MoGua

G S 6.0.APK 分析报告

APP名称: G S

包名:	com.jztb.yshj
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: S G.apk
文件大小: 5.08MB
MD5值: fe307a7f2440d71fb0c54c07c2814454
SHA1值: 7d593b78c92f6ca40a973014d882b82839008d66
SHA256值: e61b7bbf5090c4d922c35af725f45121da125a6dd4ed6ebf9f4bfc3da97d8d6c

APP 信息

App名称: G S
包名: com.jztb.yshj
主活动Activity: com.jztb.yshj.H5Activity
安卓版本名称: 6.0
安卓版本: 6

域名线索

域名	服务器信息
htz1bucket.s3.ap-east-1.amazonaws.com	**IP**: 3.5.238.168 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

URL线索

URL信息	Url所在文件
https://htz1bucket.s3.ap-east-1.amazonaws.com/index.html	com/jztb/yshj/H5Activity.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: True
找到 1 个唯一证书
主题: C=t9SMt, ST=ZhO7m, L=MIJFw, O=um1747563451715, OU=ip1747563451715, CN=rlxi
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-18 10:17:32+00:00
有效期至: 2075-05-06 10:17:32+00:00
发行人: C=t9SMt, ST=ZhO7m, L=MIJFw, O=um1747563451715, OU=ip1747563451715, CN=rlxi
序列号: 0x203b5bc6
哈希算法: sha512
md5值: c1caf2fdc33333f56ed453fba24322bd
sha1值: 6f569c864851b92020b02a27ade8de3fb6ae0a5c
sha256值: 3bfbd22383d035405fdc42e8490cf4edd4d82992f1f909ada2ee5e007f6309f8
sha512值: 535535eac9053fa50462f5318af333ccb1e326dea617b33b87830cbb07a1fda4dd8503db47372c22572e7f0518ec5faa750b42417e1f9354b2f5d494b45e7da6
公钥算法: rsa
密钥长度: 4096
指纹: bd1e8e79c022211b6db4753ebc29d6398c8b27d5432d496f4c8c9d84134bb504

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.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
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
com.jztb.yshj.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信