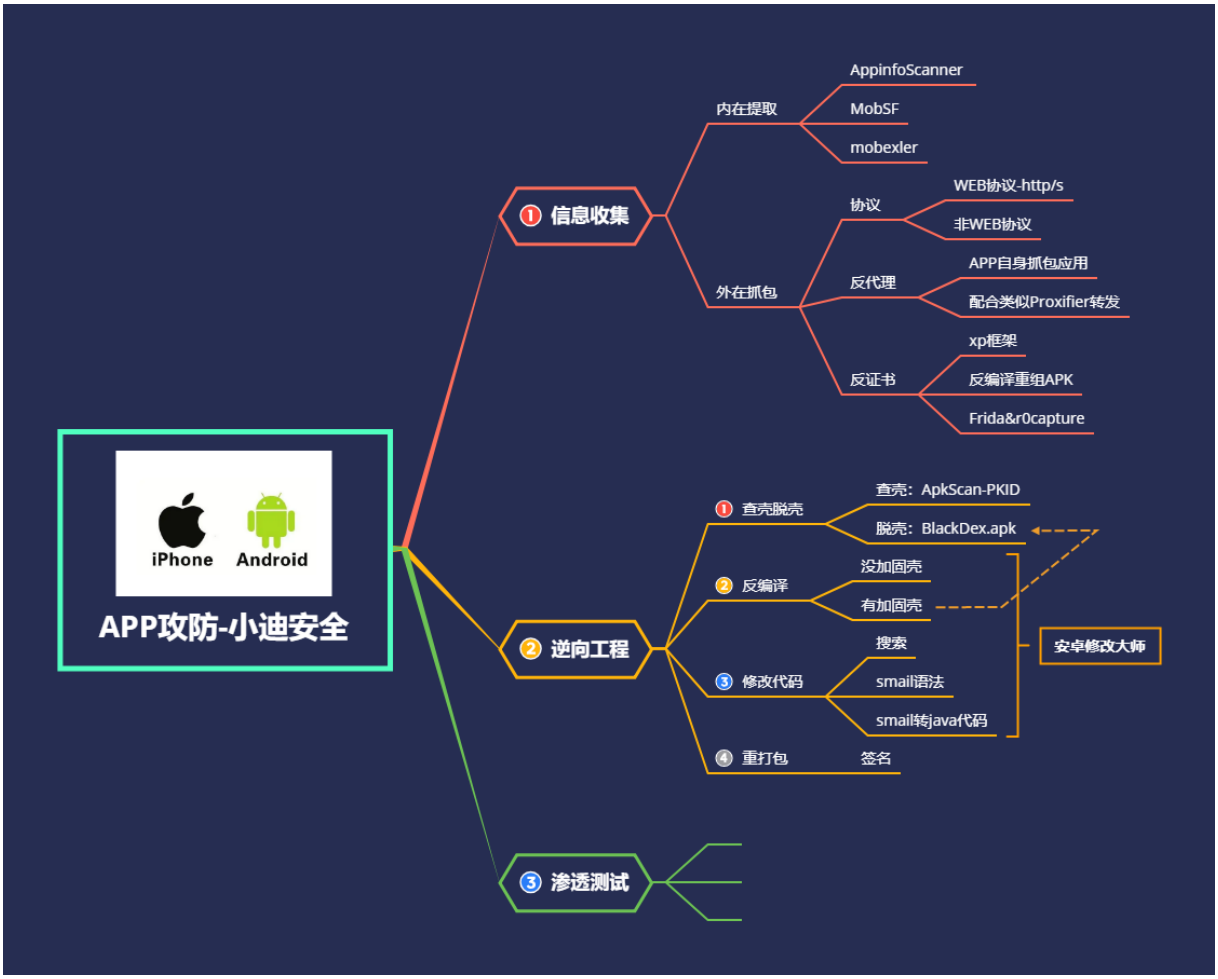
APP 攻防-微信小程序&解包反编译&数据抓包&APK 信息资源提取



#知识点：

0、APK 信息资源提取

1、微信小程序-数据抓包

2、微信小程序-解包反编译

#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：

- APP&APK-信息资源文件提取
- 微信小程序-真机&模拟器数据抓包
- 微信小程序-PC&模拟器分包反编译

#APP&APK-信息资源文件提取

APK Messenger-基本信息&资源文件&开启权限等

#微信小程序-机&模拟器数据抓包

安卓系统抓包（微信小程序）：

1、安卓系统 7.0 以下版本，不管微信任意版本，都会信任系统提供的证书

2、安卓系统 7.0 以上版本，微信 7.0 以下版本，微信会信任系统提供的证书

3、安卓系统 7.0 以上版本，微信 7.0 以上版本，微信只信任它自己配置的证书列表

基于上述我们解决的方式如下：

1、将证书安装到系统证书中（需要 root）

2、苹果手机（苹果手机不受此影响）

3、采用安卓系统低于 7.0 的模拟器

演示：逍遥模拟器 5.1 安卓系统微信小程序抓包

演示：夜神模拟器多开 5 安卓系统微信小程序抓包

演示：真机 IPhone-IOS 系统微信小程序抓包

#微信小程序-PC&模拟器分包反编译

1、高富帅版：

欢迎使用多功能小程序助手工具，点击确定开始使用。

免责声明：不得将小程序反编译源码程序和反编译图片素材挪作商业或盈利用

使用教程地：https://www.kancloud.cn/ludeqi/xcxzs/2607637

最新版下载地址：https://xcx.siqingw.top/xcx.zip

2、穷屌丝版：

https://github.com/sanriqing/WxAppUnpacker

-安装 node.js

http://nodejs.cn/download/

-安装依赖：

npm install

-模拟器取出 wxapkg 文件：

/data/data/com.tencent.mm/MicroMsg/xxxxxx/appbrand/pkg

-反编译解包

node wuWxapkg.js -s=../ xxxx.wxapkg

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址