



漏洞发现-APP 应用之漏洞探针类型利用修复

漏洞发现-小迪安全



#思路说明:

反编译提取 URL 或抓包获取 URL, 进行 WEB 应用测试, 如不存在或走其他协议的情况下, 需采用网络接口抓包进行数据获取, 转至其他协议安全测试!

#APP->WEB APP->其他 APP->逆向

#WEB 抓包, 其他协议抓包演示及说明

#未逆向层面进行抓包区分各协议测试

#逆向层面进行提取 APK 代码层面数据

#<https://www.cnblogs.com/L0ading/p/12388928.html>

案例演示:

- 抓包工具 WEB 协议面使用说明
- 抓包工具非 WEB 协议面使用说明
- 安卓逆向便捷 APK 一键提取 URL 演示
- 利用 Burp 筛选及联动功能打出军体拳
- 模拟器四个违法案例 APP 安全分析测试

涉及资源:

<https://www.wireshark.org/download.html>

<https://www.charlesproxy.com/latest-release/download.do>

<https://github.com/huolizhuminh/NetWorkPacketCapture/releases>

<https://pan.baidu.com/s/1UGro7nQoBpT9vYRONsQi4w> 提取码:

xiao
