MoGua

速信花 1.0.2.APK 分析报告

APP名称:	速信花

包名:	com.design.ridemicrocredit4
域名线索:	42条
URL线索:	33条
邮箱线索:	1条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: suxinghua.apk
文件大小: 15.56MB
MD5值: b7b64c7920a03bbda9369d53796de0b0
SHA1值: b89013a42af8a3315a069966ffa8a8282543e017
SHA256值: 93de0b3c40f76d6ff3ff202ad9dfc2b67a55e8757b4c315f310af69a65d04d76

APP 信息

App名称: 速信花
包名: com.design.ridemicrocredit4
主活动Activity: com.design.ridemicrocredit4.activity.SplashActivity
安卓版本名称: 1.0.2
安卓版本: 1

域名线索

域名	服务器信息
180.168.100.155	**IP**: 180.168.100.155 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
youtu.api.qcloud.com	**IP**: 62.234.200.11 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.geetest.com	**IP**: 60.28.220.193 **所属国家**: China **地区**: Tianjin

	城市: Tianjin **纬度**: 39.142181 **经度**: 117.176102
sxh008.7rdai.com	**IP**: 128.242.240.221 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
schemas.android.com	没有服务器地理信息.
pest.w3.org	没有服务器地理信息.
las.udcredit.com	没有服务器地理信息.
aip.baidubce.com	**IP**: 111.206.210.12 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.youtu.qq.com	**IP**: 157.255.220.211 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
schemas.xmlsoap.org	**IP**: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

mobilegw.alipay.com	**IP**: 203.209.245.129 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
idsafe-auth.udcredit.com	没有服务器地理信息.
xmlpull.org	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
mobilegw.aaa.alipay.net	没有服务器地理信息.
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
www.beijing-time.org	**IP**: 60.205.124.229 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
10.1.30.51	**IP**: 10.1.30.51 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
mpay.fuiou.com	**IP**: 211.147.68.136 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333

	经度: 121.468948
www-1.fuiou.com	IP: 180.168.100.155 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
static.geetest.com	IP: 116.162.169.116 **所属国家**: China **地区**: Hunan **城市**: Loudi **纬度**: 27.734440 **经度**: 111.994850
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
mcgw.alipay.com	IP: 111.202.5.209 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ccdcapi.alipay.com	IP: 203.209.245.120 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 111.202.5.210 **所属国家**: China

wappaygw.alipay.com	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
verify.baidubce.com	IP: 153.3.238.231 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
h5.m.taobao.com	IP: 60.9.1.94 **所属国家**: China **地区**: Hebei **城市**: Hengshui **纬度**: 37.732220 **经度**: 115.701157
mobilegw.stable.alipay.net	没有服务器地理信息.
api.geetest.com	IP: 103.143.17.142 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
static.udcredit.com	没有服务器地理信息.
mclient.alipay.com	IP: 1.190.42.122 **所属国家**: China **地区**: Heilongjiang **城市**: Harbin **纬度**: 45.750000 **经度**: 126.650002
	IP: 104.18.22.19 **所属国家**: United States of America

www.w3.org	**地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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**: 120.161583
192.168.0.170	**IP**: 192.168.0.170 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
m.alipay.com	**IP**: 203.209.245.120 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
app.7ydai.com	没有服务器地理信息.
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
www.cs.caltech.edu	**IP**: 131.215.140.31 **所属国家**: United States of America **地区**: California **城市**: Pasadena

	纬度: 34.135864 **经度**: -118.123734
qr.alipay.com	IP: 203.209.245.120 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
vip-api.youtu.qq.com	没有服务器地理信息.
fingerprint.udcredit.com	没有服务器地理信息.
gotest.7rdai.com	IP: 199.16.158.190 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
paygate-yf.meituan.com	IP: 101.236.69.63 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL**信息**	Url**所在文件**
https://github.com/Zielony/Carbon/issues.	carbon/Carbon.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java

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://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/c.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&	com/alipay/sdk/data/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/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.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple\	com/alipay/test/a.java
https://aip.baidubce.com/rest/2.0/ocr/v1/bankcard?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/idcard?	com/baidu/ocr/sdk/OCR.java
https://verify.baidubce.com/verify/1.0/token/sk?sdkVersion=1_3_3	com/baidu/ocr/sdk/OCR.java
https://verify.baidubce.com/verify/1.0/token/bin?sdkVersion=1_3_3	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/general_basic?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/general?	com/baidu/ocr/sdk/OCR.java

https://aip.baidubce.com/rest/2.0/ocr/v1/business_license?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/driving_license?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/general_enhanced?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/webimage?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/license_plate?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/receipt?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/vehicle_license?	com/baidu/ocr/sdk/OCR.java
https://verify.baidubce.com/verify/1.0/sdk/report	com/baidu/ocr/sdk/utils/CrashReporterHandler.java
https://fingerprint.udcredit.com/front/4.0/collect/platform/android/	com/authreal/m.java
https://las.udcredit.com/front/las/4.0/log/post_log/processor/idsafe_front	com/authreal/k.java
https://static.udcredit.com/id/idsafeUserAgreement.html?data=	com/authreal/ui/SuperActivity.java
http://10.1.30.51:8000/static/idsafeHelpCenter.html?time=	com/authreal/ui/d.java
https://static.udcredit.com/id/idsafeHelpCenter.html?time=	com/authreal/ui/d.java
https://fingerprint.udcredit.com/front/4.0/	com/authreal/util/d.java
https://idsafe-auth.udcredit.com/front/4.0/	com/authreal/util/d.java
http://192.168.0.170:801/index.php/api	com/design/ridemicrocredit4/okhttp/https/form/FormParams.java
http://xml.apache.org/xslt	com/design/ridemicrocredit4/okhttp/utils/log/LoggerPrinter.java
https://youtu.api.qcloud.com/youtu/	com/design/ridemicrocredit4/youtu/Youtu.java

https://vip-api.youtu.qq.com/youtu/	com/design/ridemicrocredit4/youtu/Youtu.java
http://api.youtu.qq.com/youtu/	com/design/ridemicrocredit4/youtu/Youtu.java
https://sxh008.7rdai.com/	com/design/ridemicrocredit4/config/Constant.java
http://app.7ydai.com:9999/page/index/alipayZhiMaNotify?	com/design/ridemicrocredit4/config/Constant.java
https://gotest.7rdai.com/api/udCredit/notify	com/design/ridemicrocredit4/config/Constant.java
https://ccdcapi.alipay.com/validateAndCacheCardInfo.json?_input_charset=utf-8&cardNo=	com/design/ridemicrocredit4/config/Constant.java
https://qr.alipay.com/_d?_b=PAI_LOGIN_DY&securityId=web%257Cauthcenter_qrcode_login%257C7c69672d-a66d-492b-895e-d0727e12fef2RZ14	com/design/ridemicrocredit4/activity/AlipayAuthorizedActivity.java
http://www.beijing-time.org/wannianli.htm	com/design/ridemicrocredit4/activity/WanNianLiActivity.java
http://180.168.100.155:14652/mobile_pay/applePay/backNotify.pay	com/fuiou/mobile/util/AppConfig.java
https://mpay.fuiou.com:16128/	com/fuiou/mobile/http/HttpConfig.java
http://www-1.fuiou.com:18670/mobile_pay/	com/fuiou/mobile/http/HttpConfig.java
http://static.geetest.com/static/appweb/app3-index.html	com/geetest/sdk/O00000o0.java
https://static.geetest.com/static/appweb/app3-index.html	com/geetest/sdk/O00000o0.java
https://api.geetest.com/gettype.php?gt=	com/geetest/sdk/O000000.java
https://api.geetest.com/get.php?gt=	com/geetest/sdk/O00O0Oo.java
http://www.geetest.com/first_page	com/geetest/sdk/GT3GeetestButton.java
http://static.geetest.com/static/appweb/app3-index.html	com/geetest/sdk/Bind/O00000Oo.java

https://static.geetest.com/static/appweb/app3-index.html	com/geetest/sdk/Bind/O00000Oo.java
https://api.geetest.com/gettype.php?gt=	com/geetest/sdk/Bind/O00000o0.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/b/a/a.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/b/a/e.java
http://www.cs.caltech.edu/	org/json/Test.java
http://schemas.xmlsoap.org/soap/envelope/\	org/json/Test.java
http://schemas.xmlsoap.org/soap/encoding/\	org/json/Test.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

邮箱线索

邮箱地址	所在文件
khare@mci.net adam@cs.caltech	org/json/Test.java

手机线索

手机号	所在文件
15555215554	com/authreal/n.java
15555215556	com/authreal/n.java
15555215558	com/authreal/n.java
15555215560	com/authreal/n.java
15555215562	com/authreal/n.java
15555215564	com/authreal/n.java
15555215566	com/authreal/n.java
15555215568	com/authreal/n.java
15555215570	com/authreal/n.java
15555215572	com/authreal/n.java
15555215574	com/authreal/n.java
15555215576	com/authreal/n.java
15555215578	com/authreal/n.java
15555215580	com/authreal/n.java
15555215582	com/authreal/n.java
15555215584	com/authreal/n.java
13910000003	com/fuiou/mobile/util/MD5UtilString.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: OU=huohu, CN=huohu
签名算法: rsassa_pkcs1v15
有效期自: 2018-09-09 12:31:27+00:00
有效期至: 2043-09-03 12:31:27+00:00
发行人: OU=huohu, CN=huohu
序列号: 0x43c2aeaf
哈希算法: sha256
md5值: bf3ab3b21890692465a79abf6197b743
sha1值: 8ae1273e7c28c4b75abf8f635b39d56da672ad5e
sha256值: 5f8bebbb6ed011aa2c55f10f6005dbde21a93f62733eb132e0826217aae4a5e5
sha512值: 0d0498a7f3900e4b10df61dd9ae73e553df9c4bf353c99cf37eacd25f9da4747731b9081d9b7442939edefae88a384f21f1f295938b84f6ec81a536a9f148598
公钥算法: rsa
密钥长度: 2048
指纹: 8057ac010a35a099c3c67691178142a205b5e5a7b4fcad7a6ff7490283dcbbd1

硬编码敏感信息

可能的敏感信息
"alipay_key_authorized" : "手机淘宝一键授权"
"bank_secret" : "银行级数据加密防护"
"book_auth_content" : "温馨提示 1.请使用您本人的手机授权。 2.提供通讯录信息，有助于您通过审核。 3.诚信回收将严格遵守协议，保护用户隐私"
"book_auth_tips" : "将手机通讯录授权于诚信回收平台"

"phone_auth_content" : "·电信手机号提交认证需要一次手机验证码，请注意查收 ·忘记密码可以拨打10000人工客服重置密码· ·认证需要2-3分钟，请耐心等待 ·若认证失败，提示系统繁忙，建议您在不同时间段进行多次尝试"
"super_face_auth_pass" : "稍后再认证人脸"
"super_make_username" : "请确认姓名"

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.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.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
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.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.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_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量

com.che.spider.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.design.ridemicrocredit4.activity.SplashActivity	Schemes: http://,

---