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

**AB Wallet（ 1.2.0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 | AB Wallet |
| 版本 | 1.2.0 |
| 包名 | org.ab.abwallet.android.release |
| 域名线索 | 8条 |
| URL线索 | 10条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | ABWallet\_20250620\_005839\_1.2.0\_96\_official.apk |
| 文件大小 | 112.52MB |
| MD5值 | 2966cc52ee18300b00ebb281cb7984ba |
| SHA1值 | ce191d55d44ee917659ebedd3537b546a109247d |
| SHA256值 | c55c3fcb3184408d4cfd4cfc88f9ee2ddee322809ce782b0d0cf15c84ab513b5 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | AB Wallet |
| 包名 | org.ab.abwallet.android.release |
| 主活动Activity | org.ab.abwallet.android.MainActivity |
| 安卓版本名称 | 1.2.0 |
| 安卓版本 | 96 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.android.com | IP: 142.250.73.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| schemas.android.com | 没有服务器地理信息.  |
| 10.0.2.2 | IP: 10.0.2.2 所属国家: - 地区: - 城市: -  |
| ns.adobe.com | 没有服务器地理信息.  |
| issuetracker.google.com | IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.example.com | IP: 23.32.238.235 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/Baseflow/flutter-permission-handler/issues  | B1/q.java  |
| https://issuetracker.google.com/issues/new?component=618491&template=1257717  | D/g.java  |
| https://issuetracker.google.com/issues/new?component=907884&template=1466542  | G0/j.java  |
| https://issuetracker.google.com/issues/241760537  | G0/A.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | O0/a.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/C1208i.java  |
| http://10.0.2.2:8969/stream  | io/sentry/SpotlightIntegration.java  |
| http://schemas.android.com/apk/res/android  | l0/AbstractC1446k.java  |
| https://docs.flutter.dev/deployment/android  | s4/C2189d.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | X1/s.java  |

### **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: False 找到 1 个唯一证书 主题: C=86, ST=AKA, L=SG, O=AB, OU=AB, CN=Pony 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-13 15:03:28+00:00 有效期至: 3024-09-13 15:03:28+00:00 发行人: C=86, ST=AKA, L=SG, O=AB, OU=AB, CN=Pony 序列号: 0x316d25fe 哈希算法: sha256 md5值: 6406b9a1e641ec7880ca397ae898f2a7 sha1值: 91dfca2304349a8a00ca597ab8a22125883f859e sha256值: 59a6ef66923f58bacfd45b576a30d4d134e760caa44d60f8ba72199d7f2764d2 sha512值: de0e796e9901daaf31468942443a896f76c9b233d43ab24f6011b505197ed5b21842597502e9c99b0c1650db3200bb608c34569c65e5215344fb040a5ed1525c 公钥算法: rsa 密钥长度: 2048 指纹: ca8c9ce2f1781fc1977383abc438bf80718614e6cb24bce96fa0eafe23b8bb91**

## **6. 硬编码敏感信息**

## **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.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.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.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.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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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.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.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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| org.ab.abwallet.android.release.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**