

《Web应用安全威胁与防治》

图书基本信息

书名：《Web应用安全威胁与防治》

13位ISBN编号：9787121188572

10位ISBN编号：7121188570

出版时间：2013-1

出版社：电子工业出版社

作者：王文君,李建蒙

页数：466

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

《Web应用安全威胁与防治》

前言

序1 随着社交网络、微博等一系列新型的互联网产品的诞生，尤其是Web 2.0技术的推广，基于Web环境的面向普通终端用户的互联网应用越来越广泛。在企业界，随着企业信息化的不断深入，各种服务于企业的应用都架设在Web平台上。Web业务的迅速发展把越来越多的个人和企业的敏感数据通过Web展现给用户。这引起黑客们的强烈关注，他们跃跃欲试，利用网站操作系统的漏洞和Web服务程序的SQL注入等漏洞得到Web服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据。更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。这些也使得越来越多的用户关注应用层的安全问题，业界对Web应用安全的关注度也逐渐升温。目前很多业务都依赖于互联网，如网上银行、网络购物、网游等，很多恶意攻击者会对Web服务器进行攻击，想方设法通过各种手段获取他人的个人账户信息以谋取利益。正是因为这样，Web业务平台非常容易遭受攻击。为了防止黑客的攻击，除了对Web服务器做相应的配置外，Web应用程序的设计和开发也需要杜绝黑客攻击的隐患。本书有针对性地面向广大Web应用程序员提供了系统的安全设计原则和编程技巧。作为应用程序员，你可能非常熟悉你所负责的业务逻辑，你也一定精通几种编程语言和数据库。但是，就我所接触的程序员来说，很少有懂得怎样在编程中避免留下安全漏洞的。对于产品架构师，很多产品在其设计之时没有考虑系统的安全问题，没有相应的安全标准。请仔细阅读本书，本书为你的Web产品提供了一个可行的安全标准，同时也为你提供了系统的针对各种安全漏洞的行之有效的编程技巧。

作者之一的王文君是我领导的惠普软件PPM产品研发团队的安全架构师。他将OWASP Top 10应用于PPM，使之成为该企业级产品的安全标准。事实证明，OWASP Top 10及相应的ESAPI有效地满足了用户对该产品安全方面的苛刻要求。不久前，我们的产品通过了我们的客户之一某国防部的安全攻击测试。所以，我极力将本书推荐给你。你将会有针对性地在你的程序里满足安全性要求，对于潜在的安全隐患，你将有足够的智慧和手段去解决它。 李维纲 惠普软件部研发团队经理

《Web应用安全威胁与防治》

内容概要

容提要

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和处理类似的问题。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。

《Web应用安全威胁与防治》

作者简介

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。

书籍目录

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 Scrab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	坐二望一——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

章节摘录

版权页：插图：第一种，明文存储。这种方法是最不安全的一种，系统的管理员可以直接看到所有用户的密码明文，而且，一旦有SQL注入攻击，攻击者也可以直接拿到明文。前面说的CSDN遭受攻击之后，密码泄露，主要是有些用户的密码是明文存储的。第二种，密码经过对称转换后存储。这种方法是编写一个对称的转换算法，密码经过转换后，看起来和原来的密码完全不一样，但是，这种存储方法和第一种直接存储明文在本质上是相似的，只要知道转换方法，也就能知道如何将密文转换为明文。即使不知道转换方法，通过尝试和猜测，也可以逐步找到转换的规律，进而可以根据密文推导出明文，达到破解的目的。第三种，对称加密之后存储。对于对称加密存储，用户加密和解密来说，则需要加密的密钥，那么，对于密钥的保护，就和对密码的保护一样重要，一旦密钥泄露，则所有的密码也就都处于危险的境地。而且，密钥可能事先配置好或者直接写在代码里了，这样一旦负责维护的员工因为对公司不满而离开，很有可能导致密钥泄露，导致破解的可能性很大，Skype就曾经被揭露密钥写在代码里，导致产品的安全性大大降低。而且，系统管理员或者系统的维护人员很有可能获得这些密钥，也就能很容易地把密码的原文算出来。所以，对称加密之后存储密码，需要加强对密钥的管理，而且一旦密钥泄露，切换密钥也可能导致兼容问题。第四种，非对称加密后存储。虽然使用对称加密算法，但是由于密码经过公钥加密，需要私钥才能解密，那么，私钥的安全性就变得和密码的安全性一样重要，只有保证私钥的安全，才能够保证密码的安全。但是，使用非对称加密算法仍然需要管理密钥，而且非对称加密算法的效率也很低。以上四种方法，都有一个共同的特点，就是密码都可以从加密的存储形式还原到明文。像前面所说的，如果需要通过注册的邮箱找回原来的密码，那么肯定要用到以上四种方法中的一种。但是需要铭记的是：既然通过注册的邮箱可以找回密码，那么，网站的工作人员或者管理员也就有办法通过查看配置的密钥，然后解密得到明文。这对于一些对安全性要求很高的政府或者企业是不允许的。以上介绍的几种密码的存储方法的共同弱点就是密码是可逆的，系统有可能还原得到明文，所以，最好的保存密码的方法是以连系统都不可能还原明文的方式保存，也就是用哈希算法的单向性保证服务器端保存的是哈希之后的哈希值，从而系统就不可能知道密码的明文。使用哈希算法也有几种方式，如下所示。第一种，使用MD5和SHA-1哈希之后存储。MD5和SHA-1已经被破解，这意味着虽然不能通过逆运算还原密码原文，但很容易找到一个能生成相同哈希值的密码原文的碰撞，例如，密码是12345678，通过计算，可以得到abcdefgh的哈希值和12345678的哈希值一样，那么，输入密码时，输入12345678和abcdefgh都可以登录。还有一点，这两个算法相对速度比较快，这就意味着对暴力破解来说消耗的资源少，所消耗的时间也短。所以强烈建议不要使用这两个算法。第二种，使用更安全的SHA256算法。这在一定程度上降低或者杜绝了碰撞率，也增加了暴力破解的成本。但是，一般的密码输入的长度都是8个字符左右，有的用户为了容易记忆使用更短的密码，这样通过常用密码字典，就可以很快得到密码原文。所以，单纯地只是用SHA256这样的比较安全的哈希算法还是有一定风险的。第三种，使用加入盐(Salt)的SHA256算法。将密码原文和随机生成的盐字符串混淆，进行哈希，存储哈希之后的值以及盐。在密码验证的时候，只需要用同样的算法，把密码原文和盐再做一次同样的哈希，与存储的哈希值比较就可以验证密码了。建议使用的盐最少是8个字节，而且是随机的字符串，这样密码和盐的组合值就成为了一个不同寻常的字符串，密码字典很难构造这么巨大的字典，就可以增加密码字典破解的成本，甚至使之不可能。盐的长度越长，暴力破解的难度就越大，也限制了彩虹表的效力。随着机器硬件的更新以及性能的不断提高，暴力破解的速度也得到提高，为了应对日益提高的硬件速度，可以通过将具体的哈希进行若干次迭代，如SHA256(...SHA256(salt, SHA256(salt, password))，这样，就可以增加暴力破解的难度。即使被暴力破解了，得到的也只是随机的盐和密码混淆之后的值，如果需要恢复密码原文，仍然需要进一步努力得到哪些是盐，然后才能得到密码，虽然这对一些资深的攻击者并不难，但这总是要花他们一些时间的。

《Web应用安全威胁与防治》

媒体关注与评论

这是一本带点酷酷的工程师范儿和人文气质的“硬货”。作为一名资深IT文艺老人，特别喜欢这种带着思想气息却又有着丰富案例娓娓道来的实用信息安全书，过去却往往只在国外作者中读到。正如书中开头的引子说的那样：“家有IT，如有一宝”。那么在Web安全日益火爆的今天，你会不会在读完这本书后的未来也成为传说中让我们顶礼膜拜的大牛呢^-^ ——IDF威慑防御实验室益云（公益互联网）社会创新中心联合创始人万涛@黑客老鹰

伴随互联网的高速发展，基于B/S架构的业务系统对安全要求越来越高，安全从业人员面临空前的压力。如何让安全从业人员快速掌握Web应用安全？本书以诙谐、幽默的语言，精彩、丰富的实例，帮助安全从业人员从端到端理解Web应用安全。不失为近几年Web应用安全书籍的上佳之作。 ——OWASP中国区主席SecZone高级安全顾问 RIP

很乐意看到有人将自身的资深安全积累和OWASP的最佳实践出版成书，内容严谨细致却不乏生动。这本信息安全领域的实用手册将成为银基安全致力于互联网安全的参考指导书目之一，我们广泛的电信、银行、保险、证券和政府部门等客户都会从中受益。 ——上海银基信息技术有限公司首席技术官胡绍勇（Kurau）

随着安全访问控制策略ACL的普及应用，互联网企业目前面临的安全风险面主要集中在Web服务层。其中Web应用系统在架构设计、开发编码过程中是安全漏洞和风险引入的主要阶段，而普遍地我们的架构、开发、测试岗位在安全技能与意识上恰恰是相对比较欠缺的。本书详细介绍了Web安全基础知识、测试平台与方法，常见漏洞形式与原理，并结合OWASP最佳实践经验给出预防建议、设计和编码原则等。书中举例生动形象，图文代码并茂，步骤归纳清晰。特别推荐给广大Web开发、测试、安全岗位的朋友们。 ——中国金山软件集团信息安全负责人程冲

在网络攻击愈加复杂，手段日益翻新的今天，Web攻击依然是大多数攻击者首选的入侵手段。反思CSDN泄密及新浪微博蠕虫事件，Web应用的安全突显其重要性。OWASP作为全球领先的Web应用安全研究团队，透过本书将Web应用安全的威胁、防御以及相关的工具进行了详细的探讨和研究。详尽的操作步骤说明是本书的亮点之一，这些详实且图文并茂的内容为逐步深入学习Web应用安全提供了很好的帮助。我衷心希望这本书能够成为信息安全专业的在校生以及应用安全相关从业人员的学习指导书。 ——上海交通大学信息安全工程学院施勇（CISSP CISA）

《Web应用安全威胁与防治》

名人推荐

这是一本带点酷酷的工程师范儿和人文气质的“硬货”。作为一名资深IT文艺老人，特别喜欢这种带着思想气息却又有着丰富案例娓娓道来的实用信息安全书，过去却往往只在国外作者中读到。正如书中开头的引子说的那样：“家有IT，如有一宝”。那么在Web安全日益火爆的今天，你会不会在读完这本书后的未来也成为传说中让我们顶礼膜拜的大牛呢。——IDF威慑防御实验室益云（公益互联网）社会创新中心联合创始人 万涛@黑客老鹰 伴随互联网的高速发展，基于B/S架构的业务系统对安全要求越来越高，安全从业人员面临空前的压力。如何让安全从业人员快速掌握Web应用安全？本书以诙谐、幽默的语言，精彩、丰富的实例，帮助安全从业人员从端到端理解Web应用安全。不失为近几年Web应用安全书籍的上佳之作。——OWASP中国区主席SecZone高级安全顾问 RIP 很乐意看到有人将自身的资深安全积累和OWASP的最佳实践出版成书，内容严谨细致却不乏生动。这本信息安全领域的实用手册将成为银基安全致力于互联网安全的参考指导书目之一，我们广泛的电信、银行、保险、证券和政府部门等客户都会从中受益。——上海银基信息技术有限公司首席技术官 胡绍勇（Kurau）随着安全访问控制策略ACL的普及应用，互联网企业目前面临的安全风险面主要集中在Web服务层。其中Web应用系统在架构设计、开发编码过程中是安全漏洞和风险引入的主要阶段，而普遍地我们的架构、开发、测试岗位在安全技能与意识上恰恰是相对比较欠缺的。本书详细介绍了Web安全基础知识、测试平台与方法，常见漏洞形式与原理，并结合OWASP最佳实践经验给出预防建议、设计和编码原则等。书中举例生动形象，图文代码并茂，步骤归纳清晰。特别推荐给广大Web开发、测试、安全岗位的朋友们。——中国金山软件集团信息安全负责人 程冲 在网络攻击愈加复杂，手段日益翻新的今天，Web攻击依然是大多数攻击者首选的入侵手段。反思CSDN泄密及新浪微博蠕虫事件，Web应用的安全突显其重要性。OWASP作为全球领先的Web应用安全研究团队，透过本书将Web应用安全的威胁、防御以及相关的工具进行了详细的探讨和研究。详尽的操作步骤说明是本书的亮点之一，这些详实且图文并茂的内容为逐步深入学习Web应用安全提供了很好的帮助。我衷心希望这本书能够成为信息安全专业的在校生以及应用安全相关从业人员的学习指导书。——上海交通大学信息安全工程学院 施勇（CISSP CISA）

《Web应用安全威胁与防治》

精彩短评

- 1、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
- 2、不错，正在看。总体不敢说好坏
- 3、很好，一直想买，终于到手了！
- 4、中国话的OWASP
- 5、关于TOP 10介绍的很详细！值得一看！
- 6、这本书写的尚可，入门后不久的朋友可以买来看看。本书更类似于学习笔记倾向的读物，因为写的略微有点散，且不深入，。买这本书的时候最希望看到的是作者以淘宝安全专家的身份写一些目前常见的攻击手法在时间中出现的比率以及危害等、淘宝、csdn这些商业网站常遇到的攻击问题等等，还有一个是目前中小网站在经济能力有限的情况下如何做好安全工作等。结果都没有，虽然本书有深度但是不深入，有宽度但是不够宽。中规中矩的一本书，对照着做做试验，热身下看看也就还好。给四星，建议在书店看下再考虑购买。还有就是OWASP是个好站点，里面有针对语言方面编程需要注意的事项，都是与网站安全有关的。最重要的是该站点其中将Python语言单独列出作为一项，这对于Python编程人员来说是个福音。其他语言或者演示的也可以看看，与语言自身有关的安全问题只是一小部分，大多数是来自于语言之外的软硬件环境有关的安全注意事项。
- 7、以前在学校图书馆就看这个，现在收藏一本
- 8、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。
- 9、没怎么看 品质不错
- 10、挺好的书，赶紧买，超值！
- 11、作为入门级书不错，这个你懂得
- 12、很好哦，晒晒
- 13、专业图书，很有用，正品！
- 14、与《白帽子》搭配看，实践加理论，实在！
- 15、虽然 黑客攻防技术宝典:Web实战篇 讲得更加全面，但入门知识及注入原理没有这本书细致，入门非常好的选择。
- 16、确实不错~~~，还没全部看完
- 17、尚可，至少owasp的介绍帮我扛过了面试-v-
- 18、基于OWASP Top 10与ESAPI
- 19、覆盖面很全
- 20、好书，不用多说了，实用。

《Web应用安全威胁与防治》

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