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

**91福利（ 1.0.36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 | 91福利 |
| 版本 | 1.0.36 |
| 包名 | com.lWslBu.XPeHEU |
| 域名线索 | 24条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2025年9月28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 | 100002-400099.apk |
| 文件大小 | 65.82MB |
| MD5值 | 86e0c34809947b20bd78295900648bf5 |
| SHA1值 | be7cf24ee9943bc8dd29349c487092d6f08be9ee |
| SHA256值 | dcb846d2e0e4e8d282cf5ba6fd3ea67800417a121283a825beeab51f0f7a5b6c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 91福利 |
| 包名 | com.lWslBu.XPeHEU |
| 主活动Activity | com.lWslBu.XPeHEU.MainActivity |
| 安卓版本名称 | 1.0.36 |
| 安卓版本 | 36 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| 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.  |
| developer.android.com | IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| schemas.microsoft.com | IP: 13.107.253.49 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| dartbug.com | IP: 216.239.36.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| www.example.com | IP: 88.221.83.146 所属国家: Belgium 地区: Brussels Hoofdstedelijk Gewest 城市: Brussels  |
| aomedia.org | IP: 104.244.46.246 所属国家: United States of America 地区: California 城市: San Francisco  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| ns.adobe.com | 没有服务器地理信息.  |
| developer.apple.com | IP: 17.253.85.201 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| metrics1.data.hicloud.com | IP: 111.202.17.12 所属国家: China 地区: Beijing 城市: Beijing  |
| issuetracker.google.com | IP: 142.250.73.142 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| metrics.dt.dbankcloud.ru | IP: 159.138.204.140 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://)([\\s\\S]+)  | com/huawei/hms/scankit/p/t3.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | d5/x.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | h3/b1.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | h1/q.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/g.java  |
| http://dashif.org/guidelines/last-segment-number  | n4/d.java  |
| http://dashif.org/guidelines/trickmode  | n4/d.java  |
| http://dashif.org/thumbnail\_tile  | n4/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | n4/d.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | l3/i0.java  |
| https://x</LA\_URL>  | l3/h0.java  |
| https://default.url  | l3/h0.java  |
| https://issuetracker.google.com/issues/new?component=413107&template=1096568  | k0/c.java  |
| http://ns.adobe.com/xap/1.0/  | r3/a.java  |
| https://aomedia.org/emsg/ID3  | b4/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | b4/a.java  |
| https://metrics1.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics.dt.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://github.com/nodeca/pica  | 摸瓜V2引擎  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/arm64-v8a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://dartbug.com/52121.  | lib/arm64-v8a/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | j5/a.java  |
| 18222222222  | s3/e.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: CN=., OU=., O=., L=Singapore, ST=Singapore, C=EN 签名算法: rsassa\_pkcs1v15 有效期自: 2024-08-26 15:17:21+00:00 有效期至: 2049-08-20 15:17:21+00:00 发行人: CN=., OU=., O=., L=Singapore, ST=Singapore, C=EN 序列号: 0x1 哈希算法: sha256 md5值: 02f0ff83e8a478064c411b41277025ac sha1值: 65047fbc6e0fb23d044a85807bd2aa3450b08c18 sha256值: 4e3d5dec98f9966e105312272bd08895fd629115b9092fa87c71b5b0c0131c94 sha512值: babc48115f848797f59816ee36500a3428c8bd04686843b7fc8415e405fc769d83671403c97fb825c7dec6f6cac7c0db5e3a1b68306ed627cb5b7d66d0380021 公钥算法: rsa 密钥长度: 2048 指纹: 06dc57feeb759ec77b083a52ba11fa8ed57e65d48e601072a59c46dedde2d976**

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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\_MEDIA\_IMAGES | 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\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| 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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_BASIC\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.READ\_PHONE\_NUMBERS | 危险 |  | 允许到设备的读访问的电话号码。这是 READ\_PHONE\_STATE 授予的功能的一个子集,但对即时应用程序公开 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 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 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.lWslBu.XPeHEU.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。**