

《Web入侵安全测试与对策》

图书基本信息

书名：《Web入侵安全测试与对策》

13位ISBN编号：9787302138747

10位ISBN编号：7302138745

出版时间：2006-10

出版社：清华大学

作者：MikeAndrews

页数：177

译者：汪青青

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.tushu000.com

《Web入侵安全测试与对策》

内容概要

《Web入侵安全测试与对策》主要是为了向测试人员介绍一些用于测试Web应用程序的攻击方式，其中会包含一些恶意输入的典型例子，比如一些躲避校验和身份认证的方式，以及某些由配置、语言或结构带来的问题。但这些介绍都很简单，同时给出了如何查找和测试这些问题，以及解决这些问题的方法建议。希望《Web入侵安全测试与对策》能够成为人们在测试基于Web的应用程序方面获取信息（和灵感）的有力工具。

《Web入侵安全测试与对策》

作者简介

Mike Andrews，软件安全方面的资深顾问，领导了Foundstone的Web应用程序安全评估以及对最新的Web攻击的分类。作为一位著作颇丰的作者，他还为财富500强中的多家公司进行过独立的安全测评。

书籍目录

第1章 与众不同的Web

- 11.1 本章内容
- 11.2 简介
- 11.3 World Wide Web
- 21.4 Web世界的价值
- 41.5 Web和客户机 - 服务器
- 51.6 Web应用的一个粗略模型
 - 71.6.1 Web服务器
 - 71.6.2 Web客户机
 - 81.6.3 网络
- 81.7 结论

第2章 获取目标的信息

- 112.1 本章内容
- 112.2 简介
- 112.3 攻击1：淘金
 - 112.3.1 何时使用这种攻击
 - 122.3.2 如何实施这种攻击
 - 122.3.3 如何防范这种攻击
- 182.4 攻击2：猜测文件与目录
 - 182.4.1 何时使用这种攻击
 - 192.4.2 如何实施这种攻击
 - 192.4.3 如何防范这种攻击
- 222.5 攻击3：其他人留下的漏洞——样例程序的缺陷
 - 232.5.1 何时使用这种攻击
 - 232.5.2 如何实施这种攻击
 - 232.5.3 如何防范这种攻击

第3章 攻击客户机

- 253.1 本章内容
- 253.2 简介
- 253.3 攻击4：绕过对输入选项的限制
 - 263.3.1 何时使用这种攻击
 - 273.3.2 如何实施这种攻击
 - 273.3.3 如何防范这种攻击
- 303.4 攻击5：绕过客户机端的验证
 - 313.4.1 何时使用这种攻击
 - 323.4.2 如何实施这种攻击
 - 323.4.3 如何防范这种攻击

第4章 基于状态的攻击

- 374.1 本章内容
- 374.2 简介
- 374.3 攻击6：隐藏域
 - 384.3.1 何时使用这种攻击
 - 384.3.2 如何实施这种攻击
 - 404.3.3 如何防范这种攻击
- 414.4 攻击7：CGI参数
 - 414.4.1 何时使用这种攻击
 - 424.4.2 如何实施这种攻击

- 424.4.3 如何防范这种攻击
- 454.5 攻击8：破坏cookie
 - 454.5.1 何时使用这种攻击
 - 464.5.2 如何实施这种攻击
 - 464.5.3 如何防范这种攻击
- 484.6 攻击9：URL跳跃
 - 484.6.1 何时使用这种攻击
 - 484.6.2 如何实施这种攻击
 - 494.6.3 如何防范这种攻击
- 504.7 攻击10：会话劫持
 - 514.7.1 何时使用这种攻击
 - 524.7.2 如何实施这种攻击
 - 524.7.3 如何防范这种攻击
- 544.8 参考文献
- 55第5章 攻击用户提交的输入数据
 - 575.1 本章内容
 - 575.2 简介
 - 575.3 攻击11：跨站点脚本
 - 575.3.1 何时使用这种攻击
 - 595.3.2 如何实施这种攻击
 - 595.3.3 如何防范这种攻击
 - 635.4 攻击12：SQL注入
 - 645.4.1 何时使用这种攻击
 - 655.4.2 如何实施这种攻击
 - 655.4.3 如何防范这种攻击
 - 685.5 攻击13：目录遍历
 - 695.5.1 何时使用这种攻击
 - 695.5.2 如何实施这种攻击
 - 695.5.3 如何防范这种攻击
- 71第6章 基于语言的攻击
 - 736.1 本章内容
 - 736.2 简介
 - 736.3 攻击14：缓冲区溢出
 - 736.3.1 何时使用这种攻击
 - 746.3.2 如何实施这种攻击
 - 756.3.3 如何防范这种攻击
 - 776.4 攻击15：公理化
 - 786.4.1 何时使用这种攻击
 - 796.4.2 如何实施这种攻击
 - 796.4.3 如何防范这种攻击
 - 816.5 攻击16：NULL字符攻击
 - 816.5.1 何时使用这种攻击
 - 826.5.2 如何实施这种攻击
 - 836.5.3 如何防范这种攻击
- 83第7章 获取目标的信息
 - 857.1 本章内容
 - 857.2 简介
 - 857.3 攻击17：SQL注入II——存储过程
 - 857.3.1 何时使用这种攻击

- 867.3.2 如何实施这种攻击
- 867.3.3 如何防范这种攻击
- 877.4 攻击18：命令注入
 - 887.4.1 何时使用这种攻击
- 897.4.2 如何实施这种攻击
- 907.4.3 如何防范这种攻击
- 907.5 攻击19：探测服务器
 - 907.5.1 何时使用这种攻击
 - 917.5.2 如何实施这种攻击
 - 927.5.3 如何防范这种攻击
- 957.6 攻击20：拒绝服务
 - 967.6.1 何时使用这种攻击
 - 967.6.2 如何实施这种攻击
 - 977.6.3 如何防范这种攻击
- 977.7 参考文献
- 97第8章 认证
 - 998.1 本章内容
 - 998.2 简介
 - 998.3 攻击21：伪装型加密
 - 998.3.1 何时使用这种攻击
 - 1008.3.2 如何实施这种攻击
 - 1018.3.3 如何防范这种攻击
- 1038.4 攻击22：认证破坏
 - 1038.4.1 何时使用这种攻击
- 1058.4.2 如何实施这种攻击
- 1058.4.3 如何防范这种攻击
- 1068.5 攻击23：跨站点跟踪
 - 1078.5.1 何时使用这种攻击
 - 1098.5.2 如何实施这种攻击
 - 1098.5.3 如何防范这种攻击
- 1108.6 攻击24：暴力破解低强度密钥
 - 1108.6.1 何时使用这种攻击
 - 1128.6.2 如何实施这种攻击
 - 1138.6.3 如何防范这种攻击
- 1138.7 参考文献
- 115第9章 隐私
 - 1179.1 本章内容
 - 1179.2 简介
 - 1179.3 用户代理
 - 1189.4 原文
 - 1209.5 cookie
 - 1219.6 Web Bugs
 - 1239.7 对剪切板的存取
 - 1249.8 页面缓存
 - 1259.9 ActiveX控件
 - 1279.10 浏览器辅助对象
- 127第10章 Web服务
 - 12910.1 本章内容
 - 12910.2 简介

- 12910.3 什么是Web服务
 - 12910.4 XML
 - 13010.5 SOAP
 - 13110.6 WSDL
 - 13210.7 UDDI
 - 13210.8 威胁
 - 13310.8.1 WSDL扫描攻击
 - 13310.8.2 参数篡改
 - 13410.8.3 XPATH注入攻击
 - 13410.8.4 递归负载攻击
 - 13510.8.5 过载攻击
 - 13610.8.6 外部实体攻击
 - 136附录A 软件产业50年：质量为先
 - 139A.1 1950—1959年：起源
 - 139A.2 1960—1969年：远行
 - 140A.3 1970—1979年：混乱
 - 141A.4 1980—1989年：重建
 - 142A.4.1 CASE工具
 - 142A.4.2 形式方法
 - 143A.5 1990—1999年：发展
 - 144A.6 2000—2009年：工程化？
 - 145附录B 电子花店的bug
 - 149附录C 工具
 - 155C.1 TextPad
 - 155C.2 Nikto
 - 156C.3 Wikto
 - 159C.4 Stunnel
 - 164C.5 BlackWidow
 - 165C.6 Wget
 - 167C.7 cURL
 - 169C.8 Paros
 - 171C.9 SPIKEProxy
 - 173C.10 SSLDigger
 - 176C.11 大脑
- 177

《Web入侵安全测试与对策》

编辑推荐

黑客们会对你的Web网站、应用程序和服务器进行残忍的攻击。如果网站存在漏洞，那么最好在黑客之前自己先发现这些攻击。现在就有一本对基于Web的软件进行安全性测试的权威的随身指南。在《Web入侵安全测试与对策》中，两位专家介绍了各种针对Web软件的攻击：对于客户机、服务器、状态、用户输入等方面的攻击。随着对Web架构和代码当中大量关键的和经常遭到攻击的漏洞的深入了解，你将逐步掌握强大的攻击工具和技术。

《Web入侵安全测试与对策》

精彩短评

- 1、由于篇幅所限，这本书不可能写的太详细，对大家进行一下web安全方面的科普还是很好的。举个例子来说，对于SQL injection，XSS，XSRF这几种注入攻击，只对前两者有介绍（因为时效问题），而且看过之后还是找不到相应漏洞，因为仅仅是原理介绍。要成为一个顶尖的web黑客，需要学习的东西还很多。
- 2、过的去，只是不知道是翻译问题还是原版问题，很多东西没说好。
- 3、翻译得比较差 内容比较适合做为科普读物
- 4、比较简单
- 5、虽然一些案例、方法比较老了，但引起编写安全代码的意识还是很重要的。
- 6、web安全入门书
- 7、大二的时候读过，内容较为平淡。
- 8、简明扼要。营养一般。

《Web入侵安全测试与对策》

精彩书评

1、这本书虽然没有详细的教你的如何进行攻击，但它从宏观描述了进行“Web安全测试”需要了解的问题。这本书，使我获得的不少灵感，另外是里面也列出很多外国的安全站点，Paper，工具等，也增长了我的视野。

章节试读

1、《Web入侵安全测试与对策》的笔记-第22页

本书主要的例子都是coldfusion，过时

攻击工具：Paros，nikto

防范工具：iislockdown，pagespy

防范网页遍历攻击

方法1：方法2：CGI，标记隐藏域

会话劫持不按顺序访问页面有可能可以查看到敏感信息或获得非法信息隐藏域隐藏链接跳转指向例子
隐藏域隐藏cookie例子会话劫持XSScookieXSS

2、《Web入侵安全测试与对策》的笔记-第30页

客户机是不可信任的。任何在客户机上对用户输入进行的限制都需要在服务器端进行再一次的验证。

3、《Web入侵安全测试与对策》的笔记-第12页

淘金：

1.html代码中嵌入的注释

2.html代码中敏感信息

3.服务器端的出错信息和http响应

4.应用程序出错信息

反馈给用户的信息应当简洁而有价值，避免信息泄漏

《Web入侵安全测试与对策》

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.tushu000.com