



MoGua

AB Wallet 1.2.0.APK 分析报告



APP名称:

AB Wallet

包名: org.ab.abwallet.android.release

域名线索: 8条

URL线索: 10条

邮箱线索: 1条

分析日期: 2025年7月1日

分析平台: [摸瓜APK反编译平台](#)

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: c55c3fcb3184408d4cfd4cfc88f9ee2dde322809ce782b0d0cf15c84ab513b5

i APP 信息

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

🔍 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 纬度: 37.405991 经度: -122.078514
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: - 纬度: 0.000000 经度: 0.000000

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 纬度: 37.405991 经度: -122.078514
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
www.example.com	IP: 23.32.238.235 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
docs.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

 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

 邮箱线索

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

 手机线索

 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

硬编码敏感信息

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.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

应用内通信

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