Evaluation Warning: The document was created with Spire.Doc for Python.

**小月亮（ 1.0.0版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 小月亮 |
| 版本 | 1.0.0 |
| 包名 | com.xuyu.xuyu |
| 域名线索 | 68条 |
| URL线索 | 130条 |
| APP图标 |  |
| 分析日期 | 2025年6月27日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | xiaoyueliang.apk |
| 文件大小 | 115.27MB |
| MD5值 | 89049e5d77c3a8a592418c15759ee3da |
| SHA1值 | f7b1254885b2287a90d4b4d13a3d6622f872825c |
| SHA256值 | 861e36f6427785d97436f270db94c34ef2c4a61cf3d933b75f456f5bd7782505 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小月亮 |
| 包名 | com.xuyu.xuyu |
| 主活动Activity | com.xuyu.xuyu.view.main.CoverActivity |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| open.weixin.qq.com | IP: 116.128.171.214  所属国家: China  地区: Shanghai  城市: Shanghai |
| mobilegw.alipay.com | IP: 203.209.243.98  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| yuehua123.oss-cn-beijing.aliyuncs.com | IP: 59.110.190.27  所属国家: China  地区: Beijing  城市: Beijing |
| w-.w-.hicloud.com | 没有服务器地理信息. |
| android.bugly.qq.com | IP: 124.95.225.146  所属国家: China  地区: Liaoning  城市: Shenyang |
| dualstack-a.apilocate.amap.com | IP: 106.11.43.81  所属国家: China  地区: Beijing  城市: Beijing |
| app.langlangshan.xyz | IP: 123.126.74.197  所属国家: China  地区: Beijing  城市: Beijing |
| av1.xdrig.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| dualstack-arestapi.amap.com | IP: 106.11.43.113  所属国家: China  地区: Beijing  城市: Beijing |
| ccc.sys.miui.com | IP: 111.206.174.172  所属国家: China  地区: Beijing  城市: Beijing |
| api.weixin.qq.com | IP: 116.128.170.42  所属国家: China  地区: Shanghai  城市: Shanghai |
| m.alipay.com | IP: 203.209.245.74  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| conf.xdrig.com | IP: 114.67.244.173  所属国家: China  地区: Beijing  城市: Beijing |
| apilocate.amap.com | IP: 59.82.31.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| mcgw.alipay.com | IP: 111.202.5.209  所属国家: China  地区: Beijing  城市: Beijing |
| api-push.meizu.com | IP: 221.5.93.66  所属国家: China  地区: Guangdong  城市: Foshan |
| mta.oa.com | IP: 141.144.196.217  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| metrics.data.hicloud.com | IP: 111.202.16.252  所属国家: China  地区: Beijing  城市: Beijing |
| fr.register.xmpush.global.xiaomi.com | IP: 98.64.182.160  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| metrics1.data.hicloud.com | IP: 111.202.16.252  所属国家: China  地区: Beijing  城市: Beijing |
| sandcash.mixienet.com.cn | IP: 203.107.86.172  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.mob.com | IP: 180.188.26.28  所属国家: China  地区: Zhejiang  城市: Taizhou |
| a.vmall.com | IP: 49.4.39.46  所属国家: China  地区: Guangdong  城市: Guangzhou |
| 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 |
| metok.sys.miui.com | IP: 111.206.101.98  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| crash.163.com | IP: 45.254.50.146  所属国家: China  地区: Guangdong  城市: Guangzhou |
| schemas.android.com | 没有服务器地理信息. |
| webtest.netease.im | IP: 111.124.202.79  所属国家: China  地区: Guizhou  城市: Zunyi |
| www.jivesoftware.com | IP: 23.235.209.143  所属国家: United States of America  地区: Virginia  城市: Virginia Beach |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api-push.in.meizu.com | IP: 206.161.233.191  所属国家: United States of America  地区: Virginia  城市: Herndon |
| wappaygw.alipay.com | IP: 111.202.5.209  所属国家: China  地区: Beijing  城市: Beijing |
| pingma.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| lbs.netease.im | IP: 220.197.34.90  所属国家: China  地区: Sichuan  城市: Leshan |
| h5.m.taobao.com | IP: 125.39.155.58  所属国家: China  地区: Tianjin  城市: Tianjin |
| app.shixi.love | IP: 103.248.152.110  所属国家: China  地区: Zhejiang  城市: Jinhua |
| img.chuxia12125.com.cn | IP: 101.67.62.47  所属国家: China  地区: Zhejiang  城市: Huzhou |
| nosup-hz1.127.net | IP: 122.156.130.202  所属国家: China  地区: Heilongjiang  城市: Heihe |
| cgicol.amap.com | IP: 110.253.189.211  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| me.xdrig.com | IP: 116.198.14.174  所属国家: China  地区: Beijing  城市: Beijing |
| play.google.com | IP: 142.251.215.238  所属国家: United States of America  地区: California  城市: Mountain View |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| resolver.msg.xiaomi.net | IP: 110.43.0.169  所属国家: China  地区: Beijing  城市: Beijing |
| app.chuxia12125.com.cn | IP: 101.37.88.200  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| i.tddmp.com | IP: 116.196.71.30  所属国家: China  地区: Beijing  城市: Beijing |
| register.xmpush.global.xiaomi.com | IP: 47.237.96.1  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| norma-external-collect.meizu.com | 没有服务器地理信息. |
| abroad.apilocate.amap.com | IP: 59.82.44.11  所属国家: China  地区: Shanghai  城市: Shanghai |
| www.huawei.com | IP: 121.22.232.166  所属国家: China  地区: Hebei  城市: Qinhuangdao |
| xmlpull.org | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| mclient.alipay.com | IP: 1.189.99.73  所属国家: China  地区: Heilongjiang  城市: Harbin |
| adiu.amap.com | IP: 110.253.189.147  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| long.open.weixin.qq.com | IP: 112.65.193.150  所属国家: China  地区: Shanghai  城市: Shanghai |
| h.trace.qq.com | IP: 113.56.189.162  所属国家: China  地区: Hubei  城市: Huangshi |
| store.hispace.hicloud.com | IP: 49.4.47.241  所属国家: China  地区: Guangdong  城市: Guangzhou |
| paygate-yf.meituan.com | IP: 103.37.152.89  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| mta.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| restsdk.amap.com | IP: 106.11.43.113  所属国家: China  地区: Beijing  城市: Beijing |
| dashboard.agora.io | IP: 106.14.163.9  所属国家: China  地区: Shanghai  城市: Shanghai |
| dr.netease.im | IP: 220.197.34.83  所属国家: China  地区: Sichuan  城市: Leshan |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| lbs.amap.com | IP: 110.253.188.147  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| wannos.127.net | IP: 45.127.129.16  所属国家: China  地区: Guangdong  城市: Guangzhou |
| da.dun.163.com | IP: 59.111.248.82  所属国家: China  地区: Guangdong  城市: Guangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://) | cn/sharesdk/framework/a/a.java |
| https://api.weixin.qq.com/sns/oauth2/access\_token | cn/sharesdk/wechat/utils/h.java |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token | cn/sharesdk/wechat/utils/h.java |
| https://api.weixin.qq.com/sns/userinfo | cn/sharesdk/wechat/utils/h.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.aaa.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.stable.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/cons/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/cons/a.java |
| http://m.alipay.com/?action=h5quit | com/alipay/sdk/cons/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/packet/impl/c.java |
| http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$& | com/alipay/sdk/data/a.java |
| https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple\ | com/alipay/test/a.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/ | com/amap/api/location/AMapLocation.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| http://yuehua123.oss-cn-beijing.aliyuncs.com/ | com/grm/uikit/dialog/GiftRecycleAdapter.java |
| https://www.huawei.com/auth/account/base.profile/accesstoken | com/huawei/hms/support/api/entity/hwid/HwIDConstant.java |
| https://www.huawei.com/auth/account/base.profile/serviceauthcode | com/huawei/hms/support/api/entity/hwid/HwIDConstant.java |
| https://www.huawei.com/auth/account/base.profile/servicecountrycode | com/huawei/hms/support/api/entity/hwid/HwIDConstant.java |
| https://www.huawei.com/auth/account/base.profile | com/huawei/hms/support/api/entity/hwid/HwIDConstant.java |
| https://play.google.com/store/apps/details?id= | com/huawei/hms/support/api/push/a/a/a.java |
| http://a.vmall.com/ | com/huawei/hms/support/api/push/a/a/a.java |
| http://schemas.android.com/apk/res/android | com/huawei/hms/support/api/game/ui/GifImageView.java |
| https://www.huawei.com/auth/sns/read | com/huawei/hms/support/api/sns/HuaweiSns.java |
| https://www.huawei.com/auth/sns/write | com/huawei/hms/support/api/sns/HuaweiSns.java |
| https://www.huawei.com/auth/sns/friends.account | com/huawei/hms/support/api/sns/HuaweiSns.java |
| https://metrics1.data.hicloud.com:6447 | com/huawei/hms/api/HuaweiApiClient.java |
| http://a.vmall.com/app/ | com/huawei/hms/update/e/k.java |
| https://)[\\w-]+\\.[\\w-]+(\\.hicloud\\.com:)[\\d] | com/huawei/hianalytics/v2/a/b/h.java |
| https://metrics.data.hicloud.com:6447 | com/huawei/hianalytics/v2/a/b/n.java |
| https://store.hispace.hicloud.com/hwmarket/api/ | com/huawei/updatesdk/service/a/e.java |
| https://adiu.amap.com/ws/device/adius | com/loc/bi.java |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74& | com/loc/cy.java |
| http://apilocate.amap.com/mobile/binary | com/loc/fp.java |
| http://dualstack-a.apilocate.amap.com/mobile/binary | com/loc/fp.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fp.java |
| https://restsdk.amap.com/sdk/compliance/params | com/loc/as.java |
| http://restsdk.amap.com/sdk/compliance/params | com/loc/as.java |
| http://restsdk.amap.com | com/loc/w.java |
| http://restsdk.amap.com/v3/place/text? | com/loc/a.java |
| http://restsdk.amap.com/v3/config/district? | com/loc/a.java |
| http://restsdk.amap.com/v3/place/around? | com/loc/a.java |
| https://restsdk.amap.com/v3/iasdkauth | com/loc/n.java |
| https://dualstack-arestapi.amap.com/v3/iasdkauth | com/loc/n.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fv.java |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo | com/loc/fj.java |
| http://restsdk.amap.com/v3/geocode/regeo | com/loc/fj.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fh.java |
| https://api-push.meizu.com | com/meizu/cloud/pushsdk/b/c/e.java |
| https://api-push.meizu.com/garcia/api/client/ | com/meizu/cloud/pushsdk/platform/a/a.java |
| https://api-push.in.meizu.com/garcia/api/client/ | com/meizu/cloud/pushsdk/platform/a/a.java |
| http://norma-external-collect.meizu.com/android/exchange/getpublickey.do | com/meizu/cloud/pushsdk/a/a/a.java |
| http://norma-external-collect.meizu.com/push/android/external/add.do | com/meizu/cloud/pushsdk/a/a/b.java |
| https://nosup-hz1.127.net | com/netease/nimlib/l/a/b/a/c.java |
| https://wannos.127.net/lbs | com/netease/nimlib/l/a/b/a/c.java |
| https://webtest.netease.im/lbs/conf.jsp | com/netease/nimlib/f/e.java |
| https://webtest.netease.im/1.gif | com/netease/nimlib/f/e.java |
| https://webtest.netease.im/lbsrc/conf.jsp | com/netease/nimlib/f/e.java |
| https://lbs.netease.im/lbs/conf.jsp | com/netease/nimlib/f/e.java |
| https://dr.netease.im/1.gif | com/netease/nimlib/f/e.java |
| https://crash.163.com/uploadCrashLogInfo.do | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java |
| https://crash.163.com/client/api/uploadStartUpInfo.do | com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java |
| https://da.dun.163.com/sn.gif?d= | com/netease/nis/captcha/i.java |
| https://github.com/yyued/SVGAPlayer-Android | com/opensource/svgaplayer/SVGAParser.java |
| http://xmlpull.org/v1/doc/features.html | com/ta/utdid2/b/a/a.java |
| http://xmlpull.org/v1/doc/features.html | com/ta/utdid2/b/a/e.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 |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/f.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/d.java |
| http://mta.qq.com/ | com/tencent/wxop/stat/StatServiceImpl.java |
| http://mta.oa.com/ | com/tencent/wxop/stat/StatServiceImpl.java |
| http://pingma.qq.com:80/mstat/report | com/tencent/wxop/stat/common/StatConstants.java |
| https://sandcash.mixienet.com.cn | com/pay/paytypelibrary/base/PayUtil.java |
| https://sandcash.mixienet.com.cn/gateway/v2/order/quickPayment | com/pay/paytypelibrary/base/PayUtil.java |
| https://sandcash.mixienet.com.cn/gateway/v2/order/mixedpay | com/pay/paytypelibrary/base/PayUtil.java |
| https://sandcash.mixienet.com.cn/gateway/v2/order/linkCodePayment | com/pay/paytypelibrary/base/PayUtil.java |
| https://sandcash.mixienet.com.cn/pay/sdk? | com/pay/paytypelibrary/base/PayUtil.java |
| https://sandcash.mixienet.com.cn/gateway/v2/api | com/pay/paytypelibrary/base/PayUtil.java |
| https://sandcash.mixienet.com.cn/gateway/v2/quick | com/pay/paytypelibrary/base/PayUtil.java |
| https://av1.xdrig.com/u/a | com/tendcloud/tenddata/d.java |
| https://me.xdrig.com | com/tendcloud/tenddata/e.java |
| https://conf.xdrig.com/sdk/conf? | com/tendcloud/tenddata/gb.java |
| https://i.tddmp.com/a/ | com/tendcloud/tenddata/gy.java |
| http://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/bb.java |
| https://register.xmpush.global.xiaomi.com/pass/register | com/xiaomi/push/service/t.java |
| https://fr.register.xmpush.global.xiaomi.com/pass/register | com/xiaomi/push/service/t.java |
| https://metok.sys.miui.com | com/xiaomi/metoknlp/b.java |
| http://ccc.sys.miui.com | com/xiaomi/metoknlp/a/f.java |
| http://%1$s/gslb/?ver=4.0 | com/xiaomi/network/HostManager.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/smack/g.java |
| http://www.jivesoftware.com/xmlns/xmpp/properties\ | com/xiaomi/smack/packet/d.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/smack/provider/c.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/smack/util/a.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/slim/e.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/im/uikit/common/Constans.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/im/uikit/common/ui/imageview/HeadImageView.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/BillAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/InvitationListAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/InviteAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/GeneralOptionsRecyclerAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/AddSkillRecyclerAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/InfoEditPhotoRecyclerAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/SettingBrandAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/RankAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/SocialAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/settings/adapter/VideoRecordAdapter.java |
| https://api.weixin.qq.com/sns/oauth2/access\_token? | com/xuyu/xuyu/controller/settings/manager/SettingManager.java |
| https://app.langlangshan.xyz/api/passport/base\_param | com/xuyu/xuyu/controller/constant/ConstUrl.java |
| https://app.chuxia12125.com.cn | com/xuyu/xuyu/controller/constant/ConstUrl.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/constant/ConstUrl.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/main/adapter/GiftReceivedAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/main/adapter/GuardRankAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/main/adapter/SearchAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/main/adapter/GenderUserAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/main/adapter/OneKeyAttentionAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/main/adapter/VideoAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/main/adapter/BlackAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/main/adapter/MainChannelAdapter.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/controller/dynamics/adapter/DynamicsAdapter.java |
| https://dashboard.agora.io/ | com/xuyu/xuyu/agora/WorkerThread.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/utils/ClickToastUtils.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/settings/PreSelfieActivity.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/settings/CopyBoardActivity.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/settings/InfoEditActivity.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/settings/SkillSettingActivity.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/settings/SuperMemberFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/settings/GeneralMemberFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/settings/SettingFragment.java |
| https://dashboard.agora.io/ | com/xuyu/xuyu/view/base/BaseApplication.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/base/utils/view/OtherGuardDialog.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/base/utils/view/ToastNoticeDialog.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/MainHomePageActivity.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/MainActivity.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/VideoFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/MainRecommendActiveFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/MainRecommendCityFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/MainRecommendPeopleFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/RecommendFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/AgoraWithFUVideoActivity.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/main/AgoraWithFUVideo2Activity.java |
| https://app.shixi.love/index/about/agreement.html\ | com/xuyu/xuyu/view/main/dialog/FirstTipDialog.java |
| https://app.shixi.love/index/about/privacy.html\ | com/xuyu/xuyu/view/main/dialog/FirstTipDialog.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/news/im/holder/GiftViewHolder.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/news/im/holder/DynamicHolder.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/news/im/holder/OnlineNoticeHolder.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/news/im/holder/AttentionFansHolder.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/news/activity/ChatSettingActivity.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/rank/CharmRankFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/rank/ConsumptionRankFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/rank/GiftRankFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/rank/GuardRankFragment.java |
| http://img.chuxia12125.com.cn/ | com/xuyu/xuyu/view/rank/ZhimiMiBiRankFragment.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Maybe.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Observable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Flowable.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 |
| https://github.com/panpf/sketch | me/panpf/sketch/ErrorTracker.java |
| https://github.com/panpf/sketch | me/panpf/sketch/decode/GifDecodeHelper.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 |
| http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. | 摸瓜V1引擎 |
| http://www.mob.com/about/policy>http://www.mob.com/about/policy</a> | 摸瓜V1引擎 |
| https://www.mob.com | 摸瓜V1引擎 |
| http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If | 摸瓜V1引擎 |
| http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a> | 摸瓜V1引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| dicheh@he8cifi6ebehchcc.e\_ci | cn/fly/commons/C0167r.java |
| 034fgffeflfmfkfefn@e.fm0gkhgk1f | cn/fly/tools/b/j.java |
| 011@gl2hk9hg.fk | cn/fly/tools/utils/a.java |
| xxxx@xxxx.com | com/huawei/hms/support/api/push/a/d/a.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | com/faceunity/wrapper/faceunity.java |
| 14222222222 | com/loc/n.java |

## **5. 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: CN=1 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-20 16:21:19+00:00 有效期至: 2050-06-14 16:21:19+00:00 发行人: CN=1 序列号: 0x1 哈希算法: sha256 md5值: 8fe65d9ac114ffe2ca3bf8f51e632837 sha1值: 14630e408af0d4c0341ed4ecdaf47885c20d9d50 sha256值: b0f5bbd9e70e5dbb806b0d6853c637681aa83083b2cd81bcc9632d9901f82eaf sha512值: 64afe065b215c2eedeffa800efb49ec858812a7e1b9c03b22cf95b3c061a16eada2083191bc64f17f7d81d47d37faf1c09da49705ff789b51a8101046d8f583e 公钥算法: rsa 密钥长度: 2048 指纹: 61a2d6f91db692eb41e5025830ba4f88f23df6fedb3cb884591fee7863a2e7a3**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "login\_auth\_cancle" : "授权取消" |
| "login\_auth\_failure" : "授权失败" |
| "login\_auth\_ing2" : "正在授权中" |
| "login\_auth\_success1" : "授权成功" |
| "mobcommon\_authorize\_dialog\_accept" : "Accept" |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject" |
| "mobcommon\_authorize\_dialog\_reject" : "Reject" |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use" |
| "mobdemo\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。" |
| "mobdemo\_authorize\_dialog\_title" : "服务授权" |
| "ssdk\_cmcc\_auth" : "手机认证服务由中国移动提供" |
| "ssdk\_cmcc\_login\_one\_key" : "本机号码一键登录" |
| "ssdk\_instapaper\_pwd" : "密码" |
| "ssdk\_weibo\_oauth\_regiseter" : "应用授权" |
| "team\_authentication" : "身份验证" |
| "team\_invitee\_authentication" : "被邀请人身份验证" |
| "team\_invitee\_need\_authen" : "需要验证" |
| "team\_invitee\_not\_need\_authen" : "不需要验证" |
| "team\_need\_authentication" : "需要身份验证" |
| "mobcommon\_authorize\_dialog\_accept" : "Accept" |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject" |
| "mobcommon\_authorize\_dialog\_reject" : "Reject" |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use" |
| "mobdemo\_authorize\_dialog\_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see details<a href=http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject." |
| "mobdemo\_authorize\_dialog\_title" : "service authority" |
| "ssdk\_cmcc\_auth" : "Provided by China Mobile" |
| "ssdk\_cmcc\_login\_one\_key" : "PhoneNum Login" |
| "ssdk\_instapaper\_pwd" : "Password" |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization" |
| "mobcommon\_authorize\_dialog\_accept" : "同意" |
| "mobcommon\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。" |
| "mobcommon\_authorize\_dialog\_reject" : "拒绝" |
| "mobcommon\_authorize\_dialog\_title" : "服务授权" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| 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.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.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.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.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\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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。 |
| com.xuyu.xuyu.permission.RECEIVE\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.xuyu.xuyu.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.live.yeban.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.live.yeban.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| android.permission.CAPTURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获视频输出 |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| android.permission.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.xuyu.xuyu.view.main.CoverActivity | **Schemes**: jjicfq://, |
| com.xuyu.xuyu.view.main.MainActivity | **Schemes**: xmigqv://, |
| com.xuyu.xuyu.view.settings.CaibeiRechargeActivity | **Schemes**: yuehua://,  **Hosts:** recharge, |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**