MoGua

省心素材 5.1.0.APK 分析报告

APP名称:	省心素材
包名:	com.xliang.shengxin
域名线索:	39条
URL线索:	44条
邮箱线索:	2条
分析日期:	2023年3月23日
分析平台:	摸瓜反编译平台

文件信息

文件名: sxsc_238172.apk
文件大小: 20.52MB
MD5值: a140ae060203ffc241fcb1a6af017344
SHA1值: 34fa08f258548492b45a91de80781aa13710f302
SHA256值: c470140841e7007774c4b246f31db37a35abf0c09f6f08e01f73255d7a4984d9

APP 信息

App名称: 省心素材
包名: com.xliang.shengxin
主活动**Activity:** com.xliang.shengxin.SplashActivity
安卓版本名称: 5.1.0
安卓版本: 510

域名线索

域名	服务器信息
long.open.weixin.qq.com	**IP:** 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

域名	服务器信息
www.xlgogo.com	**IP:** 124.236.110.213 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041389 经度: 114.478607
api-e189.21cn.com	**IP:** 222.93.106.185 所属国家: China 地区: Jiangsu 城市: Suzhou 纬度: 31.311390 经度: 120.618057
wap.cmpassport.com	**IP:** 120.197.235.27 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
appgo.189.cn	**IP:** 116.211.180.138 所属国家: China 地区: Hubei 城市: Wuhan 纬度: 30.583330 经度: 114.266670

域名	服务器信息
astat.bugly.qcloud.com	**IP:** 150.109.27.253 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067
astat.bugly.cros.wr.pvp.net	**IP:** 170.106.135.32 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
open.e.189.cn	**IP:** 42.123.76.52 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
sxapi23.xlgogo.com	**IP:** 123.56.98.107 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

域名	服务器信息
sdk.sms.jpush.cn	**IP:** 124.71.228.157 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000
mobilegw.alipay.com	**IP:** 203.209.250.2 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423
tulu-app.artron.net	**IP:** 81.70.127.121 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
sdkapi-smartop.jiguang.cn	没有服务器地理信息.
h5.m.taobao.com	**IP:** 124.238.245.243 **所属国家:** China **地区:** Hebei **城市:** Langfang **纬度:** 39.509720 **经度:** 116.694717

域名	服务器信息
xml.apache.org	**IP:** 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
opencloud.wostore.cn	**IP:** 116.128.209.136 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061
android.bugly.qq.com	**IP:** 109.244.244.137 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
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

域名	服务器信息
open.weixin.qq.com	**IP:** 175.24.219.72 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
upload-z2.qiniup.com	**IP:** 111.225.212.227 **所属国家:** China **地区:** Hebei **城市:** Langfang **纬度:** 39.509720 **经度:** 116.694717
mobilegw.aaa.alipay.net	没有服务器地理信息.
mp.weixin.qq.com	**IP:** 175.24.219.72 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
auth.wosms.cn	**IP:** 123.125.99.37 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232

域名	服务器信息
h.trace.qq.com	**IP:** 109.244.244.241 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
mclient.alipay.com	**IP:** 220.181.135.237 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
adata.chanwind.com	**IP:** 47.94.223.149 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423
e.189.cn	**IP:** 42.123.76.65 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
mobilegw.stable.alipay.net	没有服务器地理信息.

域名	服务器信息
ce3e75d5.jpush.cn	**IP:** 183.232.58.249 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000
work.weixin.qq.com	**IP:** 106.55.127.35 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
mcgw.alipay.com	**IP:** 220.181.135.237 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
mobilegw.alipaydev.com	**IP:** 110.75.132.131 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423

域名	服务器信息
sdk.verification.jiguang.cn	**IP:** 114.116.218.106 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
ctaccount.21cn.com	**IP:** 222.93.104.15 **所属国家:** China **地区:** Jiangsu **城市:** Suzhou **纬度:** 31.311390 **经度:** 120.618057
wappaygw.alipay.com	**IP:** 220.181.135.237 **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.
id6.me	**IP:** 42.123.77.138 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232

域名	服务器信息
m.alipay.com	**IP:** 203.209.245.74 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423

URL线索

URL信息	Url所在文件
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
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
https://sdkapi-smartop.jiguang.cn	cn/jiguang/be/c.java
https://sdk.sms.jpush.cn	cn/jiguang/verifysdk/f/d/a.java
https://ctaccount.21cn.com/agreementList.html?hidetop=true&appKey=	cn/jiguang/verifysdk/e/m.java
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	cn/jiguang/verifysdk/e/m.java
https://wap.cmpassport.com/resources/html/contract.html	cn/jiguang/verifysdk/e/m.java
https://auth.wosms.cn	cn/jiguang/verifysdk/e/a/a/e/a.java
https://id6.me/auth/preauth.do	cn/jiguang/verifysdk/e/a/a/b/b.java
https://sdk.verification.jiguang.cn/config/ver/v4/android	cn/jiguang/verifysdk/b/a.java
https://upload-z2.qiniup.com	cn/jiguang/bf/a.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/ax/c.java
https://ce3e75d5.jpush.cn/wi/d8n3hj	cn/jiguang/ax/c.java
https://ce3e75d5.jpush.cn/wi/op8jdu	cn/jiguang/s/c.java
https://open.e.189.cn/openapi/special/getTimeStamp.do	cn/com/chinatelecom/account/api/e/h.java
https://api-e189.21cn.com/gw/client/accountMsg.do	cn/com/chinatelecom/account/api/e/h.java

URL信息	Url所在文件
https://www.xlgogo.com/pages/sucaisx/downloadDetail?id=	com/ylb/home/viewmodel/SuCaiPkgViewModel.java
https://www.xlgogo.com/pages/sucaisx/downloadDetail?id=	com/ylb/mine/viewmodel/MaterialViewModel.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
https://sxapi23.xlgogo.com	com/xliang/shengxin/BuildConfig.java
https://adata.chanwind.com/app/event	com/xliang/shengxin/base/api/BaseApi.java
https://www.xlgogo.com/pages/sucaisx/commonGuide	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/contact	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/downloadDetail	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/downloadError	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/downloadGuide	com/xliang/shengxin/base/common/Constants.java

URL信息	Url所在文件
https://www.xlgogo.com/pages/sucaisx/homeGuide	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/shangjia/contact	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/md5Guide	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/privacy	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/shareAPP	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/protocol	com/xliang/shengxin/base/common/Constants.java
https://www.xlgogo.com/pages/sucaisx/waterGuide	com/xliang/shengxin/base/common/Constants.java
https://work.weixin.qq.com/kfid/kfc945b5f0fb19a0ca3?enc_scene=ENCHgMzi3VrqcsXMz2s2m72m8	com/xliang/shengxin/base/common/Constants.java
http://wap.cmpassport.com/resources/html/contract.html	com/cmic/sso/sdk/activity/LoginAuthActivity.java
https://e.189.cn/sdk/agreement/detail.do	com/cmic/sso/sdk/activity/LoginAuthActivity.java
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	com/cmic/sso/sdk/activity/LoginAuthActivity.java
http://xml.apache.org/xslt	com/orhanobut/logger/LoggerPrinter.java
https://opencloud.wostore.cn/openapi/netauth/precheck/wp?	com/unicom/xiaowo/account/shield/d/b.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java

URL信息	Url所在文件
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/d.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://appgo.189.cn:9031	com/ct/auth/b/a.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/M.java
https://mp.weixin.qq.com/publicpoc/opensdkconf? action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s	com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java

URL信息	Url所在文件
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
http://tulu-app.artron.net/static/class/020100000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/020300000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/020400000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/020500000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/020600000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/020700000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/020800000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/020900000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/021000000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/020200000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/021200000000@3x.png	Mogua Engine V2
http://tulu-app.artron.net/static/class/021300000000@3x.png	Mogua Engine V2

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java
020100000000@3x.png 020300000000@3x.png 020400000000@3x.png 020500000000@3x.png 020600000000@3x.png 020700000000@3x.png 020800000000@3x.png 020900000000@3x.png 021000000000@3x.png 020200000000@3x.png 021200000000@3x.png 021300000000@3x.png	Mogua Engine V2

手机线索

手机号	所在文件
18612345678	com/ylb/mine/viewmodel/MineViewModel.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.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: CN=shengxin
签名算法: rsassa_pkcs1v15
有效期自: 2022-07-26 07:24:08+00:00
有效期至: 2047-07-20 07:24:08+00:00
发行人: CN=shengxin
序列号: 0x418fe29b
哈希算法: sha256
md5值: 5f6de55446fd63fda765311dc7a03eec
sha1值: 16965d711e08ed0853682dab835c558967722fa3
sha256值: 7aa00d10752482f6a3fdcbe5e1e5a7b0ba78b3fbfc056418a18b3a9dd7afdddb
sha512值: 0560299d9e58b631dfea6ccbe93180d89cf726ea795ac6d5be1cfebb2dc1bdc6a17e7496de174e39ffb27731076e0512d3916327c49695da991f617cf39fda95
公钥算法: rsa
密钥长度: 2048
指纹: 68845b946e6ade9cb1ff48b51a2d70208cde998e04a1509d02bf8a040987c424

硬编码敏感信息

可能的敏感信息
"BG_PATH_KEY" : "BG_PATH_KEY"
"CHOOSE_PRE_INSTALLED_MODEL_KEY" : "CHOOSE_PRE_INSTALLED_MODEL_KEY"
"CPU_POWER_MODE_KEY" : "CPU_POWER_MODE_KEY"
"CPU_THREAD_NUM_KEY" : "CPU_THREAD_NUM_KEY"
"ENABLE_CUSTOM_SETTINGS_KEY" : "ENABLE_CUSTOM_SETTINGS_KEY"

可能的敏感信息
"IMAGE_PATH_KEY" : "IMAGE_PATH_KEY"
"INPUT_COLOR_FORMAT_KEY" : "INPUT_COLOR_FORMAT_KEY"
"INPUT_SHAPE_KEY" : "INPUT_SHAPE_KEY"
"MODEL_PATH_KEY" : "MODEL_PATH_KEY"
"load_no_authority" : "不好意思，您暂无查看权限！"
"no_authority" : "不好意思，您无权限操作！"

加壳分析

加壳类型	所属文件
腾讯Bugly	lib/arm64-v8a/libBugly.so
腾讯Bugly	libBugly.so

第三方SDK

名称	分类	URL链接
Bugly	数据分析	https://reports.exodus-privacy.eu.org/trackers/190

名称	分类	URL链接
fastjson	开发辅助	https://reports.exodus-privacy.eu.org/trackers/457
支付宝	身份识别, 支付平台, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/445
极光推送	数据分析	https://reports.exodus-privacy.eu.org/trackers/343
腾讯微信	身份识别, 支付平台, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/447

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

向手机申请的权限	是否危险	类型	详细情况
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.READ_PRIVILEGED_PHONE_STATE	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

向手机申请的权限	是否危险	类型	详细情况
android.permission.READ_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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
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。
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

应用内通信