何防治固定会话	202
10.6.2 保护你的会话令牌	204

10.7 身份验证	208
10.7.1 双因子认证流程图	209
10.7.2 双因子认证原理说明	210
10.7.3 隐藏在QR Code里的秘密	211
10.7.4 如何在服务器端实现双因子认证	212
10.7.5 我没有智能手机怎么办	216
10.8 身份认证设计的基本准则	216
10.8.1 密码长度和复杂性策略	216
10.8.2 实现一个安全的密码恢复策略	217
10.8.3 重要的操作应通过HTTPS传输	217
10.8.4 认证错误信息以及账户锁定	219
10.9 检查列表	219
10.9.1 身份验证和密码管理检查列表	219
10.9.2 会话管理检查列表	220
10.10 小结	221
第11章 不安全的直接对象引用	222
11.1 坐二望三——直接对象引用	222
11.2 不安全直接对象引用的危害	224
11.3 其他可能的不安全直接对象引用	224
11.4 不安全直接对象引用的预防	225
11.5 如何使用OWASP ESAPI预防	227
11.6 直接对象引用检查列表	230
11.7 小结	230
第12章 跨站请求伪造 (CSRF)	232
12.1 CSRF简介	232
12.2 谁动了我的奶酪	232
12.3 跨站请求伪造的攻击原理	233
12.4 剥茧抽丝见真相	235
12.5 其他可能的攻击场景	236
12.5.1 家用路由器被CSRF攻击	236
12.5.2 别以为用POST你就躲过了CSRF	238
12.5.3 写一个自己的CSRF Redirector	241
12.5.4 利用重定向欺骗老实人	243
12.6 跨站请求伪造的检测	245
12.6.1 手工检测	245
12.6.2 半自动CSRFTester	246
12.7 跨站请求伪造的预防	250
12.7.1 用户需要知道的一些小技巧	250
12.7.2 增加一些确认操作	250
12.7.3 重新认证	250
12.7.4 加入验证码 (CAPTCHA)	250
12.7.5 ESAPI解决CSRF	250
12.7.6 CSRFGuard	256
12.8 CSRF检查列表	260
12.9 小结	261
第13章 安全配置错误	262
13.1 不能说的秘密——Google hacking	262
13.2 Tomcat那些事	264
13.3 安全配置错误的检测与预防	264
13.3.1 系统配置	264
13.3.2 Web应用服务器的配置	268
13.3.3 数据库	282
13.3.4 日志配置	284
13.3.5 协议	285

13.3.6 开发相关的安全配置	291
13.3.7 编译器的安全配置	302
13.4 安全配置检查列表	305
13.5 小结	307
第14章 不安全的加密存储	308
14.1 关于加密	310
14.1.1 加密算法简介	310
14.1.2 加密算法作用	312
14.1.3 加密分类	313
14.2 加密数据分类	314
14.3 加密数据保护	315
14.3.1 密码的存储与保护	315
14.3.2 重要信息的保护	323
14.3.3 密钥的管理	336
14.3.4 数据的完整性	339
14.3.5 云系统存储安全	342
14.3.6 数据保护的常犯错误	343
14.4 如何检测加密存储数据的安全性	344
14.4.1 审查加密内容	344
14.4.2 已知答案测试 (Known Answer Test)	344
14.4.3 自发明加密算法的检测	345
14.4.4 AES加密算法的测试	345
14.4.5 代码审查	346
14.5 如何预防不安全的加密存储的数据	347
14.6 OWASP ESAPI与加密存储	348
14.6.1 OWASP ESAPI与随机数	353
14.6.2 OWASP ESAPI 与FIPS 140-2	354
14.7 加密存储检查列表	355
14.8 小结	355
第15章 没有限制的URL访问	357
15.1 掩耳盗铃——隐藏 (Disable) 页面按钮	357
15.2 权限认证模型	358
15.2.1 自主型访问控制	360
15.2.2 强制型访问控制	360
15.2.3 基于角色的访问控制	361
15.3 绕过认证	363
15.3.1 网络嗅探	364
15.3.2 默认或者可猜测用户账号	364
15.3.3 直接访问内部URL	364
15.3.4 修改参数绕过认证	365
15.3.5 可预测的SessionID	365
15.3.6 注入问题	365
15.3.7 CSRF	365
15.3.8 绕过认证小结	366
15.4 绕过授权验证	367
15.4.1 水平越权	368
15.4.2 垂直越权	369
15.5 文件上传与下载	373
15.5.1 文件上传	373
15.5.2 文件下载和路径遍历	377
15.6 静态资源	382
15.7 后台组件之间的认证	383
15.8 SSO	385
15.9 OWASP ESAPI与授权	386

- 15.9.1 AccessController的实现 387
- 15.9.2 一个AccessController的代码示例 390
- 15.9.3 我们还需要做些什么 391
- 15.10 访问控制检查列表 393
- 15.11 小结 393
- 第16章 传输层保护不足 395
- 16.1 卧底的故事——对称加密和非对称加密 395
- 16.2 明文传输问题 396
- 16.3 有什么危害 398
- 16.3.1 会话劫持 398
- 16.3.2 中间人攻击 399
- 16.4 预防措施 399
- 16.4.1 密钥交换算法 400
- 16.4.2 对称加密和非对称加密结合 401
- 16.4.3 SSL/TLS 406
- 16.5 检查列表 423
- 16.6 小结 423
- 第17章 未验证的重定向和转发 425
- 17.1 三角借贷的故事——转发和重定向 425
- 17.1.1 URL转发 425
- 17.1.2 URL重定向 426
- 17.1.3 转发与重定向的区别 429
- 17.1.4 URL 重定向的实现方式 430
- 17.2 危害 438
- 17.3 如何检测 439
- 17.4 如何预防 440
- 17.4.1 OWASP ESAPI与预防 441
- 17.5 重定向和转发检查列表 443
- 17.6 小结 443
- 第5篇 安全设计、编码十大原则
- 第18章 安全设计十大原则 448
- 设计原则1——简单易懂 448
- 设计原则2——最小特权 448
- 设计原则3——故障安全化 450
- 设计原则4——保护最薄弱环节 451
- 设计原则5——提供深度防御 452
- 设计原则6——分隔 453
- 设计原则7——总体调节 454
- 设计原则8——默认不信任 454
- 设计原则9——保护隐私 455
- 设计原则10——公开设计，不要假设隐藏秘密就是安全 455
- 第19章 安全编码十大原则 457
- 编码原则1——保持简单 457
- 编码原则2——验证输入 458
- 编码原则3——注意编译器告警 459
- 编码原则4——框架和设计要符合安全策略 459
- 编码原则5——默认拒绝 460
- 编码原则6——坚持最小权限原则 462
- 编码原则7——净化发送到其他系统的数据 463
- 编码原则8——深度预防 464
- 编码原则9——使用有效的质量保证技术 464
- 编码原则10——采用一个安全编码规范 465

• • • • • ([收起](#))

标签

安全

Web开发

Web安全测试

网络安全

OWASP

web

计算机

网络

评论

中国话的OWASP

做毕设时候看的书 理论帮助比较大 涵盖的东西也比较全面

覆盖面很全

与《白帽子》搭配看，实践加理论，实在！

书里面的ESAPI方法貌似有错误，我使用的是2.0版本。建议小心使用。

[Web应用安全威胁与防治_下载链接1](#)

书评

[Web应用安全威胁与防治_下载链接1](#)