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

**杏吧（ 5.7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 | 杏吧 |
| 版本 | 5.7 |
| 包名 | com.qnmd.axingba.vj0r7d |
| 域名线索 | 22条 |
| URL线索 | 19条 |
| APP图标 |  |
| 分析日期 | 2025年6月15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 | ozhaus1xb\_145004.apk |
| 文件大小 | 30.32MB |
| MD5值 | 7d32c23247f95b5456852b0f943af109 |
| SHA1值 | c574f652b4b0e982cd1d77995352c2fd0dd16011 |
| SHA256值 | 1566dda5596445c92d9015df3dfcbafdfd9227039cf4953cd68f54115c9b904f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 杏吧 |
| 包名 | com.qnmd.axingba.vj0r7d |
| 主活动Activity | com.media.blued\_app.ui.WelcomeActivity |
| 安卓版本名称 | 5.7 |
| 安卓版本 | 560000 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api-xbsp.kicfoakjvf.com | IP: 104.21.50.212  所属国家: United States of America  地区: California  城市: San Francisco |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| dashif.org | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| default.url | 没有服务器地理信息. |
| api-xbsp.vf43zauqc7.info | IP: 172.67.203.8  所属国家: United States of America  地区: California  城市: San Francisco |
| api.lpddpvqx7p.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| api-xbsp.x8qpjon3eh.info | IP: 104.21.85.239  所属国家: United States of America  地区: California  城市: San Francisco |
| api.o6knfapwuc.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| api-xbsp.sljghdlqpa.com | IP: 172.67.193.117  所属国家: United States of America  地区: California  城市: San Francisco |
| www.openssl.org | IP: 34.49.79.89  所属国家: United States of America  地区: California  城市: Mountain View |
| api.s8c2bhxj71.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| android.googlesource.com | IP: 142.250.99.82  所属国家: United States of America  地区: California  城市: Mountain View |
| www.baidu.com | IP: 110.242.70.57  所属国家: China  地区: Hebei  城市: Baoding |
| api-xbsp.ku0g6y1ag9.com | IP: 172.67.151.11  所属国家: United States of America  地区: California  城市: San Francisco |
| xb696.me | IP: 99.84.55.11  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| aria.laoyuyu.me | 没有服务器地理信息. |
| encrypted-tbn0.gstatic.com | IP: 142.251.33.78  所属国家: Canada  地区: Ontario  城市: Toronto |
| api.xw4karfjjk.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| aomedia.org | IP: 108.160.166.253  所属国家: United States of America  地区: California  城市: San Francisco |
| api-xbsp.uxavma85y8.com | IP: 172.67.214.178  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.android.com | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://aria.laoyuyu.me/aria\_doc/create/any\_java.html | com/arialyy/aria/core/Aria.java |
| https://aria.laoyuyu.me/aria\_doc/other/annotaion\_invalid.html | com/arialyy/aria/core/download/DownloadReceiver.java |
| https://github.com/AriaLyy/Aria/issues/597 | com/arialyy/aria/core/download/m3u8/M3U8Option.java |
| https://aria.laoyuyu.me/aria\_doc/other/annotaion\_invalid.html | com/arialyy/aria/core/upload/UploadReceiver.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/danikula/videocache/HttpUrlSource.java |
| http://%s:%d/%s | com/danikula/videocache/Pinger.java |
| http://%s:%d/%s | com/danikula/videocache/HttpProxyCacheServer.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/HttpProxyCacheServer.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/SegmentTabLayout.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/CommonTabLayout.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/SlidingTabLayout.java |
| https://www.baidu.com | com/cheap/m3u8\_download/utils/DecryptInterceptor.java |
| https://xb696.me | com/media/blued\_app/GlobalData.java |
| http://api. | com/media/common/base/net/v1/LineUtils.java |
| http://api-xbsp.sljghdlqpa.com/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api-xbsp.kicfoakjvf.com/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api-xbsp.ku0g6y1ag9.com/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api-xbsp.uxavma85y8.com/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api-xbsp.x8qpjon3eh.info/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api-xbsp.vf43zauqc7.info/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api.xw4karfjjk.com/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api.lpddpvqx7p.com/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api.o6knfapwuc.com/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api.s8c2bhxj71.com/tkai/ | com/media/common/base/net/v1/ConfigV1.java |
| http://api. | com/media/common/base/net/v1/ConfigV1.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/rxjava3/exceptions/UndeliverableException.java |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread | 摸瓜V3引擎 |
| encrypted-tbn0.gstatic.com | 摸瓜V3引擎 |
| https://aomedia.org/emsg/ID3 | 摸瓜V3引擎 |
| http://dashif.org/guidelines/trickmode | 摸瓜V3引擎 |
| https://github.com/ReactiveX/RxJava/wiki/What | 摸瓜V3引擎 |
| api.xw4karfjjk.com | 摸瓜V3引擎 |
| discover-pa.googleapis.com | 摸瓜V3引擎 |
| https://aria.laoyuyu.me/aria\_doc/create/any\_java.html | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| https://aria.laoyuyu.me/aria\_doc/other/annotaion\_invalid.html | 摸瓜V3引擎 |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted | 摸瓜V3引擎 |
| https://default.url | 摸瓜V3引擎 |
| http://schemas.android.com/aapt | 摸瓜V3引擎 |
| http://www.openssl.org/support/faq.html | 摸瓜V3引擎 |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | 摸瓜V3引擎 |
| https://xb696.me | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xingba357@gmail.com | com/media/blued\_app/GlobalData.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-08 15:52:45+00:00 有效期至: 2052-10-24 15:52:45+00:00 发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 序列号: 0xabae824 哈希算法: sha256 md5值: 2f338828d422412e2dc193f2ef713eec sha1值: c99c793cd238ba59b729e4520217559e1a1c343b sha256值: b72eef013478a494730806827b94e0531292a6fa56efc3a34911cafcedd1e162 sha512值: f867886aa9c2ce5121c0e5df03d8b3e4cba49a943c961e53ed6c1253a564735e5f57bd47ccc94a87724651baf2a222caef750f0b3b82d7c9450ca2ae411c7499 公钥算法: rsa 密钥长度: 2048 指纹: 9483eb784b5277f8a3a19b0a968e15048733c548bab800dfe339e02a53143121**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_pwd\_setting" : "设置账号密码" |
| "retrieve\_with\_certificate" : "使用账号凭证找回" |
| "scan\_credentials" : "扫描凭证" |
| "setting\_save\_certificate" : "保存账号凭证到手机" |
| "upload\_credentials" : "上传凭证" |
| "user\_name" : "用户名" |

## **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.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.POST\_NOTIFICATIONS | 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.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.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.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.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 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.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.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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.qnmd.axingba.vj0r7d.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。**