《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

《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。

《Web入侵安全测试与对策》

书籍目录

《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，那么最好在这些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。

《Web入侵安全测试与对策》

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