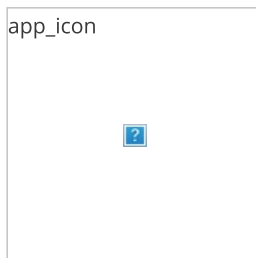




MoGua

共建大湾区 9.3.2.APK 分析报告



APP名称:

共建大湾区

包名:

com.krdlzyae.wqishv

域名线索:	21条
URL线索:	14条
邮箱线索:	1条
分析日期:	2025年10月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app_1121_7.apk

文件大小: 42.16MB

MD5值: be9a6c19f999ce77cc47b5bfdd0165ad

SHA1值: 331384147e4f2b37cacd1f356ac6e79dfca21ee1

SHA256值: fe4562d081be69651b98f791d5e415453b611c329aad7d5d28a1a1935ddf8a9c

i APP 信息

App名称: 共建大湾区
包名: com.krdlzyae.wqishv
主活动Activity: com.krqunelas.reqn.MainActivity
安卓版本名称: 9.3.2
安卓版本: 10

🔍 域名线索

域名	服务器信息
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
ns.adobe.com	没有服务器地理信息.
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
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
aomedia.org	IP: 108.160.162.115 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
.random.gjdwqjxc.buzz	没有服务器地理信息.
www.ibm.com	IP: 23.47.129.93 所属国家: Japan 地区: Osaka 城市: Osaka 纬度: 34.694218 经度: 135.502228
54.46.26.184	IP: 54.46.26.184 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
developer.apple.com	IP: 17.253.87.198 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.jsdelivr.com	IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 23.226.184.15 所属国家: United States of America

www.gjygapp.mom	地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
exoplayer.dev	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
developer.android.com	IP: 142.250.73.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ygaoss.s3.ap-east-1.amazonaws.com	IP: 3.5.239.196 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
ccatcck-1242573427.ap-east-1.elb.amazonaws.com	IP: 43.198.26.16 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
dwqapfdgjc.btjrqq.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 104.18.22.19 所属国家: United States of America 地区: California

www.w3.org	城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
gjdwtz0s-1367028863.cos.accelerate.myqcloud.com	IP: 111.202.29.113 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.example.com	IP: 2.17.107.168 所属国家: Belgium 地区: Brussels Hoofdstedelijk Gewest 城市: Brussels 纬度: 50.850849 经度: 4.348780

 URL线索

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/\u0000	c/i/a/a.java
http://www.example.com	com/pichililorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	d/c/a/a/d2.java
https://exoplayer.dev/issues/cleartext-not-permitted	d/c/a/a/a4/a0.java

https://x</LA_URL>	d/c/a/a/s3/f0.java
https://x	d/c/a/a/s3/f0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	d/c/a/a/s3/g0.java
http://ns.adobe.com/xap/1.0/	d/c/a/a/t3/f0/a.java
https://aomedia.org/emsg/ID3	d/c/a/a/v3/i/a.java
https://developer.apple.com/streaming/emsg-id3	d/c/a/a/v3/i/a.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/g.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/d/s.java
https://github.com/richttr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	摸瓜V2引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so
http://54.46.26.184:8011	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
http://dwqapfdgjc.btjrqq.cn	lib/armeabi-v7a/libapp.so
https://gjdwtzoz-1367028863.cos.accelerate.myqcloud.com/ygadwqnmbjutiousdgljhasfg654sdg54asf51213.json	lib/armeabi-v7a/libapp.so
http://ccatcck-1242573427.ap-east-1.elb.amazonaws.com	lib/armeabi-v7a/libapp.so

_growablelist@0150898._literal4 bb_growablelist@0150898._ofgrowabl x_growablelist@0150898.of storationinformation@973124995.fromserial k_colorfilter@16065589.lineartosr _cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring _list@0150898.of _list@0150898.generate n_typeerror@0150898._create _list@0150898._ofgrowabl a_routedata@1239504625.ofroute _list@0150898._ofefficie _growablelist@0150898._ofarray _growablelist@0150898._literal3 u_growablelist@0150898._ofother _timer@1026248._internal _growablelist@0150898._literal5 _list@0150898._ofother eo_bytebuffer@7027147._new ngstreamsubscription@4048458.zoned _assertionerror@0150898._create av_nativesocket@14069316.normal _uri@0150898.directory qd_growablelist@0150898._literal8 v_file@14069316.fromrawpat gh_growablelist@0150898.generate _uri@0150898.notsimple 7u_growablelist@0150898._literal7 _future@4048458.zonevalue __growablelist@0150898._ofefficie _future@4048458.immediatee	lib/armeabi-v7a/libapp.so
---	---------------------------

手机线索

手机号	所在文件
17512775099	d/c/b/c/a.java

🌟 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

🔑 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

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.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_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_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.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.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.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_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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
	未知		

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
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
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.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。
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

应用内通信