无标题-4

|  |  |  |  |
| --- | --- | --- | --- |
| 平安普惠外访APP Android版本  渗透测试报告 | | | |
| ■ 文档编号 |  | ■ 密级 | 商业机密 |
| ■ 版本编号 |  | ■ 日期 | 2017.8.17 |



|  |
| --- |
| © 2017 绿盟科技 |

|  |
| --- |
| ■ 版权声明 |
| 本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。 |

|  |  |  |  |
| --- | --- | --- | --- |
| ■ 版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
| 2017-8-17 | 1.0 | 文档创建 | 李蒙蒙 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| ■ 适用性声明 |
| 本文档为绿盟科技为平安普惠外访移动终端应用测试Android客户端出具的测试报告。 |

|  |
| --- |
| 目录 |
| [一. 测试环境 3](#_Toc490812679)  [1.1 APP安全测试目标基本信息 3](#_Toc490812680)  [二. 测试结果汇总 3](#_Toc490812681)  [三. 测试结果详述 5](#_Toc490812682)  [3.1 客户端程序安全 5](#_Toc490812683)  [3.1.1 [高]客户端程序保护 5](#_Toc490812684)  [3.1.2 [安全]安装包签名 6](#_Toc490812685)  [3.1.3 [高]应用完整性校验 6](#_Toc490812686)  [3.1.4 [安全]内存访问和修改 7](#_Toc490812687)  [3.2 敏感信息安全 8](#_Toc490812688)  [3.2.1 [安全]私有目录下的文件权限 8](#_Toc490812689)  [3.2.2 [安全]私有目录文件的安全性 9](#_Toc490812690)  [3.2.3 [安全]Logcat日志 10](#_Toc490812691)  [3.3 密码软键盘安全性 10](#_Toc490812692)  [3.3.1 [安全]键盘劫持测试 10](#_Toc490812693)  [3.3.2 [低]屏幕录像测试 11](#_Toc490812694)  [3.4 安全策略 12](#_Toc490812695)  [3.4.1 [中]帐户锁定策略 12](#_Toc490812696)  [3.4.2 [低]会话安全设置 13](#_Toc490812697)  [3.4.3 [低]界面切换保护 14](#_Toc490812698)  [3.4.4 [中]界面劫持保护 15](#_Toc490812699)  [3.4.5 [安全]UI 信息泄露 16](#_Toc490812700)  [3.4.6 [安全]帐号登录限制 17](#_Toc490812701)  [3.4.7 [安全]安全退出 18](#_Toc490812702)  [3.4.8 [中]图形验证码安全性 19](#_Toc490812703)  [3.5 手势密码安全性 20](#_Toc490812704)  [3.5.1 [安全]手势密码复杂度 20](#_Toc490812705)  [3.5.2 [安全]手势密码修改和取消 21](#_Toc490812706)  [3.5.3 [高]手势密码本地信息保存 22](#_Toc490812707)  [3.5.4 [安全]手势密码锁定策略 22](#_Toc490812708)  [3.5.5 [安全]手势密码抗攻击测试 23](#_Toc490812709)  [3.6 通信安全 24](#_Toc490812710)  [3.6.1 [低]通信加密 24](#_Toc490812711)  [3.6.2 [中]关键数据加密和校验 25](#_Toc490812712)  [3.6.3 [安全]访问控制 26](#_Toc490812713)  [3.7 业务安全 27](#_Toc490812714)  [3.7.1 [高]待外访列表查询平行越权 27](#_Toc490812715)  [3.7.2 [高]查询客户详情等平行越权（多处） 28](#_Toc490812716)  [3.7.3 [高]查询客户电话列表平行越权 29](#_Toc490812717)  [3.7.4 [高]查询客户地址列表平行越权 30](#_Toc490812718)  [3.7.5 [高]外访资料上传处任意文件上传 31](#_Toc490812719)  [四. 感谢 32](#_Toc490812720)  [附录A 移动终端APP安全测试服务概述 32](#_Toc490812721)  [4.1 移动终端APP测试概述 32](#_Toc490812722)  [4.2 工作流程 33](#_Toc490812723)  [4.3 风险管理及规避 33](#_Toc490812724)  [4.3.1 时间 34](#_Toc490812725)  [4.3.2 工具使用 34](#_Toc490812726)  [4.3.3 技术手段 34](#_Toc490812727)  [4.3.4 监控 34](#_Toc490812728)  [4.3.5 目标的选择 34](#_Toc490812729)  [4.4 收益 35](#_Toc490812730)  [附录B App测试安全等级划分 35](#_Toc490812731)  [附录C 工具及相关资源 37](#_Toc490812732) |

1. 测试环境
   1. APP安全测试目标基本信息

|  |  |
| --- | --- |
| **目标名称** | **目标信息** |
| **平安普惠外访手机客户端** | 版本Version 2.4.5 |
| **外访业务服务端** | https://test1-cfs-ms.pa18.com:41443/ |

1. 测试结果汇总

| **测试分类** | **测试项目** | **测试结果** | **风险等级** |
| --- | --- | --- | --- |
| 客户端程序  安全 | 客户端程序保护 | **不安全** | 高 |
| 安装包签名 | **安全** | - |
| 应用完整性校验 | **不安全** | 高 |
| 内存访问和修改 | **安全** | - |
| 敏感信息安全 | 私有目录下的文件权限 | **安全** | - |
| 私有目录文件的安全性 | **安全** | - |
| Logcat日志 | **安全** | - |
| 密码软键盘  安全性 | 键盘劫持测试 | **安全** | - |
| 屏幕录像测试 | **不安全** | 低 |
| 安全策略 | 账户锁定策略 | **不安全** | 中 |
| 会话安全设置 | **安全** | 低 |
| 界面切换保护 | **不安全** | 低 |
| 界面劫持保护 | **不安全** | 中 |
| UI信息泄露 | **安全** | - |
| 账号登录限制 | **安全** | - |
| 安全退出 | **安全** | - |
| 图形验证码安全性 | **不安全** | 中 |
| 手势密码安全性 | 手势密码复杂度 | **安全** | - |
| 手势密码的修改和取消 | **安全** | - |
| 手势密码本地信息保存 | **不安全** | 高 |
| 手势密码锁定策略 | **安全** | - |
| 手势密码抗攻击测试 | **安全** | - |
| 通信安全 | 通信加密 | **不安全** | 低 |
| 关键数据加密和校验 | **不安全** | 中 |
| 访问控制 | **安全** | - |
| 业务安全 | 待外放列表查询平行越权 | **不安全** | 高 |
| 查询客户详情等平行越权（多处） | **不安全** | 高 |
| 查询客户电话列表平行越权 | **不安全** | 高 |
| 查询客户地址列表平行越权 | **不安全** | 高 |
| 外访资料上传处任意文件上传 | **不安全** | 高 |

通过对平安普惠外访手机客户端进行测试后，结果如下：

风险分布统计：共测试30项，其中高危8个，中危4个，低危4个，比例如下图所示：

**结论：**

从APP安全测试结果和威胁分析中可见，平安普惠外访手机客户端及服务器系统作为一个承载外访业务的交互平台，但是却因通信存在安全风险，客户端存在接口泄露，服务器存在业务安全逻辑风险，影响了用户的数据安全。

1. 测试结果详述
   1. 客户端程序安全
      1. [高]客户端程序保护

问题描述：

判断是否能反编译为源代码，是否存在代码保护措施。

威胁等级：

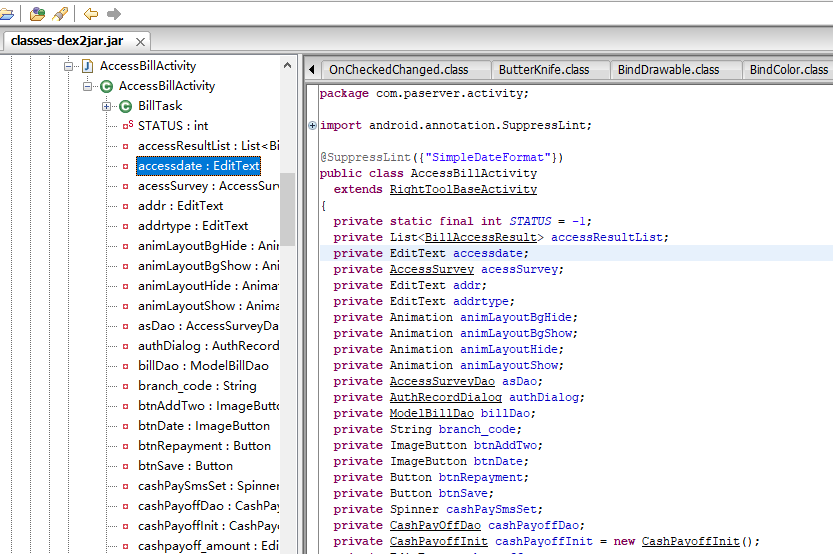
**高，未进行代码混淆等保护措施，可反编译为可读源代码。**

测试步骤：

1. 解压apk文件得到核心文件classes.dex，通过工具将其转换为jar包。



1. 使用工具观察jar包源码，确定代码部分是否进行混淆。（如下图可见应用没有进行代码混淆）



安全建议：

建议客户端进行加壳处理防止攻击者反编译客户端，同时混淆客户端代码，并且一定要对核心代码进行代码混淆。

* + 1. [安全]安装包签名

问题描述：

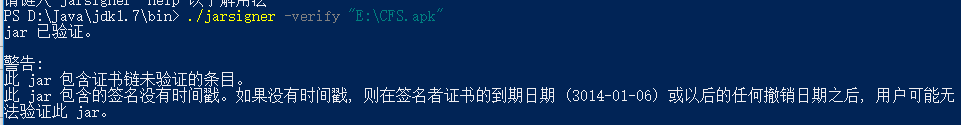
检测客户端安装包是否正确签名。通过签名，可以检测出安装包在签名后是否被修改过。

**威胁等级：**

安全

测试步骤：

使用工具检查安装包的签名。如下图所示：



* + 1. [高]应用完整性校验

问题描述：

测试客户端程序安装后，在每次启动时是否对自身文件进行完整性校验。

**威胁等级：**

**高，应用启动时未进行完整性校验。**

测试步骤：

1. 取出安装APK的资源文件。
2. 修改背景图片的内容。



1. 将修改过的apk导入设备并覆盖掉原有的apk。
2. 启动该应用，发现可以正常登录。该应用没有进行相应的完整性校验。



安全建议：

建议客户端在每次开机启动时进行客户端自身的应用完整性校验，在验证逻辑中不使用MANIFEST.MF中的数据作为验证凭证，同时需验证是否有不属于该客户端版本的新文件添加，验证过程于服务器端完成。

* + 1. [安全]内存访问和修改

**问题描述：**

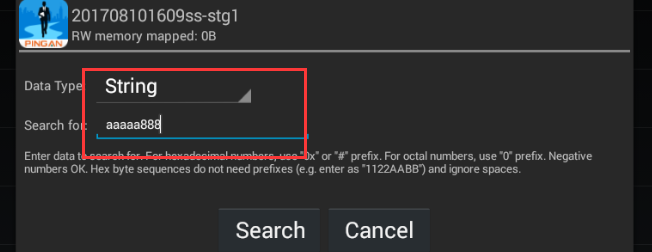
通过对客户端内存的访问，木马将有可能会得到保存在内存中的敏感信息（如登录密码，帐号等）。测试客户端内存中是否存在的敏感信息（卡号、明文密码等等）。

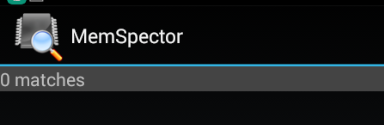
**威胁等级：**

安全，内存中没有敏感信息。

**测试步骤：**

使用MemSpector查看、搜索和修改客户端内存数据，如图所示。可见内存中没有敏感信息。





* 1. 敏感信息安全
     1. [安全]私有目录下的文件权限

**问题描述：**

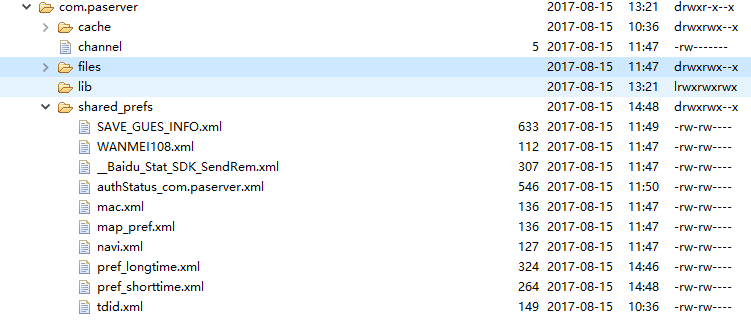
测试客户端私有目录下的文件权限是否设置正确，非root账户是否可以读，写，执行私有目录下的文件。

**威胁等级：**

安全，未发现目录和文件权限不合理的地方。

**测试步骤：**

1. 打开应用对应的私有目录文件夹，分别观察所有目录和文件的权限是否配置得当。



* + 1. [安全]私有目录文件的安全性

**问题描述：**

检测手机私有目录文件的安全性，判断是否有敏感信息的明文存储。

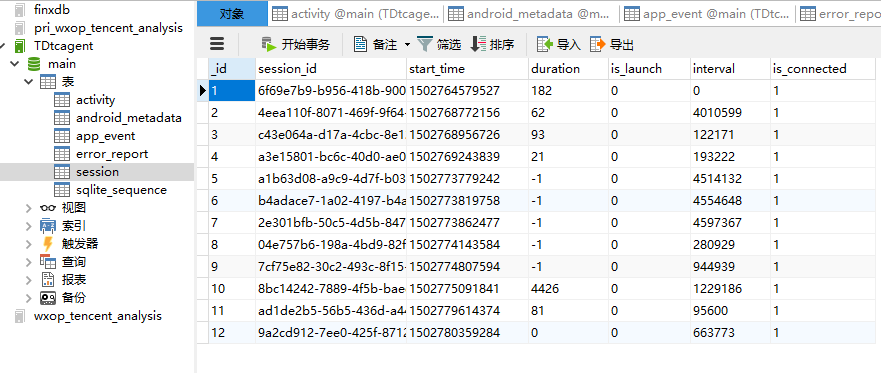
**威胁等级：**

安全，没有明文保存用户密码。

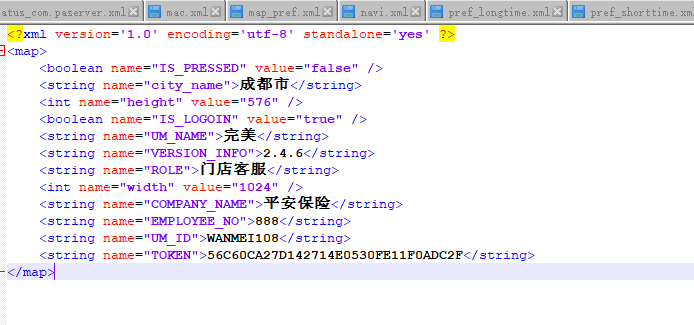
**测试步骤：**

1. 依次打开私有目录下所有文件,观察是否保存用户敏感信息，如下图所示：

数据库文件



XML文件



* + 1. [安全]Logcat日志

**问题描述：**

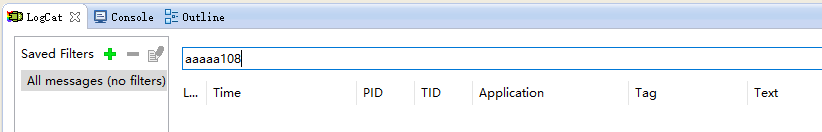
检测客户端对应的Logcat日志是否会打印一些用户或服务器的敏感信息。

**威胁等级：**

安全，没有明文密码信息。

**测试步骤：**

1. 运行客户端，正常进行登陆等敏感操作。
2. 观察Logcat日志中，没有发现1中操作对应的敏感信息（用户密码）。



* 1. 密码软键盘安全性
     1. [安全]键盘劫持测试

**问题描述：**

测试客户端程序在密码等输入框是否使用自定义软键盘。安卓应用中的输入框默认使用

系统软键盘，手机安装木马后，木马可以通过替换系统软键盘，记录应用的密码。

**威胁等级：**

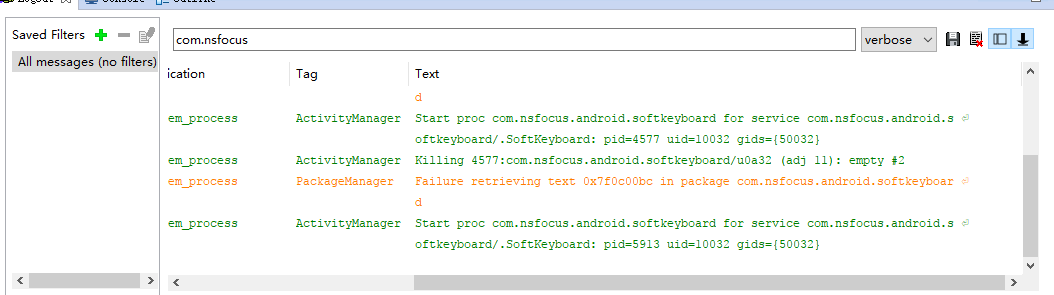
安全，键盘记录器没有成功打印出击键信息。

**测试步骤：**

1. 安装键盘记录器。
2. 在手机设置->语言和键盘设置中，勾选上一步骤安装的键盘记录器。



1. 打开客户端正常进行登录操作。
2. 查看logcat 日志观察是否3中操作的用户名和密码被记录。



* + 1. [低]屏幕录像测试

**问题描述：**

测试通过连续截图，是否可以捕捉到用户密码输入框的密码。

**威胁等级：**

**低，通过连续截图可获得用户密码。**

**测试步骤：**

1. 打开客户端，进入手机客户端登录页面。
2. 在输入账号的同时，进行连续截图，可以获取用户点击的按键，观察账号部分和密码输入部分。



**安全建议：**

建议客户端针对第三方或系统截屏编写抵抗逻辑，例如屏蔽和截屏相关的函数或是当客户端处于进程栈顶层时将截屏图片用纯黑色图片对象进行覆盖。

* 1. 安全策略
     1. [中]帐户锁定策略

**问题描述：**

测试客户端是否限制登录尝试次数。防止木马使用穷举法暴力破解用户密码。

**威胁等级：**

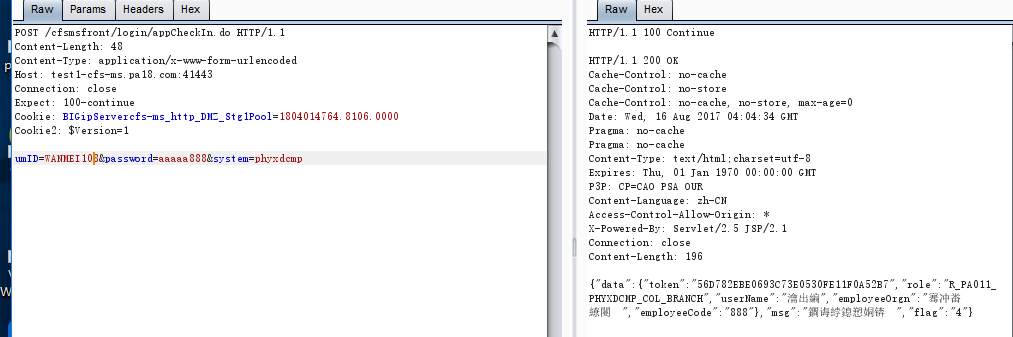
**中，登陆时校验了验证码，但校验码可绕过，仍存在暴力破解风险。**

**测试步骤：**

1. 打开客户端，使用错误的登录密码登录。结果如图：



1. 抓取登陆数据包，发现登陆数据包中没有图形校验码信息，因此可以通过数据包重放绕过图形校验码校验，从而进行暴力破解。



**安全建议：**

建议在服务端编写账户锁定策略的逻辑，当一天内多次输入密码错误时进行账号锁定以防止攻击者通过暴力猜解密码。

* + 1. [低]会话安全设置

**问题描述：**

测试客户端在一定时间内无操作后，是否会使会话超时并要求重新登录。超时时间设置

是否合理。

**威胁等级：**

**低，没有限制会话超时时间。**

**测试步骤：**

1. 登录手机客户端，然后不进行任何操作。
2. 长时间无任何操作后，客户端仍可进行修改手势密码等危险操作。



**安全建议：**

建议在客户端编写会话安全设置的逻辑，当10分钟或20分钟无操作时自动退出登录状态或是关闭客户端。

* + 1. [低]界面切换保护

**问题描述：**

检查客户端程序在切换到后台或其他应用时，是否能恰当响应（如清除表单或退出会话），防止用户敏感信息泄露。

**威胁等级：**

**低，切换页面时存在登陆信息残留的情况。**

**测试步骤：**

1. 在登录界面，输入正确的登录名和密码，如图所示：



1. 点击手机的HOME 键，切换到桌面，然后再切换回应用，登录界面的用户名和密码依然存在，并可以登录。



**安全建议：**

建议客户端添加响应的逻辑，在进行进程切换操作时提示用户确认是否为本人操作。

* + 1. [中]界面劫持保护

**问题描述：**

检查客户端是否对非正常的界面切换进行检测，并对用户进行提示。

**威胁等级：**

**中，攻击者可以通过界面劫持+钓鱼攻击的方法获取到用户的登录信息。**

**测试步骤：**

1. 安装界面劫持测试工具，输入手机客户端对应进程名，如图所示：

配置好界面劫持测试工具后，运行客户端。若劫持工具弹出自己的界面，成功覆盖手机客户端界面，则证明客户端未进行界面劫持保

**安全建议：**

由于Activity界面劫持攻击通常是将自己的页面附着在客户端之上，因此需要进行界面切换操作，因此使用界面切换保护的安全建议可以达到一定的效果。除此之外，因为Android进程栈的工作原理，建议开发客户端时针对进程栈进行相应的保护，可禁止其他进程放置于客户端之上。

* + 1. [安全]UI 信息泄露

**问题描述：**

检查客户端的各种功能，看是否存在敏感信息泄露问题。

**威胁等级：**

安全，不能从登陆错误信息来确认用户名的存在性。

**测试步骤：**

1. 观察登录名输入正确，密码输入错误时的结果
2. 观察输入不存在用户名称的登陆结果。



* + 1. [安全]帐号登录限制

**问题描述：**

测试能否在两个设备上同时登录同一个帐号。

**威胁等级：**

安全，禁止在两台设备上同时登陆客户端。

**测试步骤：**

1. 在两台设备上同时登录客户端，观察结果。



* + 1. [安全]安全退出

**问题描述：**

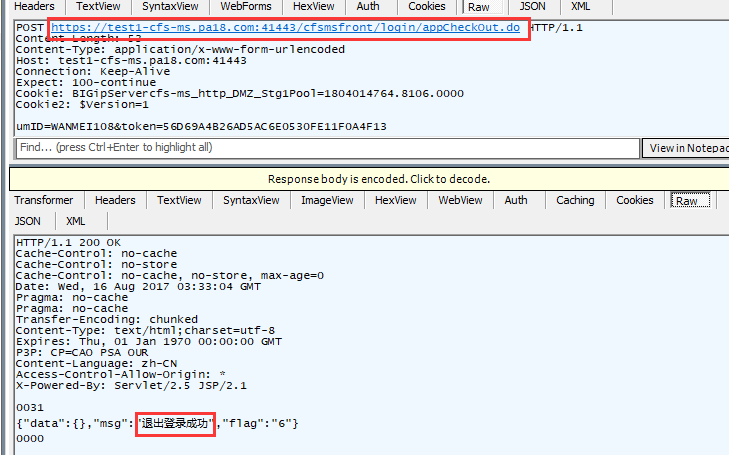
验证客户端在用户退出登录状态时是否会和服务器进行通信以保证退出的及时性。

**威胁等级：**

安全，客户端在用户退出登录状态时和服务器进行了通信。

**测试步骤：**

1. 正常启动客户端并完成登录操作。
2. 退出登陆状态，通过应用层代理工具进行数据包抓取，可以发现进行与服务端之间的数据交换。



* + 1. [中]图形验证码安全性

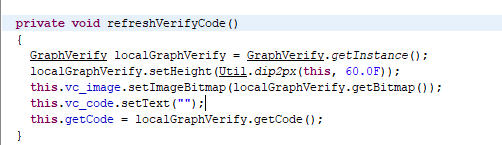
**问题描述：**

验证客户端使用的图形验证码的安全性。

**威胁等级：**

**中，图形验证码由本地生成，且安全性较低。**

**测试步骤：**

1. 通过逆向分析的方式或应用层数据包抓取的方式分析客户端代码，验证图形验证码由本地生成还是由服务器端获得。（经测试发现图形验证码由本地生成）
2. 正常使用客户端，观察客户端是否存在图像验证码，并且观察图像验证码是否符合安全策略。（如下图所示，应用中图形验证码较为简单，未经变形等操作，易被破解）



**安全建议：**

建议客户端从客户端处获取图形验证码相关信息，并且图形验证码符合图形验证码安全策略。

* 1. 手势密码安全性
     1. [安全]手势密码复杂度

**问题描述：**

测试客户端手势密码复杂度，观察是否有点位数量判断逻辑。

**威胁等级：**

安全，进行了最少点位判断。

**测试步骤：**

1. 进入客户端设置手势密码的页面进行手势密码设置。
2. 进行手势密码设置，观察客户端手势密码设置逻辑是否存在最少点位的判断。



1. 反编译APK为jar包，通过jd-gui观察对应代码逻辑是否有相应的判断和限制条件。（一般设置手势密码若输入点数过少时会有相应的文字提示，通过此文字提示可以快速定位到代码位置）



* + 1. [安全]手势密码修改和取消

**问题描述：**

检测客户端在取消手势密码时是否会验证之前设置的手势密码，检测是否存在其他导致手势密码取消的逻辑问题。

**威胁等级：**

安全，修改和忘记手势密码时，均存在了验证旧手势密码或重新登录账户的要求。

**测试步骤：**

1. 进入客户端设置手势密码的位置，一般在个人设置或安全中心等地方。
2. 进行手势密码修改或取消操作，操作时需要输入之前的手势密码。



1. 在忘记手势密码时，需要重新登录账户。



* + 1. [高]手势密码本地信息保存

**问题描述：**

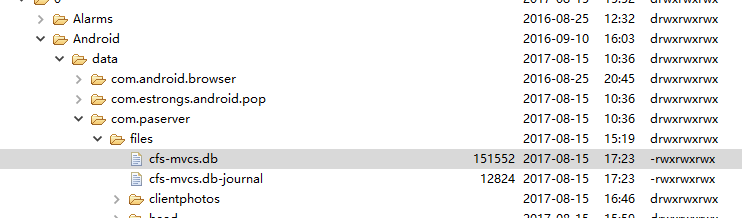
检测在输入手势密码以后客户端是否会在本地记录一些相关信息，例如明文或加密过的手势密码。

**威胁等级：**

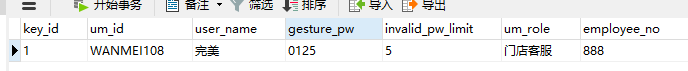
**高，在公有文件夹中明文存储手势密码。**

**测试步骤：**

1. 首先通过正常的操作流程设置一个手势密码并完整一次完整的登陆过程。
2. 反编译后，查看代码，找出手势密码的存储方式和路径



1. 若到对应的文件，观察其存储方式，发现明文存储手势验证码。



**安全建议：**

建议不在客户端保存任何与手势密码相关的敏感信息（最好也不要加密存储）。建议在保证通信安全的情况每次由服务器对手势密码正确性进行验证。

* + 1. [安全]手势密码锁定策略

**问题描述：**

测试客户端是否存在手势密码多次输入错误被锁定的安全策略。防止木马使用穷举法暴力破解用户密码。因为手势密码的存储容量非常小，一共只有9！=362880种不同手势，若手势密码不存在锁定策略，木马可以轻易跑出手势密码结果。

手势密码在输入时通常以a[2][2]这种3\*3的二维数组方式保存，在进行客户端同服务器的数据交互时通常将此二维数组中数字转化为类似手机数字键盘的b[8]这种一维形式，之后进行一系列的处理进行发送。

**威胁等级：**

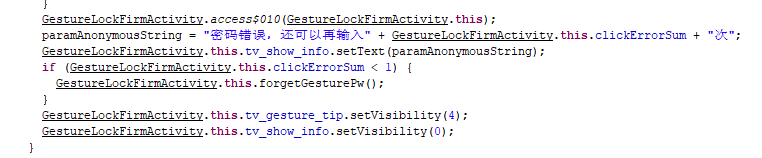
安全，限制了手势密码的错误次数。

**测试步骤：**

1. 首先通过正常的操作流程设置一个手势密码。
2. 输入不同于步骤1中的手势密码，发现客户端会提示密码错误，并限制密码错误次数。若连续输入多次手势密码错误，客户端会跳转到登录页面。



1. 反编译APK为jar包，通过jd-gui观察对应代码逻辑，发现客户端针对输入次数有相应的逻辑处理。



* + 1. [安全]手势密码抗攻击测试

**问题描述：**

验证是否可以通过插件绕过手势密码的验证页面。

**威胁等级：**

安全，不可以通过插件绕过手势密码的验证页面。

**测试步骤：**

1. 下载并安装Xposed框架及SwipeBack插件。
2. 启动客户端并进入手势密码输入页。
3. 启动SwipeBack插件，发现不可以通过滑动关闭手势密码输入页的方式进入登陆后的页面。



* 1. 通信安全
     1. [低]通信加密

**问题描述：**

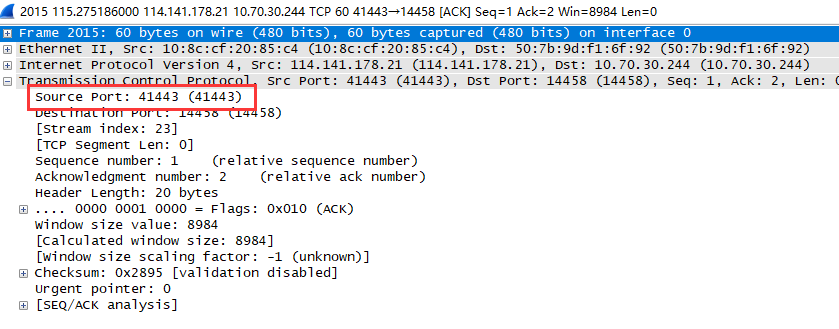
验证客户端和服务器之前的通信是否使用加密信道。

**威胁等级：**

**低，客户端和服务器之前的通信使用了加密信道，但SSL版本较低存在漏洞。**

**测试步骤：**

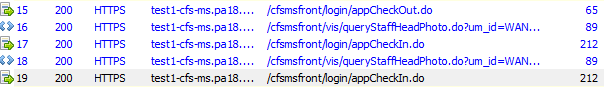
1. 使用wireshark抓取应用传输的数据包，通过分析数据包得到该应用远端服务器发包时开启的端口。



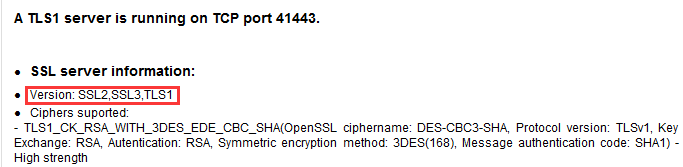
1. 手动配置http代理，如图所示：



1. 在pc端使用fiddler抓取客户端与服务器之间的通信包：



1. 检测SSL版本



**安全建议：**

建议客户端同服务器进行通信时信道使用SSL加密信道进行传输，同时保证加密信道的本身安全（SSLV2，SSLV3已被证明存在漏洞，建议至少使用TLSV1.1以上的算法），或是在通信过程中自实现类似TLS协议的算法，同时也要保证自实现算法的安全性。

* + 1. [中]关键数据加密和校验

**问题描述：**

测试客户端程序提交数据给服务端时，密码等关键字段是否进行了加密和校验，防止恶

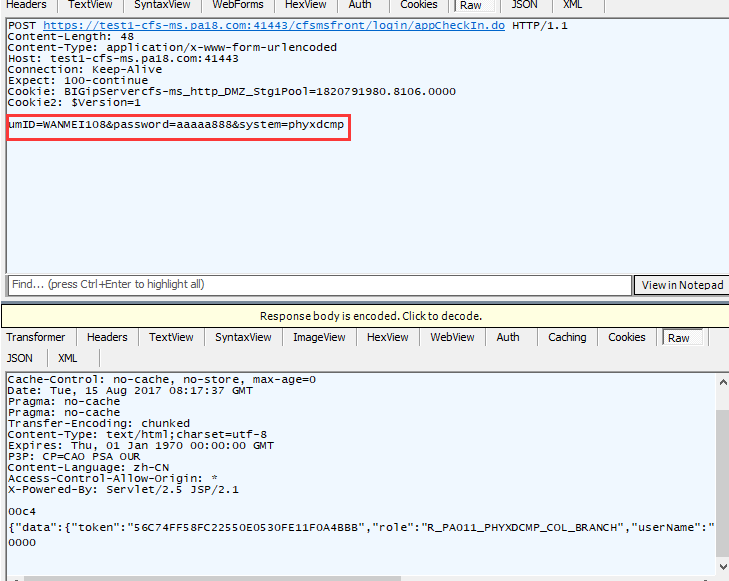
意用户嗅探和修改用户数据包中的密码等敏感信息。

**威胁等级：**

**中，明文传输用户名和密码信息。**

**测试步骤：**

1. 设置代理后，使用fiddler抓取用户登陆数据包，可发现使用明文传输用户名密码。

**安全建议：**

建议账号，密码，卡号，金额等进行加密处理，同时整个数据包进行二次加密，返回的敏感信息进行加密，同时返回数据包进行二次加密，并且使用增加随机因子的校验字段，并且确定服务器逻辑标志位正确，在删除校验字段时服务器不响应提交的数据包。

* + 1. [安全]访问控制

**问题描述：**

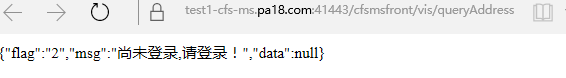
测试客户端访问的URL是否仅能由手机客户端访问。是否可以绕过登录限制直接访问登录后才能访问的页面，对需要二次验证的页面（如私密问题验证），能否绕过验证。

**威胁等级：**

安全，不可绕过登录限制直接访问页面。

**测试步骤：**

在PC机的浏览器里输入URL，尝试访问，可发现返回“尚未登陆”的错误信息。



* 1. 业务安全

对于可以通过代理的方式对交互数据进行分析的客户端，可以对涉及到敏感信息操作的具体业务功能进行测试。

* + 1. [高]待外访列表查询平行越权

**问题描述：**

待外访列表查询时，可通过修改数据包中的“um\_id”越权查询其他人的待外访列表。

**威胁等级：**

**高，可越权查询其他人的待外访列表。**

**测试步骤：**

url :

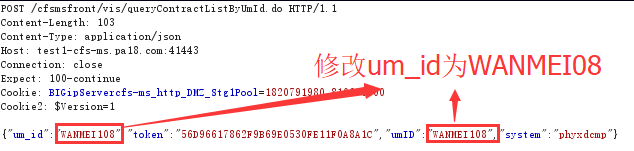
<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryContractListByUmId.do>

1. 下图所示分别是“完美108”和“cuibingxing558”的待访问列表。



wanmei108 cuibingxing558

1. 登陆“cuibingxing558”，抓取查询列表数据包，并将um\_id修改为“WANMEI108”



1. 发现可以越权查询到“wanmei108”的待访问列表



**安全建议：**

对用户提交的请求先进行权限判断，如果提交请求操作的资源属于当前用户则允许该请求，否则拒绝该请求。且注意权限判断应该依据用户的登陆凭证，而不是用户名信息。

* + 1. [高]查询客户详情等平行越权（多处）

**问题描述：**

开始外访查询客户详情时，可通过修改数据包中的“contract\_code”越权查询其他人的待外访客户详情。

**威胁等级：**

**高，可越权查询其他人的待外访客户详情。**

**测试步骤：**

问题url:

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryAccountDetailInfo.do>

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryOutvisitResultFormInfo.do>

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryLogInfoList.do>

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryCustomerInfo.do>

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/searchHisOutvisitInfo.do>

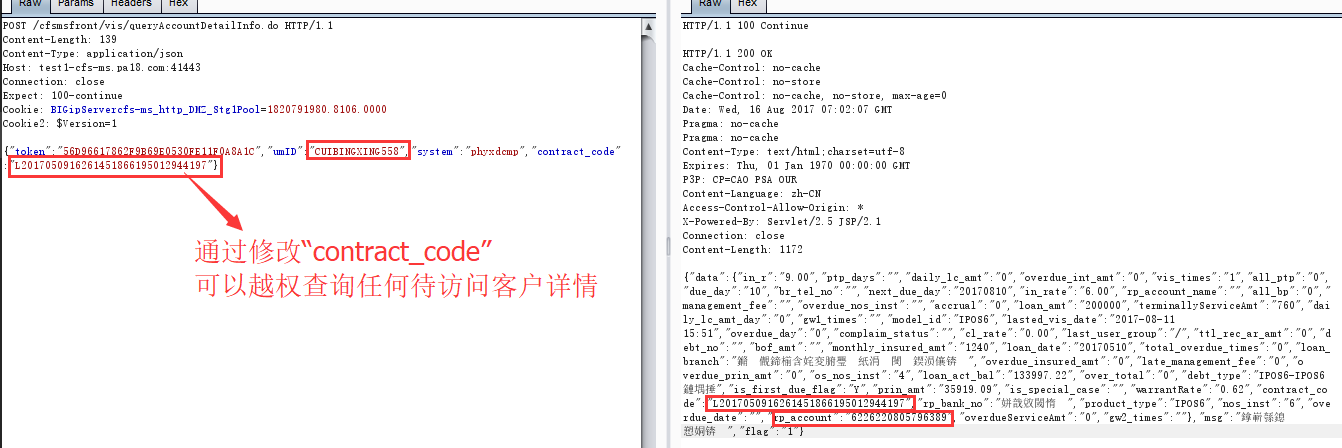
<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryAddressInfo.do>

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryAddressInfoListByUmId.do>

(测试步骤以<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryAccountDetailInfo.do>

为例)

1. 登陆“cuibingxing558”账户，选择待访问列表中一个待访问客户，点击开始访问，并抓取数据包。
2. 更改数据包中的contract\_code字段（即合同号），将其改为“wanmei108”待访问列表中的合同号，发现可以查询客户详细信息。



**安全建议：**

对用户提交的请求先进行权限判断，如果提交请求操作的资源属于当前用户则允许该请求，否则拒绝该请求。且注意权限判断应该依据用户的登陆凭证，而不是用户名信息。

* + 1. [高]查询客户电话列表平行越权

**问题描述：**

开始外访查询客户详情时，可通过修改数据包中的“contract\_code”越权查询其他人的待外访客户详情。

**威胁等级：**

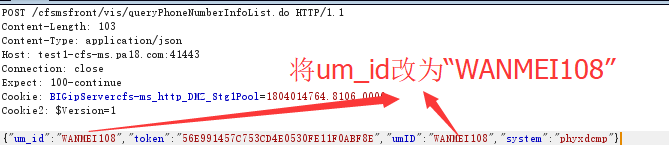
**高，可越权查询其他人的待外访客户电话列表。**

**测试步骤：**

url:

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryPhoneNumberInfoList.do>

1. 登陆“cuibingxing558”账户，在电话功能中点击“待外访客户”。
2. 更改数据包中的um\_id字段（即合同号），将其改为“wanmei108”，可以看到返回了待外访的电话列表。





**安全建议：**

对用户提交的请求先进行权限判断，如果提交请求操作的资源属于当前用户则允许该请求，否则拒绝该请求。且注意权限判断应该依据用户的登陆凭证，而不是用户名信息。

* + 1. [高]查询客户地址列表平行越权

**问题描述：**

开始外访查询客户详情时，可通过修改数据包中的“um\_id”越权查询其他人的待外访客户地址。

**威胁等级：**

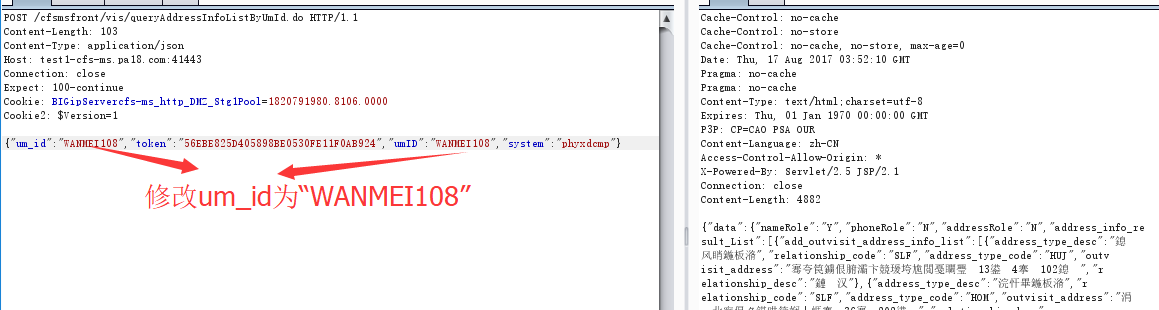
**高，可越权查询其他人的待外访客户地址列表。**

**测试步骤：**

url:

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/queryAddressInfoListByUmId.do>

1. 登陆“cuibingxing558”账户，点击地图功能。
2. 更改数据包中的um\_id字段（即合同号），将其改为“wanmei108”，可以看到返回了待外访的地址列表。



**安全建议：**

对用户提交的请求先进行权限判断，如果提交请求操作的资源属于当前用户则允许该请求，否则拒绝该请求。且注意权限判断应该依据用户的登陆凭证，而不是用户名信息。

* + 1. [高]外访资料上传处任意文件上传

**问题描述：**

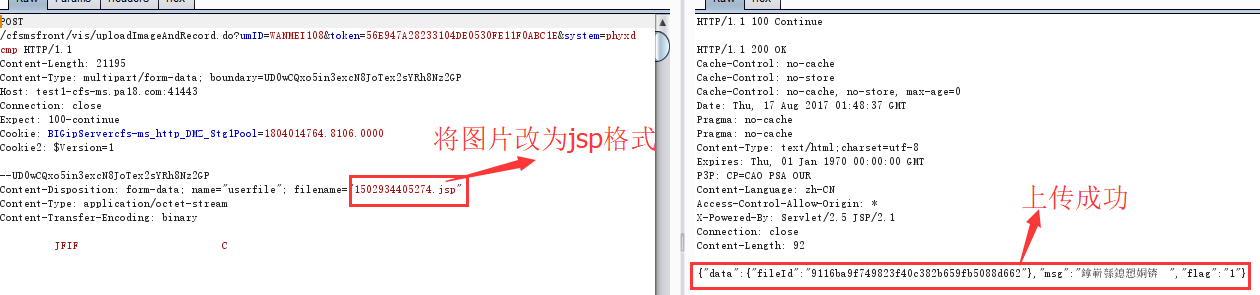
外访资料上传处，由于没有过滤文件上传类型，导致任意文件上传。

**威胁等级：**

**高，可利用此漏洞上传webshell和木马。**

**测试步骤：**

<https://test1-cfs-ms.pa18.com:41443/cfsmsfront/vis/uploadImageAndRecord.do?umID=WANMEI108&token=56E947A28233104DE0530FE11F0ABC1E&system=phyxdcmp>



**安全建议：**

应该在后端代码建立上传文件白名单，每次上传将文件后缀与白名单进行校验，如果上传的后缀名不在白名单范围内则拒绝上传该类型文件。

1. 感谢

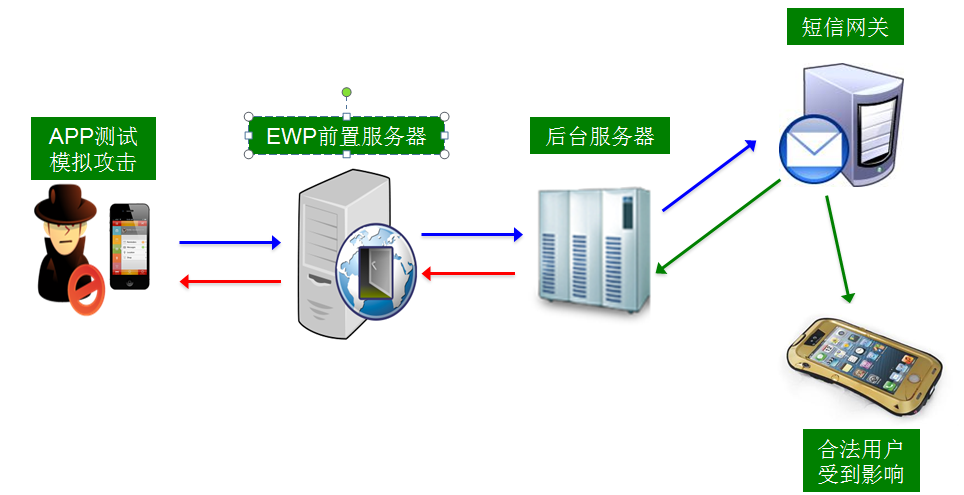
在本次APP安全测试过程中，绿盟科技感谢平安普惠的领导及相关人员的大力配合，以使得我们的工作顺利完成。

1. 移动终端APP安全测试服务概述
   1. 移动终端APP测试概述

手移动终端测试服务是一项针对移动设备业务系统推出的安全测试服务。它旨在通过一系列的技术性检查、测试和分析，挖掘移动应用业务系统可能存在的技术和业务层面的风险，指导客户来降低和规避风险，保障系统的正常运行，进而保障用户的资金和信息安全。

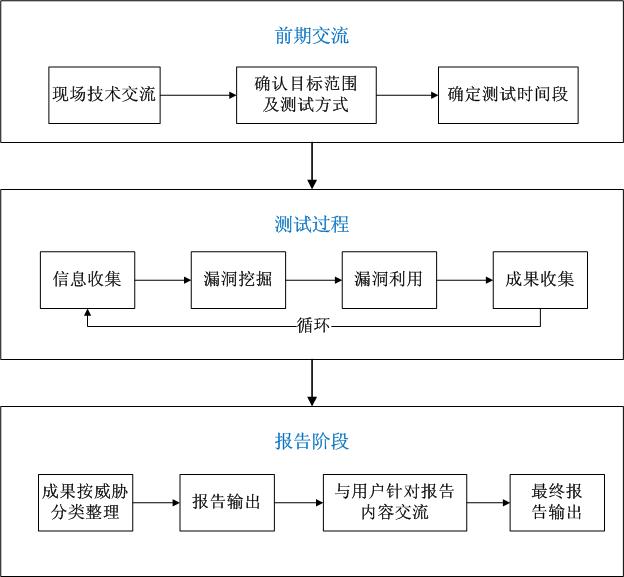
移动客户端测试服务主要是从系统、应用和业务等多个层面来开展评估工作，工作内容涵盖相关主机和应用的安全配置分析、脆弱性检查、渗透测试等。该服务的目的在于帮助客户发现威胁到业务自身安全的缺陷或隐患，及时做出修补或整改，避免因为安全问题导致的经济损失。

下图为在移动终端APP测试时可能涉及到的角色，主要有模拟攻击者、前端服务器、后端服务器、短信网关、合法用户这5个。APP测试正是通过模拟攻击者进行攻击的场景，通过服务器端反馈回来的信息，进行相应角色的风险定位。



移动终端APP测试数据流示意图

* 1. 工作流程



APP安全测试工作流程图

* 1. 风险管理及规避

为保障客户系统在APP测试过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

* + 1. 时间

从时间安排上，测试人员将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。

另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

* + 1. 工具使用

同传统渗透测试不同，APP安全测试中一般不会涉及拒绝服务攻击测试等增加系统压力的攻击场景。当出现可能增加系统压力的相关测试（例如暴力猜解密码、短信验证码、图形验证码测试）时，测试人员也会通过设置线程和参数的方式来减少其对系统的压力。

* + 1. 技术手段

绿盟科技的APP安全测试人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

* + 1. 监控

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

* + 1. 目标的选择

为更大程度的避免风险的产生，APP安全测试还可选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

针对未上线的客户端及服务器逻辑，APP安全测试可以针对生产环境进行相关测试。同时对于未开发完成的客户端，绿盟科技的测试人员可以针对已开发完成的模块进行测试。

* 1. 收益

对于客户而言，APP安全测试可以带来以下收益：

* 明确安全隐患点

APP安全测试是渗透测试的一个分支，因此它也是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此明确整体系统中的安全隐患点。

* 提高安全意识

如上所述，任何的隐患在APP安全测试服务中都可能造成“千里之堤溃于蚁穴”的效果，因此此类服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

* 提高安全技能

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的渗透测试报告，也能为用户提供当前流行安全问题的参考。

* 了解安全开发规范

在测试过程中，我们的测试人员会即时将问题提交给第三方开发商，并告知用户相应的隐患。在交付服务时，我们的测试人员还会在报告中体现和APP测试相关的部分安全开发规范，例如图形验证码规范，方便用户及第三方开发商进行了解，学习。

1. App测试安全等级划分

以下表格是绿盟科技进行安全等级判断的具体方法，本次平安普惠外访手机客户端及服务器系统安全等级为**高度危险系统。**

|  |  |
| --- | --- |
| **安全等级** | **内容描述** |
| 高风险等级  （每一个高风险问题计3分，其中第1项，第3项，第7项为5分） | 1. 通信数据明文传输，包括服务器返回数据包。 2. SSL证书验证逻辑存在风险或未使用SSL证书。 3. Session机制不完善，允许数据包重放（交易数据包重放，短信验证为中风险）； 4. 用户敏感信息本地存储（明文密码，cookie等）。 5. 客户端存在未关闭的Debug接口，泄露用户敏感信息或服务器通信信息。 6. 内存中可搜索到明文密码。 7. 可越权查询/修改账户信息。（极高风险） 8. 服务器返回数据包包含敏感信息（例如短信验证码）。 |
| 中风险等级  （每一个问题计2分） | 1. 存在短信轰炸攻击（服务器端短信网关配置问题）。 2. 可进行Activity界面劫持攻击。 3. 存在so文件注入问题。 4. 服务器未校验客户端完整性。 5. 验证码安全策略安全性低或验证码由本地生成。 6. 未使用自定义软键盘。 7. 存在屏幕回显。（输入框和软键盘均有回显为中风险，只有其中一种为低风险） 8. 修改密码不需要输入原始密码。 9. 多次输入密码错误不锁定账号。 10. 客户端退出时是否会和服务器进行通信确认退出登录状态。 |
| 低风险问题  （每一个问题计1分） | 1. 密码复杂度未设置； 2. 存在UI信息泄露。 3. 未设置会话超时时间 4. 未使用随机软键盘。（未使用自定义键盘为中风险，此处不累计计算） 5. 允许多个设备同时登陆一个账号。 6. 不存在私密问题验证。 7. 进行界面切换不会提示用户。 8. 未进行数据混淆。 |
| 当评分≥10时，被测试系统为**高度危险系统。**  当5≤评分＜10时，被测试系统为**中度危险系统。**  当0≤评分＜5时，被测试系统为**较安全系统。** | |

1. 工具及相关资源

|  |  |
| --- | --- |
| **工具名称** | **Apktool** |
| **工具用途** | GOOGLE提供的APK编译工具，能够反编译及回编译apk。 |
| **相关信息** | https://code.google.com/p/android-apktool/ |

测试工具：apktool信息

|  |  |
| --- | --- |
| **工具名称** | **Dex2jar** |
| **工具用途** | 将Android的dex文件反编译为java源码。 |
| **相关信息** | https://code.google.com/p/dex2jar/w/list |

测试工具：Dex2jar信息

|  |  |
| --- | --- |
| **工具名称** | **Jd-gui** |
| **工具用途** | 反编译代码阅读工具。 |
| **相关信息** | http://jd.benow.ca/ |

测试工具：JD-GUI信息

|  |  |
| --- | --- |
| **工具名称** | **Portecle** |
| **工具用途** | 证书管理工具，可以进行证书维护。 |
| **相关信息** | http://www.oschina.net/p/portecle |

测试工具：Portecle信息

|  |  |
| --- | --- |
| **工具名称** | **SuperOneClick** |
| **工具用途** | Android手机root工具 |
| **相关信息** | http://www.superoneclick.cc/ |

测试工具：SuperOneClick信息

|  |  |
| --- | --- |
| **工具名称** | **Proxydroid** |
| **工具用途** | Android手机用代理软件。 |
| **相关信息** | https://github.com/madeye/proxydroid |

测试工具：ProxyDroid信息

|  |  |
| --- | --- |
| **工具名称** | **ComponentTest** |
| **工具用途** | 绿盟科技自主研发的组件暴露分析工具。 |
| **相关信息** | 详情请与绿盟科技安全团队沟通。 |

测试工具：ComponentTest信息

|  |  |
| --- | --- |
| **工具名称** | **Activity劫持工具** |
| **工具用途** | 绿盟科技自主研发的Activity劫持测试工具。 |
| **相关信息** | 详情请与绿盟科技安全团队沟通。 |

测试工具：Activity劫持工具信息

|  |  |
| --- | --- |
| **工具名称** | **Ns\_keylogger** |
| **工具用途** | 绿盟科技自主研发的软键盘，具有键盘记录功能。 |
| **相关信息** | 详情请与绿盟科技安全团队沟通。 |

测试工具：NSKeylogger信息

|  |  |
| --- | --- |
| **工具名称** | **MemSpector** |
| **工具用途** | Android手机内存修改工具 |
| **相关信息** | http://www.nosec.org |

测试工具：MemSpector信息

|  |  |
| --- | --- |
| **工具名称** | **BurpSuite** |
| **工具用途** | HTTP数据包修改、转发工具 |
| **相关信息** | http://portswigger.net/burp/ |

测试工具：BurpSuite信息

|  |  |
| --- | --- |
| **工具名称** | **Fiddler** |
| **工具用途** | HTTP数据包修改、转发工具 |
| **相关信息** | http://www.fiddler2.com/fiddler2/ |

测试工具：Fiddler信息

|  |  |
| --- | --- |
| **工具名称** | **Xposed框架** |
| **工具用途** | 系统级框架，用于开发底层插件进行测试 |
| **相关信息** | http://repo.xposed.info/module/de.robv.android.xposed.installer |

测试工具：Xposed框架信息

|  |  |
| --- | --- |
| **工具名称** | **SwipeBack** |
| **工具用途** | Xposed插件，用于绕过登陆界面 |
| **相关信息** | http://repo.xposed.info/module/us.shandian.mod.swipeback |

测试工具：SwipeBack信息

|  |  |
| --- | --- |
| **工具名称** | **Android Development Tools** |
| **工具用途** | 支持Android开发的工具 |
| **相关信息** | http://developer.android.com/tools/help/adt.html |

测试工具：Android Development Tools信息