

APP人工渗透测试

服务介绍

北京智游网安科技有限公司

目 录

[1 移动应用人工渗透测试服务介绍 2](#_Toc501117258)

[1.1 检测依据 2](#_Toc501117259)

[1.2 安卓人工渗透测试 2](#_Toc501117260)

[1.2.1 审计常规工具 2](#_Toc501117261)

[1.2.2 安全分析内容 3](#_Toc501117262)

[1.3 iOS人工渗透测试服务介绍 5](#_Toc501117263)

[1.3.1 程序安全 5](#_Toc501117264)

[1.3.2 数据安全 5](#_Toc501117265)

[1.3.3 网络传输安全 6](#_Toc501117266)

[1.3.4 业务安全 6](#_Toc501117267)

[1.3.5 动态调试安全 7](#_Toc501117268)

# 移动应用人工渗透测试服务介绍

爱加密人工渗透测试服务，是基于移动应用程序数据的完整生命周期的安全检测服务。从黑客思维和调试角度出发，多方面对移动应用的程序安全、数据安全、业务逻辑安全、系统环境安全等内容进行静态、动态的人工分析，以获取应用安装卸载的过程、用户数据的输入、存储处理、网络传输以及所处系统环境等方面的安全隐患，为应用加固提供专业的可靠依据。

## 检测依据

* **《信息安全技术移动智能终端个人信息保护技术要求》**
* **《YD/T 1438-2006 数字移动台应用层软件功能要求和测试方法》**
* **《YD/T 2307-2011 数字移动通信终端通用功能技术要求和测试方法》**
* **《电子银行业务管理办法》**
* **《电子银行安全评估指引》**
* **《中国金融移动支付客户端技术规范》**
* **《中国金融移动支付应用安全规范》**
* **《移动互联网应用软件安全评估大纲》**

## 安卓人工渗透测试

### 审计常规工具

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具名称** | **类别说明** | **功能描述** |
| **1** | AndroidKiller | 反编译工具 | AndroidKiller集成了apktool、dex2jar、jd-gui、signapk.jar等各款流行的apk线性反编译工具，能集中实现对apk的反编译、查看Java代码、回编译、签名等操作。 |
| **2** | Jeb | 反编译工具 | Jeb可将apk、dex文件转化为smali、java等代码，且可读性极高，方便方法逻辑的逆向分析。 |
| **3** | IDA Pro | 二进制工具 | Ida Pro是二进制分析工具，可以对apk中C/C++代码编写的so文件进行流程分析，其附带的F5插件功能更是可以将ARM汇编生成伪代码，方便查看逻辑。 |
| **4** | Fiddler2 | 抓包工具 | 在同一局域网内，通过代理的方式将手机端的流量转向该工具，从而对特定APP的网络传输数据进行分析。 |
| **5** | DDMS | 开发工具 | 在adb桥连手机的情况下，使用DDMS监视Android系统上APP运行产生的流程日志。 |
| **6** | 应用劫持 | 劫持工具 | 应用劫持是爱加密开发的一款在Android手机上对特定界面进行劫持的小工具，通过它来检测APP是否有防止界面劫持的提示。 |
| **7** | Inject | 注入工具 | Inject是爱加密为测试进程注入而来发的Native工具，在执行命令后，会将同路径下的libhello.so注入到指定的进程中。 |

### 安全分析内容

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 漏洞大类 | 漏洞点 | 检测结果 |
| 1 | 身份鉴别 | 身份鉴别安全 | **高危** |
| 2 | 登录限制策略 | **中危** |
| 3 | 会话管理机制 | **高危** |
| 4 | 访问控制 | 敏感组件安全 | **低危** |
| 5 | 敏感数据安全 | **中危** |
| 6 | 系统安全审计 | 系统安全审计分析 | **低危** |
| 7 | 源码控制安全 | 源码反编译安全 | **高危** |
| 8 | 二次打包安全 | **高危** |
| 9 | 键盘监控安全 | **低危** |
| 10 | 屏幕截屏安全 | **低危** |
| 11 | 签名校验安全 | **中危** |
| 12 | 代码质量分析 | 输入验证安全 | **低危** |
| 13 | API误用 | 安全 |
| 14 | 硬编码安全 | 安全 |
| 15 | 日志控制安全 | **低危** |
| 16 | 时间和状态 | 安全 |
| 17 | 异常处理 | 安全 |
| 18 | 安全漏洞分析 | WebView远程代码执行 | **低危** |
| 19 | HTTPS主机名验证安全 | 安全 |
| 20 | URL攻击漏洞 | 安全 |
| 21 | WebView忽略SSL证书漏洞 | 安全 |
| 22 | Intent隐式调用意图 | **低危** |
| 23 | X509 TrustManager信任任意证书 | 安全 |
| 24 | Dex动态加载风险 | 安全 |
| 25 | 弱加密算法风险 | **中危** |
| 26 | 本地SQL注入 | 安全 |
| 27 | 拒绝服务漏洞 | **中危** |
| 28 | 文件遍历漏洞 | 安全 |
| 29 | allowbackup备份风险 | 安全 |
| 30 | 其他安全漏洞 | 界面劫持安全 | **中危** |
| 31 | 进程注入安全 | **中危** |
| 32 | 任意资源文件篡改风险 | **低危** |

## iOS人工渗透测试服务介绍

### 程序安全

#### iPA砸壳解包分析

通过APP Store商城发布的iPA包都经过了苹果官方的一层加壳，要想分析一款iPA应用就必须把外壳“砸”掉，一般使用工具Clutch/ Dumpdecrypted。对于iPA的解包，是因为iPA其实是一个ZIP+签名的执行程序，解压之后里面的文件基本一览无余。

#### 源码头Dump安全

iOS程序iPA使用的是O-bject语言进行编写，像apk一样包含了各种类、方法、字段、控件等，通过class-dump可以将已经砸壳的iPA程序中的类名、方法名、字段名称以及他们之间的相关继承、调用关系都罗列出来，极大的方便了逆向分析。

#### HTML5的安全

虽然HTML5的盛行，越来越多的客户端开始使用HTML5进行编写，甚至包括一些金融、银行、购物商城等用户信息相对敏感的APP。HTML5看到即是源码，一般分为本地加载和线上加载两种形式，HTML5本地文件通常在apk包中的assets下的某个文件夹中，包括.html/.js/.css和一些图。.html是布局，.js是方法逻辑，.css是样式。线上也可以通过抓包进行下载分析。检测分析的主要是js的加密代码是否安全。

#### 主程序逆向分析风险

如果ipa在编译时未使用混淆编译，或者借助第三方提供的安全编译手段，在使用IDA Pro对其进行反编译时，根据类名、方法名、字符串等都可以很迅速的定位到关键核心要分析的代码处分析，从而大大降低了分析定位的时间成本。

### 数据安全

#### 敏感界面截屏安全

客户端的敏感界面，如登录界面、注册界面、支付界面等，用户再输入敏感信息时，如登录密码、支付密码、银行卡号等，无论调用的是系统默认输入法，还是第三方的安全键盘都会有明文回显的可能，这时候被黑客连续非法截屏会造成密码的泄露。

**解决方式**：控制好敏感字符的回显。

#### 日志泄露隐私风险

在APP的开发过程中，为了方便调试，通常会使用log函数输出一些关键流程的信息，这些信息中通常会包含敏感内容，如执行流程、明文的用户名密码等，这会让攻击者更加容易的了解APP内部结构方便破解和攻击，甚至直接获取到有价值的敏感信息。

#### 敏感数据明文储存漏洞

大部分APP为了方便用户再次打开客户端的登录，往往会把登录凭证保存在本地，比如登录token、session、cookie、手势密码、账号密码等，如果这些凭证都是明文保存，就可能被有权限的恶意第三方应用所窃取，造成用户敏感信息的泄露。

### 网络传输安全

#### HTTPS请求中间人攻击漏洞

HTTPS请求中间人攻击漏洞是指开发者在封包传递时虽然使用了SSL加密链接，但是由于没有严格校验SSL证书，造成了可被抓包分析明文数据、修改封包重发的危险漏洞。

#### 网络协议数据安全

客户端内的Post/Get请求的数据是否明文；加密的数据、各个参数的生成是否可在客户端进行逆向分析，这关系到程序的业务逻辑，如果若是弱加密、接口校验不足将影响到业务安全。

### 业务安全

#### 手机验证码机制的安全

客户端APP在进行账号注册、找回密码、登陆的时候一般会关联到手机号码，几乎都是验证码凭证来对身份验证，如果验证码机制缺陷，比如验证码的错误次数无限制、返回封包包含验证码、验证码本地生成、最终完成注册的请求脱离验证码验证等，都可能会造成验证码存在爆破风险、任意手机号码注册、重置任意手机号码账号、任意手机号码登录等危害比较大的漏洞。

#### 越权访问平行漏洞

含有账号机制的客户端，不同的账号会有不同的订单、财产金额、银行卡号、基本信息、消费记录、投资记录等敏感信息，如果在进行这些业务的查询时，不严格校验请求封包身份凭证，就有可能造成平行越权访问的漏洞，泄露数据库中所有账户的敏感信息。

### 动态调试安全

#### Introspy追踪分析程序

Introspy是一种开源的、对iOS系统中某个程序的数据流转做运行跟踪分析，并将结果以db数据库、HTML网页友好展示出来的动态分析工具。从中可以分析跟踪出程序所有的HTTP/HTTPS请求封包、数据的加密解密、数据储存读取等。

#### Cycript调试程序

Cycript相当于Objective-C语法的javascript解释器，这意味着它能够在一个命令中用Objective-C或者 javascript。它能够挂钩正在运行的进程，从而修改程序运行时的内存数据。