APP 攻防-Frida 反证书抓包&移动安全系统&资产提取&评估扫描

```
#知识点：
1、资产提权-AppinfoScanner
2、评估框架-MobSF&mobexler
3、抓包利器-Frida&r0capture

#章节点：
1、信息收集-应用&资产提取&权限等
2、漏洞发现-反编译&脱壳&代码审计
3、安全评估-组件&敏感密匙&恶意分析

#核心点：
0、内在点-资产提取&版本&信息等
1、抓包点-反代理&反证书&协议等
2、逆向点-反编译&脱壳&重打包等
3、安全点-资产&接口&漏洞&审计等
```

演示案例：

- 内在-资产提取-AppinfoScanner
- 内在-安全评估-MobSF&mobexler
- 外在-证书抓包-Frida-server&r0capture

#内在-资产提取-AppinfoScanner

AppinfoScanner 一款适用于以 HW 行动/红队/渗透测试团队为场景的移动端(Android、iOS、WEB、H5、静态网站)信息收集扫描工具，可以帮助渗透测试工程师、攻击队成员、红队成员快速收集到移动端或者静态 WEB 站点中关键的资产信息并提供基本的信息输出,如：Title、Domain、CDN、指纹信息、状态信息等。

https://github.com/kelvinBen/AppInfoScanner

#内在-安全评估-MobSF&mobexler

-移动安全框架 (MobSF) 是一种自动化的一体化移动应用程序(Android/iOS/Windows) 渗透测试、恶意软件分析和安全评估框架，能够执行静态和动态分析。MobSF 支持移动应用程序二进制文件（APK、XAPK、IPA 和 APPX）以及压缩源代码，并提供 REST API 以与您的 CI/CD 或 DevSecOps 管道无缝集成。动态分析器可帮助您执行运行时安全评估和交互式仪器测试。

-Mobexler 是基于 Elementary OS 的定制虚拟机，旨在帮助进行 Android 和 iOS 应用程序的渗透测试。Mobexler 预装了各种开源工具，脚本，黑客必备软件等，这些都是安全测试 Android 和 iOS 应用程序所必需的。

https://mobexler.com/

https://github.com/MobSF/Mobile-Security-Framework-MobSF

```
docker pull opensecurity/mobile-security-framework-mobsf
docker run -it -p 8008:8000 opensecurity/mobile-security-framework-mobsf:latest
```

#外在-证书抓包-frida-server&r0capture

-r0capture 仅限安卓平台，测试安卓 7、8、9、10、11 可用 ；

无视所有证书校验或绑定，不用考虑任何证书的事情；

通杀 TCP/IP 四层模型中的应用层中的全部协议；

通杀协议包括：Http,WebSocket,Ftp,Xmpp,Imap,Smtp,Protobuf 等、及它们的 SSL 版本；

通杀所有应用层框架，包括 HttpUrlConnection、Okhttp1/3/4、Retrofit/Volley 等等；

无视加固，不管是整体壳还是二代壳或 VMP，不用考虑加固的事情；

-Firda 是一款易用的跨平 Hook 工具， Java 层到 Native 层的 Hook 无所不能，是一种 动态 的插桩工具，可以插入代码到原生 App 的内存空间中，动态的去监视和修改行为，原生平台包括 Win、Mac、Linux、Android、iOS 全平台。

测试环境：

Windows10 Python3.7 夜神模拟器 r0capture frida-server wireshark

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址