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

**杏吧（ 5.1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 | 5.1 |
| 包名 | com.media.xingba.night |
| 域名线索 | 13条 |
| URL线索 | 14条 |
| APP图标 |  |
| 分析日期 | 2025年6月21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 | ozcll1xb\_2.apk |
| 文件大小 | 22.58MB |
| MD5值 | 50fbb606934110df7203c5f8159f9f71 |
| SHA1值 | 34d11fa4c3a75287206ec2762c673e198a051c65 |
| SHA256值 | 08a75be0ea52c55f7c762083e5f4c434ec81bc275302c4e572f9b041a8578cef |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 杏吧 |
| 包名 | com.media.xingba.night |
| 主活动Activity | com.media.xingba.night.ui.welcome.WelcomeActivity |
| 安卓版本名称 | 5.1 |
| 安卓版本 | 510000 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| api.qghvs87s0e.com | IP: 3.173.254.117  所属国家: United States of America  地区: Washington  城市: Seattle |
| aria.laoyuyu.me | 没有服务器地理信息. |
| api-xingba.kicfoakjvf.com | IP: 104.21.50.212  所属国家: United States of America  地区: California  城市: San Francisco |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| api.ybdzd8kdqg.com | IP: 3.173.254.92  所属国家: United States of America  地区: Washington  城市: Seattle |
| api.qsbg70jjlc.com | 没有服务器地理信息. |
| api.j7osrtggtg.com | IP: 3.173.254.117  所属国家: United States of America  地区: Washington  城市: Seattle |
| schemas.android.com | 没有服务器地理信息. |
| api-xingba.sljghdlqpa.com | IP: 104.21.73.241  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 |
| api.pofy11dzpv.com | 没有服务器地理信息. |
| api.tjkck5h6u0.com | IP: 3.173.254.117  所属国家: United States of America  地区: Washington  城市: Seattle |

### **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 |
| 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://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://127.0.0.1: | com/media/xingba/night/utils/DownloadRunnable$downLoadWork$1.java |
| http://api-xingba.kicfoakjvf.com/xbai/ | com/media/xingba/base/net/v1/ConfigV1.java |
| http://api-xingba.sljghdlqpa.com/xbai/ | com/media/xingba/base/net/v1/ConfigV1.java |
| http://api.qsbg70jjlc.com/xbai/ | com/media/xingba/base/net/v1/ConfigV1.java |
| http://api.pofy11dzpv.com/xbai/ | com/media/xingba/base/net/v1/ConfigV1.java |
| http://api.qghvs87s0e.com/xbai/ | com/media/xingba/base/net/v1/ConfigV1.java |
| http://api.tjkck5h6u0.com/xbai/ | com/media/xingba/base/net/v1/ConfigV1.java |
| http://api.j7osrtggtg.com/xbai/ | com/media/xingba/base/net/v1/ConfigV1.java |
| http://api.ybdzd8kdqg.com/xbai/ | com/media/xingba/base/net/v1/ConfigV1.java |

### **4.3 邮箱线索**

### **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: 2024-11-09 07:45:05+00:00 有效期至: 2052-03-27 07:45:05+00:00 发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 序列号: 0x14407836 哈希算法: sha256 md5值: 9add83c967f75687ddb345afb03186a2 sha1值: d3338aec6b63e0285a932cc61982260828ef8253 sha256值: ebed1390d10be0b059ed458a3042797c8cbb61d1ef2353cccea9bc0231e95c9b sha512值: fd35485f3dd0123395f3c487a3cfa4db814e0750779dbb79a7cbfb84ebc565eb9042f14a5fc566a348f3eca96d118ece7144880e9aac14ebad09dafbe7fa6d53 公钥算法: rsa 密钥长度: 2048 指纹: 53210ed72d5a463fbc841dc282126f395087d3609e33cf83f9651def9938a0aa**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "mine\_author" : "创作中心" |
| "post\_private" : "私密" |
| "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" |
| "short\_user\_name" : "@%1$s" |
| "upload\_credentials" : "上传凭证" |
| "user\_name" : "昵称" |

## **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.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\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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 |
| com.media.xingba.night.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。**