Fuzzing

1.简介

Fuzzing是一种基于缺陷注入的自动软件测试技术。Fuzzing技术的思想就是利用“暴力”来实现对目标程序的自动化测试，然后监视检查其最后的结果，如果符合某种情况就认为程序可能存在某种漏洞或者问题。这里的“暴力”并不是说我们通常说得武力，而是说利用不断地向目标程序发送或者传递不同格式的数据来测试目标程序的反应。

2.Fuzzer  
 Fuzzer就是指用来进行Fuzzing工作的工具。常见类型

（1）文件型

文件型Fuzzer主要针对有文件作为程序输入的情况下的Fuzzing。  
 1》.对于可读的文件，你可以使用改变其内容的具体数值来进行Fuzzing  
 2》.对于未公布格式的，你可以按照一定规律修改文件格式来进行Fuzzing

1. 网络型  
    网络型Fuzzer是最为广泛的一种Fuzzer，因此这个方面的杰出的Fuzzer工具非常丰富。  
    1》.对于Web应用型的程序Fuzzing的主要用来发现XSS漏洞、注入漏洞之类等等  
    2》.用来发现溢出或者拒绝服务式漏洞的网络型Fuzzer－基于协议的网络型Fuzzer
2. 接口型  
    接口型Fuzzer是利用应用程序提供的外部接口来进行Fuzzing的工具。

3.Fuzzer的工作原理  
 一种是不断地对目标程序进行随机数据或者某种类型格式的数据发送、输入，这种Fuzzer在使用中，往往会因为所发送的数据不符合目标程序要求的格式，而直接被程序拒绝，不能够深入检测程序内部。这样导致的直接结果就是会大大降低对目标程序漏洞的发掘，效率低下。  
 还有一种就是建立在“可能性覆盖”理论模型上的Fuzzer。“可能性覆盖”理论是指将程序所有可能接受的外部数据，经过抽象划分为不同的类型，然后从每个类型中选取一个测试实例，使用这些测试实例进行对程序的Fuzzing检查。