<<软件安全测试艺术>>

图书基本信息

书名：<<软件安全测试艺术>>

13位ISBN编号：9787111219736

10位ISBN编号：7111219732

出版时间：2007-8

出版时间：机械工业

作者：威斯波尔

页数：213

<<软件安全测试艺术>>

内容概要

本书囊括了应用程序和网络安全分析和测试方面的内容。
分为三部分，第一部分讨论一些现实情况，主要介绍漏洞的产生、安全的软件开发生命周期、基于风险的安全测试和分析：白盒、黑盒和灰盒测试；第二部分主要分析网络上发现应用程序并对其进行攻击的方法；第三部分介绍如何判定漏洞的可利用性。
本书内容涉及广泛，叙述详尽，适合作为安全工程师、软件测试工程师及软件开发人员等的参考用书。

作者简介

Chris Wysopal是Veracode公司CTO。
曾任stake公司的研发副总。
他领导了无线、架构及应用程序安全工具的开发。
他是LOphtCrack密码审计攻击的合作开发者。
他曾在美国国会进行过安全声明，并曾在Black Hat大会和西点军校讲演。

<<软件安全测试艺术>>

书籍目录

<<软件安全测试艺术>>

编辑推荐

本书深入讲解软件安全方面最新的实用技术，用于在破坏之前预防并识别软件的安全问题。
本书作者具有近十年应用和渗透测试方面的经验，从简单的“ 验证 ”性测试方法讲起，进而介绍先发制人的“ 攻击 ”性测试方法。
作者首先系统地回顾了软件中出现的设计和编码方面的安全漏洞，并提供了避免出现这些安全漏洞的实用指导。
然后，向读者展示了定制用户化软件调试工具的方法，用以对任何程序的各个方面独立地进行测试，之后对结果进行分析，从而识别可被利用的安全漏洞。
主要内容●如何从软件攻击者的角度来思考从而增强防御策略。
●兼顾成本效益，将安全测试整合到软件开发的生命周期。
●基于最高风险领域，使用威胁模型来排定测试的优先顺序。
●构建用于进行白盒测试、灰盒测试和黑盒测试的软件测试实验。
●针对每个测试工程，选用恰当的工具。
●执行当前主要的软件攻击，从故障注入到缓冲区溢出。
●哪些缺陷在现实世界中最可能被攻击者利用。
本书是每一个负责软件安全的技术人员必备的读物：无论是测试人员、QA专家、安全从业者、开发人员，还是其他相关的人员。
对于IT管理人员，本书提供了经实践检验的行动计划，用于实现有效安全测试或加强现有测试流程。

版权说明