



MoGua

递福巴士 3.1.0.APK 分析报告



APP名称:

递福巴士

包名:	fhfbcm.beaccn.feccho
域名线索:	31条
URL线索:	34条
邮箱线索:	3条
分析日期:	2025年7月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: fhfbcm.beaccn.feccho.apk

文件大小: 110.34MB
MD5值: 651b3545c3667598e32b78c11cfedcb6
SHA1值: f4e12d3a981baeb49c5db8e229a02aa62e77544e
SHA256值: b3de78e891930d035b5529f62fc140d6ad074961e06d053d8c43b939a0976810

i APP 信息

App名称: 递福巴士
包名: fhfbcm.beaccn.feccho
主活动Activity: fhfbcm.beaccn.feccho.MainActivity
安卓版本名称: 3.1.0
安卓版本: 2

🔍 域名线索

域名	服务器信息
feedback.cn.ronghub.com	IP: 47.94.128.69 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
stats.cn.ronghub.com	IP: 47.94.172.98 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
api-us.faceplusplus.com	IP: 3.99.14.36 所属国家: Canada 地区: Quebec 城市: Montreal 纬度: 45.508839

	经度: -73.587807
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
www.example.com	IP: 93.184.216.34 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
dev.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
paulbakaus.com	IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
www.webrtc.org	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
	IP: 104.16.45.99 所属国家: United States of America 地区: California

tools.ietf.org	城市: San Francisco 纬度: 37.775700 经度: -122.395203
nav.cn.ronghub.com	IP: 39.106.1.81 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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
nav2-cn.ronghub.com	IP: 139.196.191.67 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
mqqad.html5.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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

s3.amazonaws.com	IP: 52.217.136.160 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
www.ietf.org	IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
data.facegl.com	IP: 47.104.165.23 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
api-cn.faceplusplus.com	IP: 60.205.234.99 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mdc.html5.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
log.tbs.qq.com	IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221

	经度: 123.432877
journeyapps.com	IP: 18.65.168.85 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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
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
developer.android.com	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.gnu.org	IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville 纬度: 42.387600 经度: -71.099503
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
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
cfg.imtt.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
stackoverflow.com	IP: 104.18.32.7 所属国家: United States of America 地区: California 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
tbsrecovery.imtt.qq.com	IP: 60.28.172.122 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102

URL线索

URL信息	Url所在文件
http://data.facegl.com/appapi/face/index	com/meihu/beautylibrary/constant/b.java
https://data.facegl.com/appapi/Sticker/index	com/meihu/beautylibrary/constant/a.java
https://data.facegl.com/appapi/Sticker/high	com/meihu/beautylibrary/constant/a.java
https://data.facegl.com/appapi/mask/index	com/meihu/beautylibrary/constant/a.java
https://data.facegl.com/appapi/mask/high	com/meihu/beautylibrary/constant/a.java
https://data.facegl.com/appapi/gift/index	com/meihu/beautylibrary/constant/a.java
https://api-cn.faceplusplus.com/sdk/v3/auth	com/meihu/beautylibrary/utils/f.java
https://api-us.faceplusplus.com/sdk/v3/auth	com/meihu/beautylibrary/utils/f.java
http://www.example.com	com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java
https://github.com/pichillilorenzo/flutter_inappwebview	com/pichillilorenzo/flutter_inappwebview/in_app_webview/FlutterWebView.java
https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects\n\n\n	com/pichillilorenzo/flutter_inappwebview/in_app_webview/FlutterWebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/l.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java

https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utls/n.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utls/n.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utls/n.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utls/n.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utls/n.java
https://mqqqad.html5.qq.com/adjs	com/tencent/smtt/utls/n.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utls/n.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utls/n.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utls/d.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/videoplayer/VideoPlayerPlugin.java
https://feedback.cn.ronghub.com	io/rong/common/dlog/LogEntity.java
https://feedback.cn.ronghub.com	io/rong/common/rlog/RLogConfig.java
https://stats.cn.ronghub.com/active.json	io/rong/imlib/RongCoreClientImpl.java

http://%/s/active.json	io/rong/imlib/RongCoreClientImpl.java
http://s3.amazonaws.com/doc/2006-03-01/	io/rong/imlib/filetransfer/MinioSliceCompleteRequest.java
http://s3.amazonaws.com/doc/2006-03-01/	io/rong/imlib/filetransfer/StcSliceCompleteRequest.java
http://%/s	io/rong/imlib/httpdns/HttpDnsClient.java
https://nav2-cn.ronghub.com/	io/rong/imlib/navigation/NavigationConstant.java
http://nav2-cn.ronghub.com/	io/rong/imlib/navigation/NavigationConstant.java
https://nav.cn.ronghub.com/	io/rong/imlib/navigation/NavigationConstant.java
http://nav.cn.ronghub.com/	io/rong/imlib/navigation/NavigationConstant.java
https://stats.cn.ronghub.com	io/rong/libcore/BuildConfig.java
http://nav.cn.ronghub.com/navipush.json	io/rong/push/common/PushConst.java
http://%/s/	io/rong/rtlog/upload/RtLogTimingUploadConfig.java
http://%/s/	io/rong/rtlog/upload/RtLogUploadManager.java
http://%/s/	io/rong/rtslog/RtsConfigEnv.java
https://journeyapps.com/	Mogua Engine V1
https://github.com/journeyapps/zxing-android-embedded	Mogua Engine V1
http://paulbakaus.com/tutorials/html5/web-audio-on-ios/	Mogua Engine V2
http://stackoverflow.com/questions/24119684	Mogua Engine V2

http://dev.w3.org/html5/spec-author-view/spec.html	Mogua Engine V2
">https://www.gnu.org/licenses/>.	Mogua Engine V2
">https://www.gnu.org/licenses/>.	Mogua Engine V2
">https://www.gnu.org/licenses/>.	Mogua Engine V2
https://github.com/richtr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	Mogua Engine V2
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so
http://www.w3.org/XML/1998/namespace	lib/arm64-v8a/libflutter.so
http://www.w3.org/2000/xmlns/	lib/arm64-v8a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so
http://www.webrtc.org/experiments/rtp-hdext/generic-frame-descriptor-00	lib/arm64-v8a/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdext/generic-frame-descriptor-01	lib/arm64-v8a/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdext/abs-send-time	lib/arm64-v8a/libRongRTCLib.so
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	lib/arm64-v8a/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdext/transport-wide-cc-02	lib/arm64-v8a/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdext/payout-delay	lib/arm64-v8a/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdext/video-content-type	lib/arm64-v8a/libRongRTCLib.so

http://www.webrtc.org/experiments/rtp-hdext/video-timing	lib/arm64-v8a/libRongRTCLib.so
http://tools.ietf.org/html/draft-ietf-avtext-framemarking-07	lib/arm64-v8a/libRongRTCLib.so
http://www.webrtc.org/experiments/rtp-hdext/color-space	lib/arm64-v8a/libRongRTCLib.so

 邮箱线索

邮箱地址	所在文件
guide_page1@2x.png guide_page2@2x.png guide_page3@2x.png abf_group@3x.png abf_newfriend@3x.png back@3x.png biaoqing@3x.png reate_group_selected@3x.png reate_group_unselect@3x.png enter_background@3x.png enter_closed@3x.png enter_delete@2x.png enter_donot@3x.png enter_look@3x.png group_notice_nothing@2x.png groupback@2x.png ntee_accept_initiate@3x.png icon_home_avatar@3x.png icon_invite_copy@3x.png icon_sign@3x.png icon_video@3x.png im_dialog_keyboard@3x.png im_dialog_voice@3x.png im_add_friends_scan@3x.png im_chat_add_card@3x.png im_chat_add_file@3x.png im_chat_add_picture@3x.png	

im_chat_add_shooting@3x.png
im_chat_add_transfer@3x.png
im_chat_add_voice@3x.png
im_set_addbuddy@2x.png
im_set_banned@2x.png
im_set_banned_un@2x.png
im_set_delete@2x.png
im_set_nodisturb@2x.png
im_set_note@2x.png
im_set_protect@2x.png
im_set_protect_un@2x.png
im_set_record_link@2x.png
im_set_search@2x.png
im_set_slsx@2x.png
im_top_add_friends@3x.png
im_top_add_group@3x.png
im_top_delete@3x.png
im_top_scan_back@3x.png
_top_scan_collection@3x.png
im_top_scan_figure@3x.png
im_top_scan_personal@3x.png
im_top_search@3x.png
resslist_friend_card@3x.png
jia@3x.png
sg_select_forwarding@3x.png
msg_seleect_delete@3x.png
ssets_withdrawal_def@3x.png
ssets_withdrawal_win@3x.png
news_video@3x.png
reply_quote_delete@3x.png
saoyisao@3x.png
sousuo@3x.png
tianjia@3x.png
tianjiadikuang@3x.png
top_more@3x.png
top_return@3x.png
xiugaibeizhu@3x.png
my_assets_access@3x.png
my_background@3x.png
et_alter_user_camera@3x.png
my_set_user_id@3x.png
my_top_set@3x.png
my_user_id@3x.png

Mogua Engine V2

appro@openssl.org	lib/arm64-v8a/libflutter.so
appro@openssl.org	lib/arm64-v8a/libRongRTCLib.so

手机线索

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=cn, ST=aifjcl, L=accefk, O=eefeaj, OU=bcieji, CN=didadh
签名算法: rsassa_pkcs1v15
有效期自: 2023-09-28 03:03:24+00:00
有效期至: 2123-09-04 03:03:24+00:00
发行人: C=cn, ST=aifjcl, L=accefk, O=eefeaj, OU=bcieji, CN=didadh
序列号: 0x163d07f0
哈希算法: sha256
md5值: fee359efdfbcac56a8300e44ff455721
sha1值: e8aa2ec25f5a4efa3e140cfe8311e0feabd82ffd
sha256值: 2d9e216d4324aa1078610ee1fde491e48772d21310b92ed67cbfe79642f7b19f
sha512值: 826c2db556865cd7ca411cbcec8dc075bd1a9ae53157e65bc26859edbbb9880ddee45d4746142147a749a17e02492bfa4e979a7eff90548118a4f8248f3cdda6
公钥算法: rsa
密钥长度: 1024
指纹: aa4d5dd41dbfc0beba0eee32ed24e041a1396e31f1509fea94e0b5a0132a115d

硬编码敏感信息

可能的敏感信息

"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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.USE_FINGERPRINT	正常	allow use of 指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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
Manifest.permission.CAPTURE_AUDIO_OUTPUT	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.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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的

android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.POST_NOTIFICATIONS	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.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
fhfbcm.beaccn.feccho.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
fhfbcm.beaccn.feccho.permission.RONG_ACCESS_RECEIVER	未知	Unknown permission	Unknown permission from android reference
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。

应用内通信