《模糊测试》

图书基本信息

书名：《模糊测试》

13位ISBN编号：9787111257554

10位ISBN编号：7111257553

出版时间：2009-1

出版社：斯顿 (Michael Sutton)、 Adam Greene、 Pedram Amini、 黄陇 机械工业出版社 (2009-01出版)

作者：[美] Michael Sutton,Adam Greene,Pedram Amini

页数：363

译者：黄陇,于莉莉,李虎

《模糊测试》

前言

安全漏洞是研究安全问题的生命线。无论是执行渗透测试、评价新产品还是审核关键构件的源代码，安全漏洞都驱动着我们的决策，让我们有理由花费时间，并且很多年来一直影响着我们的选择。源代码审核是一种白盒测试技术，这是一种很长时间以来都流行的软件产品安全漏洞检测方法。这种方法需要审核者了解编程概念和产品功能的每一个细节，深入洞察产品的运行环境。除此之外，源代码审核还有一个显而易见的缺陷——必须首先要获得产品的源代码。幸运的是，除了白盒技术外，我们还可以使用不需要访问源代码的黑盒技术。模糊测试就是黑盒技术中的一种可选方法，这种方法在发掘那些用审核方法无法发现的产品关键安全漏洞方面披证明是成功的。模糊测试是这样的一个过程：向产品有意识地输入无效数据以期望触发错误条件或引起产品的故障。这些错误条件可以指导我们找出那些可挖掘的安全漏洞。

《模糊测试》

内容概要

《模糊测试强制性安全漏洞发掘》主要内容：模糊测试的工作原理，模糊测试相比其他安全性测试方法的关键优势，模糊测试在查找网络协议，文件格式及Web应用安全漏洞中的技术现状等。演示了自动模糊工具的用法，并给出多个说明模糊测试强大效力的历史案例。

《模糊测试》

作者简介

Michael Sutton是SPI Dynamics公司的安全布道师。他还是Web应用安全组织(WASC)的成员，负责其中的Web应用安全统计项目。
Adam Greene目前担任纽约某大型金融新闻公司的工程师。此前他曾经是iDefense公司的工程师，这是位于Re ston，VA．的一家智能技术公司。Adam Greene在计算机安全领域的主要研究兴趣是可靠挖掘方法、模糊测试和基于UNIX系统的审核和挖掘开发。
Pedram Amini是Tipping Point公司的安全研究和产品安全评估组的项目领导。此前他曾经是iDefence实验室的主任助手，同时也是该实验室的创建者之一。他的主要兴趣是研究逆向工程——开发自动支持工具、插件和脚本。
这三位作者经常出席Black Hat安全大会并在其中做主题报告。

《模糊测试》

书籍目录

《模糊测试》

章节摘录

如果询问任何一位有成就的安全领域的研究者如何发现漏洞，很可能会得到一大堆答案。为什么？因为可用于安全性测试的方法太多，每种方法都有自己的优点和缺点。没有一种方法是绝对正确的，也没有一种方法能够揭示一个给定目标下所有可能的漏洞。在较高的层次上，有三种主要的方法用来发现安全漏洞：白盒测试、黑盒测试和灰盒测试。这些方法之间的差别是由测试者可得到的资源决定的。白盒测试是一个极端，它需要对所有资源进行充分地访问。这包括访问源代码、设计规约，甚至有可能还要访问程序员本人。黑盒测试是另一个极端，它几乎不需要知道软件的内部细节，很大程度上带有盲目测试的味道。远程Web应用的Pen测试是黑盒测试的一个好例子，它不需要访问程序源码。位于两个极端方法之间的是灰盒测试，它的定义因询问的人不同而不同。就我们的应用目的而言，灰盒测试需要访问编译后得到的二进制代码，或许还要访问一些基本的文档。本章将考察漏洞发掘的各种不同的高层和低层方法，起点是白盒测试，你以前可能听说过这种方法也被称为玻璃、透明或半透明测试。之后我们再定义黑盒测试和灰盒测试，模糊测试可能就属于后两者。我们将阐述每种方法的利弊，这些方法的利弊将成为本书后面介绍模糊测试时所需要的背景知识。模糊测试只是漏洞发掘的一种方法，了解其他可选的实用方法也是相当重要的。

《模糊测试》

编辑推荐

《模糊测试强制性安全漏洞发掘》可作为开发者，安全工程师、测试人员以及QA专业人员的参考用书。掌握揭露安全性缺陷的最强大技术模糊测试现在已经发展成为一种最有效的软件安全性测试方法。模糊测试是指将一个随机的数据源作为程序的输入，然后系统地找出这些输入所引起的程序失效。著名的模糊测试专家将告诉你如何抢在别人之前使用模糊测试来揭示软件的弱点。《模糊测试强制性安全漏洞发掘》是第一部也是唯一一部自始至终讨论模糊测试的专著，将以往非正式的技巧转变为训练有素的最佳实践，进而将其总结为一种技术。作者首先回顾了模糊测试的工作原理并勾勒出模糊测试相比其他安全性测试方法的关键优势。然后，介绍了在查找网络协议，文件格式及Web应用安全漏洞中的先进的模糊测试，演示了自动模糊工具的用法，并给出多个说明模糊测试强大效力的历史案例。攻击者早已经开始使用模糊测试技术。当然，你也应该使用。不论你是一位开发者、一位安全工程师还是测试人员或QA专业人员，《模糊测试强制性安全漏洞发掘》都将教会你如何构建安全的软件系统。

《模糊测试》

精彩短评

1、书不错，模糊测试的思想和技巧都讲到了，想自己写个Fuzzer也能明白个七八。但翻译的就够呛了，诸多的语句不通，第24章介绍DynamoRIO的时候把MIT翻译成“马萨诸塞技术研究所”也是又一次拉低了技术翻译界的下限。
2、书可以，就是翻译上有不少错误，但是可以接受。看了几章了
3、内容很全面，作者也很有功力。其中还有一位是paimei的开发者，崇敬。
4、都是军方代表。这项技术不错。
5、不错，这么好的书要绝版了，真可惜。之前还以为绝版了，突然看到居然还有，很喜欢。
6、偏实用的一本书，不算深，但从工具到方法都介绍的很全面，如果想深入了解，可以根据书上提供的链接继续摸瓜。总之作为入门书还是很好的。书中定义的Fuzzing Test指的是通过提供非预期输入并监视异常结果来发现软件故障的方法，唔，所以你知道封面为啥有只毛茸茸的大熊了...毛茸茸测试，误，模糊测试的好处是无需大量逆向工程就可以自动化的找到比较容易发现的漏洞，但对于某些类型的漏洞，很可能永远也没法通过这种方法找到，比如由多个步骤链起来的缺陷。另外，在漏洞检测实例分析中，此书用前东家的服务器保护当靶子，我看了很亲切...
7、中英文结合着看吧。
8、非常棒。。。。。。。。。。。。。。。。
9、做黑盒模糊测试的入门书籍，建议有时间的话读英文原版的。对于黑盒测试的整体概念的理解会有帮助，实际测试时可以当做工具书参考。
10、太深奥了对我来说
11、内容还行，书质量挺好
12、对这个方向是个不错的指导书
13、内容浅显，一下午就能看完。但是介绍比较笼统宽泛，windows和linux的工具都有介绍，讲解却不深入，知其然不知所以然，而且部分软件已经过时，总之与我想象的有区别
14、翻译也很好。第一本写fuzz的书籍。

《模糊测试》

版权说明