MoGua

自动售货机 1.0.8.APK 分析报告

APP名称:	自动售货机

包名:	com.example.vendingmachine
域名线索:	15条
URL线索:	18条
邮箱线索:	0条
分析日期:	2025年5月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 自动售货机.apk
文件大小: 24.9MB
MD5值: 4db301006394f8e247e1c14193fa6bcf
SHA1值: e44016a4e9cc18fb64c3345cdeb1db917e6a8fc2
SHA256值: fb0cf65875ae2cbad71f714b98acbf919495eb5931f6bac030084a19d3fe2a47

APP 信息

App名称: 自动售货机
包名: com.example.vendingmachine
主活动Activity: com.example.vendingmachine.view.activity.MainActivity
安卓版本名称: 1.0.8
安卓版本: 108

域名线索

域名	服务器信息
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
www.xunfei.cn	**IP**: 123.125.46.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
log.iflytek.com	**IP**: 103.8.33.178 **所属国家**: China **地区**: Anhui

	城市: Hefei **纬度**: 31.863815 **经度**: 117.280830
ns.wxs1988.com	**IP**: 112.74.107.119 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
www.baidu.cn	**IP**: 110.242.70.57 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
astat.bugly.cros.wr.pvp.net	**IP**: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
www.erweicaihong.cn	**IP**: 140.179.152.195 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
logconf.iflytek.com	**IP**: 103.8.33.178 **所属国家**: China **地区**: Anhui **城市**: Hefei **纬度**: 31.863815 **经度**: 117.280830

dev.voicecloud.cn	**IP**: 125.254.169.47 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
open.xf-yun.com	**IP**: 121.37.244.117 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
astat.bugly.qcloud.com	**IP**: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
wke.openspeech.cn	没有服务器地理信息.
openapi.openspeech.cn	**IP**: 114.118.65.76 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
android.bugly.qq.com	**IP**: 124.95.225.169 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
	IP: 42.62.43.145 **所属国家**: China

iss.openspeech.cn	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
https://ns.wxs1988.com	com/example/androidbase/model/network/Url.java
https://www.baidu.cn	com/example/gravitylocker/view/fragment/GravityMainFragment.java
https://[^/]*)/	com/example/navmde/presenter/HomePresenter.java
https://www.erweicaihong.cn/?bd_vid=8816467385947915772	com/example/springlocker/view/activity/ScanPayActivity.java
https://www.baidu.cn	com/example/springlocker/view/activity/ScanPayActivity.java
https://ns.wxs1988.com	com/example/vendingmachine/AppBaseApplication.java
https://open.xf-yun.com/msp.do	com/iflytek/cloud/msc/module/z743z.java
http://wke.openspeech.cn/wakeup/	com/iflytek/cloud/msc/ivw/z743z.java
http://iss.openspeech.cn/v?	com/iflytek/speech/UtilityConfig.java
https://logconf.iflytek.com/hotupdate	com/iflytek/idata/extension/z895z.java
https://log.iflytek.com/log	com/iflytek/idata/extension/z986z.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java

https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://openapi.openspeech.cn/webapi/wfr.do	x861x/z235z.java
http://www.xunfei.cn/?appid=	x102x/z895z.java
http://dev.voicecloud.cn/msc/help.html\	x963x/z235z.java
http://dev.voicecloud.cn/msc/help.html	x963x/z235z.java
http://dev.voicecloud.cn/msc/help.html\	x963x/z895z.java
http://dev.voicecloud.cn/msc/help.html	x963x/z895z.java
http://dev.voicecloud.cn/msc/help.html\	x963x/z986z.java
http://dev.voicecloud.cn/msc/help.html	x963x/z986z.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True

v3 签名: False
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-04-15 22:40:50+00:00
有效期至: 2035-09-01 22:40:50+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0xb3998086d056cffa
哈希算法: md5
md5值: 8ddb342f2da5408402d7568af21e29f9
sha1值: 27196e386b875e76adf700e7ea84e4c6eee33dfa
sha256值: c8a2e9bccf597c2fb6dc66bee293fc13f2fc47ec77bc6b2b0d52c11f51192ab8
sha512值: 5d802f24d6ac76c708a8e7afe28fd97e038f888cef6665fb9b4a92234c311d6ff42127ccb2eb5a898f4e7e4e553f6ef602d43d1a2ebae9f002a6598e72fd2d83
公钥算法: rsa
密钥长度: 2048
指纹: 65ba0830722d5767f8779e37d0d9c67562f03ec63a2889af655ee9c59effb434

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.USB_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息

android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.READ_BRIGHTNESS	未知	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用

android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
com.example.vendingmachine.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信