移动应用安全检测清单

客户端

- 应用可被进行逆向工程/缺乏代码混淆
- 跨站脚本攻击
- 认证绕过
- 应用代码中存在硬编码敏感信息 (包含秘钥)
- 恶意文件上传
- 固定会话攻击
- 权限提升
- SQL 注入
- 双因子认证绕过
- LDAP 注入
- 系统命令执行
- iOS snapshot/backgrounding 漏洞 (iOS)
- Debug 设置为 TRUE (Andriod)
- 应用使用不安全的加密方式
- 在SSL 隧道下传递明文信息
- 客户端验证可被绕过

- 非法的 SSL 证书
- 敏感信息明文(缺乏数据保护)传输
- 登录页面缺乏验证码机制
- 修改密码页面未设计或设计不当
- 应用日志文件存放敏感信息
- 敏感信息作为参数传递
- 敏感信息可通过内存 Dump
- 应用允许运行在已root或越狱的设备上
- 返回刷新（Back-and-Refresh）攻击
- 目录浏览
- Cookie过期机制设计不当
- URL 重定向攻击
- 代码中缺乏异常处理机制或设计不当
- 不安全的应用权限
- 未确认证书链
- 内网 IP 泄露
- 通过修改 RMS/JAR 文件显示 UI
- 操作过期或已被释放的资源
- 未设置证书锁定机制（Certificate Pinning）/ SSL通信未检查证书有效性
- 应用关闭后缓存的Cookie或敏感信息未被删除
- 未使用 ASLR
- Android ADB 备份漏洞
- 数据存储未加密的认证信息 (sqlite db)
- 在 APP 沙盒外存储敏感信息 (在 SDCard 上)
- 应用数据允许全部权限
- 秘钥或敏感数据明文存储
- 证书锁定机制（Certificate Pinning）绕过
- 忽略证书验证
- 忽略 SSL 证书错误
- Weak Custom Hostname Verifier
- App/Web 缓存的敏感文件泄露
- 授权额外权限

- 使用可被伪造的内容（IMEI, UDID）进行用户验证
- 使用不安全或已被弃用的算法
- 本地文件包含 (可能通过 XSS 漏洞)
- Android Activity 劫持
- Android 应用服务劫持
- Android 广播窃取
- Android 恶意广播注入
- 使用设备标识符作为 Session
- 缺乏和校验或文件篡改检测

服务器端

- 响应包返回明文密码
- 未授权引用内网文件
- 后端对缺乏会话管理或会话设计不当
- 跨域脚本漏洞
- 服务器端缺乏输入验证机制
- 错误页面泄露敏感信息
- 应用允许除 GET 和 POST 外的其他 HTTP 方法
- 跨站伪造请求/服务器端请求伪造
- Cookie 中未设置 Path、HttpOnly、Secure 属性
- 应用可被点击劫持或触屏劫持
- 缺乏适当的超时机制
