MoGua

联掌门户 4.10.10.APK 分析报告

APP名称:	联掌门户

包名:	com.fxicrazy.sjml
域名线索:	26条
URL线索:	10条
邮箱线索:	1条
分析日期:	2025年7月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 第三方浏览器下载包.apk
文件大小: 59.82MB
MD5值: 4ba79c1c2479e32c5fe2c01b05866c87
SHA1值: e105ad17c5b83c25b7d68fb5f808aba22327615f
SHA256值: 0fec88a93dd19e37b71e6fb469a7a0117622dbeaa9e2b8f3171abbb4c868ea01

APP 信息

App名称: 联掌门户
包名: com.fxicrazy.sjml
主活动Activity: com.fxicrazy.sjml.ui.welcome.WelcomeActivity
安卓版本名称: 4.10.10
安卓版本: 202506191

域名线索

域名	服务器信息
www.jsdelivr.com	**IP**: 104.21.23.24 **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**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
data-drcn.push.dbankcloud.com	**IP**: 49.4.40.58 **所属国家**: China **地区**: Guangdong

	城市: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics5.data.hicloud.com	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
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
grs.dbankcloud.asia	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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
grs.platform.dbankcloud.ru	没有服务器地理信息.
metrics2.data.hicloud.com	**IP**: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358

	经度: 10.134532
lzmh.co	**IP**: 180.76.132.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
data-dra.push.dbankcloud.com	**IP**: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
www.videolan.org	**IP**: 213.36.253.2 **所属国家**: France **地区**: Ile-de-France **城市**: Paris **纬度**: 48.859077 **经度**: 2.293486
grs.dbankcloud.eu	没有服务器地理信息.
metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
www.mob.com	**IP**: 180.188.26.28 **所属国家**: China **地区**: Zhejiang **城市**: Taizhou **纬度**: 28.666668 **经度**: 121.349998

grs.dbankcloud.com	**IP**: 60.28.200.159 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
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
metrics1-drcn.dt.dbankcloud.cn	**IP**: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
yuudnn.lz-qs.com	**IP**: 106.75.11.96 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
sf3-fe-tos.pglstatp-toutiao.com	**IP**: 60.9.0.235 **所属国家**: China **地区**: Hebei **城市**: Hengshui **纬度**: 37.732220 **经度**: 115.701157
data-drru.push.dbankcloud.com	**IP**: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498

	经度: 60.612499
metrics-dra.dt.hicloud.com	**IP**: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
grs.dbankcloud.cn	**IP**: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
lzmh.lz-qs.com	**IP**: 106.75.24.108 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
journeyapps.com	**IP**: 13.35.37.111 **所属国家**: Taiwan (Province of China) **地区**: Taipei **城市**: Taipei **纬度**: 25.038172 **经度**: 121.563599

URL线索

URL信息	Url所在文件
https://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎
http://www.mob.com	摸瓜V1引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1-drcn.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎

https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	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://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/shake.webp	摸瓜V2引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/shake_text.png	摸瓜V2引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/swipe_right.webp	摸瓜V2引擎
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
http://lzmh.co/resource/PrivacyProtocol/lznewapp-agreement.html	lib/armeabi-v7a/libapp.so
http://lzmh.co/resource/Personal/Information-authorization.html	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://yuudnn.lz-qs.com:9002/api-auth	lib/armeabi-v7a/libapp.so
https://lzmh.lz-qs.com:6025/lzmh_app_api	lib/armeabi-v7a/libapp.so
http://lzmh.co/resource/UserAgreement/lznewapp-agreement.html	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new.	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so

http://www.videolan.org/x264.html	lib/armeabi-v7a/librtcsdk.so

邮箱线索

邮箱地址	所在文件
_httpparser@13463476.responsepa ._future@4048458.immediate _growablelist@0150898._literal _link@14069316.fromrawpat c_growablelist@0150898.withcapaci storationinformation@692124995.fromserial _receiveportimpl@1026248.fromrawrec m_growablelist@0150898._literal2 g_bigintimpl@0150898.from _list@0150898.empty _directory@14069316.fromrawpat r_growablelist@0150898.empty _colorfilter@16065589.srgbtoline q_imagefilter@16065589.blur _growablelist@0150898._literal4 x_growablelist@0150898.of 3_list@0150898._ofimmutab k_colorfilter@16065589.lineartosr _list@0150898.of _list@0150898.generate n_typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie _list@0150898._ofother eo_bytebuffer@7027147._new av_nativesocket@14069316.normal qd_growablelist@0150898._literal8 _double@0150898.fromintege _growablelist@0150898._literal6 z_timer@1026248.periodic _casterror@0150898._create	lib/armeabi-v7a/libapp.so

l_invocationmirror@0150898._withtype _colorfilter@16065589.mode lectiontoolbarbutton@286392285.text _growablelist@0150898._literal1 4_uri@0150898.file bb_growablelist@0150898._ofgrowabl lectiontoolbarbutton@405113492.text v_utf8encoder@9003594.withbuffer _growablelist@0150898._ofimmutab _cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring _growablelist@0150898._withdata _growablelist@0150898._literal3 u_growablelist@0150898._ofother _list@0150898._oflist _timer@1026248._internal _growablelist@0150898._literal5 ngstreamsubscription@4048458.zoned _assertionerror@0150898._create _uri@0150898.directory v_file@14069316.fromrawpat gh_growablelist@0150898.generate _uri@0150898.notsimple 7u_growablelist@0150898._literal7 __growablelist@0150898._ofefficie _future@4048458.immediatee m_growablelist@0150898._oflist	

手机线索

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: CN=tyy
签名算法: rsassa_pkcs1v15
有效期自: 2015-01-17 14:24:35+00:00
有效期至: 2040-01-11 14:24:35+00:00
发行人: CN=tyy
序列号: 0x34da208d
哈希算法: sha256
md5值: 5d3f166461254f4b8c1fd5fb8e05154b
sha1值: 9c41f6cce36e380e74275dd1ca2ce64a03fa94f6
sha256值: ac28df444106437ee791f4ed94845dfc704262f19055a3c5f8436f0df7f9b177
sha512值: 96c9c0905fa8a2ad77707db550a83ee373ff8e622bf161687c46166741592976ae71cc01c8a170e613b2d2ff76ff91e8f44dccfe64c4b59cbb2c27becc20724b
公钥算法: rsa
密钥长度: 2048
指纹: 35063149cca0374b9581ebce981fa502035648c038838999c22be374fddc2531

🔑 硬编码敏感信息

可能的敏感信息
"anythink_myoffer_feedback_violation_of_laws" : "Illegal"
"forgetPassword" : "Forgot your password gestures"
"gestures_pwd_set" : "gestures password set"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"pwd3" : "Two password is not the same"
"security_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"
"ssdk_instapaper_pwd" : "密码"

"ssdk_weibo_oauth_regiseter" : "应用授权"
"forgetPassword" : "忘记手势密码"
"gestures_pwd_set" : "手势密码设置"
"pwd3" : "两次密码不一样"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"anythink_myoffer_feedback_violation_of_laws" : "违规违法"

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_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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_SCAN	未知	Unknown permission	Unknown permission from android reference

android.permission.BLUETOOTH_ADVERTISE	未知	Unknown permission	Unknown permission from android reference
com.android.alarm.permission.SET_ALARM	未知	Unknown permission	Unknown permission from android reference
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.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_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.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.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.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
com.fxicrazy.sjml.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
com.fxicrazy.sjml.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference

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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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
com.fxicrazy.sjml.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.fxicrazy.sjml.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.BATTERY_STATS	合	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用

	法		
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.fxicrazy.sjml.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.BLUETOOTH_PRIVILEGED	系统需要		允许应用程序在没有用户交互的情况下配对蓝牙设备,并允许或禁止电话簿访问或消息访问。这不适用于第三方应用程序

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.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
cn.swiftpass.wxpay.permission.MMOAUTH_CALLBACK	未知	Unknown permission	Unknown permission from android reference
cn.swiftpass.wxpay.permission.MM_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.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.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	正	重新排序正在运行的	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的

	常	应用程序	情况下将自己强加于前
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
com.fxicrazy.sjml.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
android.permission.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
android.permission.GET_PACKAGE_INFO	未知	Unknown permission	Unknown permission from android reference
com.fxicrazy.sjml.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.fxicrazy.sjml.push.OppoDeeplinkActivity	Schemes: https://, http://, command://,
com.fxicrazy.sjml.push.VivoDeeplinkActivity	Schemes: vpushscheme://, Hosts: com.push.vivopush, Paths: /detail,
com.fxicrazy.sjml.push.HonorDeeplinkActivity	Schemes: pushscheme://, Hosts: com.honor.push, Paths: /honordeeplink,
com.fxicrazy.sjml.push.DeeplinkActivity	Schemes: pushscheme://, Hosts: com.huawei.codelabpush, Paths: /deeplink,
com.mob.tools.MobUIShell	Schemes: tencent100371282://,
com.wangmai.insightvision.openadsdk.view.web.WebViewActivity	Schemes: fanti://, Hosts: webview,