安全小课堂第117期【关于 fuzz 的一些简单思考】

京东安全应急响应中心 3天前

在计算机领域，Fuzz Testing（模糊测试）是一种测试方法，即构造一系列无规则的“坏”数据插入应用程序，判断程序是否出现异常，以发现潜在的bug。在信息安全领域，也有人尝试引入fuzz testing思想进行安全漏洞挖掘，而且效果不错

JSRC **安全小课堂第117期**，邀请到**dogboy**作为讲师就**fuzz的一些简单思考**为大家进行分享。同时感谢各位小伙伴们的精彩讨论。

fuzz的优缺点?

京安小妹

dogboy：

优点：

1 手法简单，容易操作,可以省去不少人力，程序跑起来以后只需要分析结果就行了

2 发现漏洞速度快、误报相对来说很低

缺点：

1 黑盒测试的全部缺点

2 不通用，构造测试用例周期长，如果是复杂的协议

3 Undocumented的接口无法测试

通常情况下fuzz哪些内容？？

京安小妹

dogboy：

文件格式的Fuzz　　多见于软件漏洞的挖掘，好像 ImageMagick的不少crash都是靠这样fuzz出来的

– 图像格式
– 文档格式
– 等等

协议的Fuzz

– RPC协议
– Http协议（参数=值、路径）
– 等等

讲师

挖掘漏洞时fuzz的用处?

京安小妹

dogboy：

大佬们一般会在过sql注入的waf的时候用上fuzz技术，靠强大的字典，绕过waf的关键词检测

https://xz.aliyun.com/t/2418

或者像key一样对参数名等进行fuzz，寻找jsonp劫持、越权或者rce

https://gh0st.cn/archives/2018-07-25/1

key使用的是对参数进行增删改的fuzz方式，尝试挖掘无法直接发现的漏洞（一般适用于挖掘逻辑类漏洞）

而我这样的就只能fuzz一下url跳转时的参数，挖一挖url跳转

讲师

fuzz最关键的是什么？

京安小妹

dogboy：

我觉得字典第一关键，字典要足够大，覆盖所有的可能。

关于字典：

1. 收集网站本身自有传递参数和值

```
CATALOGID=48&PAGE_INDEX=1&PAGE_COUNT=10&DICTIONARYID=&REQUESTTYPE=0&ITEMTYPE=0&ISSAMETYPE=1
```

2. 收集和整理常见字典
3. 收集和整理字典的规则

讲师

有哪些比较不错的fuzz工具？

京安小妹

dogboy：

Web向的Fuzz工具

https://github.com/xmendez/wfuzz

https://github.com/maK-/parameth

可以用在做请求参数类的模糊测试，以上所列项目的所有功能都依赖于字典和字典规则完成测试。

HTTP Fuzzer

https://fuzzer.test404.com/?/article/5

好处就是可以拖拖拽拽出插件，不用写脚本，并且是图形化，windows用起来方便，适

合偷懒的时候使用23333

XssSniper插件
chrome上的插件，360的0kee Team写的插件，值得玩味的是我靠这个插件fuzz出了一个360主站的一个xss

总结

模糊测试只是自动化发现漏洞的一个重要手段，就像自动化漏洞扫描器一样。我们并不能完全依靠它，在测试过程中，人工对结果进行适时的分析，对字典做出合理的改进，不仅能提高模糊测试的效率，还能够帮助我们挖掘到更多潜在的设计缺陷。毕竟，机器终究是“死板”的，而人是“灵活”的。

讲师

互动问答环节：

1. fuzz是靠规则还是累积的字典?

讲师:

规则和累积的字典都有

字典可以好好整理这个项目

https://github.com/fuzzdb-project/fuzzdb

猪猪侠的字典

https://fuzz.wget.lc/Fuzz/

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心