Day09　信息收集–APP及其他资产等

> 在安全测试中，若WEB无法取得进展或无WEB的情况下，我们需要借助APP或其他资产在进行信息收集,从而开展后续渗透

9.1 APE提取——一键反编译提取

- 使用反编译工具，尝试获取包了里的源码

9.2 APP抓数据包进行工具配合

- 使用burp suite设置代理，或者wireshark抓数据包，进行分析

9.3 各种第三方应用相关探针技术

- https://www.shodan.io/
- https://fofa.so/

记录

使用burp代理模拟器时，提示证书错误，后将burp生成的证书导入后正常，导入时需要将.cer改成.der。