MoGua

None 3.0.APK 分析报告

APP名称:	None

包名:	com.innagadgaafdhasbgf9.xvpn
域名线索:	5条
URL线索:	3条
邮箱线索:	1条
分析日期:	2025年6月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: gj yjb.apk
文件大小: 27.84MB
MD5值: 24ad7f08c390bbb18296fbb1d4b63577
SHA1值: acdb86cfac73d8693bff0f2996ee2a708ce842d0
SHA256值: 8e484e3880066958ab88d6c5635f8705e15922de11ec81c12a47ec0fe87bf2c1

APP 信息

App名称: None
包名: com.innagadgaafdhasbgf9.xvpn
主活动Activity: com.westpm.hlahl.ui.activity.OpeningActivity
安卓版本名称: 3.0
安卓版本: 1

域名线索

域名	服务器信息
cdbdy.cd.bcebos.com	**IP**: 182.61.129.20 **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
bjbdy.bj.bcebos.com	**IP**: 119.249.103.5 **所属国家**: China **地区**: Hebei

	城市: Baoding **纬度**: 38.851109 **经度**: 115.490280
gzbdy.gz.bcebos.com	**IP**: 153.3.238.105 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
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

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/ilndex.html	com/westpm/hlahl/ui/activity/webActivity.java
https://gzbdy.gz.bcebos.com/gjzx0522.json	com/westpm/hlahl/ui/activity/OpeningActivity.java
https://cdbdy.cd.bcebos.com/gjzx0522.json	com/westpm/hlahl/ui/activity/OpeningActivity.java
https://bjbdy.bj.bcebos.com/gjzx0522.json	com/westpm/hlahl/ui/activity/OpeningActivity.java

邮箱线索

邮箱地址	所在文件
123456789@qq.com	com/westpm/hlahl/ui/activity/OpeningActivity.java

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=HexUF, ST=m5mpi, L=MblsV, O=il1747887129486, OU=ff1747887129486, CN=ekdb
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-22 04:12:09+00:00
有效期至: 2075-05-10 04:12:09+00:00
发行人: C=HexUF, ST=m5mpi, L=MblsV, O=il1747887129486, OU=ff1747887129486, CN=ekdb
序列号: 0x136fe216
哈希算法: sha512
md5值: f4bd6e88e9c5bc576210d172176a4d00
sha1值: 7dd58e1acdc59e54ffb035005786eca82c169238
sha256值: 699be5f486375fdc5268ee6650a99fab0bfe6da0dbf06644140c5acd14bc2f3d
sha512值: cc5cbbb20a1a2a86b54cb0bc4043c5414277f1848776c8c447326da48b3cd5fa5000326417a368b49841ad5d926790996475120ea5864f3e474ea404e7a3ce00
公钥算法: rsa
密钥长度: 4096
指纹: 4e2a623ea1484f1f6f4ea5d541bd39ed1cdd55244e4a7dd5b40bdc5d4991e5d3

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_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	允许应用程序写入外部存储

		内容	
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