MoGua

宜花呗 null.APK 分析报告

APP名称:	宜花呗

包名:	gbv5pggdsf.c3fdrgrghvf.dsfwfg6Fwhjfbfl
域名线索:	33条
URL线索:	31条
邮箱线索:	1条
分析日期:	2025年6月26日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: cyfq.apk
文件大小: 22.83MB
MD5值: 3cc01e9a1e068b7e7c678eeaca3f89a6
SHA1值: 3aac393472e3c16f3a42687afb056cef26bf3968
SHA256值: 76c3908afddadbe054ab2fe7a9335069c684f1083304646ea43e629b922076dd

APP 信息

App名称: 宜花呗
包名: gbv5pggdsf.c3fdrgrghvf.dsfwfg6Fwhjfbfl
主活动Activity: com.yihuabeidfd.hyf.ui.activitys.FlowerdHY_01UEO3ACT
安卓版本名称: null
安卓版本:

域名线索

域名	服务器信息
i.open.t.sina.com.cn	**IP**: 10.6.64.38 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
render.alipay.com	**IP**: 124.95.153.221 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
	IP: 106.11.172.8 **所属国家**: China **地区**: Zhejiang

cloudauth-dualstack.aliyuncs.com	**城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com	**IP**: 140.206.110.66 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
plus.google.com	**IP**: 104.244.43.104 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
mdc.html5.qq.com	**IP**: 125.39.196.199 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
debugtbs.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

debugx5.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.youtube.com	**IP**: 199.16.158.12 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
androwad.oss-cn-hans.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
cfg.imtt.qq.com	**IP**: 60.29.240.17 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
pms.mb.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.beizhuabao.com	没有服务器地理信息.
	IP: 116.133.8.18 **所属国家**: China

service.weibo.com	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
open.weibo.cn	IP: 123.125.107.13 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
tianshu.alicdn.com	IP: 116.142.234.241 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
pop.yuncloudauth.com	IP: 106.11.232.51 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
nice800.com	IP: 43.132.110.135 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
soft.tbs.imtt.qq.com	IP: 119.167.147.86 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941

log.tbs.qq.com	**IP**: 124.95.231.218 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
cjalkdjqioac-1358177159.cos.ap-shanghai.myqcloud.com	**IP**: 61.241.129.102 **所属国家**: China **地区**: Anhui **城市**: Hefei **纬度**: 31.863815 **经度**: 117.280830
schemas.android.com	没有服务器地理信息.
cloudauth-dualstack.cn-beijing.aliyuncs.com	**IP**: 8.141.244.37 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
zcvkjlkajsldjfiowr-1358164145.cos.ap-guangzhou.myqcloud.com	**IP**: 36.248.13.186 **所属国家**: China **地区**: Fujian **城市**: Fuzhou **纬度**: 26.061390 **经度**: 119.306107
android.bugly.qq.com	**IP**: 124.95.225.146 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
	IP: 59.24.3.174 **所属国家**: Korea (Republic of)

accounts.google.com	**地区**: Gyeonggi-do **城市**: Seongnam **纬度**: 37.420624 **经度**: 127.126717
cloudauth.aliyuncs.com	**IP**: 106.11.232.51 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
mgw.mpaas.cn-hangzhou.aliyuncs.com	**IP**: 47.118.173.135 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
auth.yunverify.com	**IP**: 106.11.232.51 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

cloudauth.cn-beijing.aliyuncs.com	**IP**: 8.141.244.36 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	b/h/f/d/g.java
https://mgw.mpaas.cn-hangzhou.aliyuncs.com	com/alipay/alipaysecuritysdk/common/config/Configuration.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://render.alipay.com/p/f/fd-j8l9yjja/index.html	com/dtf/face/config/NavigatePage.java
https://cloudauth-dualstack.aliyuncs.com	com/dtf/face/api/DTFacadeExt.java
https://cloudauth.aliyuncs.com	com/dtf/face/api/DTFacadeExt.java
https://cloudauth-dualstack.cn-beijing.aliyuncs.com	com/dtf/face/api/DTFacadeExt.java
https://cloudauth.cn-beijing.aliyuncs.com	com/dtf/face/api/DTFacadeExt.java
https://auth.yunverify.com	com/dtf/face/api/DTFacadeExt.java
https://pop.yuncloudauth.com	com/dtf/face/api/DTFacadeExt.java
https://nice800.com	com/yihuabeidfd/hyf/ui/activitys/FlowerEOT7ACT.java

https://nice800.com/	com/yihuabeidfd/hyf/ui/activitys/FlowerUEO4ACT.java
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://service.weibo.com/share/mobilesdk.php	com/sina/weibo/sdk/web/WebActivity.java
https://open.weibo.cn/oauth2/authorize?	com/sina/weibo/sdk/web/WebActivity.java
https://cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com/model/toyger.face.dat	d/h/a/n/k.java
https://tianshu.alicdn.com/7504f3f0-aca8-4636-b486-e396559d3efb.png	d/h/a/n/k.java
https://plus.google.com/	d/k/a/c/c/k/s1.java
https://accounts.google.com/o/oauth2/revoke?token=	d/k/a/c/a/a/e/c/f.java
http://schemas.android.com/apk/res-auto	d/k/a/d/v/a.java
https://www.youtube.com	d/n/a/i/a/d/a.java
https://www.youtube.com	d/n/a/i/a/f/a.java
http://www.youtube.com/watch?v=	d/n/a/i/b/a.java
https://android.bugly.qq.com/rqd/async	d/r/a/d/a/b/a.java
http://pms.mb.qq.com/rsp204	d/r/b/b/w.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	d/r/b/b/p/e.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	d/r/b/c/w.java

http://log.tbs.qq.com/ajax?c=pu&tk=	d/r/b/c/w.java
http://log.tbs.qq.com/ajax?c=dl&k=	d/r/b/c/w.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	d/r/b/c/w.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	d/r/b/c/w.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	d/r/b/c/m.java
https://androWad.oss-cn-hans.com/domainNRame/51dfsdWE00635.text/	d/u/b/c/a/d.java
http://www.beizhuabao.com	d/u/b/c/a/a.java
https://cjalkdjqioac-1358177159.cos.ap-shanghai.myqcloud.com	d/u/b/c/a/e.java
https://zcvkjlkajsldjfiowr-1358164145.cos.ap-guangzhou.myqcloud.com	d/u/b/c/a/e.java
https://jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com	d/u/b/c/a/e.java
http://www.beizhuabao.com	d/u/b/c/a/b.java
https://service.weibo.com/share/mobilesdk.php	d/q/a/a/i/c/d.java
https://service.weibo.com/share/mobilesdk_uppic.php	d/q/a/a/a/d.java
http://i.open.t.sina.com.cn/mobilesdk/sendmessage.php	d/q/a/a/a/c.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	d/k/a/c/c/v.java

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=TR, ST=Xvddgbtugovorc, L=Berlin, O=Xeykkhzggspqv, OU=ddgxyywjuhp, CN=Xipvsdqokcp
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-25 04:11:05+00:00
有效期至: 2028-06-24 04:11:05+00:00
发行人: C=TR, ST=Xvddgbtugovorc, L=Berlin, O=Xeykkhzggspqv, OU=ddgxyywjuhp, CN=Xipvsdqokcp
序列号: 0x6045a1f3
哈希算法: sha1
md5值: 8038512b0685cb5a8ce642d67aaea816
sha1值: 1da06827ede6b6825591357979c7b79ddeacac27
sha256值: 135d6ff4f33183bb4d1e7cbf6f6feb08e609520387b119a6d455b80c27202f3a
sha512值: 4f0b85b67bb9aa387dccb5ed6ba98f55eb891ee00ff14145f61af3a0a8dd1199b6d7165b9b02232e1e6848ee730b8f43f9f2264882aaaadf8b7f074ccfa9fb69
公钥算法: rsa
密钥长度: 1024
指纹: 19f30e3749aea20a7fc6eb71e93d11604d0e4993caa07a70432c455e8c0c0deb

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.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.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.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.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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.WRITE_CALL_LOG	危险		允许应用程序写入（但不读取）用户号召日志数据。
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
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_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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference

android.permission.READ_MEDIA_IMAGES	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.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference

应用内通信