聊聊app手工安全检测

京东安全应急响应中心 2016-09-18

点击上方“蓝字”关注本宝宝公众号

安全小课堂第二十七期

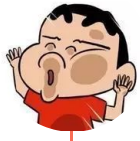
借助相关工具进行针对性的测试，就是app手工安全检测。隐患、风险点距离实际的漏洞利用还有一定距离， 即使是用借助语法分析的引擎去做自动化审计，也是需要手工确认， 这是无法替代的。由此可见app手工安全检测的重要性。本期我们来聊一聊app手工安全检测。

本期邀请到
盘古安全专家小G
盘古安全专家zhao
猪八戒网安全专家H3arts
大家欢迎~

/ 01 /

豌豆妹

什么是app手工安全检测？

小新 

在我看来，借助相关工具进行针对性的测试，就是app手工安全测试。具体场景包括安全问题分析、恶意行为安全检测等。

柴可夫斯基 

因为应用安全的检测可以做到反编译源代码级别，所以手工安全检测的时候，可以去阅读反编译的代码，以便针对一些场景和问题进行检测。

/ 02 /

豌豆妹

app手工安全检测的必要性有哪些呢？

小丸子 

安卓应用通过静态分析经常会扫描到问题，但准确性比较有限，自动化分析工具只能起到辅助作用，所以要借助手工安全检测去查看源代码上下文才好确定安全问题。有很多第三方平台都提供自动化的审计，但真正要确定这些漏洞或者风险的话，还得手工分析。

葫芦娃 

是的，自动化审计一般是提供的隐患、风险点等，无法做类似web的漏洞自动化验证。隐患、风险点距离实际的漏洞利用还有一定距离， 即使是用借助语法分析的引擎去做自动化审计，也是需要手工确认， 这是无法替代的。

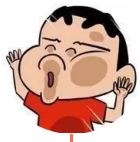
/ 03 /

豌豆妹

能介绍下app手工安全检测的思路么？

哆啦A梦

ios的话无法做到反编译，因此一般会借助反汇编的工具，比如IDA，越狱后的环境的话，会借助idb、classdump等辅助工具，方便利用应用的逻辑进行分析。android更多的是先进行反编译，apktool、dex2jar和jd-gui的组合。一般来说，ios下还会借助动态分析，然后用静态分析的方式去过一下那些问题点。动态分析会做系统行为hook，对加解密、http请求、文件系统访问、ios剪切板、日志记录、keychain访问进行分析。此外还有UIWebView的监控，因为ios里面也会用到内嵌网页的开发。



小新

在android apk安全检测的时候我一般是这个思路：先看一下是不是加壳的，如果是的话会对apk进行脱壳，然后通过反汇编、反编译工具得到汇编代码或反编译代码，然后根据特征定位代码位置，然后结合上下文分析，有时候可能要动态调试。在android apk里面有很多小技巧，antianalysis的技术要积累一些的。

豌豆妹

apk扫描开源框架哪个效果比较好一些？

柴可夫斯基

apk扫描开源框架，我看目前大家用的比较多的还是：https://github.com/mwrlabs/drozer。
静态扫描的有：https://github.com/androguard/androguard。

/ 04 /

豌豆妹

选一个合适的工具很重要，能推荐app手工安全检测小工具吗？

哆啦A梦

安利一下盘古的janus。脱壳的话可以试试dexhunter。

小新

目前能了解到的，国内做出来的就腾讯的金刚他们做了一个ios应用的安全检测系统，不过好像没有看到对外使用的地方，目前应该还是对内保障为主吧。

葫芦娃

推荐drozer、ida、jeb。drozer是开源的，还可以自定义脚本，感觉不错。

小丸子

android平台的话我也介绍几家。有360的显危镜，阿里的聚安全，还有梆梆、爱加密的，他们几家做的安全检测引擎功能差不多。

豌豆妹

好哒~谢谢小伙伴们的热情推荐！本期话题告一段落噢~咱们下期见。

安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）；
9、电商和O2O行业诈骗那些事儿（下）；
10、CSRF的攻击与防御；
11、账户体系安全管理探讨；
12、远程代码执行漏洞的探讨；
13、服务器安全管控的探讨；
14、畅谈端口安全配置；
15、谈一谈github泄露；
16、撞库攻击是场持久战；
17、url重定向攻击的探讨；
18、聊聊弱口令的危害（一）；
19、聊聊弱口令的危害（二）；
20、聊聊XML注入攻击；
21、聊聊暴力破解；
22、谈谈上传漏洞；
23、浅谈内网渗透；
24、聊聊短信验证码安全；
25、深聊waf那些事儿（一）。
26、深聊waf那些事儿（二）

jsrc_team

京东安全应急响应中心

更多精彩，尽在JSRC