MoGua

XB-yun 1.4.APK 分析报告

APP名称: XB-yun

包名:	com.weideapp.yufeng
域名线索:	18条
URL线索:	27条
邮箱线索:	0条
分析日期:	2025年1月29日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 7.54MB
MD5值: fffb5094993502f2bce2f2807ae45ea1
SHA1值: feb08ebceb8cfc67da319d88fb8ef5bc77891924
SHA256值: f7d73e5eafc87f895cf17486461d2999a3ca1de23d64e323b33c7ee6507fb7af

APP 信息

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

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 **纬度**: 30.293650 **经度**: 120.161423
upload.qiniu.com	**IP**: 115.231.27.138 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
cmnsguider.yunos.com	**IP**: 203.119.169.246 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397232
developer.umeng.com	IP: 59.82.29.248 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
app-router.com	IP: 106.75.98.168 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.paycashin.com	IP: 34.102.136.180 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
console-mock.apipost.cn	IP: 39.103.217.160 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
alogus.umeng.com	IP: 223.109.148.178 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

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 **纬度**: 47.682899 **经度**: -122.120903
alogsus.umeng.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
greenrobot.org	**IP**: 85.13.129.145 **所属国家**: Germany **地区**: Thuringen **城市**: Friedersdorf **纬度**: 50.604919 **经度**: 11.035770
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 **纬度**: 22.285521 **经度**: 114.157692
plbslog.umeng.com	**IP**: 36.156.202.73 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

ouplog.umeng.com	**IP**: 47.246.110.93 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
ulogs.umeng.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
ulogs.umengcloud.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

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

邮箱线索

手机线索

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

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

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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

应用内通信