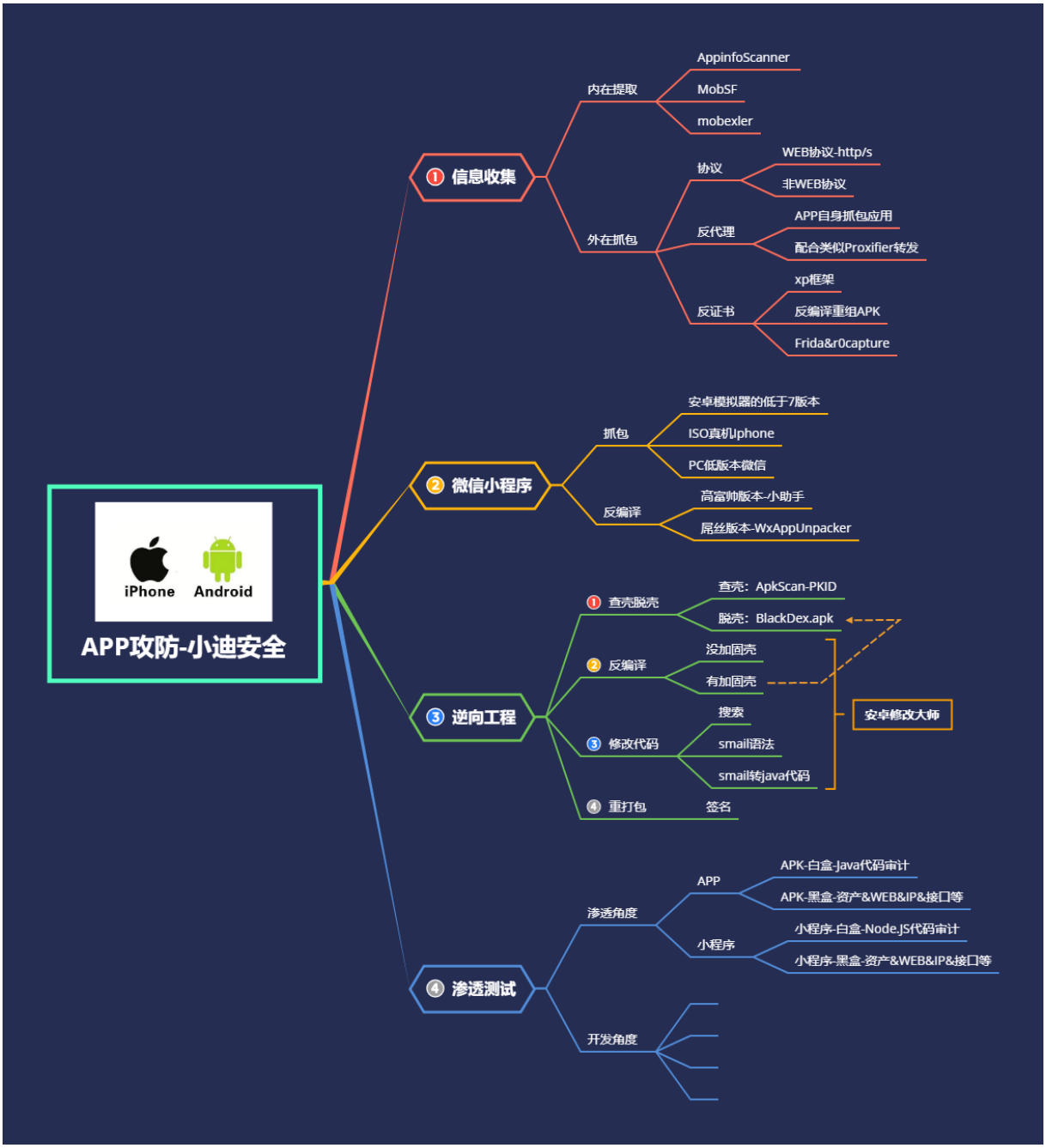
APP 攻防-实战拿下&Springboot 未授权&HeapDump 提取&OSS 利用



#知识点：

0、APK-反编译&抓包

1、SpringBoot-漏洞利用

2、HeapDump-分析提取

3、AccessKEY-利用后续

#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

#安全点：

1、渗透角度：测试的 app 提供服务的服务器，网站，接口等，一旦这个有安全问题，被不法分子利用，相当于 APP 正常服务就会受到直接的影响！

APK-白盒-Java 代码审计

APK-黑盒-资产&WEB&IP&接口等

小程序-白盒-Node.JS 代码审计

小程序-黑盒-资产&WEB&IP&接口等

2、开发角度：测试的 app 里代码的设计安全，采用没加密的发送数据，采用权限过高的设置导致攻击者利用 app 获取到手机的敏感信息等。

弱加密，逻辑安全，授权，中间人等

演示案例：

➢ 对着操作讲解-吃瓜就完事了

安全测试报告：

1、Spring Boot Actuator v2 未授权访问

2、Spring Boot RCE

3、HeapDump-信息泄漏-帐号密码等

```
select s from java.lang.String s
    where /pass/.test(s.value.toString())
```

-HeapDump 分析：

JVisualVM MAT heapdump_tool 等

JVisualVM：jdk 自带

MAT：https://www.eclipse.org/mat/downloads.php

heapdump_tool：https://github.com/wyzxxz/heapdump_tool

-Actuator 未授权检测：

https://github.com/rabbitmask/SB-Actuator

-SpringBoot 漏洞利用：

https://github.com/LandGrey/SpringBootVulExploit

-OSS_AccessKey 利用：

https://github.com/mrknow001/aliyun-accesskey-Tools

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址
