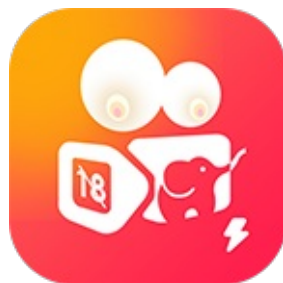




MoGua

快色极速版 1.0.6.APK 分析报告



APP名称:

快色极速版

包名: com.fs.s81db8c6c2ad946aaa41ce35396d69f44

域名线索: 39条

URL线索: 45条

邮箱线索: 2条

分析日期: 2025年9月3日

分析平台: [摸瓜APK反编译平台](#)

文件名: kuaise.apk
文件大小: 18.48MB
MD5值: 20483a464b9d02817dbcf256a10223ba
SHA1值: d73e5eff88b5b6f9a807f86fef55d9005a7dc9aa
SHA256值: dd8ae2a1170a5e7197fb65e0fb5539c495d9b90279f45ec7a84e3def9243ec39

i APP 信息

App名称: 快色极速版
包名: com.fs.s81db8c6c2ad946aaa41ce35396d69f44
主活动Activity: com.limit.cache.ui.page.main.WelComeActivity
安卓版本名称: 1.0.6
安卓版本: 7

🔍 域名线索

域名	服务器信息
momo3.live	IP: 18.166.29.73 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
ck533.com	没有服务器地理信息.
alogus.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

hd66.app	IP: 18.166.29.73 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
schemas.android.com	没有服务器地理信息.
developer.apple.com	IP: 17.253.87.205 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
huapuya.com	IP: 47.246.20.171 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.783058 经度: -96.806671
pslog.umeng.com	IP: 59.82.29.248 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
xiaou.co	IP: 18.166.29.73 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
	IP: 203.119.169.9 所属国家: China

ucc.umeng.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ulogs.umeng.com	IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
errlog.umeng.com	IP: 223.109.148.143 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
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
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
momo7.live	IP: 18.166.29.73 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

ns.adobe.com	没有服务器地理信息.
www.obao22.com	IP: 34.102.136.180 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
github.com	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
aaaid.umeng.com	IP: 218.91.197.68 所属国家: China 地区: Jiangsu 城市: Nantong 纬度: 32.030281 经度: 120.874718
jsd91.com	IP: 154.197.15.21 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
plbslog.umeng.com	IP: 36.156.202.68 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
	IP: 157.185.188.1 所属国家: United States of America

px-intl.ucweb.com	地区: California 城市: Monrovia 纬度: 34.142773 经度: -117.999565
xmlpull.org	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
ouplog.umeng.com	IP: 47.246.110.94 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
aria.laoyuyu.me	IP: 118.24.25.24 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
alogsus.umeng.com	IP: 223.109.148.177 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
developer.umeng.com	IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

px.ucweb.com	IP: 106.8.139.15 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810001 经度: 114.879440
91db.net	没有服务器地理信息.
www.openssl.org	IP: 104.71.138.221 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
errlogos.umeng.com	IP: 47.246.110.18 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
aomedia.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
mpush-api.aliyun.com	IP: 106.11.172.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
	IP: 40.70.71.156 所属国家: United States of America 地区: Virginia

playready.directtaps.net	城市: Boynton 纬度: 36.667641 经度: -78.387497
schemas.microsoft.com	IP: 13.107.237.49 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
exoplayer.dev	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
ulogs.umengcloud.com	IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
momoav.co	IP: 18.166.29.73 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
longfengshan.net	IP: 58.218.208.84 所属国家: China 地区: Jiangsu 城市: Xuzhou 纬度: 34.266666 经度: 117.166664

URL线索

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	d/a/g.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	d/a/p/e.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	d/a/p/c.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	c/h/a/a/w1.java
http://ns.adobe.com/xap/1.0/	c/h/a/a/i2/h0/a.java
http://www.w3.org/ns/ttml	c/h/a/a/n2/t/b.java
https://aomedia.org/emsg/ID3	c/h/a/a/k2/j/a.java
https://developer.apple.com/streaming/emsg-id3	c/h/a/a/k2/j/a.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	c/h/a/a/g2/g0.java
<a href="https://x</LA_URL>">https://x</LA_URL>	c/h/a/a/g2/f0.java
https://x	c/h/a/a/g2/f0.java
https://github.com/danikula/AndroidVideoCache/issues/43	c/f/a/i.java
https://github.com/danikula/AndroidVideoCache/issues	c/f/a/i.java
https://github.com/danikula/AndroidVideoCache/issues/88	c/f/a/i.java

http://%s:%d/%s	c/f/a/g.java
http://%s:%d/%s	c/f/a/l.java
https://github.com/danikula/AndroidVideoCache/issues/134.	c/f/a/l.java
https://mpush-api.aliyun.com/v2.0/a/audid/req/	c/m/a/e/h.java
http://xmlpull.org/v1/doc/features.html	c/m/b/b/a/e.java
http://xmlpull.org/v1/doc/features.html	c/m/b/b/a/a.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/n.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.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
http://schemas.android.com/apk/res/android	com/alimuzaffar/lib/pin/PinEntryEditText.java
https://errlogos.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java
https://px-intl.ucweb.com	com/uc/crashsdk/a/h.java
https://px.ucweb.com	com/uc/crashsdk/a/h.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java

https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/f/c.java
https://momoav.co	com/limit/cache/e.java
https://xiaou.co	com/limit/cache/e.java
https://momo3.live	com/limit/cache/e.java
https://91db.net	com/limit/cache/e.java
https://jsd91.com	com/limit/cache/e.java
https://hd66.app	com/limit/cache/e.java
https://momo7.live	com/limit/cache/e.java
https://ck533.com	com/limit/cache/e.java
https://huapuya.com/text/momo4.txt	com/limit/cache/d.java
https://longfengshan.net/text/momo4.txt	com/limit/cache/d.java
https://www.obao22.com/?i_code=	com/limit/cache/ui/fragment/web/AppWebFragment.java
https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java

https://github.com/AriaLyy/Aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://pslog.umeng.com/ablog	com/umeng/cconfig/UMRemoteConfig.java
https://ucc.umeng.com/v1/fetch	com/umeng/cconfig/UMRemoteConfig.java

https://ucc.umeng.com/v1/fetch	com/umeng/cconfig/c/b.java
https://pslog.umeng.com/ablog	com/umeng/cconfig/c/b.java
http://ns.adobe.com/xap/1.0/\u0000	b/k/a/a.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi/libcrashsdk.so
http://www.openssl.org/support/faq.html	lib/armeabi/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	c/f/a/i.java
ffmpeg-devel@ffmpeg.org	lib/armeabi/libijkplayer.so

手机线索

手机号	所在文件
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=99, ST=99, L=99, O=99, OU=99, CN=99
签名算法: rsassa_pkcs1v15
有效期自: 2022-07-13 09:23:07+00:00
有效期至: 2121-06-19 09:23:07+00:00
发行人: C=99, ST=99, L=99, O=99, OU=99, CN=99
序列号: 0xe34c094
哈希算法: sha256
md5值: 0625b949021649dc6c2843ecc03d448f
sha1值: 6cd00ab59e013b9aa19119f5315fbb0c32c67009
sha256值: 52437dd92708632f62a189f33a0644e0acbad52cbda49dbe1cbfbf94b58eccc4
sha512值: eb381afaddf196928a321b93b3233d5f33cb8f7c1f1fff4dece0aa111fc108d268ad71b4eaa670a01b41ffed03c2ca631a8ba850ffe5614b55e91c10d0357fa4
公钥算法: rsa
密钥长度: 2048
指纹: 551098f86697fd46abf6c6b1a8597076546b392d47098628f2704f6329a89dc7

🔑 硬编码敏感信息

可能的敏感信息
"digits_username" : "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
"modify_pwd" : "修改密码"

"pwd_inconsistent" : "密码不一致"
"pwd_not_rule" : "密码不符合规则"

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
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.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.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.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文 件系统	允许应用程序为可移动存储安装和卸载文件系统
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.CALL_PHONE	危险	直接拨打电话 号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序	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。

		请求安装包。	
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信

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