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

**武汉农商银行（ 2.1.5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 | 武汉农商银行 |
| 版本 | 2.1.5 |
| 包名 | com.whrcbank.mbank |
| 域名线索 | 54条 |
| URL线索 | 11条 |
| APP图标 |  |
| 分析日期 | 2025年7月18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 | 武汉农商银行\_2.1.5\_Apkpure.apk |
| 文件大小 | 111.41MB |
| MD5值 | 7593c20fce6d6ba7f3e3b5008ccb63ea |
| SHA1值 | e9005bf43753236536bf0b4c6ef9beb5b465bf7c |
| SHA256值 | 6556ceb6b54be9e42edf7590d5e8cf51f8dbd67be85a8524e6e78c9811efe145 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 武汉农商银行 |
| 包名 | com.whrcbank.mbank |
| 主活动Activity | com.yitong.mobile.biz.launcher.app.SplashActivity |
| 安卓版本名称 | 2.1.5 |
| 安卓版本 | 45 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| tc39.es | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| grs.dbankcloud.asia | IP: 119.8.176.236 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mall.whrcbank.com | 没有服务器地理信息.  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| grs.dbankcloud.com | IP: 113.201.107.54 所属国家: China 地区: Shaanxi 城市: Baoji  |
| stackoverflow.com | IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| device.95516.com | IP: 61.156.245.13 所属国家: China 地区: Shandong 城市: Xintai  |
| reactjs.org | IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut  |
| openapi.baidu.com | IP: 110.242.69.36 所属国家: China 地区: Hebei 城市: Baoding  |
| vop.baidu.com | IP: 111.206.209.68 所属国家: China 地区: Beijing 城市: Beijing  |
| vse.baidu.com | IP: 110.242.68.241 所属国家: China 地区: Hebei 城市: Baoding  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| content.95516.com | IP: 115.85.201.37 所属国家: China 地区: Gansu 城市: Baiyin  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.mob.com | IP: 45.113.201.237 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| analytics.95516.com | IP: 101.28.252.14 所属国家: China 地区: Hebei 城市: Handan  |
| 172.18.64.187 | IP: 172.18.64.187 所属国家: - 地区: - 城市: -  |
| open.95516.com | IP: 106.74.11.232 所属国家: China 地区: Shandong 城市: Jinan  |
| people.mozilla.org | IP: 52.10.15.159 所属国家: United States of America 地区: Oregon 城市: Boardman  |
| ebank1.nongxinyin.com | 没有服务器地理信息.  |
| metrics1.data.hicloud.com | IP: 111.202.17.12 所属国家: China 地区: Beijing 城市: Beijing  |
| wallet.95516.com | IP: 115.85.201.36 所属国家: China 地区: Gansu 城市: Baiyin  |
| html.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| weixin.allinfinance.com | IP: 58.246.110.143 所属国家: China 地区: Shanghai 城市: Shanghai  |
| upl.baidu.com | IP: 110.242.68.241 所属国家: China 地区: Hebei 城市: Baoding  |
| 172.21.111.12 | IP: 172.21.111.12 所属国家: - 地区: - 城市: -  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 172.21.101.31 | IP: 172.21.101.31 所属国家: - 地区: - 城市: -  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| 172.17.249.30 | IP: 172.17.249.30 所属国家: - 地区: - 城市: -  |
| fb.me | IP: 157.240.199.35 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| 172.18.179.11 | IP: 172.18.179.11 所属国家: - 地区: - 城市: -  |
| wxtest.allinfinance.com | IP: 140.207.147.252 所属国家: China 地区: Shanghai 城市: Shanghai  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| 172.18.179.10 | IP: 172.18.179.10 所属国家: - 地区: - 城市: -  |
| 120.132.3.51 | IP: 120.132.3.51 所属国家: China 地区: Beijing 城市: Beijing  |
| 172.18.64.34 | IP: 172.18.64.34 所属国家: - 地区: - 城市: -  |
| 172.21.101.19 | IP: 172.21.101.19 所属国家: - 地区: - 城市: -  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| code.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| youhui.95516.com | IP: 115.85.201.37 所属国家: China 地区: Gansu 城市: Baiyin  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mse.baidu.com | IP: 180.101.49.124 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| mp.weixin.qq.com | IP: 140.207.58.67 所属国家: China 地区: Shanghai 城市: Shanghai  |
| facebook.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| bugzilla.mozilla.org | IP: 34.110.178.183 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| bugs.chromium.org | IP: 172.217.160.115 所属国家: United States of America 地区: California 城市: Mountain View  |
| 172.17.254.165 | IP: 172.17.254.165 所属国家: - 地区: - 城市: -  |
| 172.18.64.46 | IP: 172.18.64.46 所属国家: - 地区: - 城市: -  |
| 101.231.204.80 | IP: 101.231.204.80 所属国家: China 地区: Shanghai 城市: Shanghai  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>.  | Mogua Engine V1  |
| http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>  | Mogua Engine V1  |
| http://www.mob.com  | Mogua Engine V1  |
| http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If  | Mogua Engine V1  |
| http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>  | Mogua Engine V1  |
| https://metrics1.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics-dra.dt.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics2.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.dt.dbankcloud.ru:6447  | Mogua Engine V2  |
| https://data-drcn.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dra.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dre.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-drru.push.dbankcloud.com  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/mobile/entrance.do?path=page/ML01/13/01/ML011301.html&webDevMark=NYXLifeService  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/YYW/entrance.do?path=page/ML01/12/01/ML011201.html&webDevMark=NYXLifeService  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/mobile/entrance.do?path=page/ML01/08/01/ML010801.html&webDevMark=NYXLifeService  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/mobile/entrance.do?path=page/ML01/15/01/ML011501.html&webDevMark=NYXLifeService  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/mobile/entrance.do?path=page/ML01/14/01/ML011401.html&webDevMark=NYXLifeService  | Mogua Engine V2  |
| http://wxtest.allinfinance.com/evercos/assets/creditcard/apply/index.html  | Mogua Engine V2  |
| https://github.com/wendux/Ajax-hook\n  | Mogua Engine V2  |
| https://stackoverflow.com/questions/27176983/dispatchevent-not-working-in-ie11\n  | Mogua Engine V2  |
| https://tc39.es/ecma262/  | Mogua Engine V2  |
| https://github.com/tc39/proposal-array-filtering\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/677\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/306\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/86  | Mogua Engine V2  |
| https://github.com/mozilla/rhino/issues/346\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/339\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/898\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/475\n  | Mogua Engine V2  |
| https://github.com/es-shims/es5-shim/issues/150\n//  | Mogua Engine V2  |
| https://github.com/kitcambridge/es5-shim/commit/4f738ac066346\n//  | Mogua Engine V2  |
| https://bugs.chromium.org/p/chromium/issues/detail?id=830565\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/679\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/1008\nvar  | Mogua Engine V2  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=773687\n  | Mogua Engine V2  |
| https://html.spec.whatwg.org/multipage/timers-and-user-prompts.html  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/blob/v3.24.0/LICENSE',\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js'\n  | Mogua Engine V2  |
| https://github.com/mathiasbynens/String.prototype.at\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/624\n  | Mogua Engine V2  |
| https://bugs.chromium.org/p/v8/issues/detail?id=3334\nmodule.exports  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/679\nvar  | Mogua Engine V2  |
| https://bugs.chromium.org/p/chromium/issues/detail?id=1049982\nvar  | Mogua Engine V2  |
| https://github.com/tc39/proposal-well-formed-stringify\nvar  | Mogua Engine V2  |
| https://bugs.chromium.org/p/v8/issues/detail?id=3443\nvar  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/640\n  | Mogua Engine V2  |
| https://github.com/zloirock/core-js/issues/173\nvar  | Mogua Engine V2  |
| https://code.google.com/p/v8/issues/detail?id=687\nvar  | Mogua Engine V2  |
| https://github.com/tc39/proposal-Symbol-description\n  | Mogua Engine V2  |
| https://people.mozilla.org/  | Mogua Engine V2  |
| https://github.com/facebook/regenerator/issues/274  | Mogua Engine V2  |
| http://mall.whrcbank.com/TopMallPreview/mobileGoodsAction!goodsDetail.action?goodsId=0114398A0  | Mogua Engine V2  |
| https://mp.weixin.qq.com/s/kNEPmhas3-b8umu9bi9Qdw  | Mogua Engine V2  |
| https://weixin.allinfinance.com/evercos/assets/creditcard/apply/index.html  | Mogua Engine V2  |
| https://mp.weixin.qq.com/s/DI034m5ntaC0r5PRIKoSSw  | Mogua Engine V2  |
| http://mall.whrcbank.com/TopMallPreview/mobileGoodsAction!goodsDetail.action?goodsId=01643281H  | Mogua Engine V2  |
| https://mp.weixin.qq.com/s/J01tAQYvA-Y-bVm7ulZGYw  | Mogua Engine V2  |
| http://mall.whrcbank.com/TopMall/mmall/goods/01242973G/01242973G.html  | Mogua Engine V2  |
| https://mp.weixin.qq.com/s/99DMJ7T3aZeE27ljyZ9IHg  | Mogua Engine V2  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://grs.platform.dbankcloud.ru  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/YYW/entrance.do?path=page/ML01/12/01/ML011201.html&webDevMark=NYXLifeService&location=true  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/mobile/entrance.do?path=page/ML01/08/01/ML010801.html&webDevMark=NYXLifeService&location=true  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/mobile/entrance.do?path=page/ML01/13/01/ML011301.html&webDevMark=NYXLifeService  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/page/index2.html?path=page/ML01/15/01/ML011501.html&webDevMark=NYXLifeService&location=true  | Mogua Engine V2  |
| http://ebank1.nongxinyin.com/jmlive/nxy/mobile/entrance.do?path=page/ML01/14/01/ML011401.html&webDevMark=NYXLifeService  | Mogua Engine V2  |
| https://reactjs.org/docs/error-decoder.html?invariant=  | Mogua Engine V2  |
| https://fb.me/nolistview  | Mogua Engine V2  |
| https://github.com/react-native-community/react-native-masked-view  | Mogua Engine V2  |
| https://github.com/react-native-community/react-native-slider  | Mogua Engine V2  |
| https://github.com/react-native-community/react-native-viewpager  | Mogua Engine V2  |
| https://github.com/react-native-community/react-native-webview  | Mogua Engine V2  |
| https://github.com/react-native-community/react-native-async-storage  | Mogua Engine V2  |
| https://github.com/react-native-community/react-native-netinfo  | Mogua Engine V2  |
| http://facebook.github.io/react-native/docs/navigation.html  | Mogua Engine V2  |
| http://fb.me/use-check-prop-types  | Mogua Engine V2  |
| https://fb.me/react-refs-must-have-owner  | Mogua Engine V2  |
| https://fb.me/react-invalid-hook-call)  | Mogua Engine V2  |
| https://fb.me/react-polyfills  | Mogua Engine V2  |
| https://github.com/facebook/react-native/issues/11094  | Mogua Engine V2  |
| http://\*','https://\*'],extractOrigin:function(t)  | Mogua Engine V2  |
| https://vse.baidu.com/echo.fcgi  | lib/armeabi-v7a/libBaiduSpeechSDK.so  |
| https://mse.baidu.com/echo.fcgi  | lib/armeabi-v7a/libBaiduSpeechSDK.so  |
| https://vop.baidu.com/echo.fcgi  | lib/armeabi-v7a/libBaiduSpeechSDK.so  |
| https://openapi.baidu.com/oauth/2.0/token  | lib/armeabi-v7a/libBaiduSpeechSDK.so  |
| http://upl.baidu.com/auth.php  | lib/armeabi-v7a/libBaiduSpeechSDK.so  |
| https://wallet.95516.com/wl/entry  | lib/armeabi-v7a/libupsdkencrypt.so  |
| https://101.231.204.80:443/wl/entry  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.18.179.10/wl/entry  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.18.64.187:12000/gateway/entry  | lib/armeabi-v7a/libupsdkencrypt.so  |
| https://youhui.95516.com  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.17.254.165:36000  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.18.179.11  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.18.64.46:36080  | lib/armeabi-v7a/libupsdkencrypt.so  |
| https://youhui.95516.com/wm-non-biz-web/v3  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.17.254.165:36000/wm-non-biz-web/v3  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.18.179.11/wm-non-biz-web/v3  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.18.64.46:36080/wm-non-biz-web/v3  | lib/armeabi-v7a/libupsdkencrypt.so  |
| https://open.95516.com/open/access  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.18.64.34:38080/open/access  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.17.249.30:8185/wl-sdk/access  | lib/armeabi-v7a/libupsdkencrypt.so  |
| https://content.95516.com  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.21.101.19:8088  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://120.132.3.51:8080  | lib/armeabi-v7a/libupsdkencrypt.so  |
| https://analytics.95516.com/sa?project=production  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.21.111.12:7878/sa?project=default  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.21.111.12:7878/sa?project=wallet\_functest  | lib/armeabi-v7a/libupsdkencrypt.so  |
| https://device.95516.com/config/?project=default  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.21.111.12:7878/config/?project=default  | lib/armeabi-v7a/libupsdkencrypt.so  |
| http://172.21.101.31:8080  | lib/armeabi-v7a/libupsdkencrypt.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 824783146@qq.com  | Mogua Engine V2  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 16505513277  | lib/armeabi-v7a/libSipCryptor.so  |

## **5. 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=whnsbank 签名算法: rsassa\_pkcs1v15 有效期自: 2019-02-28 02:23:24+00:00 有效期至: 3017-07-01 02:23:24+00:00 发行人: CN=whnsbank 序列号: 0x69fbcf49 哈希算法: sha256 md5值: 7bdcca1ed0e5cee1960d459aac6104dd sha1值: 21edfdbb729bc85edb2a1557caab45b936bbe4f7 sha256值: 129d37b2561c5204e9a0882edc959c603e9ba657e4a6cef2abf351a672e32855 sha512值: f9a692de8e619050dd5c34528a2f6e08311993eb6506dc18430689b82d650ea8ab1b01259ab235969ffbc8ba1f7abaa32622a61a14ffe88914b0f2c83650d2ff 公钥算法: rsa 密钥长度: 2048 指纹: 3d343b7df7650b7cc724ca4d607b95fe403e89c89870deb311f40a5e04e23259**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "login\_forget\_pwd\_str" : "忘记密码?"  |
| "login\_input\_pwd\_str" : "请输入登录密码"  |
| "login\_pwd\_min\_six" : "请输入4位及以上的密码"  |
| "login\_pwd\_str" : "登录密码"  |
| "mobcommon\_authorize\_dialog\_accept" : "Accept"  |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"  |
| "mobcommon\_authorize\_dialog\_reject" : "Reject"  |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use"  |
| "mobdemo\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobdemo\_authorize\_dialog\_title" : "服务授权"  |
| "ssdk\_cmcc\_auth" : "手机认证服务由中国移动提供"  |
| "ssdk\_cmcc\_login\_one\_key" : "本机号码一键登录"  |
| "ssdk\_instapaper\_pwd" : "密码"  |
| "ssdk\_weibo\_oauth\_regiseter" : "应用授权"  |
| "upsdk\_care\_forget\_password" : "忘记密码按钮"  |
| "mobcommon\_authorize\_dialog\_accept" : "Accept"  |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"  |
| "mobcommon\_authorize\_dialog\_reject" : "Reject"  |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use"  |
| "mobdemo\_authorize\_dialog\_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see details<a href=http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."  |
| "mobdemo\_authorize\_dialog\_title" : "service authority"  |
| "ssdk\_cmcc\_auth" : "Provided by China Mobile"  |
| "ssdk\_cmcc\_login\_one\_key" : "PhoneNum Login"  |
| "ssdk\_instapaper\_pwd" : "Password"  |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization"  |
| "mobcommon\_authorize\_dialog\_accept" : "同意"  |
| "mobcommon\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobcommon\_authorize\_dialog\_reject" : "拒绝"  |
| "mobcommon\_authorize\_dialog\_title" : "服务授权"  |

## **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.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\_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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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\_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.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\_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.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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.MANAGE\_FINGERPRINT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.UPDATE\_DEVICE\_STATS | 系统需要 | 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 |
| android.permission.USE\_FINGERPRINT  | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| com.whrcbank.mbank.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.whrcbank.mbank.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| 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.ACCESS\_GPS | 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.whrcbank.mbank.permission.XGPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.whrcbank.mbank.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.whrcbank.mbank.push.permission.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.whrcbank.mbank.permission.C2D\_MESSAGE | 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.yitong.mobile.biz.launcher.app.SplashActivity | **Schemes**: whrcbankapp://, **Hosts:** jp.app, **Paths:** /skipUrl,  |
| com.mob.tools.MobUIShell | **Schemes**: line.1477692153://,  |
| cn.sharesdk.tencent.qq.ReceiveActivity | **Schemes**: tencent100371282://,  |
| com.tencent.android.tpush.TpnsActivity | **Schemes**: tpns://, **Hosts:** com.whrcbank.mbank,  |
| com.tencent.android.tpush.InnerTpnsActivity | **Schemes**: stpns://, **Hosts:** com.whrcbank.mbank,  |

**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。**