msof工具

项目地址

<https://github.com/ajinabraham/Mobile-Security-Framework-MobSF/>

ios分析需要mac系统

搜索MobSF使用

needle 安全测试框架

要求越狱设备

项目地址

<https://github.com/mwrlabs/needle>

https://github.com/mwrlabs/needle/wiki/Installation-Guide

搜索needle使用

<http://www.hackdig.com/09/hack-39039.htm> 环境搭建

<https://labs.mwrinfosecurity.com/blog/needle-how-to/> 操作文档

https://zhuanlan.zhihu.com/iOSRe/19646016

Reveal使用

 iOS 安装文件其实就是一个 zip 包，所以我们可以通过解压，看到包内的内容

IDA等调试工具

Reveal 要求越狱设备以及mac ，一些分析工具都需要mac

UI分析工具（个人理解是看代码结构的）

**class\_dump\_z**

Clutch

iOS 安全攻防。破解以及防御手段

<http://wiki.jikexueyuan.com/project/ios-security-defense/code-fusion.html>

本地数据

程序结构

ios mac分析系列

<http://wufawei.com/2013/11/ios-application-security-2/>

越狱设备—安装工具

**连接设备--class\_dump\_z下载或导出信息**

mac 分析脱壳

<https://github.com/ianisme/IANDecryptiOSApp/tree/master/dumpdecrypted> 要先越狱

<https://github.com/ianisme/IANDecryptiOSApp>

<https://www.ianisme.com/ios/2326.html> 脱壳详细步骤文章

<http://www.mottoin.com/92530.html>脱壳详细步骤文章

<http://blog.csdn.net/u013538542/article/details/70196590> 脱壳步骤

6.Hopper有个强大的功能，能将汇编变成伪代码，方便查看定位问题

由于手里没有越狱机子，也没有进行脱壳试验，按 [Urinx/iOSAppHook] 中提到的方法直接从 xx助手 市场里下载越狱应用可用

<https://juejin.im/entry/5836599dc59e0d005775c90d> 重打包详细文章

脱壳及重打包汇总

<http://www.devhua.com/2016/11/05/iOS%E5%BA%94%E7%94%A8%E8%84%B1%E5%A3%B3%E5%92%8C%E9%87%8D%E7%AD%BE%E5%90%8D/>

分析IPA 文件

分析沙盒

脱壳之后可以用classdump导出肉文件，class-dump -H WeChat.decrypted --arch arm64 -o output/

使用   
otool -l WeChat.decrypted | grep -B 2 crypt

查看是否是揭秘状态

解密后的包可以直接解压缩

脱壳之后可以用classdump导出头文件

将解密后的包放进hopper,ida