MoGua

赌圣西游 1.0.APK 分析报告

APP名称:	赌圣西游

包名:	caizhou.top
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 赌圣西游_1.0(1).apk
文件大小: 1.68MB
MD5值: 17ae19f27b81e027ba700389191959a5
SHA1值: ed67814239d131d7687983b1c30fc71b552cf875
SHA256值: 830e59f317df9543ae0a22d67afbf5289044c55ac80808fb257b977aa5e25d19

APP 信息

App名称: 赌圣西游
包名: caizhou.top
主活动Activity: mt.webapp.MainActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
bzyapp.gitee.io	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://bzyapp.gitee.io/app/mtxz	mt/webapp/MainActivity.java
https://bzyapp.gitee.io/app/mtsc	mt/webapp/MainActivity.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=inject, ST=inject, L=inject, O=inject, OU=inject, CN=inject.keystore
签名算法: rsassa_pkcs1v15
有效期自: 2019-10-11 02:39:57+00:00
有效期至: 2841-02-23 02:39:57+00:00
发行人: C=inject, ST=inject, L=inject, O=inject, OU=inject, CN=inject.keystore
序列号: 0x47f931c3
哈希算法: sha256
md5值: 64843786c6ada15ca4254f4da77e4978
sha1值: b2e643d00042e8e23481794e88eedd3966c65dfa
sha256值: 28afa96de62296ef3b7598b27d00b673920d3e0bf5fad9c95ad4ef8de5d8df99
sha512值: 2bcfcb9c6759eb8689d05d7f2393725c1ebea61bf8c4559c9057dc654ad28c1c776ddbe55a6f8a6af71968f2883555e7a74e6c588854a5a2c275ddb4cf0536d2
公钥算法: rsa
密钥长度: 1024
指纹: 61cc7d71417395a5265a787e508b72c4fdc6d6d0107c97d17221206671ae528f

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.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.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.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.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_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.BIND_VPN_SERVICE	合法		VpnService 必须要求,以确保只有系统可以绑定到它
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.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.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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
mt.webapp.MainActivity	Schemes: http://, https://, mtapp://,
