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

**优趣商店（ 2.0.5.110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 | 优趣商店 |
| 版本 | 2.0.5.110 |
| 包名 | com.yqusoft.appstore |
| 域名线索 | 2条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年5月22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 | 优趣商店.apk |
| 文件大小 | 8.78MB |
| MD5值 | 273b27051526ed5d93163bfd9ff1c583 |
| SHA1值 | 9b0a5e0a08fe74964e6d0d2d5a8950620aadfa25 |
| SHA256值 | d888fb9cc3c20f9c625dbb889eb8aca903aed1a68a57b902eb3c6ca716179766 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 优趣商店 |
| 包名 | com.yqusoft.appstore |
| 主活动Activity | cn.mycarsoft.store.SplashActivity |
| 安卓版本名称 | 2.0.5.110 |
| 安卓版本 | 25 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| errlogos.umeng.com | IP: 47.246.110.18 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| errlog.umeng.com | IP: 223.109.148.180 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://errlog.umeng.com/api/crashsdk/logcollect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlogos.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | lib/x86/libcrashsdk.so  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | lib/x86/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/x86/libcrashsdk.so  |
| https://errlogos.umeng.com  | lib/x86/libcrashsdk.so  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | lib/arm64-v8a/libcrashsdk.so  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | lib/arm64-v8a/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/arm64-v8a/libcrashsdk.so  |
| https://errlogos.umeng.com  | lib/arm64-v8a/libcrashsdk.so  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | lib/armeabi/libcrashsdk.so  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | lib/armeabi/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/armeabi/libcrashsdk.so  |
| https://errlogos.umeng.com  | lib/armeabi/libcrashsdk.so  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: False Found 1 unique certificates Subject: C=CN, ST=福建, L=厦门, O=优趣软件, OU=福建优趣软件有限公司, CN=张锦祥 Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2020-09-14 04:23:18+00:00 Valid To: 2045-09-08 04:23:18+00:00 Issuer: C=CN, ST=福建, L=厦门, O=优趣软件, OU=福建优趣软件有限公司, CN=张锦祥 Serial Number: 0x2de9113b Hash Algorithm: sha1 md5: 7454397eba53c570b694e07c369f1f41 sha1: 1fe06d5d3891e732c1417273d578b18da2698f19 sha256: b9de5cbe5b37fdd13d87ad11d734e28644266ff8e5c29bea7d6323549b2025d5 sha512: 65774b20a62fe27c1a7d90e7805f574ee90f4266394948958e02cd7ec0838cd2f1bd2cb33d275f507ed057675d31a8150bcf047bf82ea607cc46adddaf6b6937 PublicKey Algorithm: rsa Bit Size: 1024 Fingerprint: cda44b04e1a9d65d51e17be1bf8f6a7f1f6fb3eaf79ec5be2aaf30aa75e81a1d**

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.PROCESS\_OUTGOING\_CALLS | 危险 | 拦截拨出电话 | 允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话 |
| 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\_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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**