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

**讼答（ 1.1.0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 | 讼答 |
| 版本 | 1.1.0 |
| 包名 | com.beijing.wusong.kingkong |
| 域名线索 | 32条 |
| URL线索 | 40条 |
| APP图标 |  |
| 分析日期 | 2025年6月14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 | 讼答\_1.1.0.apk |
| 文件大小 | 16.4MB |
| MD5值 | 1cbfbe147a140656edacc2c22a641602 |
| SHA1值 | 6bcf11c628f378caae10b8851fbd8a44d3731f9b |
| SHA256值 | 07a85fe9dacb68e42043429bb5aab1798e6bc97bc163a683807cc4cf05820acc |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 讼答 |
| 包名 | com.beijing.wusong.kingkong |
| 主活动Activity | com.tiantonglaw.kingkong.LaunchActivity |
| 安卓版本名称 | 1.1.0 |
| 安卓版本 | 20 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| community.wusong.com | IP: 123.56.230.250 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| developer.umeng.com | IP: 59.82.60.43 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.weixin.qq.com | IP: 140.207.121.14 所属国家: China 地区: Shanghai 城市: Shanghai  |
| ulogs.umengcloud.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| tbsrecovery.imtt.qq.com | IP: 60.28.172.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| plbslog.umeng.com | IP: 36.156.202.68 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| errlog.umeng.com | IP: 223.109.148.143 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| lkme.cc | IP: 120.53.207.65 所属国家: China 地区: Shandong 城市: Qingdao  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| beacon.wusong.com | IP: 123.56.230.250 所属国家: China 地区: Beijing 城市: Beijing  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| github.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| errlogos.umeng.com | IP: 47.246.110.18 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| upload-z2.qiniup.com | IP: 163.142.153.211 所属国家: China 地区: Guangdong 城市: Foshan  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| alogus.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| cfg.imtt.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ce3e75d5.jpush.cn | IP: 120.233.50.89 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| aaid.umeng.com | IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| mdc.html5.qq.com | IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| alogsus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| configapi-api.glqa.jpushoa.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ce3e75d5.jpush.cn/wi/op8jdu  | cn/jiguang/s/c.java  |
| https://upload-z2.qiniup.com  | cn/jiguang/bd/a.java  |
| http://configapi-api.glqa.jpushoa.com/v1/status  | cn/jiguang/bc/f.java  |
| https://ce3e75d5.jpush.cn  | cn/jiguang/b/b.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/f/c.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://lkme.cc/i/  | com/microquation/linkedme/android/b/d.java  |
| https://lkme.cc/i  | com/microquation/linkedme/android/b/a/f.java  |
| https://lkme.cc/i  | com/microquation/linkedme/android/b/a/b.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/MaybeLife.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/CompletableLife.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/FlowableLife.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/SingleLife.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/rxjava/rxlife/ObservableLife.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/l.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/m.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/m.java  |
| https://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/m.java  |
| https://tbsrecovery.imtt.qq.com/getconfig  | com/tencent/smtt/utils/m.java  |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/i.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://errlogos.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlog.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | e/c/a/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | e/c/a/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | e/c/a/h.java  |
| http://%s:%d/%s  | e/c/a/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | h/a/a/b/j.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://xml.apache.org/xslt  | l/a/a/d/b.java  |
| https://beacon.wusong.com/api/ws/  | 摸瓜V1引擎  |
| https://community.wusong.com/  | 摸瓜V1引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/Document/execCommand  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | e/c/a/h.java  |

### **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: False 找到 1 个唯一证书 主题: C=100000, ST=beijing, L=beijing, O=wusong, OU=beijingwusong, CN=wusong 签名算法: rsassa\_pkcs1v15 有效期自: 2021-04-09 03:28:06+00:00 有效期至: 2046-04-03 03:28:06+00:00 发行人: C=100000, ST=beijing, L=beijing, O=wusong, OU=beijingwusong, CN=wusong 序列号: 0x6bc7f748 哈希算法: sha256 md5值: d959ecd4b0704da451a30912eb96f5df sha1值: 51fdab0bf8c5b1f3715265af1d8cfdff206290f0 sha256值: 4dd8b4626be5919c22cb16ff6cc3f8d0b38c05a1a4af25dbededbbb704b2b586 sha512值: 17ead0c3b1ec51576e972f8dbdea9f9a126e86da1a45be8c69fb425019d5a3e387f6412ba676c5fc2d0f3765a8011de2059b041ba7c9f679179c029e5f75d838 公钥算法: rsa 密钥长度: 2048 指纹: 9db3c8991f8b8a277f9163afcf7f176f89ea04771cf08b7ab42628460c82fe14**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 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.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.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.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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| com.beijing.wusong.kingkong.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 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.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。 |
| 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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| 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 |
| 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.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.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\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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.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.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 |
| 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.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。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| deeplink.UriSchemeProcessActivity | **Schemes**: songda://, https://, http://, **Hosts:** linkedme, at7y.lkme.cc, **Path Prefixes:** /huG,  |

**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。**