



MoGua

新社惠农 1.0.5.APK 分析报告



APP名称:

新社惠农

包名:	com.xx.zzdf
域名线索:	20条
URL线索:	24条
邮箱线索:	0条
分析日期:	2025年5月15日
分析平台:	摸瓜APK反编译平台

文件名: GR73525[1].apk
文件大小: 48.17MB
MD5值: 83b366a9e3ef188170ea2ba96f174904
SHA1值: 573ac87c30e16705d9b3f8aa46c1622ead565c69
SHA256值: e3c5e2fa55b19ee4532ee065e1735f082183016cb257c78244f032b216a8f9c6

i APP 信息

App名称: 新社惠农
包名: com.xx.zzdf
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.5
安卓版本: 105

🔍 域名线索

域名	服务器信息
www.google.com	IP: 31.13.112.9 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
api.xaccsp.top	IP: 154.38.66.160 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
43.248.100.19	IP: 43.248.100.19 所属国家: China 地区: Jiangsu

	城市: Zhenjiang 纬度: 32.209366 经度: 119.434372
at.alicdn.com	IP: 61.182.131.251 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
api.fuwxs.top	IP: 43.163.219.84 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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
api.sxinshe.top	IP: 154.38.66.202 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
ns.adobe.com	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
er.dcloud.net.cn	IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
images.weserv.nl	IP: 172.67.220.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
er.dcloud.io	没有服务器地理信息.
apis.map.qq.com	IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.chuinong.top	IP: 154.38.66.30 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521

	经度: 114.157692
quilljs.com	IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
m3w.cn	IP: 119.188.209.130 所属国家: China 地区: Shandong 城市: Zaozhuang 纬度: 34.864719 经度: 117.554169
ask.dcloud.net.cn	IP: 221.204.20.100 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
service.dcloud.net.cn	IP: 111.229.199.57 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
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java

https://ask.dcloud.net.cn/article/35627	b/a.java
https://ask.dcloud.net.cn/article/35877	b/a.java
https://er.dcloud.io/rv	d/c.java
https://er.dcloud.net.cn/rv	d/c.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.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
https://ask.dcloud.net.cn/article/283	j/b.java
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎

http://feross.org >	摸瓜V2引擎
https://images.weserv.nl/?url=	摸瓜V2引擎
https://api.xaccsp.top	摸瓜V2引擎
http://43.248.100.19:2998	摸瓜V2引擎
https://api.sxinshe.top	摸瓜V2引擎
https://api.chuinong.top	摸瓜V2引擎
https://api.fuwxs.top	摸瓜V2引擎
http://43.248.100.19:1998	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://feross.org/opensource >	摸瓜V2引擎
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf)	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎

 邮箱线索

 手机线索

手机号	所在文件
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: True
找到 1 个唯一证书
主题: C=chengdu, ST=chengdu, L=chengdu, O=rn1743496384256, OU=gq1743496384256, CN=vhlv
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-01 08:33:04+00:00
有效期至: 2075-03-20 08:33:04+00:00
发行人: C=chengdu, ST=chengdu, L=chengdu, O=rn1743496384256, OU=gq1743496384256, CN=vhlv
序列号: 0x59647cff
哈希算法: sha1
md5值: 04f06cb3a1ee1e12c623e35090a0a078
sha1值: 566714179cf6921e0fb9136ba001cc7ee7f2282e
sha256值: 669495405ff170fa3dcdd7b15db9dafb37a65789f26e9010cff97d2faa8c67dd
sha512值: 5006b74b490bfcb8a57cb632f61773cf5a7dc1e7580905802edbea3c5c7bb854d4156aa95889b56827f43c1110bc66f16f32716830f557bc0bdf1dac41e2ee
公钥算法: rsa
密钥长度: 1024
指纹: e0aa647b2c8dfb6a9dabcd57067c248faac3fad74ae4b2f070e11d0d77f72fdf

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"

"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"
"dcloud_tips_certificate" : "证书"

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.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_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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
		允许应用程序请	

android.permission.REQUEST_INSTALL_PACKAGES	危险	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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.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。

应用内通信