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

**啪哩啪哩（ 2.6.11-3496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 | 啪哩啪哩 |
| 版本 | 2.6.11-3496 |
| 包名 | com.palipali |
| 域名线索 | 1条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年6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 | Palipali\_tianya01.apk |
| 文件大小 | 14.11MB |
| MD5值 | 04499d009f5b4ec8846714454f3bf675 |
| SHA1值 | 2dae85c6e9e93454f62bb8b9cfb3a3641d37a8ac |
| SHA256值 | e053cc1898f9b4671dc31a01113036213454910c0cd621a24e7234476ea48d93 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 啪哩啪哩 |
| 包名 | com.palipali |
| 主活动Activity | com.palipali.activity.splash.SplashActivity |
| 安卓版本名称 | 2.6.11-3496 |
| 安卓版本 | 3496 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| jav-app-1460f.firebaseio.com | IP: 35.190.39.113 所属国家: United States of America 地区: Missouri 城市: Kansas City  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://jav-app-1460f.firebaseio.com  | Mogua Engine V1  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| palipali@pali.live  | Mogua Engine V1  |

### **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: True 找到 1 个唯一证书 主题: O=pali, OU=china, CN=palipali 签名算法: rsassa\_pkcs1v15 有效期自: 2020-04-22 10:24:10+00:00 有效期至: 2045-04-16 10:24:10+00:00 发行人: O=pali, OU=china, CN=palipali 序列号: 0x1c6e7771 哈希算法: sha256 md5值: b9fa6649a49ff9f89ac603a711e35d56 sha1值: b81db09a2bc0434d9b0e9cc1ebf40a10f924e322 sha256值: 94dc34881b25672895293e5cddaeda112ca3c94bbe40da4bc765ce6deac4ae3b sha512值: 1e80877f8ed6d9a8c2be2d2bfa3d6bfc1b3207fe6e97cb76396ed61249cb0b415e37e0fc0c0a4e398a3e333e31227d34d107c936659db2841c997f1cfa9a4a77 公钥算法: rsa 密钥长度: 2048 指纹: e152f101279bf79d988db8c4534e5c72618abb1f9867d1bf872a39d1bd0284ce**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_manage\_list\_item\_modify\_pwd" : "變更密碼"  |
| "aeskey" : "palipali"  |
| "com\_facebook\_device\_auth\_instructions" : "Visit <b>facebook.com/device</b> and enter the code shown above."  |
| "firebase\_database\_url" : "https://jav-app-1460f.firebaseio.com"  |
| "g\_authors" : "作者："  |
| "g\_password" : "密碼"  |
| "google\_api\_key" : "AIzaSyAeiGb6hkqDIiZi3hu7pH0GIWeULvxX64U"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAeiGb6hkqDIiZi3hu7pH0GIWeULvxX64U"  |
| "member\_input\_pwd" : "密碼"  |
| "member\_input\_pwd\_6\_16" : "密碼(6-16位密碼)"  |
| "password\_succeed\_modify\_pwd" : "密碼變更成功"  |
| "password\_succeed\_reset\_pwd" : "密碼重設成功"  |
| "account\_manage\_list\_item\_modify\_pwd" : "变更密码"  |
| "com\_facebook\_device\_auth\_instructions" : "请访问<b>facebook.com/device</b>并输入以上验证码。"  |
| "g\_password" : "密码"  |
| "member\_input\_pwd" : "密码"  |
| "member\_input\_pwd\_6\_16" : "密码(6-16位密码)"  |
| "password\_succeed\_modify\_pwd" : "密码变更成功"  |
| "password\_succeed\_reset\_pwd" : "密码重设成功"  |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。"  |

## **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.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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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.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.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 |
| getui.permission.GetuiService.com.palipali | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| 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。 |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 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.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.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.facebook.CustomTabActivity | **Schemes**: @string/fb\_login\_protocol\_scheme://, fbconnect://, **Hosts:** cct.com.palipali,  |

**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。**