



MoGua

None 3.1.APK 分析报告



APP名称:

None

包名: vccidl.xnbskmxcd.dbmrzq

域名线索: 8条

URL线索: 4条

邮箱线索: 0条

分析日期: 2025年6月19日

分析平台: [摸瓜APK反编译平台](#)

文件名: Ht Zq (1).apk
文件大小: 28.0MB
MD5值: 35a0cf2fa5abf1c53c1b378d44f41bf6
SHA1值: d14b9f05c2f24bc5b8c7328ec3836ea7f52250a4
SHA256值: 72e5faecb7a6529954ec76406376758b1914b8d83f0872f78acbc2366cd6a209

i APP 信息

App名称: None
包名: vccidl.xnbskmxcd.dbmrzq
主活动Activity: com.westpm.hlahl.ui.activity.OpeningActivity
安卓版本名称: 3.1
安卓版本: 2

🔍 域名线索

域名	服务器信息
54.249.168.14	IP: 54.249.168.14 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
146.56.203.61	IP: 146.56.203.61 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
57.180.55.222	IP: 57.180.55.222 所属国家: Japan 地区: Tokyo

	城市: Tokyo 纬度: 35.689499 经度: 139.692322
d.alipay.com	IP: 111.202.5.210 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dong3-1348306641.cos.ap-chongqing.myqcloud.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.migu.cn	IP: 117.135.165.90 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
111.230.33.221	IP: 111.230.33.221 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
172.20.10.4	IP: 172.20.10.4 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

URL线索

URL信息	Url所在文件
http://172.20.10.4:8080/food	com/westpm/hlahl/util/Constant.java
https://www.migu.cn/ilIndex.html	com/westpm/hlahl/ui/activity/webActivity.java
https://d.alipay.com	com/westpm/hlahl/ui/activity/webActivity.java
https://d.alipay.com	com/westpm/hlahl/ui/activity/H5Activity.java
https://54.249.168.14:51000/snake/	com/westpm/hlahl/ui/activity/OpeningActivity.java
https://57.180.55.222:51000/snake/	com/westpm/hlahl/ui/activity/OpeningActivity.java
https://111.230.33.221:10608/snake/	com/westpm/hlahl/ui/activity/OpeningActivity.java
https://146.56.203.61:10608/snake/	com/westpm/hlahl/ui/activity/OpeningActivity.java
https://dong3-1348306641.cos.ap-chongqing.myqcloud.com/t2huatai0502.json	com/westpm/hlahl/ui/activity/OpeningActivity.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: True
找到 1 个唯一证书
主题: C=jSZGG, ST=sQzHV, L=bLEEM, O=tj1748526280887, OU=va1748526280887, CN=nlbm
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-29 13:44:42+00:00
有效期至: 2075-05-17 13:44:42+00:00
发行人: C=jSZGG, ST=sQzHV, L=bLEEM, O=tj1748526280887, OU=va1748526280887, CN=nlbm
序列号: 0x20baf8eb
哈希算法: sha512
md5值: 66bede063299ed449626e15335140038
sha1值: 6f42117d8f50b3dce8af1b88abbda89b6d910bd6
sha256值: f0682ce76ebeaaa9adb2d7b9298a612be8fd6346b174caf06382147c46004e0e
sha512值: 3e7ceed66dafa106f062d4a8567315ea6d8d5606225df99a4ae4294ddf181da951271fa1fcce71463ac595f15358abef2fef98f05746f1302edfec74e3a9ec1
公钥算法: rsa
密钥长度: 4096
指纹: 3cdeaad5e46939142a8d29c6313e99413123a3a855a8b816680f92cdbe057437

 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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
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.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.NETWORK_PROVIDER	未知	Unknown permission	Unknown permission from android reference
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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference

android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
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。
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference

应用内通信