



MoGua

PQLA 1.0.APK 分析报告



APP名称:

PQLA

包名:	sbhhd.pqbz.sdcc
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年3月15日
分析平台:	摸瓜APK反编译平台

文件名: sbhhd.pqbz.sdcc.apk

文件大小: 14.56MB

MD5值: f94aee6712ab5b458c6f6e6b5c75d154

SHA1值: be9d1d701e2e6ecd96e702254859f40fb739d42e

SHA256值: e36d4fb7888bf5763e2b6d47d9872bb03575dc5edf0f1de5b1b022683a494f81

APP 信息

App名称: PQLA

包名: sbhhd.pqbz.sdcc

主活动Activity: com.rummy.tttss.activity.SplashJavaActivity

安卓版本名称: 1.0

安卓版本: 1

域名线索

域名	服务器信息
qp1-1322631819.cos.ap	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://qp1-1322631819.cos.ap-	com/rummy/tttss/activity/SplashJavaActivity.java

邮箱线索

手机线索

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: CN=d

签名算法: rsassa_pkcs1v15

有效期自: 2023-12-16 05:51:45+00:00

有效期至: 2048-12-09 05:51:45+00:00

发行人: CN=d

序列号: 0x1

哈希算法: sha256

md5值: ded623bb846123d6113e66f124d7a506

sha1值: f1206ebe1e326aefd765bd36467f53572bf6fd43

sha256值: ced6dde56b7c43a17c50c5620e55161d82a984049b2af65c01d3b468bf325c3c

sha512值: 9e9b542d8a9c36c1820e32be879ed32cd66ecc9c4b01ecfb853eaf6712802dd088930cd58c26b90a03ab93921ca04a730462670e9578fb5cdfc845b69435173a

公钥算法: rsa

密钥长度: 2048

指纹: b7734569343e081f60606836564d5f3e53a6033dd1480ca615cff3b98c18c287

硬编码敏感信息

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.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.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
sbhhd.pqbz.sdcc.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信