Evaluation Warning: The document was created with Spire.Doc for Python.

**递福巴士（ 3.1.0版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 递福巴士 |
| 版本 | 3.1.0 |
| 包名 | fhfbcm.beaccn.feccho |
| 域名线索 | 31条 |
| URL线索 | 34条 |
| APP图标 |  |
| 分析日期 | 2025年7月5日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | fhfbcm.beaccn.feccho.apk |
| 文件大小 | 110.34MB |
| MD5值 | 651b3545c3667598e32b78c11cfedcb6 |
| SHA1值 | f4e12d3a981baeb49c5db8e229a02aa62e77544e |
| SHA256值 | b3de78e891930d035b5529f62fc140d6ad074961e06d053d8c43b939a0976810 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| stats.cn.ronghub.com | IP: 47.94.172.98 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api-us.faceplusplus.com | IP: 3.99.14.36 所属国家: Canada 地区: Quebec 城市: Montreal  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.example.com | IP: 93.184.216.34 所属国家: United States of America 地区: California 城市: Los Angeles  |
| dev.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| paulbakaus.com | IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| www.webrtc.org | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| tools.ietf.org | IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| nav.cn.ronghub.com | IP: 39.106.1.81 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| nav2-cn.ronghub.com | IP: 139.196.191.67 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| s3.amazonaws.com | IP: 52.217.136.160 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.ietf.org | IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| data.facegl.com | IP: 47.104.165.23 所属国家: China 地区: Shandong 城市: Qingdao  |
| api-cn.faceplusplus.com | IP: 60.205.234.99 所属国家: China 地区: Beijing 城市: Beijing  |
| mdc.html5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |
| journeyapps.com | IP: 18.65.168.85 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| developer.android.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.gnu.org | IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| stackoverflow.com | IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| tbsrecovery.imtt.qq.com | IP: 60.28.172.122 所属国家: China 地区: Tianjin 城市: Tianjin  |

### **4.2 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/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/n.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/n.java  |
| https://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/n.java  |
| https://tbsrecovery.imtt.qq.com/getconfig  | com/tencent/smtt/utils/n.java  |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/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-hdrext/generic-frame-descriptor-00  | lib/arm64-v8a/libRongRTCLib.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-01  | lib/arm64-v8a/libRongRTCLib.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/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-hdrext/transport-wide-cc-02  | lib/arm64-v8a/libRongRTCLib.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay  | lib/arm64-v8a/libRongRTCLib.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type  | lib/arm64-v8a/libRongRTCLib.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/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-hdrext/color-space  | lib/arm64-v8a/libRongRTCLib.so  |

### **4.3 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  |

### **4.4 手机号线索**

## **5. 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**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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。 |

## **10. 应用内通信**

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