杭州逐一科技有限公司智慧停车云平台

渗透测试报告

**杭州安信检测技术有限公司**

二零一八年八月

# 1.综述

本次对杭州逐一科技有限公司智慧停车云平台及任意停车apk进行渗透测试，发现了存在4处高风险，3处中风险和2处低风险。共计9处风险。

## 安全漏洞汇总

|  |  |  |  |
| --- | --- | --- | --- |
| 测试对象 | 登陆链接/主机IP | 安全漏洞名称 | 漏洞等级 |
| 任意停车Apk | http://api.zhuyitech.com/ | 任意手机号注册 | 高 |
| 信息泄露、敏感信息遍历 | 高 |
| 任意用户密码重置 | 高 |
| 越权修改他人车辆信息 | 高 |
| 用户遍历 | 中 |
| 组件安全 | 中 |
| 数据备份配置 | 中 |
| Apk反编译 | 低 |
| 错误信息为屏蔽 | 低 |

## 漏洞等级定

|  |  |
| --- | --- |
| **漏洞等级** | **描述** |
| 高 | 可直接威胁到网络、操作系统、业务系统的安全性，可导致业务中断或敏感信息泄漏。此类风险如高危性质远程缓冲区溢出、SQL注入、关键业务弱口令、验证绕过、未授权的访问、敏感信息泄漏等。 |
| 中 | 存在一定的危害性，一经利用即可威胁到操作系统、业务系统的安全性，进而威胁到网络的安全性。此类风险如远程缓冲区溢出、非关键业务弱口令、XSS跨站、敏感信息泄漏等。 |
| 低 | 存在相对较小的危害性，并不直接对系统或应用造成危害。一旦被利用时影响相对较小，在渗透测试中通常会为进一步的渗透产生辅助性作用。此类风险如信息泄漏、非关键业务拒绝服务漏洞等。 |
| 无 | 无风险，未发现相关安全问题 |

# 2.测试结果及加固建议

## 任意停车APP

### 任意手机号注册

|  |  |
| --- | --- |
| 风险名称 | 任意手机号注册 |
| 风险级别 | 高 |
| 测试过程 | 逻辑设计问题，前面两个包验证了手机号、验证码、时效、频率。但是最后一个包没有进行验证直接插入数据库，导致前面的验证全部时效。根据图中post数据填写即可注册任意手机号，测试号码18888888888。 |
| 风险描述 | 恶意注册他人手机号、钓鱼。 |
| 加固建议 | 重构后端的验证逻辑。 |
| 整改情况 | \ |

### 信息泄露、车辆信息任意遍历

|  |  |
| --- | --- |
| 风险名称 | 信息泄露、车辆信息任意遍历 |
| 风险级别 | 高 |
| 测试过程 | 修改id的值以遍历所有车辆信息，只读session进行了登陆验证。并未验证是否为该车所有人导致的越权。 |
| 风险描述 | 攻击者获取该平台绑定的所有车辆信息。 |
| 加固建议 | 重构逻辑，允许查询的车辆只应是该用户所拥有的车辆。 |
| 整改情况 | \ |

### 任意用户密码重置

|  |  |
| --- | --- |
| 风险名称 | 任意用户密码重置 |
| 风险级别 | 高 |
| 测试过程 | 1. 修改发送验证码的请求中的电话号码，获取验证码  1. 找回密码，修改掉电话号码，就可以修改掉其他人的密码。   第二步把phoneNumber改成其他用户的号码，就可以重置他人密码。 |
| 风险描述 | 攻击者获取重置他人密码 |
| 加固建议 | 重置密码处对短信验证码进行二次验证，防止手机号和验证码不一致情况 |
| 整改情况 | \ |

### 越权修改他人车辆信息

|  |  |
| --- | --- |
| 风险名称 | 越权修改他人车辆信息 |
| 风险级别 | 高 |
| 测试过程 | 车辆认证时，修改车辆图片。  只需要将carID修改后，就可以修改他人车辆的图像信息。 |
| 风险描述 | 攻击者获取可以修改他人绑定的车辆的图片信息 |
| 加固建议 | 重构逻辑，允许修改的车辆只应是该用户所拥有的车辆。 |
| 整改情况 | \ |

### 用户遍历

|  |  |
| --- | --- |
| 风险名称 | 用户遍历 |
| 风险级别 | 中 |
| 测试过程 | 有验证用户是否存在的请求  <http://api.zhuyitech.com/v2/platform/security/accountexist> |
| 风险描述 | 攻击者获取可以获取他人账号，通过获取他人账号获得进一步利用 |
| 加固建议 | 重构逻辑，服务端返回信息应规避掉用户是否存在。 |
| 整改情况 | \ |

### 组件安全

|  |  |
| --- | --- |
| 风险名称 | Apk组件安全 |
| 风险级别 | 中 |
| 测试过程 | 1.com.zhuyi.parking.apshare.ShareEntryActivity组件导出  2.com.zhuyi.parking.service.VersionBroadcastReceiver组件默认导出为true  3. com.zhuyi.parking.WXPayRegister组件默认导出为true |
| 风险描述 | 导出的组件能被第三方APP任意调用，攻击者可构造恶意payload进行攻击，攻击者可构造恶意payload进行攻击，造成用户敏感信息泄露、拒绝服务攻击等风险。 |
| 加固建议 | 如果组件不需要与其它系统共享数据或交互，应在AndroidManifest.xml配置文件中将该组件的android:exported属性值设置为false。 |
| 整改情况 | \ |

### 数据备份配置

|  |  |
| --- | --- |
| 风险名称 | Apk数据备份配置 |
| 风险级别 | 中 |
| 测试过程 | 1. android:allowBackup=true |
| 风险描述 | 当这个allowBackup标志被设置为true时应用程序数据可以在手机未获取 ROOT 的情况下通过adb调试工具来备份和恢复。在接触用户手机的情况下攻击者可以在启动手机USB调试功能来窃取那些能够受到AllowBackup漏洞影响的APP数据，造成用户敏感信息泄露甚至财产损失。 |
| 加固建议 | AndroidManifest.xml文件中Application节点的android:allowBackup属性设置为false或是删除该属性。 |
| 整改情况 | \ |

### Apk反编译

|  |  |
| --- | --- |
| 风险名称 | Apk反编译 |
| 风险级别 | 中 |
| 测试过程 | Apk可以用jeb反编译出代码： |
| 风险描述 | 没有做防护，apk可以被反编译，还能够被二次打包。 |
| 加固建议 | 使用梆梆加固或者360加固进行apk加固。 |
| 整改情况 | \ |

### 错误信息为屏蔽

|  |  |
| --- | --- |
| 风险名称 | 错误信息为屏蔽 |
| 风险级别 | 低 |
| 测试过程 | Java里面string转int错误未屏蔽： |
| 风险描述 | 通过错误信息可以查看服务端中间件信息进行进一步利用 |
| 加固建议 | 屏蔽错误信息。 |
| 整改情况 | \ |