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

**西安银行（ 8.1.2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 | 西安银行 |
| 版本 | 8.1.2 |
| 包名 | com.yitong.xian.mbank |
| 域名线索 | 21条 |
| URL线索 | 5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 | XACBMobileBank.apk |
| 文件大小 | 167.56MB |
| MD5值 | 329089d256799e33c4be6a9d1c1d5a58 |
| SHA1值 | 65945dca6d1632e32f577211d9987a431590791d |
| SHA256值 | ec210ca1cddc0572c141f3cb1be1c486caaebba5ee4f5ccbe3d33aa38c86642d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 西安银行 |
| 包名 | com.yitong.xian.mbank |
| 主活动Activity | com.yitong.mbank.app.android.activity.SplashActivity |
| 安卓版本名称 | 8.1.2 |
| 安卓版本 | 812 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| gcc.gnu.org | IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh  |
| woodpecker.uc.cn | IP: 116.132.223.111 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing  |
| wpk-auth.ucweb.com | IP: 157.185.188.1 所属国家: Canada 地区: Ontario 城市: North York  |
| www.ronganchina.com | IP: 123.57.148.160 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| c.tenor.com | IP: 128.242.240.253 所属国家: United States of America 地区: Washington 城市: Redmond  |
| applog.uc.cn | IP: 116.132.216.103 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| newsstand.googleusercontent.com | IP: 142.251.215.225 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.bangcle.com | IP: 47.93.77.202 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cn.bing.com | IP: 202.89.233.100 所属国家: China 地区: Beijing 城市: Beijing  |
| encrypted-tbn0.gstatic.com | IP: 172.217.14.206 所属国家: United States of America 地区: California 城市: Mountain View  |
| googlehosted.l.googleusercontent.com | IP: 142.251.215.225 所属国家: United States of America 地区: California 城市: Mountain View  |
| gjapplog.ucweb.com | IP: 157.185.189.158 所属国家: Canada 地区: Ontario 城市: North York  |
| store.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| media.tenor.com | IP: 199.59.148.8 所属国家: United States of America 地区: California 城市: San Francisco  |
| lh3-dz.googleusercontent.com | IP: 172.217.14.225 所属国家: United States of America 地区: California 城市: Mountain View  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.baidu.com | IP: 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.xacbank.com | IP: 124.115.228.235 所属国家: China 地区: Shanxi 城市: Taiyuan  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://www.baidu.com  | com/bangcle/everisk/checkers/https/HttpsChecker.java  |
| https://cn.bing.com  | com/bangcle/everisk/checkers/https/HttpsChecker.java  |
| https://www.bangcle.com  | com/bangcle/everisk/util/http/HttpClient.java  |
| http://www.xacbank.com  | 摸瓜V1引擎  |
| https://play.google.com/store  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com/app/  | 摸瓜V1引擎  |
| https://play.google.com/store/apps/details?id=  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com  | 摸瓜V1引擎  |
| https://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V1引擎  |
| https://applog.uc.cn/collecthttps://gjapplog.ucweb.com/collectauthuhttps://woodpecker.uc.cnhttps://w  | 摸瓜V3引擎  |
| https://applog.uc.cn/collect  | 摸瓜V3引擎  |
| https://wpk-auth.ucweb.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://gjapplog.ucweb.com/collect  | 摸瓜V3引擎  |
| https://www.bangcle.com  | 摸瓜V3引擎  |
| social-magazines-prod.storage.googleapis.com  | 摸瓜V3引擎  |
| http://www.xacbank.com  | 摸瓜V3引擎  |
| https://www.ronganchina.com/android/ronganui  | 摸瓜V3引擎  |
| c.tenor.com  | 摸瓜V3引擎  |
| play.googleapis.com  | 摸瓜V3引擎  |
| newsstand.googleusercontent.com  | 摸瓜V3引擎  |
| encrypted-tbn0.gstatic.com  | 摸瓜V3引擎  |
| googlehosted.l.googleusercontent.com  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| https://woodpecker.uc.cn  | 摸瓜V3引擎  |
| https://www.baidu.com  | 摸瓜V3引擎  |
| media.tenor.com  | 摸瓜V3引擎  |
| lh3-dz.googleusercontent.com  | 摸瓜V3引擎  |
| http://gcc.gnu.org/bugs.html):  | 摸瓜V3引擎  |
| https://github.com/opencv/opencv/pull/15050  | lib/arm64-v8a/libhfyuv.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 6i@ci.\_ihh  | 摸瓜V2引擎  |
| 1@aز.pdb٢u  | 摸瓜V2引擎  |
| pg1@cز.pdbآ ӈw@6.fz  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15555215554  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215556  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215558  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215560  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215562  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215564  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215566  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215568  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215570  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215572  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215574  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215576  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215578  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215580  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215582  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |
| 15555215584  | com/bangcle/everisk/checkers/emulator/EmulatorDetector.java  |

## **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: C=中国, ST=陕西省, L=西安市, O=西安银行股份有限公司, OU=西安银行股份有限公司, CN=西安银行股份有限公司 签名算法: rsassa\_pkcs1v15 有效期自: 2015-01-16 12:06:49+00:00 有效期至: 3014-05-19 12:06:49+00:00 发行人: C=中国, ST=陕西省, L=西安市, O=西安银行股份有限公司, OU=西安银行股份有限公司, CN=西安银行股份有限公司 序列号: 0xba58e09 哈希算法: sha256 md5值: 0f31b3bcd0439fa7ae4a9228eb3bdedf sha1值: 7c9bbbff9db6da6718fa11d312c718b5e3b40b30 sha256值: 4d56a44921612f26666ce8654a7f2df3c7ea2e3f29636bf23f1ab15bfd49b662 sha512值: d14576639fe7e9673a1522e5a34491a4fe072c10d36a326a8f58a8a1f92c3e3e14d24711758e84aec11375937b9787c7ba026d7208c609d727a420b403e18071 公钥算法: rsa 密钥长度: 2048 指纹: c83db8aa8e0dcf4290b2a83d6ae97065ab3119d8314efc94733ff955c51d79cc**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "fh\_no\_session\_info" : "未获取到会话信息，请稍后重试！"  |
| "function\_description\_connect\_bluetoothkey" : "连接蓝牙Key"  |
| "gesture\_pwd\_verify\_fatal" : "手势密码验证失败，请重新登录"  |
| "get\_location\_auth\_failed" : "请确认定位相关权限已开启"  |
| "getcontact\_failed\_auth" : "获取授权失败"  |
| "go\_to\_alipay\_auth" : "去支付宝授权"  |
| "h5\_bug\_me\_err\_user" : "非法用户"  |
| "h5\_sessiontab\_notice\_failmsg" : "耽误您的时间，我们深表歉意！"  |
| "h5\_sessiontab\_notice\_failtitle" : "服务暂不可用，请稍后再试"  |
| "h5\_sessiontab\_toast" : "提示: 入口url不在tabbar内，仅RC和测试可见"  |
| "h5\_sessionwarningpart1" : "业务内已有"  |
| "h5\_sessionwarningpart2" : "个页面,谨慎新开页面,否则内存溃坝业务异常! 此弹框只是开发版警告，对业务无影响!"  |
| "iconfont\_add\_user" : ""  |
| "iconfont\_systen\_key" : ""  |
| "iconfont\_user" : ""  |
| "input\_init\_pwd" : "柜面签约用户，请输入柜面签约初始密码。"  |
| "locate\_failed\_auth" : "GPS打开，但用户未授权"  |
| "not\_authed\_exit" : "退出"  |
| "not\_authed\_retry" : "重试"  |
| "password" : "密码"  |
| "private\_service\_tip" : "我是您的%1$s 您可以给我留言，我将第一时间与您联系。"  |
| "pwd" : "登录密码"  |
| "pwd\_input\_dialog\_titile" : "标题"  |
| "setting\_taobao\_auth" : "淘宝账户信息"  |
| "updatapwd\_tip" : "为了您的资金安全，请勿将交易密码设置成与常用软件相同或相似密码，请勿使用生日、手机号、身份证号等作为交易密码"  |
| "use\_fingerprint\_to\_authenticate\_key" : "使用指纹认证key"  |
| "use\_fingerprint\_to\_authenticate\_title" : "使用指纹认证"  |
| "username" : "用户名"  |
| "h5\_sessiontab\_notice\_failmsg" : "We apologize for the delay!"  |
| "h5\_sessiontab\_notice\_failtitle" : "Service is temporarily unavailable, please try again later"  |
| "h5\_sessionwarningpart1" : "contained in business"  |
| "h5\_sessionwarningpart2" : "pages. Please be cautious to open new page, which may cause memory crash and business error. "  |
| "locate\_failed\_auth" : "GPS is on, but authorization of user is requested"  |
| "pwd\_input\_dialog\_titile" : "Title"  |
| "h5\_sessiontab\_notice\_failmsg" : "耽誤您的時間，我們深表歉意！"  |
| "h5\_sessiontab\_notice\_failtitle" : "服務暫不可用，請稍後再試"  |
| "h5\_sessionwarningpart1" : "業務內已有"  |
| "h5\_sessionwarningpart2" : "個頁面,謹慎新開頁面,否則內存潰壩業務異常!"  |
| "locate\_failed\_auth" : "GPS打開，但用戶未授權"  |
| "pwd\_input\_dialog\_titile" : "標題"  |
| "h5\_sessiontab\_notice\_failmsg" : "耽誤您的時間，我們深表歉意！"  |
| "h5\_sessiontab\_notice\_failtitle" : "服務暫不可用，請稍後再試"  |
| "h5\_sessionwarningpart1" : "業務內已有"  |
| "h5\_sessionwarningpart2" : "個頁面,謹慎新開頁面,否則內存潰壩業務異常!"  |
| "locate\_failed\_auth" : "GPS打開，但用戶未授權"  |
| "pwd\_input\_dialog\_titile" : "標題"  |

## **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.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.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.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.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.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.ACCESS\_GPS | 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.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.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.BIND\_NFC\_SERVICE | 合法 |  | HostApduService 或 OffHostApduService 必须要求,以确保只有系统可以绑定到它 |
| 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 |
| 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.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\_ASSISTED\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_LOCATION | 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.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.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.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.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.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 |
| com.yitong.xian.mbank.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_CALENDAR | 危险 | 读取日历事件 | 允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人 |
| android.permission.WRITE\_CALENDAR | 危险 | 添加或修改日历事件并向客人发送电子邮件 | 允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件 |
| 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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 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情况下将自己强加于前 |
| android.permission.FLAG\_ACTIVITY\_NEW\_TASK | 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.ACTIVITY\_RECOGNITION | 危险 | 允许应用程序识别身体活动 | 允许应用程序识别身体活动 |
| 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.hardware.camera.autofocus | 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.PACKAGE\_USAGE\_STATS | 合法 | 更新组件使用统计 | 允许修改收集的组件使用统计。不供普通应用程序使用 |
| com.yitong.xian.mbank.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.yitong.xian.mbank.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ZTE\_HEARTYSERVICE\_MANAGEMENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| 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 |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.yitong.mbank.app.android.activity.SplashActivity | **Schemes**: xamobile://, **Hosts:** xianmobilebank,  |

**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。**