

<<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

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>

## <<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。

## <<软件安全测试艺术>>

### 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

本书的“美誉”译者序序言前言致谢关于作者第一部分 综述 第1章 从传统软件测试转变 1.1 安全测试和软件测试的对比 1.2 安全测试转变的范式 1.3 高级安全测试策略 1.4 像攻击者一样思考 1.5 小结 第2章 漏洞是怎样藏到软件中的 2.1 设计漏洞与实现漏洞 2.2 常见的安全设计问题 2.3 编程语言的实现问题 2.4 平台的实现问题 2.5 常见的应用程序安全实现问题 2.6 开发过程中的问题 2.7 部署上的薄弱性 2.8 漏洞根源分类法 2.9 小结 第3章 安全的软件开发生命周期 3.1 将安全测试融入到软件开发生命周期中 3.2 阶段1：安全原则、规则及规章 3.3 阶段2：安全需求：攻击用例 3.4 阶段3：架构和设计评审/威胁建模 3.5 阶段4：安全的编码原则 3.6 阶段5：白盒/黑盒/灰盒测试 3.7 阶段6：判定可利用性 3.8 安全地部署应用程序 3.9 补丁管理：对安全漏洞进行管理 3.10 角色和职责 3.11 SSDL与系统开发生命周期的关系 3.12 小结 第4章 基于风险的安全测试 第5章 白盒、黑盒和灰盒测试 第二部分 攻击演练 第6章 常见的网络故障注入 第7章 会话攻击 第8章 Web应用程序的常见问题 第9章 使用WebScarab 第10章 实现定制的侦探工具 第11章 本地故障注入 第三部分 分析 第12章 判定可利用性

## <<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上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。

<<软件安全测试艺术>>

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>