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

**毅德（ 1.1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 | 毅德 |
| 版本 | 1.1 |
| 包名 | com.yide |
| 域名线索 | 11条 |
| URL线索 | 19条 |
| APP图标 |  |
| 分析日期 | 2025年6月13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 | base.apk |
| 文件大小 | 3.13MB |
| MD5值 | 0d5fa050762cc8dae7f20cab65b38366 |
| SHA1值 | 7447f5a330a053ba04bd870590d50925fa7985e0 |
| SHA256值 | 2b19767cc8940ef935ebeb07c9054c601c99920f8a746c92ad342f756e23294a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 毅德 |
| 包名 | com.yide |
| 主活动Activity | com.yide.MainActivity |
| 安卓版本名称 | 1.1 |
| 安卓版本 | 11 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| schemas.android.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| new-api.meiqia.com | IP: 114.117.133.42  所属国家: China  地区: Beijing  城市: Beijing |
| logback.qos.ch | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| notify.bugsnag.com | IP: 35.186.205.6  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| yde-t-1327923657.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.151  所属国家: China  地区: Fujian  城市: Fuzhou |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| meiqia.com | IP: 114.117.133.42  所属国家: China  地区: Beijing  城市: Beijing |
| yde-doc-img.s3.ap-east-1.amazonaws.com | IP: 3.5.236.11  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| yde-sz.oss-accelerate.aliyuncs.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| yde-hk.oss-accelerate.aliyuncs.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| www.slf4j.org | IP: 159.100.250.151  所属国家: Switzerland  地区: Zurich  城市: Zurich |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://logback.qos.ch/codes.html | c/a/a/b/q/b/d.java |
| http://logback.qos.ch/codes.html | c/a/a/b/q/c/c.java |
| http://xml.org/sax/features/external-general-entities | c/a/a/b/q/d/e.java |
| http://xml.org/sax/features/external-parameter-entities | c/a/a/b/q/d/e.java |
| http://logback.qos.ch/codes.html | c/a/a/b/r/a.java |
| http://logback.qos.ch/codes.html | c/a/a/b/s/k/e.java |
| http://schemas.android.com/apk/res/android | b/g/b/g.java |
| https://new-api.meiqia.com/captchas | com/meiqia/meiqiasdk/util/HttpUtils.java |
| https://new-api.meiqia.com | com/meiqia/meiqiasdk/util/HttpUtils.java |
| https://new-api.meiqia.com/unified-api/conversations/v1/client/sdk/mass\_message\_receipts | com/meiqia/core/r0.java |
| https://new-api.meiqia.com/client/send\_msg | com/meiqia/core/m1.java |
| https://new-api.meiqia.com/client/msg\_delivered | com/meiqia/core/m1.java |
| https://new-api.meiqia.com/conversation/ | com/meiqia/core/m1.java |
| https://new-api.meiqia.com/sdk/init\_sdk\_user | com/meiqia/core/m1.java |
| https://new-api.meiqia.com/client/msg\_read | com/meiqia/core/m1.java |
| https://new-api.meiqia.com/conversation/ | com/meiqia/core/MeiQiaService.java |
| https://new-api.meiqia.com/client/tickets\_v2/ | com/meiqia/core/j.java |
| https://new-api.meiqia.com/client/tickets\_v2 | com/meiqia/core/j.java |
| https://new-api.meiqia.com/client/send\_msg | com/meiqia/core/j.java |
| https://new-api.meiqia.com/client/file\_downloaded | com/meiqia/core/j.java |
| https://new-api.meiqia.com/sdk/init | com/meiqia/core/j.java |
| https://new-api.meiqia.com/sdk/get\_dev\_client\_id | com/meiqia/core/j.java |
| https://new-api.meiqia.com/sdk/statistics | com/meiqia/core/j.java |
| https://new-api.meiqia.com/upload?user\_id= | com/meiqia/core/j.java |
| https://new-api.meiqia.com/upload/oss/policies | com/meiqia/core/j.java |
| https://new-api.meiqia.com/client/forms | com/meiqia/core/j.java |
| https://new-api.meiqia.com/client/tickets | com/meiqia/core/j.java |
| https://new-api.meiqia.com/client/attrs | com/meiqia/core/j.java |
| https://new-api.meiqia.com/mpush/copy/statistics | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/client/end\_conversation | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/knowledge/questions/ | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/conversation/ | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/client/queue/position | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/client/tickets\_v2/categories | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/unified-api/conversations/v1/client/unreceived\_mass\_messages | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/sdk/refresh\_push\_info | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/client/ | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/client/inputting | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/client/client\_events | com/meiqia/core/MQManager.java |
| https://new-api.meiqia.com/client/tickets\_v2/ | com/meiqia/core/w.java |
| https://new-api.meiqia.com/unified-api/conversations/v1/client/sdk/mass\_messages/ | com/meiqia/core/g0.java |
| https://new-api.meiqia.com/client/device\_token | com/meiqia/core/g0.java |
| https://new-api.meiqia.com/client/prechat-survey-msg | com/meiqia/core/g0.java |
| https://new-api.meiqia.com/scheduler | com/meiqia/core/f0.java |
| https://notify.bugsnag.com | com/meiqia/core/k0.java |
| http://meiqia.com/ | com/meiqia/core/k0.java |
| http://www.slf4j.org/codes.html | i/b/d.java |
| http://www.slf4j.org/codes.html | i/b/c.java |
| http://logback.qos.ch/codes.html | i/b/c.java |
| https://yde-sz.oss-accelerate.aliyuncs.com/vv/ | 摸瓜V1引擎 |
| https://yde-hk.oss-accelerate.aliyuncs.com/vv/ | 摸瓜V1引擎 |
| https://yde-t-1327923657.cos.ap-guangzhou.myqcloud.com/vv/ | 摸瓜V1引擎 |
| https://yde-doc-img.s3.ap-east-1.amazonaws.com/vv/ | 摸瓜V1引擎 |

### **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=CN, ST=安徽, L=马鞍山, O=zhanle, OU=renshi, CN=chentian 签名算法: rsassa\_pkcs1v15 有效期自: 2025-03-23 13:08:11+00:00 有效期至: 2027-12-18 13:08:11+00:00 发行人: C=CN, ST=安徽, L=马鞍山, O=zhanle, OU=renshi, CN=chentian 序列号: 0x31914f99 哈希算法: sha256 md5值: e489d11bc54121e10e205f1a76d07efe sha1值: 001b4aa46e51c1bd5fa57d165403e42cd044d6f3 sha256值: 56edfbaa65692bfc39d10f2a2f2426809ec261d4c6ec5b31d0fd55a261397ef1 sha512值: 99c3debea483c63e25336de573c30f24945ab450f700b3bcad8c4a693b8664d6f34fcfe3595faafb1ff6488acdc7e7f1e32102a4c176b709e686398abe9b3c64 公钥算法: rsa 密钥长度: 2048 指纹: 9db987a0a8f0e8d223f650755ef3351b928a3dcecb4f5bd9a19540d3032dbdd2**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "mq\_auth\_code" : "验证码" |
| "mq\_auth\_code" : "CAPTCHA" |
| "mq\_auth\_code" : "Kode verifikaso" |
| "mq\_auth\_code" : "Kod pengesahan" |
| "mq\_auth\_code" : "驗證碼" |

## **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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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.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\_DOWNLOAD\_MANAGER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_DOWNLOAD\_MANAGER\_ADVANCED | 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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |

## **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。**