



Failed.APK 分析报告



APP名称:

包名:

Failed

域名线索:

62条

URL线索:

60条

邮箱线索:

4条

分析日期:	2025年7月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 友人 (5551) .apk
文件大小: 46.0MB
MD5值: 75d884048482de3b78d71d249f79a777
SHA1值: db98b37bae7eabf615d13481057ab98599732efe
SHA256值: 4982e1ba1af1a1b2167f0a083bde5859a98d586dddc5d7e12ac70cdb833f0a3

APP 信息

App名称:
包名: Failed
主活动Activity:
安卓版本名称: Failed
安卓版本: Failed

域名线索

域名	服务器信息

register.xmpush.global.xiaomi.com	IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067
nos.netease.com	IP: 45.127.129.36 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
apiinit.amap.com	IP: 203.119.175.194 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
www.jivesoftware.com	IP: 35.238.7.255 所属国家: United States of America 地区: Iowa 城市: Council Bluffs 纬度: 41.261940 经度: -95.860832
wannos.127.net	IP: 223.252.196.42 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
apilocatesrc.amap.com	IP: 59.82.60.15 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
aws1388we.s3.ap-east-1.amazonaws.com	IP: 52.95.161.62 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
lbs.chatnos.com	IP: 59.111.248.109 所属国家: China 地区: Guangdong 城市: Guangzhou

	纬度: 23.116671 经度: 113.250000
appgallery.cloud.huawei.com	IP: 49.4.35.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
yuntuapi.amap.com	没有服务器地理信息.
s3.amazonaws.com	IP: 54.231.162.240 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
resolver.msg.xiaomi.net	IP: 120.92.96.13 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
mst0d.is.autonavi.com	没有服务器地理信息.
45.127.128.25	IP: 45.127.128.25 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
cgicol.amap.com	IP: 59.82.31.164 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
grid.amap.com	IP: 203.119.169.44 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
	IP: 59.111.248.105 所属国家: China

lbs-test.netease.im	地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
new.api.ad.xiaomi.com	没有服务器地理信息.
59.111.110.28	IP: 59.111.110.28 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
wap.amap.com	IP: 182.40.18.217 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
nosup-hz1.127.net	IP: 45.127.129.9 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
maps.google.cn	IP: 220.181.174.98 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
m5.amap.com	IP: 106.11.35.98 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
norma-external-collect.meizu.com	IP: 113.106.27.98 所属国家: China 地区: Guangdong 城市: Zhongshan 纬度: 22.520580 经度: 113.382317
api-push.in.meizu.com	IP: 206.161.233.191 所属国家: United States of America 地区: Virginia

	城市: Herndon 纬度: 38.978210 经度: -77.386993
apilocate.amap.com	IP: 59.82.60.15 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
imtest.netease.im	IP: 59.111.241.163 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
ru.register.xmpush.global.xiaomi.com	IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752220 经度: 37.615559
idmb.register.xmpush.global.xiaomi.com	IP: 3.110.15.184 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
xmlpull.org	IP: 74.50.61.58 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204
169.254.169.254	IP: 169.254.169.254 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

check-ipv6.netease.im	没有服务器地理信息.
api-push.meizu.com	IP: 125.94.213.129 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
play.google.com	IP: 172.217.160.110 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
rs.qiniu.com	IP: 140.249.3.105 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
dr.netease.im	IP: 59.111.238.11 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
lbs.amap.com	IP: 59.82.29.156 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
wb.amap.com	IP: 59.82.31.137 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
yunxin.163.com	IP: 59.111.243.80 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
	IP: 45.127.128.24

45.127.128.24	所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
wprd0d.is.autonavi.com	没有服务器地理信息.
cn.register.xmpush.xiaomi.com	IP: 118.26.252.220 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
169.254.170.2	IP: 169.254.170.2 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
fr.register.xmpush.global.xiaomi.com	IP: 18.195.152.179 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.115520 经度: 8.684170
api.xmpush.xiaomi.com	IP: 118.26.252.230 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
app.netease.im	IP: 59.111.243.80 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
www.163.com	IP: 118.121.192.154 所属国家: China 地区: Sichuan 城市: Chengdu 纬度: 30.666670 经度: 104.066673
	IP: 128.30.52.100 所属国家: United States of America

www.w3.org	地区: Massachusetts 城市: Cambridge 纬度: 42.365078 经度: -71.104523
store.hispac.hicloud.com	IP: 49.4.44.164 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
tm.amap.com	IP: 59.82.60.56 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
check-ipv4.netease.im	IP: 59.111.211.9 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
statistic.live.126.net	IP: 183.136.182.46 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
nim.nosdn.127.net	IP: 220.181.158.238 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
webrd0d.is.autonavi.com	没有服务器地理信息.
aws1388we.oss-cn-hongkong.aliyuncs.com	IP: 47.75.19.2 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
154.197.24.8	IP: 154.197.24.8 所属国家: Hong Kong 地区: Hong Kong

	城市: Hong Kong 纬度: 22.285521 经度: 114.157692
lbs.netease.im	IP: 59.111.211.9 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
gitee.com	IP: 212.64.63.190 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
www.baidu.com	IP: 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
restapi.amap.com	IP: 106.11.43.113 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
logs.amap.com	IP: 59.82.31.149 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

 URL线索

URL信息	Url所在文件
http://second	com/gaoyuan/mianshu/f.java
http://second	com/gaoyuan/mianshu/NimApplication.java
http://59.111.110.28:8281/lbs/demoConfig.jsp	com/gaoyuan/mianshu/main/activity/PrivatizationConfigActivity.java

http://maps.google.cn/maps/api/staticmap?size=200x100&zoom=13&markers=color:red	com/gaoyuan/mianshu/location/activity/LocationAmapActivity.java
https://gitee.com/jianliao/project1/raw/master/readme.md	com/gaoyuan/mianshu/network/MyGitFile\$mList\$2.java
https://gitee.com/ccdfddxcg/mytest/raw/master/readme.md	com/gaoyuan/mianshu/network/MyGitFile\$mList\$2.java
https://gitee.com/zhang-zhenyue/kratos/raw/master/readme.md	com/gaoyuan/mianshu/network/MyGitFile\$mList\$2.java
https://gitee.com/ph-on/gateway/raw/master/readme.md	com/gaoyuan/mianshu/network/MyGitFile\$mList\$2.java
http://rs.qiniu.com/stat/aGVhZHBpYy1hOmhlYWRRpY29uLnBuZw==#@#@#QBox	com/gaoyuan/mianshu/network/MyGitFile\$mListqQnNew\$2.java
http://rs.qiniu.com/stat/aGVhZHBpYy1iOmhlYWRRpY29uLnBuZw==#@#@#QBox	com/gaoyuan/mianshu/network/MyGitFile\$mListqQnNew\$2.java
http://rs.qiniu.com/stat/aGVhZHBpYy1jOmhlYWRRpY29uLnBuZw==#@#@#QBox	com/gaoyuan/mianshu/network/MyGitFile\$mListqQnNew\$2.java
https://gitee.com/	com/gaoyuan/mianshu/network/MyGitFile\$testGit\$1.java
http://rs.qiniu.com	com/gaoyuan/mianshu/network/MyGitFile\$testQn\$1.java
http://154.197.24.8/	com/gaoyuan/mianshu/network/MyGitFile.java
https://nim.nosdn.127.net/MTAxMTAxMA==/bmltYV8yNDM0MzQ0V8xNTMyMDUzNzM3ODkzXzJlNGQ3ZjA5LWI2MjgtNDNiNy1hZTIwLTBhYTgzMjZhYzBjZQ==?thumbnail=540x540&imageView&tostatic=0	com/gaoyuan/mianshu/chatroom/activity/ChatRoomActivity.java
https://app.netease.im/api/	com/gaoyuan/mianshu/j/a/a.java
https://statistic.live.126.net/dispatcher/req	com/netease/nimlib/c/b.java
https://statistic.live.126.net/	com/netease/nimlib/c/b/d/b.java
http://wannos.127.net/lbs;http://wannos-hz.127.net/lbs;http://wannos-bj.127.net/lbs;http://wannos-oversea.127.net/lbs;http://223.252.196.38/lbs	com/netease/nimlib/f/g.java
https://nosup-hz1.127.net	com/netease/nimlib/f/g.java
https://lbs-test.netease.im/lbs/conf.jsp	com/netease/nimlib/f/e.java
https://imtest.netease.im/1.gif	com/netease/nimlib/f/e.java
http://check-ipv4.netease.im/	com/netease/nimlib/f/e.java
http://check-ipv6.netease.im/	com/netease/nimlib/f/e.java
https://imtest.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
www.163.com	com/netease/nimlib/s/l.java
http://statistic.live.126.net/statics/report/common/form	com/netease/nimlib/d/g/a.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/push/android/external/add.do	com/meizu/cloud/pushsdk/a/a/b.java
http://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/a/a/a.java
http://apilocate.amap.com/mobile/binary	com/amap/api/col/f.java
http://apilocatesrc.amap.com/mobile/binary	com/amap/api/col/f.java
http://abroad.apilocate.amap.com/mobile/binary	com/amap/api/col/f.java
https://restapi.amap.com/v3/iasdkauth	com/amap/api/col/es.java
http://apiinit.amap.com/v3/log/init	com/amap/api/col/et.java
http://tm.amap.com	com/amap/api/col/bg.java
http://wprd0%d.is.autonavi.com	com/amap/api/col/bg.java
http://webrd0%d.is.autonavi.com	com/amap/api/col/bg.java
http://grid.amap.com/grid/%d/%d/%d?ds=	com/amap/api/col/bg.java
http://mst0%d.is.autonavi.com	com/amap/api/col/bg.java
http://cgicol.amap.com/collection/writedata?ver=v1.0_ali&	com/amap/api/col/hi.java
http://restapi.amap.com/v3/geocode/regeo	com/amap/api/col/hi.java
http://abroad.apilocate.amap.com/mobile/binary	com/amap/api/col/ia.java
http://restapi.amap.com/v3	com/amap/api/col/dc.java
https://restapi.amap.com/v3	com/amap/api/col/dc.java

http://yuntuapi.amap.com	com/emap/api/col/dc.java
https://yuntuapi.amap.com	com/emap/api/col/dc.java
http://m5.amap.com/ws/mapapi/shortaddress/transform	com/emap/api/col/dc.java
https://m5.amap.com/ws/mapapi/shortaddress/transform	com/emap/api/col/dc.java
http://restapi.amap.com	com/emap/api/col/ey.java
http://wb.amap.com/?r=%f,%f,%s,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0	com/emap/api/col/eo.java
http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0	com/emap/api/col/eo.java
http://wb.amap.com/?n=%f,%f,%f,%d&sourceapplication=openapi/0	com/emap/api/col/eo.java
http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0	com/emap/api/col/eo.java
http://logs.amap.com/ws/log/upload?product=%s&type=%s&platform=%s&channel=%s&sign=%s	com/emap/api/col/fd.java
http://restapi.amap.com/v3/place/around?	com/emap/api/col/a.java
http://restapi.amap.com/v3/place/text?	com/emap/api/col/a.java
http://restapi.amap.com/v3/config/district?	com/emap/api/col/a.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明.	com/emap/api/location/AMapLocation.java
http://wap.amap.com/	com/emap/api/maps2d/AMapUtils.java
http://xmllpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/fq.java
http://xmllpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gs.java
http://www.jivesoftware.com/xmlns/xmpp/properties	com/xiaomi/push/gl.java
http://%1\$s/gslb/?ver=4.0	com/xiaomi/push/db.java
http://new.api.ad.xiaomi.com/logNotificationAdActions	com/xiaomi/push/cs.java
http://xmllpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gt.java
http://xmllpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/ga.java
http://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bc.java

https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/l.java
https://register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://fr.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://ru.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
https://idmb.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/l.java
www.baidu.com:80	com/xiaomi/push/service/ae.java
https://api.xmpush.xiaomi.com/upload/xmsf_log?file=	com/xiaomi/mipush/sdk/u.java
https://api.xmpush.xiaomi.com/upload/app_log?file=	com/xiaomi/mipush/sdk/u.java
https://api.xmpush.xiaomi.com/upload/crash_log?file=	com/xiaomi/mipush/sdk/w.java
https://aws1388we.s3.ap-east-1.amazonaws.com/czEzODg%3D	Android String Resource
https://aws1388we.oss-cn-hongkong.aliyuncs.com/czEzODg%3D	Android String Resource
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://store.hispac.hicloud.com/hwmarket/api/	Android String Resource
https://statistic.live.126.net	lib/armeabi-v7a/libhigh-available.so
https://lbs.netease.im/lbs/conf.jsp	lib/armeabi-v7a/libhigh-available.so
https://lbs.chatnos.com/lbs/conf.jsp	lib/armeabi-v7a/libhigh-available.so
https://yunxin.163.com/lbs/conf.jsp	lib/armeabi-v7a/libhigh-available.so
http://45.127.128.24	lib/armeabi-v7a/libhigh-available.so
http://45.127.128.25	lib/armeabi-v7a/libhigh-available.so
http://nos.netease.com	lib/armeabi-v7a/libhigh-available.so
http://s3.amazonaws.com/doc/2006-03-01/	lib/armeabi-v7a/libhigh-available.so
http://www.w3.org/2001/XMLSchema-instance	lib/armeabi-v7a/libhigh-available.so

http://169.254.170.2	lib/armeabi-v7a/libhigh-available.so
http://169.254.169.254	lib/armeabi-v7a/libhigh-available.so
https://statistic.live.126.net	lib/x86_64/libhigh-available.so
https://lbs.netease.im/lbs/conf.jsp	lib/x86_64/libhigh-available.so
https://lbs.chatnos.com/lbs/conf.jsp	lib/x86_64/libhigh-available.so
https://yunxin.163.com/lbs/conf.jsp	lib/x86_64/libhigh-available.so
http://45.127.128.24	lib/x86_64/libhigh-available.so
http://45.127.128.25	lib/x86_64/libhigh-available.so
http://nos.netease.com	lib/x86_64/libhigh-available.so
http://s3.amazonaws.com/doc/2006-03-01/	lib/x86_64/libhigh-available.so
http://www.w3.org/2001/XMLSchema-instance	lib/x86_64/libhigh-available.so
http://169.254.170.2	lib/x86_64/libhigh-available.so
http://169.254.169.254	lib/x86_64/libhigh-available.so
https://statistic.live.126.net	lib/x86/libhigh-available.so
https://lbs.netease.im/lbs/conf.jsp	lib/x86/libhigh-available.so
https://lbs.chatnos.com/lbs/conf.jsp	lib/x86/libhigh-available.so
https://yunxin.163.com/lbs/conf.jsp	lib/x86/libhigh-available.so
http://45.127.128.24	lib/x86/libhigh-available.so
http://45.127.128.25	lib/x86/libhigh-available.so
http://nos.netease.com	lib/x86/libhigh-available.so
http://s3.amazonaws.com/doc/2006-03-01/	lib/x86/libhigh-available.so
http://www.w3.org/2001/XMLSchema-instance	lib/x86/libhigh-available.so
http://169.254.170.2	lib/x86/libhigh-available.so

http://169.254.169.254	lib/x86/libhigh-available.so
https://statistic.live.126.net	lib/arm64-v8a/libhigh-available.so
https://lbs.netease.im/lbs/conf.jsp	lib/arm64-v8a/libhigh-available.so
https://lbs.chatnos.com/lbs/conf.jsp	lib/arm64-v8a/libhigh-available.so
https://yunxin.163.com/lbs/conf.jsp	lib/arm64-v8a/libhigh-available.so
http://45.127.128.24	lib/arm64-v8a/libhigh-available.so
http://45.127.128.25	lib/arm64-v8a/libhigh-available.so
http://nos.netease.com	lib/arm64-v8a/libhigh-available.so
http://s3.amazonaws.com/doc/2006-03-01/	lib/arm64-v8a/libhigh-available.so
http://www.w3.org/2001/XMLSchema-instance	lib/arm64-v8a/libhigh-available.so
http://169.254.170.2	lib/arm64-v8a/libhigh-available.so
http://169.254.169.254	lib/arm64-v8a/libhigh-available.so

 邮箱线索

邮箱地址	所在文件
ftp@example.com	lib/armeabi-v7a/libhigh-available.so
ftp@example.com	lib/x86_64/libhigh-available.so
ftp@example.com	lib/x86/libhigh-available.so
ftp@example.com	lib/arm64-v8a/libhigh-available.so

 手机线索

 签名证书

无法读取代码签名证书.

🔑 硬编码敏感信息

可能的敏感信息
"cloud_session_list" : "云端会话列表"
"input_password" : "请输入密码，6~20位字母或者数字"
"main_tab_session" : "会话"
"meizuKey" : "111111111111111111111111111111111111"
"no_more_session" : "没有更多会话了"
"private_config_note" : " 1.私有化配置的将在app重启后生效，请注销登陆并杀掉进程。 2.如果要切换到环境，关闭或打开开关退出登陆杀掉进程即可。 "
"setting_private_config" : "私有化配置"
"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"
"view_cloud_session" : "查看云端会话"
"xiaomiKey" : "5392017527970"

🔗 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

 应用内通信