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

**丝袜美女壁纸4（ 1.0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 | 丝袜美女壁纸4 |
| 版本 | 1.0 |
| 包名 | com.alan.siwameinv4 |
| 域名线索 | 27条 |
| URL线索 | 30条 |
| APP图标 |  |
| 分析日期 | 2025年4月3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 | 5ea66f982dd60d5ba6251d2e23ecaa9a50927f0c12298ac522a28480be235eb4.apk |
| 文件大小 | 9.54MB |
| MD5值 | 1cefad7479369163c70e1a1198381aa0 |
| SHA1值 | 925d63b1f67e1becd6f7235e358e0577585d1f8e |
| SHA256值 | 5ea66f982dd60d5ba6251d2e23ecaa9a50927f0c12298ac522a28480be235eb4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 丝袜美女壁纸4 |
| 包名 | com.alan.siwameinv4 |
| 主活动Activity | .PictureGrid |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| clk.adsmogo.com | 没有服务器地理信息.  |
| tw.ad.adon.vpon.com | 没有服务器地理信息.  |
| googleads.g.doubleclick.net | IP: 114.250.67.38 所属国家: China 地区: Beijing 城市: Beijing  |
| c.admob.com | IP: 114.250.70.38 所属国家: China 地区: Beijing 城市: Beijing  |
| maps.google.com | IP: 142.250.69.206 所属国家: United States of America 地区: California 城市: Mountain View  |
| ditu.google.cn | IP: 114.250.70.34 所属国家: China 地区: Beijing 城市: Beijing  |
| maps.google | 没有服务器地理信息.  |
| market.android.com | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| app.waps.cn | 没有服务器地理信息.  |
| www.googleadservices.com | IP: 114.250.67.38 所属国家: China 地区: Beijing 城市: Beijing  |
| www.vpon.com | IP: 172.105.218.228 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| schemas.android.com | 没有服务器地理信息.  |
| gad.ju6666.com | IP: 38.55.63.20 所属国家: United States of America 地区: California 城市: Los Angeles  |
| cn.ad.adon.vpon.com | 没有服务器地理信息.  |
| cus.adsmogo.com | 没有服务器地理信息.  |
| r2.adwo.com | IP: 42.62.76.40 所属国家: China 地区: Beijing 城市: Beijing  |
| www.youtube.com | IP: 31.13.73.9 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| ads.waps.cn | 没有服务器地理信息.  |
| www.adsmogo.com | 没有服务器地理信息.  |
| www.adwo.com | IP: 49.232.84.161 所属国家: China 地区: Beijing 城市: Beijing  |
| 219.234.85.214 | IP: 219.234.85.214 所属国家: China 地区: Beijing 城市: Beijing  |
| req.adsmogo.com | 没有服务器地理信息.  |
| ditu.google.com | IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.gstatic.com | IP: 203.208.50.34 所属国家: China 地区: Beijing 城市: Beijing  |
| blk.adsmogo.com | 没有服务器地理信息.  |
| imp.adsmogo.com | 没有服务器地理信息.  |
| cfg.adsmogo.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://app  | com/waps/n.java  |
| http://app.waps.cn  | com/waps/n.java  |
| http://ads.waps.cn  | com/waps/n.java  |
| http://219.234.85.214  | com/waps/k.java  |
| http://app.waps.cn/action/account/getinfo?  | com/waps/f.java  |
| http://app.waps.cn/action/account/spend?  | com/waps/i.java  |
| http://app.waps.cn/action/  | com/waps/g.java  |
| http://ads.waps.cn/action/user\_info  | com/waps/h.java  |
| http://app.waps.cn/action/connect/active?  | com/waps/j.java  |
| http://app.waps.cn/action/app/update?  | com/waps/j.java  |
| http://app.waps.cn/action/account/offerlist?  | com/waps/AppConnect.java  |
| http://app.waps.cn/action/account/ownslist?  | com/waps/AppConnect.java  |
| http://ads.waps.cn/action/  | com/waps/AppConnect.java  |
| http://app  | com/waps/ads/AdGroupManager.java  |
| http://app.waps.cn  | com/waps/ads/AdGroupManager.java  |
| http://ads  | com/waps/ads/AdGroupManager.java  |
| http://ads.waps.cn  | com/waps/ads/AdGroupManager.java  |
| http://ads.waps.cn/action/adgroup/ad\_custom?  | com/waps/ads/AdGroupManager.java  |
| http://app  | com/waps/ads/d.java  |
| http://app.waps.cn  | com/waps/ads/d.java  |
| http://ads  | com/waps/ads/d.java  |
| http://ads.waps.cn  | com/waps/ads/d.java  |
| http://ads.waps.cn/action/adgroup/ad\_click?  | com/waps/ads/AdGroupLayout.java  |
| http://ads.waps.cn/action/adgroup/ad\_impression?  | com/waps/ads/AdGroupLayout.java  |
| http://ads.waps.cn/action/adgroup/config?  | com/waps/ads/c/a.java  |
| http://www.vpon.com/v/index.jsp  | com/vpon/adon/android/AdDisplay.java  |
| http://www.vpon.com/v/index.jsp88623698333service@vpon.com  | com/vpon/adon/android/AdManager.java  |
| http://tw.ad.adon.vpon.com/api/webviewAdReq  | com/vpon/adon/android/utils/AdOnUrlUtil.java  |
| http://cn.ad.adon.vpon.com/api/webviewAdReq  | com/vpon/adon/android/utils/AdOnUrlUtil.java  |
| http://tw.ad.adon.vpon.com/api/webviewSdkError  | com/vpon/adon/android/utils/AdOnUrlUtil.java  |
| http://cn.ad.adon.vpon.com/api/swebviewSdkError  | com/vpon/adon/android/utils/AdOnUrlUtil.java  |
| http://tw.ad.adon.vpon.com/api/webviewAdClick  | com/vpon/adon/android/utils/AdOnUrlUtil.java  |
| http://cn.ad.adon.vpon.com/api/webviewAdClick  | com/vpon/adon/android/utils/AdOnUrlUtil.java  |
| http://www.vpon.com/v/index.jsp88623698333service@vpon.com  | com/vpon/adon/android/utils/IOUtils.java  |
| http://maps.google  | com/vpon/adon/android/webClientHandler/GoogleMapHandler.java  |
| http://www.youtube.com/  | com/vpon/adon/android/webClientHandler/YoutubeHandler.java  |
| http://clk.adsmogo.com/exclick.ashx?appid=%s&nid=%s&type=%d&uuid=%s&country=%s&appver=%d&client=2&nt=%s&os=%s&dn=%s&adtype=%s  | com/admogo/util/AdMogoUtil.java  |
| http://cfg.adsmogo.com/GetInfo.ashx?appid=%s&appver=%d&client=2&country=%s&nt=%s&os=%s&dn=%s&adtype=%s&size=%s  | com/admogo/util/AdMogoUtil.java  |
| http://cus.adsmogo.com/custom.ashx?appid=%s&nid=%s&uuid=%s&country=%s&appver=%d&client=2&nt=%s&os=%s&dn=%s  | com/admogo/util/AdMogoUtil.java  |
| http://imp.adsmogo.com/exmet.ashx?appid=%s&nid=%s&type=%d&uuid=%s&country=%s&appver=%d&client=2&nt=%s&os=%s&dn=%s&adtype=%s  | com/admogo/util/AdMogoUtil.java  |
| http://www.adsmogo.com/adserv.php?appid=%s&nid=%s&uuid=%s&country=%s&ad\_type=%d&gender=%s&birthday=%s&keywords=%s&appver=%d&client=2&nt=%s&os=%s&dn=%s  | com/admogo/util/AdMogoUtil.java  |
| http://blk.adsmogo.com/blank.ashx?appid=%s&nid=%s&type=%s&country=%s&appver=%s&nt=%s&os=%s&dn=%s&adtype=%s  | com/admogo/util/AdMogoUtil.java  |
| http://req.adsmogo.com/exrequest.ashx?appid=%s&nid=%s&country=%s&appver=%d&type=%d&client=2&nt=%s&os=%s&dn=%s&adtype=%s  | com/admogo/util/AdMogoUtil.java  |
| http://r2.adwo.com/ad  | com/adwo/adsdk/O.java  |
| http://www.adwo.com  | com/adwo/adsdk/AdwoAdBrowserActivity.java  |
| http://market.android.com  | com/adwo/adsdk/w.java  |
| https://market.android.com  | com/adwo/adsdk/w.java  |
| http://schemas.android.com/apk/res/  | com/adwo/adsdk/AdwoAdView.java  |
| http://maps.google.com/maps?q=  | com/adwo/adsdk/C0008g.java  |
| http://gad.ju6666.com/adserver/android/1.0/GetAd  | com/ju6/a.java  |
| http://gad.ju6666.com/adserver/android/1.0/GetAd&  | com/ju6/a.java  |
| http://gad.ju6666.com/adserver/android/1.0/GetAd?  | com/ju6/a.java  |
| http://ditu.google.com/maps?q=  | net/youmi/android/ay.java  |
| http://ditu.google.cn/staticmap?center=  | net/youmi/android/ay.java  |
| http://schemas.android.com/apk/res/  | net/youmi/android/AdView.java  |
| http://www.gstatic.com/afma/sdk-core-v  | defpackage/c.java  |
| http://googleads.g.doubleclick.net  | defpackage/h.java  |
| http://clk  | defpackage/h.java  |
| http://c.admob.com  | defpackage/h.java  |
| http://googleads.g.doubleclick.net/aclk  | defpackage/h.java  |
| http://www.googleadservices.com/pagead/aclk  | defpackage/h.java  |
| http://market.android.com/details  | defpackage/h.java  |
| ads.waps.cn  | 摸瓜V3引擎  |
| app.waps.cn  | 摸瓜V3引擎  |
| cfg.adsmogo.com  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| service@vpon.com sp88623698333service@vpon.com  | com/vpon/adon/android/AdManager.java  |
| sp88623698333service@vpon.com  | com/vpon/adon/android/utils/IOUtils.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18591940421  | net/youmi/android/aa.java  |
| 16151604435  | net/youmi/android/aa.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: CN=alan 签名算法: rsassa\_pkcs1v15 有效期自: 2011-04-03 04:22:30+00:00 有效期至: 2036-03-27 04:22:30+00:00 发行人: CN=alan 序列号: 0x4d97f606 哈希算法: md5 md5值: 151dbd377248bc07007fccc2aeec611e sha1值: 4f3abf661800af1ba7ccc02bac5ee292aa0cdc43 sha256值: 90bc2aeb876bab3bba3ede46a1b70fa93b207de0d93388bdedfa9165410fb900 sha512值: 87881ba975525afaae35e12ac1006fd4aa9f7823b03d28aa9d66ade5d893f94bc43772fe88ac55e18cff79c9e2046e3f33e10561980095a5f087865ad786f0fb**

## **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.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| 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.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.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.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.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\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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\_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\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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.WRITE\_SMS | 危险 | 编辑短信或彩信 | 允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息 |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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**

**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。**