



MoGua

小黄书™ 2.5.5.APK 分析报告



APP名称:

小黄书™

包名:	com.xhsyb.kankan
域名线索:	23条
URL线索:	30条
邮箱线索:	3条
分析日期:	2025年7月4日
分析平台:	摸瓜APK反编译平台

文件名: 小黄书™.apk
文件大小: 48.7MB
MD5值: d7b370aa5cd4cf1ea9ae99709c101300
SHA1值: e99b6b94e7091b745c989e6ae19ee9ca3f2d0994
SHA256值: c2f335e65f1885db2c8302e9fd7e11d14608f13a96eff1c0934bacece255251a

i APP 信息

App名称: 小黄书™
包名: com.xhsyb.kankan
主活动Activity: androidx.twoshare.TwoShareActivity
安卓版本名称: 2.5.5
安卓版本: 1

🔍 域名线索

域名	服务器信息
app.16769app.com	IP: 107.148.13.61 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.333698 经度: -121.889297
api.photoeditorsdk.com	IP: 35.190.50.119 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
docs.videoeditorsdk.com	IP: 151.101.1.195 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
docs.photoeditorsdk.com	IP: 151.101.65.195 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.
www.videoeditorsdk.com	IP: 151.101.1.195 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.android.com	IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
lsj6.lanzouq.com	IP: 36.99.200.132 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
www.smpte-ra.org	IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720

	经度: -77.487488
cdn.liudou.com	IP: 59.49.89.55 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.560280
app.langshilunzh.com	IP: 107.148.13.61 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.333698 经度: -121.889297
d.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
www.sl4j.org	IP: 83.173.251.158 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366669 经度: 8.550000
app.kangyankun.com	没有服务器地理信息.
app.vzvz.com	没有服务器地理信息.
xhs-app8888.firebaseio.com	IP: 34.120.160.131 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731

	经度: -94.578568
app.yinfangjituan.com	IP: 104.233.151.36 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.333698 经度: -121.889297
javax.xml.xmlconstants	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
app.vaavb.com	没有服务器地理信息.
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
www.photoeditorsdk.com	IP: 151.101.1.195 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
8.210.139.97	IP: 8.210.139.97 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521

URL线索

URL信息	Url所在文件
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	org/java_websocket/AbstractWebSocket.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html	org/slf4j/MDC.java
https://github.com/grpc/grpc-java/issues/5015	io/grpc/internal/ManagedChannelImpl.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://www.photoeditorsdk.com/login	ly/img/android/LicenseInvalidException.java
https://api.photoeditorsdk.com	ly/img/android/e.java

https://www.photoeditorsdk.com/login.	ly/img/android/f.java
https://developer.android.com/guide/practices/screens_support.html	ly/img/android/pesdk/backend/decoder/ImageSource.java
https://www.photoeditorsdk.com/signup	ly/img/android/pesdk/backend/model/state/manager/StateHandler.java
https://www.photoeditorsdk.com/pricing.	ly/img/android/pesdk/backend/model/state/manager/StateHandler.java
https://docs.photoeditorsdk.com/guides/android/v6/introduction/getting_started	ly/img/android/pesdk/backend/model/state/manager/StateHandler.java
https://www.videoeditorsdk.com/pricing.	ly/img/android/pesdk/backend/model/state/manager/StateHandler.java
https://docs.videoeditorsdk.com/guides/android/v6/introduction/getting_started	ly/img/android/pesdk/backend/model/state/manager/StateHandler.java
http://jaxax.xml.XMLConstants/feature/secure-processing	com/fasterxml/jackson/databind/ext/DOMDeserializer.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
http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	com/googlecode/mp4parser/authoring/tracks/SMPTETrackImpl.java
http://www.w3.org/ns/ttml	com/googlecode/mp4parser/authoring/tracks/SMPTETrackImpl.java
http://schemas.android.com/apk/res/android	com/xhsyb/kankan/view/SlidingTabLayout.java
http://cdn.liudou.com/avatar/202006/06/1591415289135.jpg?x-oss-	

process=image/resize,w_450	com/xhsyb/kankan/activity/SearchActivity.java
https://d.alipay.com	com/xhsyb/kankan/activity/WebViewActivity.java
http://8.210.139.97	com/xhsyb/kankan/activity/SplashActivity.java
https://lsj6.lanzouq.com/s/qmscs	com/xhsyb/kankan/activity/AdActivity.java
https://app.kangyankun.com\	com/xhsyb/kankan/http/RetrofitHttpUtil.java
https://app.yinfangjituan.com\	com/xhsyb/kankan/http/RetrofitHttpUtil.java
https://app.16769app.com\	com/xhsyb/kankan/http/RetrofitHttpUtil.java
https://app.vaavb.com\	com/xhsyb/kankan/http/RetrofitHttpUtil.java
https://app.vvzvz.com\	com/xhsyb/kankan/http/RetrofitHttpUtil.java
https://app.langshilunzh.com\	com/xhsyb/kankan/http/RetrofitHttpUtil.java
https://lsj6.lanzouq.com/s/qmscs	com/xhsyb/kankan/vod/VodReFragment.java
https://xhs-app8888.firebaseio.com	Mogua Engine V1

 邮箱线索

邮箱地址	所在文件
sales@photoeditorsdk.com	ly/img/android/LicenseInvalidException.java
sales@photoeditorsdk.com	ly/img/android/e.java

danikula@gmail.com	com/danikula/video/cache/HttpUrlSource.java
--------------------	---

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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

硬编码敏感信息

可能的敏感信息
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"enter_password" : "输入密码"
"firebase_database_url" : "https://xhs-app8888.firebaseio.com"
"forget_password" : "忘记密码"
"google_api_key" : "AlzaSyAG3p68PKDPxhrQJMwoSisCezwhawqbwE"
"google_crash_reporting_api_key" : "AlzaSyAG3p68PKDPxhrQJMwoSisCezwhawqbwE"
"login_pwd" : "登录密码"
"no_find_user" : "没有找到相关内容，换个词试试吧"
"notify_setting_private" : "私信通知"
"notify_setting_private_letter" : "私信"
"please_input_pwd" : "请输入密码"
"please_input_pwd_again" : "请再次输入密码"
"private_secutity" : "隐私设置"
"pwd_setting" : "設置密碼"
"reset_password" : "重置密码"
"seach_user" : "更多破解软件免费分享QQ群985421用户"
"two_pwd_not_same" : "两次密码不一致"

two_pwd_not_same . 两次密码不一致
"user" : "用户"
"withdraws" : "提现"
"com_facebook_device_auth_instructions" : "Besoek facebook.com/device en voer die kode wat hierbo gewys word, in."
"com_facebook_device_auth_instructions" : "وإدخال الرمز الموضح أعلاه facebook.com/device تفضل بزيارة"
"com_facebook_device_auth_instructions" : "facebook.com/device দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান।"
"com_facebook_device_auth_instructions" : "Přejděte na facebook.com/device a zadejte nahoře uvedený kód."
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og indtast koden, som er vist ovenfor."
"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."
"com_facebook_device_auth_instructions" : "Πηγαίνετε στη διεύθυνση facebook.com/device και εισαγάγετε τον παραπάνω κωδικό."
"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e introduce el código que se muestra más arriba."
"com_facebook_device_auth_instructions" : "Siirry osoitteeseen facebook.com/device ja anna oheinen koodi."
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "Accédez à facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "facebook.com/device नी मुलकात लो; अने उपर आपेले कोड दाखल करो."
"com_facebook_device_auth_instructions" : "facebook.com/device पर विज़िट करें और ऊपर दिखाया गया कोड डालें."
"com_facebook_device_auth_instructions" : "Posjetitw facebook.com/device i unesite gore prikazani kôd."

"com_facebook_device_auth_instructions" : "Keresd fel a facebook.com/device címet, és írd be a fent megjelenített kódot."
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di bawah ini."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e inserisci il codice mostrato qui sotto."
"com_facebook_device_auth_instructions" : "װלה״ן את הקוד המוצג למעלה facebook.com/device ולבקר בכתובת"
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"
"com_facebook_device_auth_instructions" : "facebook.com/device ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ."
"com_facebook_device_auth_instructions" : "facebook.com/device에 방문하여 위 코드를 입력하세요."
"com_facebook_device_auth_instructions" : "facebook.com/device സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക."
"com_facebook_device_auth_instructions" : "facebook.com/device भेट द्या आणि वरील कोड प्रविष्ट करा."
"com_facebook_device_auth_instructions" : "Lawati facebook.com/device dan masukkan kod yang ditunjukkan di atas."
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og skriv inn koden som vises over."
"com_facebook_device_auth_instructions" : "Ga naar facebook.com/device en voer de bovenstaande code in."
"com_facebook_device_auth_instructions" : "facebook.com/device 'ਤੇ ਵਿਜ਼ਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।"
"com_facebook_device_auth_instructions" : "Odwiedź stronę facebook.com/device i wprowadź powyższy kod."
"com_facebook_device_auth_instructions" : "Acesse facebook.com/device e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e insere o código apresentado abaixo."
"com_facebook_device_auth_instructions" : "Vizitează facebook.com/device și introdu codul de mai sus."

"com_facebook_device_auth_instructions" : "Откройте facebook.com/device и введите код, показанный выше."
"com_facebook_device_auth_instructions" : "Navštívte stránku facebook.com/device a zadajte kód zobrazený vyššie."
"com_facebook_device_auth_instructions" : "Gå till facebook.com/device och skriv in koden som visas ovan."
"com_facebook_device_auth_instructions" : "facebook.com/device ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்."
"com_facebook_device_auth_instructions" : "facebook.com/deviceని సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి."
"com_facebook_device_auth_instructions" : "ไปที่ facebook.com/device แล้วป้อนรหัสที่ปรากฏด้านล่าง"
"com_facebook_device_auth_instructions" : "Puntahan ang facebook.com/device at ilagay ang code na ipinapakita sa itaas."
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir."
"com_facebook_device_auth_instructions" : "Truy cập facebook.com/device và nhập mã được hiển thị bên trên."
"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"
"com_facebook_device_auth_instructions" : "前往facebook.com/device>，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "前往facebook.com/device>，並輸入上方顯示的代碼。"
"enter_password" : "輸入密碼"
"forget_password" : "忘記密碼"
"login_pwd" : "登錄密碼"
"no_find_user" : "沒有找到相關內容，換個詞試試吧"
"notify_setting_private" : "私信通知"

"notify_setting_private_letter" : "私信"
"please_input_pwd" : "請輸入密碼"
"please_input_pwd_again" : "請再次輸入密碼"
"private_secutity" : "隱私設置"
"pwd_setting" : "设置密码"
"reset_password" : "重置密碼"
"two_pwd_not_same" : "兩次密碼不一致"
"user" : "用戶"
"withdraws" : "提現"

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.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
	系		

android.permission.MODIFY_PHONE_STATE	统 需 要	修改电话状态	允许应用程序控制设备的电话功能。具有此权限的应用程序可以切换网络,打开和关闭电话收音机等,而无需通知您
com.android.providers.media.MediaProvider	未知	Unknown permission	Unknown permission from android reference
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.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。
ly.img.sdk.RECEIVE_RESULT_PERMISSION	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.xhsyb.kankan,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, 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。