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

**兴农兴邦（ 1.0.9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 | 兴农兴邦 |
| 版本 | 1.0.9 |
| 包名 | uni.app.UNIF0BEA52 |
| 域名线索 | 25条 |
| URL线索 | 24条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | 兴农兴邦.apk |
| 文件大小 | 28.19MB |
| MD5值 | c76326dae3c1da7439b00af3f3de8042 |
| SHA1值 | 0b320de4914ef90a4bc49844ffcdae58b87cbdc4 |
| SHA256值 | 0d5a3d27237af791558f96c1b03c61ba261861a9b872edc4fcb56e497584ccec |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 兴农兴邦 |
| 包名 | uni.app.UNIF0BEA52 |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.9 |
| 安卓版本 | 109 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| xnxb3829-1325325705.cos.accelerate.myqcloud.com | IP: 111.202.29.113 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.android.com | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| img11.360buyimg.com | IP: 60.9.3.148 所属国家: China 地区: Hebei 城市: Hengshui  |
| goo.gl | IP: 74.125.195.113 所属国家: United States of America 地区: California 城市: Mountain View  |
| service.dcloud.net.cn | IP: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing  |
| xnxb3111-1351049253.cos.accelerate.myqcloud.com | IP: 111.202.29.114 所属国家: China 地区: Beijing 城市: Beijing  |
| m3w.cn | IP: 221.15.67.88 所属国家: China 地区: Henan 城市: Luoyang  |
| er.dcloud.net.cn | IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing  |
| ask.dcloud.net.cn | IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin  |
| er.dcloud.io | 没有服务器地理信息.  |
| quilljs.com | IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| apis.map.qq.com | IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.google.com | IP: 199.59.148.20 所属国家: United States of America 地区: California 城市: San Francisco  |
| ccdcapi.alipay.com | IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| vuejs.org | IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle  |
| ns.adobe.com | 没有服务器地理信息.  |
| maps.googleapis.com | IP: 173.194.202.95 所属国家: United States of America 地区: California 城市: Mountain View  |
| xn-1325328864.cos.accelerate.myqcloud.com | IP: 111.202.29.114 所属国家: China 地区: Beijing 城市: Beijing  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| webapi.amap.com | IP: 111.202.5.197 所属国家: China 地区: Beijing 城市: Beijing  |
| map.qq.com | IP: 116.130.224.19 所属国家: China 地区: Beijing 城市: Beijing  |
| next.vuex.vuejs.org | IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle  |
| uqrcode.cn | IP: 60.211.209.109 所属国家: China 地区: Shandong 城市: Jining  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| https://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/feature/utsplugin/ProxyModule.java  |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://er.dcloud.io/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://er.dcloud.net.cn/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://ask.dcloud.net.cn/article/35627  | io/dcloud/e/b/a.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/e/b/a.java  |
| https://er.dcloud.io/rv  | io/dcloud/e/c/h/c.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/e/c/h/c.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/g/b.java  |
| https://ask.dcloud.net.cn/article/287  | io/dcloud/share/IFShareApi.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifViewUtils.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| https://ask.dcloud.net.cn/article/36199  | 摸瓜V1引擎  |
| https://github.com/uuidjs/uuid  | 摸瓜V2引擎  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=$  | 摸瓜V2引擎  |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=  | 摸瓜V2引擎  |
| https://www.google.com/maps/?daddr=  | 摸瓜V2引擎  |
| https://www.google.com/maps/  | 摸瓜V2引擎  |
| https://quilljs.com/  | 摸瓜V2引擎  |
| https://quilljs.com  | 摸瓜V2引擎  |
| https://xn-1325328864.cos.accelerate.myqcloud.com  | 摸瓜V2引擎  |
| https://xnxb3111-1351049253.cos.accelerate.myqcloud.com  | 摸瓜V2引擎  |
| https://xnxb3829-1325325705.cos.accelerate.myqcloud.com  | 摸瓜V2引擎  |
| https://next.vuex.vuejs.org/  | 摸瓜V2引擎  |
| https://vuejs.org/images/icons/favicon-96x96.png  | 摸瓜V2引擎  |
| https://uqrcode.cn/doc  | 摸瓜V2引擎  |
| http://goo.gl/MqrFmX\n  | 摸瓜V2引擎  |
| http://goo.gl/rRqMUw  | 摸瓜V2引擎  |
| http://goo.gl/MqrFmX\n\n  | 摸瓜V2引擎  |
| https://ccdcapi.alipay.com/validateAndCacheCardInfo.json?\_input\_charset=utf-8&cardNo=  | 摸瓜V2引擎  |
| https://img11.360buyimg.com/imagetools/jfs/t1/146371/38/8485/738/5f606425Eca239740/14f4b4f5f20d8a68.png  | 摸瓜V2引擎  |
| https://img11.360buyimg.com/imagetools/jfs/t1/129395/8/12735/2030/5f61ac37E70cab338/fb477dc11f46056c.png  | 摸瓜V2引擎  |
| https://vuejs.org/error-reference/  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 摸瓜V2引擎  |
| https://map.qq.com/api/js?v=2.exp&  | 摸瓜V2引擎  |
| https://maps.googleapis.com/maps/api/js?  | 摸瓜V2引擎  |
| https://webapi.amap.com/maps?v=2.0&  | 摸瓜V2引擎  |
| https://api.map.baidu.com/api?type=webgl&v=1.0&  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| jhruby.web@gmail.com  | 摸瓜V2引擎  |

### **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=CN, ST=, L=, O=Android, OU=Android, CN=G0dwmOkQPHkqpLkM3DGIjccelyerg9BWi62su2GIYDGCqF8Sh9spj0kDjIYGFJ6E4sCY4ljT94f3wLuv2RV7FA%3D%3D 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-31 16:11:12+00:00 有效期至: 2125-05-07 16:11:12+00:00 发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=G0dwmOkQPHkqpLkM3DGIjccelyerg9BWi62su2GIYDGCqF8Sh9spj0kDjIYGFJ6E4sCY4ljT94f3wLuv2RV7FA%3D%3D 序列号: 0x42046e2a 哈希算法: sha256 md5值: 289a82884abc3761c5d336cf3e0a84ae sha1值: 6acc2071a2fe2ec4c3c20700e8f535fe1cc74771 sha256值: caf85fef72157ee1938d2b5d04c32f74980b1fdf1298210fe8f2e3f6ae42ff00 sha512值: 4c96bb78de65d5b313739e9a4cf3b9856a8f972ca308e742540173c229eeb2f07788361e28ef9c8c7efba1f2d196f4e375eb35b2cf30246b6bb7eda0b76f5e47 公钥算法: rsa 密钥长度: 2048 指纹: cd023bb6ad1cd70dfb96da80d13a4685f75654a17083e3b617cd20caadcdb1f1**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API"  |
| "dcloud\_io\_without\_authorization" : "not authorized"  |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service"  |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed"  |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained"  |
| "dcloud\_oauth\_token\_failed" : "failed to get token"  |
| "dcloud\_permissions\_reauthorization" : "reauthorize"  |
| "dcloud\_tips\_certificate" : "certificate"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_io\_without\_authorization" : "没有获得授权"  |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权"  |
| "dcloud\_oauth\_token\_failed" : "获取token失败"  |
| "dcloud\_permissions\_reauthorization" : "重新授权"  |
| "dcloud\_tips\_certificate" : "证书"  |

## **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\_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.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\_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\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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。 |

## **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。**