MoGua

51萝莉 4.1.0.APK 分析报告

APP名称: 51萝莉

包名:	me.sixdq.rsrpxb
域名线索:	13条
URL线索:	18条
邮箱线索:	1条
分析日期:	2025年6月14日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: qd_4.1.0_250610_6.apk
文件大小: 15.9MB
MD5值: f673f188cddaa8d751ef4c5c3341b030
SHA1值: f86f0469ae234d847e071532ea8ea73d08263978
SHA256值: 0a613941aec1de48c0bc21bb2c61c1b2838ea4d318ec6e676adbdbae0275754c

APP 信息

App名称: 51萝莉
包名: me.sixdq.rsrpxb
主活动Activity: com.spaceseven.qidu.activity.SplashActivity
安卓版本名称: 4.1.0
安卓版本: 410

域名线索

域名	服务器信息
raw.githubusercontent.com	**IP**: 185.199.108.133 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
sapi01.xkpamyk.xyz	**IP**: 156.255.123.38 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
schemas.microsoft.com	**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
exoplayer.dev	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
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.
api.login.yahoo.com	**IP**: 74.6.160.138 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
dashif.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
schemas.android.com	没有服务器地理信息.
	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore

github.com	**城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
cfg.flurry.com	**IP**: 69.147.80.15 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
data.flurry.com	没有服务器地理信息.
www.example.com	**IP**: 23.193.186.17 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

URL线索

URL**信息**	Url**所在文件**
https://github.com/danikula/AndroidVideoCache/issues/88.	c/d/a/i.java
https://github.com/danikula/AndroidVideoCache/issues/43.	c/d/a/i.java
https://github.com/danikula/AndroidVideoCache/issues.	c/d/a/i.java
http://%s:%d/%s	c/d/a/k.java
https://github.com/danikula/AndroidVideoCache/issues/134.	c/d/a/k.java

http://%s:%d/%s	c/d/a/g.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	c/g/a/a/i2.java
https://x</LA_URL>	c/g/a/a/s2/i0.java
https://x	c/g/a/a/s2/i0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	c/g/a/a/s2/j0.java
http://dashif.org/guidelines/trickmode	c/g/a/a/z2/u0/f.java
http://dashif.org/guidelines/last-segment-number	c/g/a/a/z2/u0/m/d.java
http://dashif.org/guidelines/trickmode	c/g/a/a/z2/u0/m/d.java
http://ns.adobe.com/xap/1.0/	c/g/a/a/u2/h0/a.java
https://sapi01.xkpamyk.xyz/api.php,https://sapi02.xjargryv.xyz/api.php,https://sapi03.xkpamyk.xyz/api.php	c/n/a/m/x0.java
http://www.example.com	com/flurry/sdk/ed.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/cl.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/by.java
https://data.flurry.com/v1/flr.do	com/flurry/sdk/br.java
https://api.login.yahoo.com/oauth2/device_session	com/flurry/sdk/ef.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/PermissionUtils.java
https://raw.githubusercontent.com/little-5/backup/master/seven.txt	com/spaceseven/qidu/activity/SplashActivity.java
https://github.com/vinc3m1	摸瓜V1引擎

https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	c/d/a/i.java

手机线索

手机号	所在文件
17512775099	c/g/b/c/a.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: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
签名算法: rsassa_pkcs1v15

有效期自: 2025-06-10 23:46:29+00:00
有效期至: 2026-06-10 23:46:29+00:00
发行人: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
序列号: 0x1e7b8b74
哈希算法: sha256
md5值: cc636659f8b072efee50d0ba88d12b15
sha1值: 5a8d07fe5708560e847cfcc50dab1c181759ebc2
sha256值: e594a45bbfe93393a0739dedc972a39062981dbef4c832565676643c36d88466
sha512值: bc80ffd8faf0d83e8e0cdc9bfe93b55d88861886b5b6ba309d476ffd29da3feeffdf2c96045052f13814ee790f0561ae015c37e1e19e9624b686564bc031b0d5
公钥算法: rsa
密钥长度: 2048
指纹: 2502011a9c594b31e7b3aad076f1ed52a1fb7b1bf0391a2c0d50ac387fc77d32

硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"str_auth_apply" : "认证申请"
"str_input_account_user_name" : "请输入持卡人姓名"
"str_mod_pwd" : "修改密码"
"str_mod_pwd_success" : "密码修改成功"
"str_official_auth" : "官方认证"

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.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.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.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	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

		存储中的外部存储	户管理文件的应用程序使用
android.permission.READ_PRIVILEGED_PHONE_STATE	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.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_CLIPBOARD_IN_BACKGROUND	未知	Unknown permission	Unknown permission from android reference
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_CLIPBOARD	未知	Unknown permission	Unknown permission from android reference
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference

android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信
