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

**XB-yun（ 1.4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 | XB-yun |
| 版本 | 1.4 |
| 包名 | com.weideapp.yufeng |
| 域名线索 | 18条 |
| URL线索 | 27条 |
| APP图标 |  |
| 分析日期 | 2025年1月29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 | 7.54MB |
| MD5值 | fffb5094993502f2bce2f2807ae45ea1 |
| SHA1值 | feb08ebceb8cfc67da319d88fb8ef5bc77891924 |
| SHA256值 | f7d73e5eafc87f895cf17486461d2999a3ca1de23d64e323b33c7ee6507fb7af |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | XB-yun |
| 包名 | com.weideapp.yufeng |
| 主活动Activity | com.jiazheng.app.ui.activity.SplashActivity |
| 安卓版本名称 | 1.4 |
| 安卓版本 | 4 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| lark.alipay.com | IP: 119.42.230.126 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| upload.qiniu.com | IP: 115.231.27.138 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cmnsguider.yunos.com | IP: 203.119.169.246 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.umeng.com | IP: 59.82.29.248 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| app-router.com | IP: 106.75.98.168 所属国家: China 地区: Beijing 城市: Beijing  |
| www.paycashin.com | IP: 34.102.136.180 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| console-mock.apipost.cn | IP: 39.103.217.160 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogus.umeng.com | IP: 223.109.148.178 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: United States of America 地区: Washington 城市: Redmond  |
| alogsus.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Beijing 城市: Beijing  |
| greenrobot.org | IP: 85.13.129.145 所属国家: Germany 地区: Thuringen 城市: Friedersdorf  |
| s.s.s | 没有服务器地理信息.  |
| litengweb.top | IP: 156.232.191.194 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| plbslog.umeng.com | IP: 36.156.202.73 所属国家: China 地区: Beijing 城市: Beijing  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| ulogs.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umengcloud.com | IP: 223.109.148.177 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://greenrobot.org/greendao/documentation/database-encryption/  | org/greenrobot/greendao/database/DatabaseOpenHelper.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://app-router.com  | cn/leancloud/core/AppRouter.java  |
| http://upload.qiniu.com  | cn/leancloud/upload/QiniuAccessor.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SlidingTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SegmentTabLayout.java  |
| http://litengweb.top/privacy.html  | com/panda/basework/dialog/ProtocolDialog.java  |
| http://litengweb.top/privacy.html  | com/panda/basework/activity/AboutmeActivity.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com/unify\_logs  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com/unify\_logs  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com/unify\_logs  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com/unify\_logs  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://cmnsguider.yunos.com:443/genDeviceToken  | com/umeng/commonsdk/statistics/idtracking/s.java  |
| https://lark.alipay.com/yj131525/byt0wl/ufnf3i  | com/umeng/commonsdk/statistics/internal/c.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://developer.umeng.com/docs/66632/detail/70018?um\_channel=sdk  | com/umeng/analytics/b.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/h.java  |
| https://www.paycashin.com/api/v6/public/index.php/  | com/jiazheng/app/utils/GlideUtils.java  |
| https://console-mock.apipost.cn/app/mock/project/4aa4ef39-59bd-480e-8e26-ce4c6d963e4d/XBYUN  | com/jiazheng/app/ui/activity/SplashActivity.java  |
| https://www.paycashin.com/api/v6/public/index.php/  | com/jiazheng/app/network/RetrofitManager.java  |
| https://www.paycashin.com/api/v6/public/index.php/  | com/jiazheng/app/network/SystemConst.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13812341234  | com/jiazheng/app/base/MyApplication.java  |

## **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=SZ, ST=GD, L=shenzhen, O=fushineng, OU=fushineng, CN=fushineng 签名算法: rsassa\_pkcs1v15 有效期自: 2018-04-11 09:28:26+00:00 有效期至: 2078-03-27 09:28:26+00:00 发行人: C=SZ, ST=GD, L=shenzhen, O=fushineng, OU=fushineng, CN=fushineng 序列号: 0x32ccdfc5 哈希算法: sha256 md5值: cc198c53ca6e7056f88f09239ff89ff3 sha1值: f094dff37c18e057fb37af5d9524eabf1ac8b73e sha256值: 2192df8a1da4426b137064ec17bbedd732009f6f28b7628be36fcc19ec313819 sha512值: 2516623390dfdb8054996a9c3e20c099a29c392c9c70a9817cd9fdcfeba3ecd186e7a807fe7adeb460958dbc4593e969b3763f7d339b909b758ac5a37c06240d 公钥算法: rsa 密钥长度: 2048 指纹: 99f5a55381f87d3fec3167e44fc1451930c50710431a81a3f438347e53abdc22**

## **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.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.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\_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.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\_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.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 |

## **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。**