<<Web安全测试>>

图书基本信息

书名：<<Web安全测试>>

13位ISBN编号：9787302219682

10位ISBN编号：7302219680

出版时间：2010-3

出版时间：清华大学出版社

作者：霍普(Paco Hope),沃尔瑟(Ben Waltber)

页数：281

译者：傅鑫

前言

Web应用遭受着格外多的安全攻击。
其原因在于，网站及在网站上运行的应用在某种意义上是所有公司和组织的虚拟正门。
Web自1993年以来的发展令人瞠目结舌，就其被广泛采用的速度而言，甚至超过了电视和电力技术。
Web应用在软件开发中所扮演的角色不断成长并且越来越重要。
事实上，评论家日前称我们已经进入了Web 3.0时代。
问题在于，安全性确实没能跟上这种发展步伐。
目前，我们在加固Web 1.0应用的安全方面仍有很多的问题，以致于还没有开始加固Web 2.0的安全，更别提Web 3.0了。
在继续之前，我有一些话不吐不快。
Web应用是很重要而且正在不断发展的一类软件，但它们并不是唯一的软件类型！
事实上，考虑到遗留应用，嵌入式设备以及世界上的其他代码，我相信Web应用只占到所有软件的一小部分。
因此，当世人将所有对软件安全的注意力全部倾注在Web应用上时，我感到担忧。
有大量其他类型的重要软件并不依赖于Web。
这就是我自称是软件安全人员而不是Web应用安全人员的原因。
无论如何，Web应用安全和软件安全确实存在许多共同的问题和缺陷（这一点也不奇怪，因为前者是后者的子集）。
一个共同的问题是将安全作为一项功能，或者某种“东西”。
安全并不是某种“东西”，它是系统的一项属性。
这意味着再多的身份验证技术、神奇的加密技术或者面向服务架构（SOA）Web服务安全API都无法自动地解决安全问题。
事实上，与任何其他方面相比，安全与测试及保障都有着更多的关联。
打开这本书，哦，我们确实需要一种有效的Web应用安全测试方法么？
要知道，许多由安全专家为Web应用测试所设计的“测试”都不具有任何测试严密性。
原来测试本身就是一门学科，背后有整套的学问。
Paco和Ben带给我们的是对测试线索的深入了解。
这真是一对珍贵的组合。
所有称职的测试人员都理解，关于测试的一项关键要素是：测试结果必须能够用于指导行动。
差的测试结果会给出像“bigjavaglob.java文件中存在XSS问题”这样含糊的报告。
开发人员怎么会知道如何去修复这个问题呢？
这里缺少的是适当地说明XSS是什么（当然，它指的是跨站式脚本），指出在成千上万行代码的文件中问题可能出现的位置，以及如何做才能修复它。
本书中包含了大量技术信息，足以供像样的测试人员向真正起作用的开发人员报告可用于指导行动的结果。
但愿本书中的内容不仅能够被安全人员采用，而且也能够被Web应用的测试人员所采用。
事实上，质量保证（QA）人员会高兴地看到，本书正好面向测试人员，书中采用了回归测试、覆盖率以及单元测试等术语。
以我的经验来看，就测试而言，测试人员做得要比安全人员好得多。
使用得当的话，本书可以将安全人员改造成更优秀的测试人员，将测试人员改造成更优秀的安全人员。
本书的另一重要特点在于，它明确地将重点放在工具和自动化上。
与现代安全人员一样，现代测试人员也使用工具。
本书包含了大量基于实际工具的真实例子，其中许多工具都可以从网上免费下载。
事实上，本书适用于指导正确的工具使用方法，因为书中描述的许多开源工具都没有自带内置的手册或入门指导。

我喜欢实践性的资料，而这本书在实际动手方面做到了极致。
一种过度乐观的软件开发方法必然会创造出令人吃惊的东西，但是从安全角度而言，它同样也会使我们陷入困境。
简单地说，我们会忽视去考虑自己的软件在遭到故意和恶意攻击时会发生什么。
攻击者就在大门口，每天都在探查我们的Web应用。

<<Web安全测试>>

内容概要

在你对Web应用所执行的测试中，安全测试可能是最重要的，但它却常常是最容易被忽略的。本书中的秘诀演示了开发和测试人员在进行单元测试、回归测试或探索性测试的同时，如何去检查最常见的Web安全问题。

与即兴的安全评估不同的是，这些秘诀是可重复的、简洁的、系统的——可以完美地集成到你的常规测试套装中。

本书中的秘诀所覆盖的基础知识包括了从观察客户端和服务器之间的消息到使用脚本完成登录并执行Web应用功能的多阶段测试。

在本书的最后，你将能够建立精确定位到Ajax函数的测试，以及适用于常见怀疑对象(跨站式脚本和注入攻击)的大型多级测试。

本书将帮助你：

· 获取、安装和配置有用的——且免费的——安全测试工具

· 理解你的应用如何与用户通信，这样你就可以在测试中更好地模拟攻击

· 从许多不同的模拟常见攻击(比如SQL注入、跨站式脚本和操纵隐藏表单域)的方法中进行选择

· 作为自动化测试的出发点，通过使用秘诀中的脚本和例子，使你的测试可重复

不用再担心午夜来电话告诉你站点被破坏了。

通过本书和示例中所用的免费工具，你可以将安全因素加入到你的测试套装中，从而得以睡个安稳觉。

作者简介

Paco Hope，是Cigital公司的一名技术经理，《Mastering FreeBsD and 0penBsDsecurity》（由O ’ Reilly出版）的合著者之一。
他也发表过有关误用、滥用案例和PKI的文章。
他曾被邀请到会议就软件安全需求、Web应用安全和嵌入式系统安全等话题发表演讲。
在Cigital，他曾担任MasterCard Internationa！
在安全策略方面的主题专家，而且曾协助一家世界500强的服务业公司编写软件安全策略。
他也为软件开发和测试人员提供软件安全基础方面的培训。
他还曾为博彩业和移动通信行业中的几家公司提出过软件安全方面的建议。
Paco曾在威廉玛丽学院主修计算机科学和英语，并从弗吉尼亚大学获得计算机科学方面的理学硕士学位。
Ben Waltller，是Cigital公司的一名顾问，Edit C00kies工具的开发者之一。
他同时参与标准质量保证和软件安全方面的工作。
他日复一日地设计和执行测试一一因此他理解忙碌的QA领域对简单秘诀的需求。
他也曾对开放式Web应用程序安全项目（0WAsP）的成员就w曲应用测试工具发表过演讲。

<<Web安全测试>>

书籍目录

章节摘录

插图：提供证据在安全测试中，我们考虑无法接受的输入的全体集合——无限集——并重点关注那些很可能在我们软件的安全需求方面造成严重失效的输入子集——仍然是无限集。
我们需要确定这些安全需求是什么，并决定什么类型的测试能够证明这些需求得到满足。
这并不简单，但是通过逻辑和勤奋，我们能够向产品所有者提供有用的证据。
我们证明安全满足需求的方式将与证明功能满足要求的方法相同。
我们建立输入，确定预期结果，然后建立并运行测试来锻炼系统。
以我们与不熟悉安全测试的测试人员交往的经历来看，第一步和最后一步是最难的。
设计反安全的输入和对软件进行测试是最难做的事情。
大多数时间，预期的结果相当简单。
如果我询问产品经理：“有人能够在不登录的情况下下载敏感数据吗？”。
通常他很容易就会说不。
因此，提供证据过程中较难的部分是创造出可能会造成这种状况的输入，然后确定这种状况是否会发生。
满足需求有关软件工程学的ANSI／IEEE标准729将“需求”定义为用户为了解决问题或达成目标所需要的条件或功能，或为了满足合同、标准，规范或其他正式起效的文档.系统所必须拥有或满足的条件或功能。
在得知需求的情况下，所有测试人员都进行测试直到满足需求。
即使需求并不是以充斥着“该软件应当”语句的形式出现。
软件测试人员也往往能够就正确的响应达成共识，然后以预期结果的形式将其整理到测试之中。
安全测试与功能测试相似，因为它同样也依赖于对“我们想要怎样的行为”的理解。
当然也可以说，与功能测试相比，安全测试更加依赖于需求，因为它有更多可能的输入和输出可供筛选。
在需求编写者的脑海里，安全行为的定义往往更加模糊，因为大多数软件都不是安全软件。
该软件有一些其他方面的主要用途，而安全是一种必须存在的非功能性需求。
因为对安全的关注不够，所以这方面的需求常常缺失或不完整。

媒体关注与评论

“贯穿整本书的精彩的真实示例，使理论生动起来，并使攻击引人入胜。”
——Lee Copeland.StarEast和StarWest测试会议的议程主席“最后，这是一本供测试人员使用的普通意义上的手册，它讲授安全测试的机制。
与其秘诀使用方法不相符的是，这本书实际上武装了测试人员，使他们能够找出甚至连某些最著名的安全工具也无法发现的漏洞。”
——MattFisher，Piscis有限责任公司的创始人和CEO

编辑推荐

《Web安全测试》将帮助你：获取、安装和配置有用的——且免费的——安全测试工具理解你的应用如何与用户通信，这样你就可以在测试中更好地模拟攻击从许多不同的模拟常见攻击（比如SQL注入、跨站式脚本和操纵隐藏表单域）的方法中进行选择作为自动化测试的出发点，通过使用秘诀中的脚奉和例子，使你的测试可重复不用再担心午夜来电话告诉你站点被破坏了。
通过《Web安全测试》和示例中所用的免费工具，你可以将安全因素加入到你的测试套装中，从而得以睡个安稳觉。

<<Web安全测试>>

版权说明