<<安全漏洞追踪>>

图书基本信息

书名：<<安全漏洞追踪>>

13位ISBN编号：9787121073717

10位ISBN编号：7121073714

出版时间：2008-10

出版时间：电子工业出版社

作者：（美）盖弗，（美）詹弗瑞斯，（美）兰德　著，钟力，朱敏，何金勇　译

页数：508

字数：686000

前言

你可能想知道微软为什么要出版这样一本关于安全测试的书，因为加强软件安全是一件非常困难的事情。
当然，微软已经遇到过相当多的软件安全问题，因而有大量的经验供测试人员参考。
在2002年可信计算计划被提出之前，我们就已经在微软工作了。
自微软实施该计划以来，我们已经看到微软在处理安全问题方面的重大改变。
现在，安全问题已经不仅仅是安全专家的职责，已经成为了我们每一个人的责任。
这本具有创见性的关于软件安全测试的书，源于我们在微软的工作经验以及为开发出用户购买后能持续安全可靠运行的软件而做出的努力。

<<安全漏洞追踪>>

内容概要

这是一本针对安全测试的书籍，同时也是一本十分适合信息安全研究人员的优秀参考书。
本书共20章，其中前3章讨论了安全测试的基础，包括如何从攻击者的角度去思考测试方法，以及如何进行威胁建模和入口点查找。
第4章至第19章则通过详细的示例与代码，分别深入地阐述了网络流量和内存数据的操控方法，包括缓冲区溢出、格式化字符串、HTML脚本、XML、规范化、权限、拒绝服务、托管代码、SQL注入和ActiveX再利用等安全漏洞追踪方法，以及在二进制代码条件下查找安全漏洞的逆向工程技术。
第20章论述了合理报告安全漏洞的程序，并提出了一个负责的安全漏洞公开流程。
最后，本书还提供了一个适于初学者的测试用例列表。

作者简介

Tom Gallagher，微软Office安全测试组负责人，擅长渗透测试、编写安全测试工具和安全培训。

<<安全漏洞追踪>>

书籍目录

媒体关注与评论

我们必须培养一类新型的测试员——一种能像恶意攻击者那样思考的人——一种基于白盒和黑盒测试基础的通过攻击来追踪安全漏洞的人。

——微软主席兼软件体系结构首席执行官　比尔·盖茨

<<安全漏洞追踪>>

编辑推荐

如何识别高风险的入口点并创建测试用例；　　如何测试客户端和服务器，以追踪恶意的请求／响应漏洞；　　如何利用黑盒和白盒测试方法揭示安全漏洞；　　如何发现欺骗问题，包括标识欺骗和用户接口欺骗；　　如何检测能够利用程序逻辑的漏洞，比如SQL注入；　　如何测试×ML、SOAP和Web服务的安全漏洞；　　如何识别信息泄露和弱权限问题；　　如何查找攻击者能够直接操纵内存的地方；　　如何利用不同的数据表现方式来揭示规范化问题；　　如何曝光COM和Active×再利用攻击。

《安全漏洞追踪》是来自专家的完美的软件安全测试参考书，你将学会像攻击者那样去思考，并发现软件中潜在的安全问题。

在这本优秀的参考书中，三位安全测试专家提供了明确实用的指南和代码实例，帮助你在软件发布之前发现、分类和评估安全漏洞。

版权说明