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

**大漢易經書院（ 1.0.1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 | 大漢易經書院 |
| 版本 | 1.0.1 |
| 包名 | me.dhtv.app |
| 域名线索 | 43条 |
| URL线索 | 27条 |
| APP图标 |  |
| 分析日期 | 2025年7月11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 | newdahann.apk |
| 文件大小 | 6.36MB |
| MD5值 | 62e4d8654d46980462be3dc5f1f89238 |
| SHA1值 | 1822f317aa81cc3674a6ec3c3069a2d9c12b2c92 |
| SHA256值 | 9c26f73cc82cc20c924811544a82b29766f5eb3befee1a81bc64ee416b0c5371 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 大漢易經書院 |
| 包名 | me.dhtv.app |
| 主活动Activity | com.lt.app.MainActivity |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 101 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| resolver.msg.global.xiaomi.net | IP: 8.219.211.108 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| store2.hispace.hicloud.com | IP: 13.225.183.77 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| cn.register.xmpush.xiaomi.com | IP: 118.26.252.220 所属国家: China 地区: Beijing 城市: Beijing  |
| fr.register.xmpush.global.xiaomi.com | IP: 3.120.167.167 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| plbslog.umeng.com | IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| www.jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| alogsus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ouplog.umeng.com | IP: 47.246.110.94 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| store.hispace.hicloud.com | IP: 49.4.47.71 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing  |
| api-push.meizu.com | IP: 125.94.213.129 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.com | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| idmb.register.xmpush.global.xiaomi.com | IP: 43.205.173.134 所属国家: India 地区: Maharashtra 城市: Mumbai  |
| norma-external-collect.meizu.com | IP: 113.106.27.98 所属国家: China 地区: Guangdong 城市: Zhongshan  |
| store3.hispace.hicloud.com | IP: 96.17.215.230 所属国家: United States of America 地区: California 城市: Los Angeles  |
| ulogs.umengcloud.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics1.data.hicloud.com | IP: 114.115.188.159 所属国家: China 地区: Beijing 城市: Beijing  |
| alogus.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| developer.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| aaid.umeng.com | IP: 218.91.197.68 所属国家: China 地区: Jiangsu 城市: Nantong  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| store-at-dre.hispace.dbankcloud.com | 没有服务器地理信息.  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| play.google.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| store-drru.hispace.hicloud.com | IP: 159.138.202.186 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.asia | 没有服务器地理信息.  |
| pslog.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| resolver.msg.xiaomi.net | IP: 120.92.96.13 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.android.com | 没有服务器地理信息.  |
| ulogs.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| store1.hispace.hicloud.com | IP: 118.194.33.169 所属国家: China 地区: Shanghai 城市: Shanghai  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/baidu/techain/i/c.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | com/xiaomi/push/gg.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gn.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/go.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fj.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fv.java  |
| https://%1$s/gslb/?ver=4.0  | com/xiaomi/push/cv.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://fr.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://ru.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://idmb.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://resolver.msg.global.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bt.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bt.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/namespace-prefixes  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-general-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/string-interning  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xmlpull.org/v1/doc/features.html  | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java  |
| https://api-push.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.in.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.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://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://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| https://play.google.com/store/apps/details?id=  | Mogua Engine V1  |
| https://appgallery.cloud.huawei.com  | Mogua Engine V1  |
| https://store.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V1  |
| https://data-drcn.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dra.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dre.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-drru.push.dbankcloud.com  | Mogua Engine V2  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://store1.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://metrics1.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics-dra.dt.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics2.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.data.hicloud.com:6447  | Mogua Engine V2  |

### **4.3 邮箱线索**

### **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=UB, ST=UB, L=UB, O=UB, OU=UBWU, CN=UB 签名算法: rsassa\_pkcs1v15 有效期自: 2021-10-11 11:27:51+00:00 有效期至: 2121-09-17 11:27:51+00:00 发行人: C=UB, ST=UB, L=UB, O=UB, OU=UBWU, CN=UB 序列号: 0x2334b4d1 哈希算法: sha256 md5值: 7fd5a557ffca3ea284c941a532e4b731 sha1值: 212d75441935641021e8273e4e8e653b17be0824 sha256值: 7be6432ba9a313fcae88eceaea4defe02bea0ea89c2ba4da0114d439e28913c4 sha512值: 6d59ac55916cfbe635fcd545a8f3f99b700155ec630fbdaf7af60e839cfb19657eeed66d720dc43e021b333f0c927da478da8fb578c2e19cb511d8531b1ca444 公钥算法: rsa 密钥长度: 2048 指纹: 7ecbd925011411388316eb536884402641c28628ba345b49c35214970e3c4f58**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "p\_ht\_appkey" : "700020336"  |
| "p\_ht\_mz\_appkey" : ""  |
| "p\_ht\_op\_appkey" : ""  |
| "p\_ht\_op\_appsecret" : ""  |
| "p\_ht\_vv\_appkey" : ""  |
| "p\_ht\_xm\_appkey" : ""  |
| "p\_rcpush\_mzAppKey" : ""  |
| "p\_rcpush\_opAppKey" : ""  |
| "p\_rcpush\_opAppSecret" : ""  |
| "p\_rcpush\_vvAppKey" : ""  |
| "p\_rcpush\_xmAppKey" : ""  |
| "p\_u\_appkey" : "61641fb9ac9567566e926f18"  |
| "p\_weibo\_appkey" : ""  |

## **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.RECEIVE\_USER\_PRESENT | 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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 |
| 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。 |
| me.dhtv.app.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| me.dhtv.app.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| me.dhtv.app.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 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 |
| me.dhtv.app.permission.techain.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| me.dhtv.app.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| me.dhtv.app.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| me.dhtv.app.permission.YM\_APP | 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.RECORD\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.lt.app.JumpActivity | **Schemes**: ltapp276502://,  |
| com.baidu.techain.push.VivoPushActivity | **Schemes**: vpushscheme://, **Hosts:** me.dhtv.app, **Paths:** /detail,  |

**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。**