



MoGua

寻欢阁 1.1.0.APK 分析报告



APP名称:

寻欢阁

包名:	com.xhg2017.app
域名线索:	21条
URL线索:	30条
邮箱线索:	0条
分析日期:	2025年5月19日
分析平台:	摸瓜APK反编译平台

文件名: xhg2023.apk
文件大小: 24.06MB
MD5值: c53308e7c410369e1ace5d8cb42cb094
SHA1值: 4a744da4be16d4975fe57251acfb374a26da504f
SHA256值: fadb50c55e3e64f0ec3d4fb3ba810e1dae74c2ba15608c574e9c8acdfc341067

i APP 信息

App名称: 寻欢阁
包名: com.xhg2017.app
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.1.0
安卓版本: 110

🔍 域名线索

域名	服务器信息
service.dcloud.net.cn	IP: 47.96.82.164 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
c-hzgt2.getui.com	IP: 115.227.15.15 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998
	IP: 106.39.240.45 所属国家: China 地区: Beijing

www.mescroll.com	城市: Beijing 纬度: 39.907501 经度: 116.397232
sdk-open-phone.getui.com	IP: 115.227.15.9 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998
stream.dcloud.net.cn	IP: 47.96.140.36 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
www.google.com	IP: 69.63.186.30 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690
lame.sf.net	IP: 104.18.26.198 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

stream.mobihtml5.com	IP: 112.80.255.152 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777779
er.dcloud.net.cn	IP: 47.97.228.179 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
restapi.amap.com	IP: 203.119.175.194 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ask.dcloud.net.cn	IP: 36.102.212.39 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
quilljs.com	IP: 216.24.57.3 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
schemas.android.com	没有服务器地理信息.
	IP: 134.122.164.254 所属国家: Japan 地区: Tokyo

www.21xhg.com	城市: Tokyo 纬度: 35.689507 经度: 139.691696
crbug.com	IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ns.adobe.com	没有服务器地理信息.
m3w.cn	IP: 36.102.212.34 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
d-gt.getui.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
apis.map.qq.com	IP: 109.244.244.109 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://stream.mobih5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/b.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.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
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
https://sdk-open-phone.getui.com/api.php	com/igexin/push/a.java

https://c-hzgt2.getui.com/api.php	com/igexin/push/a.java
https://d-gt.getui.com/api.htm	com/igexin/push/a.java
http://bi.	com/igexin/push/config/g.java
http://config.	com/igexin/push/config/g.java
http://bi.	com/igexin/push/config/b.java
http://config.	com/igexin/push/config/b.java
https://ask.dcloud.net.cn/article/36199	Mogua Engine V1
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	Mogua Engine V2
https://service.dcloud.net.cn/uniapp/feedback.html	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	Mogua Engine V2
https://www.google.com/maps/?daddr=	Mogua Engine V2
https://www.google.com/maps/	Mogua Engine V2
https://www.21xhg.com/	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2

https://restapi.amap.com/v3/geocode/regeo?parameters	Mogua Engine V2
https://restapi.amap.com/v3/weather/weatherInfo	Mogua Engine V2
https://www.21xhg.com/plugin.php?id=guiigo_appmanage&api=download	Mogua Engine V2
http://www.mescroll.com/img/mescroll-totop.png?v=1	Mogua Engine V2
http://www.mescroll.com/img/mescroll-empty.png?v=1	Mogua Engine V2
https://quilljs.com/	Mogua Engine V2
https://quilljs.com	Mogua Engine V2
https://www.21xhg.com/source/plugin/guiigo_appmanage/template/xyh5.htm\	Mogua Engine V2
https://www.21xhg.com/source/plugin/guiigo_appmanage/template/ysh5.htm\	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://www.21xhg.com/	Mogua Engine V2
https://crbug.com/v8/8520	lib/arm64-v8a/libweexjss.so
http://lame.sf.net	lib/arm64-v8a/liblamemp3.so

 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=CN, ST=xhg2017.com, L=xhg2017.com, O=xhg2017.com, OU=xhg2017.com, CN=xhg2017.com
签名算法: rsassa_pkcs1v15
有效期自: 2020-11-08 06:30:25+00:00
有效期至: 2120-10-15 06:30:25+00:00
发行人: C=CN, ST=xhg2017.com, L=xhg2017.com, O=xhg2017.com, OU=xhg2017.com, CN=xhg2017.com
序列号: 0x30917bd2
哈希算法: sha256
md5值: ee6d8fb22bc82b2ed9760567f7f74c01
sha1值: 770f3d59cd684e0d4004cfef548bb2e4f4f13ad3
sha256值: 8c5a4651d8b849c42905e756093098ef18aec614cd9049b6e26d703f9bb4fc4
sha512值: cf64eb6319950c69181ce1b9e32416f8c0ac463804e846f200de879f40f20f2939ee89e1715a80e270a534e46998b5483fc6bc632de31b40aea47351e15f9420
公钥算法: rsa
密钥长度: 2048
指纹: 904d21795a2f6a55edecbdea7f29e5b2337a1050a51b5f34b993b7a43ca43442

🔑 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_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"

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.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_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
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.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.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
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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_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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_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.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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
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
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
getui.permission.GetuiService.com.xhg2017.app	未知	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
com.vivo.notification.permission.BADGE_ICON	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。

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: unipush://, xhg2017://, xhg2017app://, Hosts: io.dcloud.unipush, Paths: /,

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。