

<<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

出版时间：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，请支持正版图书。

更多资源请访问：<http://www.tushu007.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。

<<Web入侵安全测试与对策>>

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	41.1
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	9	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	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: 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	24	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: 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	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	645.1 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 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	796.1 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 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	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	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	173 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，那么最好在這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>>

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>