MoGua

多多应急 4.1.2.APK 分析报告

APP名称: 多多应急

包名:	com.android.lixiangjinronh
域名线索:	43条
URL线索:	33条
邮箱线索:	2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: com.android.lixiangjinronh.apk
文件大小: 19.1MB
MD5值: 42e0a3f8b9edb34f768336cd2fe191bd
SHA1值: 967dd843058f8b07b5b1f2b973b0b2569f9e1b3b
SHA256值: 01ae37b46a9cee5907f122157eb7a3a2efa34ad42356fa117c095aed030546dc

APP 信息

App名称: 多多应急
包名: com.android.lixiangjinronh
主活动Activity: com.duoduoyingjidf.ui.activitys.JDXF0ACT
安卓版本名称: 4.1.2
安卓版本: 52

域名线索

域名	服务器信息
i.open.t.sina.com.cn	**IP**: 10.7.129.112 **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**: 108.160.163.117 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
c.y.qq.com	**IP**: 116.128.171.220 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
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
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
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
www.youtube.com	**IP**: 199.16.158.182 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
y.gtimg.cn	**IP**: 59.83.212.234 **所属国家**: China **地区**: Jiangsu **城市**: Wuxi **纬度**: 31.569349 **经度**: 120.288788
music.163.com	**IP**: 220.197.30.65 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
api.xiami.com	没有服务器地理信息.
	IP: 60.28.172.238 **所属国家**: China

cfg.imtt.qq.com	**地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
h.xiami.com	没有服务器地理信息.
pms.mb.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
www.beizhuabao.com	没有服务器地理信息.
service.weibo.com	**IP**: 123.125.107.14 **所属国家**: China **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
y.qq.com	**IP**: 58.144.243.128 **所属国家**: China **地区**: Chongqing **城市**: Chongqing **纬度**: 29.562780 **经度**: 106.553101
	IP: 59.82.44.22 **所属国家**: China

pop.yuncloudauth.com	**地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
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
tianshu.alicdn.com	**IP**: 122.156.129.119 **所属国家**: China **地区**: Heilongjiang **城市**: Heihe **纬度**: 50.266670 **经度**: 127.466667
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**: 124.95.224.248 **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.
cloudauth-dualstack.cn-beijing.aliyuncs.com	**IP**: 39.97.154.8 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou

	纬度: 30.293650 **经度**: 120.161583
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
mxncvjkhkaherwq.oss-accelerate.aliyuncs.com	IP: 39.107.134.21 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
android-donwload.oss-cn-hangzhou.aliyuncs.com	IP: 101.67.62.58 **所属国家**: China **地区**: Zhejiang **城市**: Huzhou **纬度**: 30.870550 **经度**: 120.093300
accounts.google.com	IP: 173.194.203.84 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
cloudauth.aliyuncs.com	IP: 59.82.44.22 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
	IP: 203.119.145.40 **所属国家**: China

acs.m.xiami.com	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
u.y.qq.com	**IP**: 220.194.111.241 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
mgw.mpaas.cn-hangzhou.aliyuncs.com	**IP**: 47.118.168.189 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
auth.yunverify.com	**IP**: 59.82.44.22 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
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

ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com	**IP**: 36.248.13.185 **所属国家**: China **地区**: Fujian **城市**: Fuzhou **纬度**: 26.061390 **经度**: 119.306107
feross.org	**IP**: 50.116.11.184 **所属国家**: United States of America **地区**: California **城市**: Fremont **纬度**: 37.548271 **经度**: -121.988571
cloudauth.cn-beijing.aliyuncs.com	**IP**: 39.97.154.134 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
www.xiami.com	**IP**: 59.82.31.244 **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

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
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://nice800.com	com/duoduoyingjidf/ui/activitys/MT7ACT.java
https://nice800.com/	com/duoduoyingjidf/ui/activitys/MT10ACT.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://android-donwload.oss-cn-hangzhou.aliyuncs.com/domai0dsfnName/5100sdfh0635.text/	d/i/b/d/a/d.java
https://mxncvjkhkaherwq.oss-accelerate.aliyuncs.com	d/i/b/d/a/e.java
https://ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com	d/i/b/d/a/e.java
https://jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com	d/i/b/d/a/e.java
http://www.beizhuabao.com	d/i/b/d/a/a.java
http://www.beizhuabao.com	d/i/b/d/a/b.java
https://plus.google.com/	d/l/a/c/c/k/s1.java
https://accounts.google.com/o/oauth2/revoke?token=	d/l/a/c/a/a/e/c/f.java
http://schemas.android.com/apk/res-auto	d/l/a/d/v/a.java
http://www.youtube.com/watch?v=	d/o/a/i/b/a.java
https://www.youtube.com	d/o/a/i/a/d/a.java
https://www.youtube.com	d/o/a/i/a/f/a.java
https://service.weibo.com/share/mobilesdk.php	d/r/a/a/i/c/d.java
https://service.weibo.com/share/mobilesdk_uppic.php	d/r/a/a/a/d.java
http://i.open.t.sina.com.cn/mobilesdk/sendmessage.php	d/r/a/a/a/c.java
https://android.bugly.qq.com/rqd/async	d/s/a/d/a/b/a.java
http://pms.mb.qq.com/rsp204	d/s/b/b/w.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	d/s/b/b/p/e.java

http://log.tbs.qq.com/ajax?c=pu&v=2&k=	d/s/b/c/w.java
http://log.tbs.qq.com/ajax?c=pu&tk=	d/s/b/c/w.java
http://log.tbs.qq.com/ajax?c=dl&k=	d/s/b/c/w.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	d/s/b/c/w.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	d/s/b/c/w.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	d/s/b/c/m.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html	摸瓜V1引擎
http://feross.org>	摸瓜V2引擎
https://github.com/crypto-browserify/crypto-browserify	摸瓜V2引擎
https://music.163.com/	摸瓜V2引擎
http://music.163.com/discover	摸瓜V2引擎
http://music.163.com	摸瓜V2引擎
https://y.gtimg.cn/music/photo_new/T002R300x300M000	摸瓜V2引擎
https://y.qq.com/n/yqq/song/	摸瓜V2引擎
http://y.gtimg.cn/music/photo_new/T001R300x300M000	摸瓜V2引擎

https://c.y.qq.com/v8/fcg-bin/fcg_v8_album_info_cp.fcg	摸瓜V2引擎
https://github.com/indutny/elliptic/issues	摸瓜V2引擎
https://github.com/indutny/elliptic	摸瓜V2引擎
https://www.xiami.com/song/	摸瓜V2引擎
https://c.y.qq.com	摸瓜V2引擎
https://y.qq.com/portal/player.html	摸瓜V2引擎
https://u.y.qq.com	摸瓜V2引擎
http://acs.m.xiami.com/h5	摸瓜V2引擎
http://api.xiami.com	摸瓜V2引擎
http://h.xiami.com/	摸瓜V2引擎
https://music.163.com	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	d/l/a/c/c/v.java
feross@feross.org git@github.com fedor@indutny.com	摸瓜V2引擎

手机线索

手机号	所在文件
19919152923	摸瓜V2引擎

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=hslvkdkztkapk, ST=uppjmpsmthlsi, L=euaxvjukeaamv, O=ckt1747561005683, OU=dpp1747561005683, CN=TG@apken888
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-18 09:36:45+00:00
有效期至: 2075-05-06 09:36:45+00:00
发行人: C=hslvkdkztkapk, ST=uppjmpsmthlsi, L=euaxvjukeaamv, O=ckt1747561005683, OU=dpp1747561005683, CN=TG@apken888
序列号: 0xa1ab221
哈希算法: sha1
md5值: a24a5d7dd6a9b1bf9a6c7c153e6b09b0
sha1值: 17d19c27b96358cdfe8c6bcca4877f1f10550494
sha256值: 71ab5171de9889a058652818d71c8907785b55297474239198daee40a6f5d15d
sha512值: 2be7f8dd57fca06546321e60ca211a732f6003450937951bc2a00eea2c6022decfc163df2e7cb75f62d82e99c62a0295ce87ba0ba3e99f565fe1d09528f4366b
公钥算法: rsa
密钥长度: 1024
指纹: 5a540b8a7b56e9f82e86db3a4aed49fe309aee1b164982c9e92ff9b47f7b8148

硬编码敏感信息

可能的敏感信息
[illegible]

"agreee_user" : "请先同意并勾选用户协议"

"check_gesture_pwd" : "验证手势密码"

"check_login_pwd" : "验证登录密码"

"dear_user" : "尊敬的用户:"

"find_pwd" : "找回密码"

"gesture_pwd" : "手势密码"

"has_authd" : "已授权"

"info_auth_fee" : "信息认证费： "

"info_auth_fee2" : "信息认证费"

"input_orgin_pwd" : "请输入原密码"

"input_pwd" : "请输入验证码"

"input_pwd_number" : "请输入新密码(6-16位数字字母组合)"

"modify_pwd" : "修改密码"

"ple_agree_auth_agreement" : "请先同意授权及借款协议"

"ple_input_service_pwd" : "请输入服务密码"

"real_auth" : "实名认证"

"reset_service_pwd" : "重置服务密码"

"service_pwd" : "服务密码:"

"to_authorize" : "去授权"
"user" : "用户"

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	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。

		求安装包。	
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