MoGua

海农国积 2.2.0.APK 分析报告

APP名称:	海农国积

包名:	top.exchange.guoji
域名线索:	4条
URL线索:	5条
邮箱线索:	1条
分析日期:	2025年8月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: gjhainong-2.2.0.apk
文件大小: 10.25MB
MD5值: bb5f75699be58e1f2a995a5f9e0a94d3
SHA1值: 6c120f85d9af7135b3536aaa4e120dfea84b37b5
SHA256值: 5dd9d73b4a7c0454f2bcdb21833c941ddf443c4ecbae038cc65b16ea03c8b581

APP 信息

App名称: 海农国积
包名: top.exchange.guoji
主活动Activity: top.biduo.exchange.ui.common.StartActivity
安卓版本名称: 2.2.0
安卓版本: 40

域名线索

域名	服务器信息
gjhainong.gjhnkj.cn	**IP**: 8.141.94.11 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
rqd.uu.qq.com	**IP**: 60.29.240.104 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
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
schemas.android.com	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://gjhainong.gjhnkj.cn	top/biduo/exchange/config/AppConfig.java

邮箱线索

邮箱地址	**所在文件**
sgdtd@outlook.com	摸瓜V1引擎

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=86, ST=henanzhengzhou, L=china, O=zhengtuo, OU=zhengtuo, CN=zhengtuo
签名算法: rsassa_pkcs1v15
有效期自: 2018-11-07 10:51:13+00:00
有效期至: 2043-11-01 10:51:13+00:00
发行人: C=86, ST=henanzhengzhou, L=china, O=zhengtuo, OU=zhengtuo, CN=zhengtuo
序列号: 0x4c54e1c3
哈希算法: sha256
md5值: 593a6af64ee24f5e8b05d14fe13fc4ca
sha1值: b5a1c8d38e250c4b326074d8d04ea623ed996280
sha256值: 42730a5240a4a86ef706f2571de34128b7786760721b4372bb023d5348656ad5
sha512值: 317a0cf96cef44f17c8ed210285beb7c3c57e38b5f384c232dcaa41a0272d2e26a9895427ca3adfe2a23e30a3142f63dff4f26eb0f2f932982f001cbb8ab65ae
公钥算法: rsa
密钥长度: 2048
指纹: 5467400c3d1ad299230a3536f6f646a6c8ae97f80d216fccd94a83668d1c8d3b

硬编码敏感信息

可能的敏感信息
"add_user" : "添加新账号登录"
"capital_password" : "资金密码"
"certainMoneyPassword" : "确认资金密码"

"certainPassword" : "确认密码"

"changeLoginPassword" : "更改登录密码"

"changeMoneyPassword" : "修改资金密码"

"forgetGesturesPassword" : "忘记手势密码？"

"gesturesPassword" : "手势密码"

"keep_password" : "记住密码"

"login_password" : "登录密码"

"modify_password" : "请先修改登录密码"

"password" : "密码"

"pwd_diff" : "两次密码不一致！"

"repeat_password" : "重复密码"

"setMoneyPassword" : "设置资金密码"

"user_name" : "用户名"

"username" : "手机号"

"withdrawSystem" : "提积到系统"

"add_user" : "Add a new account"

"capital_password" : "Fund password"

"certainMoneyPassword" : "confirmFundPassword"

"certainPassword" : "certainPassword"
"changeLoginPassword" : "Change Login Password"
"changeMoneyPassword" : "Change Fund Password"
"forgetGesturesPassword" : "Forget gestures password？"
"gesturesPassword" : "Gestures Password"
"keep_password" : "Keep password"
"login_password" : "Login password"
"modify_password" : "Modify Login Password first!"
"password" : "Password"
"pwd_diff" : "Passwords are different."
"repeat_password" : "Repeat password"
"setMoneyPassword" : "Set Fund Password"
"user_name" : "Username"
"username" : "Your Phone Number"
"withdrawSystem" : "Withdraw to System"

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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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.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.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.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.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信