模糊测试

模糊测试_下载链接1_

著者:[美] Michael Sutton

出版者:机械工业出版社

出版时间:2009-1

装帧:

isbn:9787111257554

《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。

作者介绍:

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。

目录: 译者序

・・・・・・・(收起)

模糊测试_下载链接1_

标签

安全

漏洞

模糊测试

测试

fuzzing

软件安全漏洞发掘

软件

计算机科学

评论

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...

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。

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。

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。

对这个方向是个不错的指导书

详细阅读了部分章节,粗略阅读了部分章节,省略了几章.总体来讲对fuzz各类型和各平台都有介绍.翻译错误较多.

模糊测试_下载链接1_

书评

模糊测试是对协议的测试，协议可以看成一组输入的向量。
一个模糊测试框架，包括这些部分：
0.协议的交互器（更好的是一个ProxyFuzzer，能支持正常交互的拦截与重放）；可配置payload在协议中的填充的位置 1.协议自身约束的自动化生成，如校验和，web request的token等 2.paylo...

模糊测试_下载链接1_