



MoGua

涩里番 3.5.APK 分析报告



APP名称:

涩里番

包名:	com.qnmd.aslf.zy04sd
域名线索:	24条
URL线索:	26条
邮箱线索:	4条
分析日期:	2025年9月29日
分析平台:	摸瓜APK反编译平台

文件名: nifan.apk
文件大小: 13.69MB
MD5值: 567187020aa7bbba26815b533419a4ed
SHA1值: 730821df3ad6e95db6e8be0c145ad298642da6a2
SHA256值: eff1b0088ca8bb340930db323841733403be7effcfc049e8a0f75ce1aabbec4b

i APP 信息

App名称: 涩里番
包名: com.qnmd.aslf.zy04sd
主活动Activity: com.qnmd.qz.ui.splash.SplashActivity
安卓版本名称: 3.5
安卓版本: 3

🔍 域名线索

域名	服务器信息
slfvne3u647.com	IP: 47.243.69.174 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Manchester 纬度: 53.480949 经度: -2.237430
mobilegw.aaa.alipay.net	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
schemas.microsoft.com	IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903

slf3z8719zx.com	没有服务器地理信息.
loggw-exsdk.alipay.com	IP: 110.76.3.1 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
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
api.slfa23m22e.com	没有服务器地理信息.
playready.directtaps.net	IP: 104.45.231.79 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mobilegw.stable.alipay.net	没有服务器地理信息.

mobilegw.alipay.com	IP: 203.209.247.65 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mclient.alipay.com	IP: 220.181.135.162 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.slfwkcm4ki6.com	没有服务器地理信息.
wappaygw.alipay.com	IP: 124.239.239.236 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
h5.m.taobao.com	IP: 220.181.135.167 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.slfbk6ezwnn.com	没有服务器地理信息.
dashif.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724

m.alipay.com	IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mcgw.alipay.com	IP: 124.239.239.236 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
api-slf.kffggnz.com	IP: 172.67.148.246 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
x981tqddoy7.com	IP: 46.8.8.100 所属国家: Czechia 地区: Praha, Hlavni mesto 城市: Prague 纬度: 50.087936 经度: 14.420798

 URL线索

URL信息	Url所在文件
https://h5.m.taobao.com/mlapp/olist.html	d/c/b/c/a.java
https://mobilegw.alipay.com/mgw.htm	d/c/b/c/d.java

https://mobilegw.alipay.com/mgw.htm	d/c/b/f/c.java
https://mcgw.alipay.com/sdklog.do	d/c/b/f/d/c.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	d/c/b/f/d/d.java
http://m.alipay.com/?action=h5quit	d/c/b/j/h.java
http://www.w3.org/ns/ttml	d/k/a/a/l1/r/a.java
http://dashif.org/guidelines/last-segment-number	d/k/a/a/k1/l0/k/c.java
https://github.com/kongzue/DialogX/wiki	d/o/a/d/g.java
https://github.com/kongzue/DialogX	d/o/a/d/b.java
https://github.com/kongzue/DialogX	d/o/a/b/p.java
http://api-slf.kffggz.com/cxapi/	d/a/a/d/g.java
http://x981tqddoy7.com/cxapi/	d/a/a/d/g.java
http://slfvne3u647.com/cxapi/	d/a/a/d/g.java
http://slf3z8719zx.com/cxapi/	d/a/a/d/g.java
http://api.slfkb6ezwnn.com/cxapi/	d/a/a/d/g.java
http://api.slfd23m22e.com/cxapi/	d/a/a/d/g.java
http://api.slfwkcm4ki6.com/cxapi/	d/a/a/d/g.java
https://github.com/danikula/AndroidVideoCache/issues/43	d/g/a/i.java
https://github.com/danikula/AndroidVideoCache/issues	d/g/a/i.java

https://github.com/danikula/AndroidVideoCache/issues/88 .	d/g/a/i.java
http://%s:%d/%s	d/g/a/g.java
https://github.com/danikula/AndroidVideoCache/issues/134 .	d/g/a/g.java
http://%s:%d/%s	d/g/a/l.java
http://schemas.android.com/apk/res/android	n/a/a/a/a.java
http://ns.adobe.com/xap/1.0/\u0000	o/o/a/a.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	p/a/a/c/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	p/a/a/c/d.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/ShitTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java

http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.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
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java

邮箱线索

邮箱地址	所在文件
this@videodetailactivity.id	d/a/a/a/c/n.java
slfmh520@gmail.com	d/a/a/e/b.java
danikula@gmail.com	d/g/a/i.java
this@videodetailactivitv.id	defoackage/f.iava

手机线索

手机号	所在文件
18222222222	d/k/a/a/f1/a0/a.java
17222222222	d/k/a/a/f1/a0/a.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

签名算法: rsassa_pkcs1v15

有效期自: 2022-08-30 20:00:02+00:00

有效期至: 2050-01-15 20:00:02+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

序列号: 0x3d3ccc55

哈希算法: sha256

md5值: 098bda03d72b16624ebd9dea71c0b35c

sha1值: aa5d368933b3c0b0fb10f2ce48ea64261947629a

sha256值: 743cbc569b9b3efd4ac7e66d5cc240dbb9c937056289dc5df1f64dec76466435

sha512值: a60b9725f93465482d427b586477ec26fe1a9ed313ac0576b75f917cbbf368d71268557a6c162c9366edf43191c9a1990c3c80fa119b322abde325317ecbe5f3

公钥算法: rsa

密钥长度: 2048

指纹: b08a71a496aeeb703594e7b522e46e47c48e4d9c06bf113dbd12951ba4588639

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_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.VIBRATE	正常	可控震源	允许应用程序控制振动器

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_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.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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信