



MoGua

51品茶 4.0.0.APK 分析报告



APP名称:

51品茶

包名: `com.example.chaguaner2023`

域名线索: 25条

URL线索: 15条

邮箱线索: 2条

分析日期: 2025年1月15日

分析平台: [摸瓜APK反编译平台](#)

文件名: cg_0719.apk

文件大小: 33.68MB

MD5值: c1163fcc4e53869837aaf4124568a92b

SHA1值: 5950ea5ed527503ff05f8ea7faf89eb9b577365a

SHA256值: e81776265b1b4a3ccc993ffe44a85007caa7ddccc031aa579f432255946f3751

i APP 信息

App名称: 51品茶

包名: com.example.chaguaner2023

主活动Activity: com.example.chaguaner2023.MainActivity

安卓版本名称: 4.0.0

安卓版本: 400

🔍 域名线索

域名	服务器信息
aomedia.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
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
vbwtbv.wehzmex.com	IP: 104.21.47.210 所属国家: United States of America 地区: California

	<p>城市: San Francisco 纬度: 37.775700 经度: -122.395203</p>
scripts.sil.org	<p>IP: 104.22.11.254 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203</p>
www.w3.org	<p>IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203</p>
h0fr77y9.slt.sched.intlscdn.com	<p>IP: 170.187.231.7 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281</p>
flutter.dev	<p>IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514</p>
developer.apple.com	<p>IP: 17.253.85.203 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692</p>

gitee.com	IP: 180.76.198.77 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
default.url	没有服务器地理信息.
exoplayer.dev	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
vbwtbv.uyijwwn.com	IP: 172.67.203.38 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
www.jsdelivr.com	IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 172.67.175.194

wwsee.jsbacjr.com	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
raw.githubusercontent.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
new1.wanzhuoli.top	IP: 122.189.171.115 所属国家: China 地区: Hubei 城市: Xiangyang 纬度: 32.042267 经度: 112.144836
www.ibm.com	IP: 23.13.189.250 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521

	<p>经度: 114.157692</p>
dashif.org	<p>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</p>
www.unicode.org	<p>IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204</p>
developer.android.com	<p>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</p>
android.googleusercontent.com	<p>IP: 142.251.170.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514</p>
ns.adobe.com	<p>没有服务器地理信息.</p>

URL线索

URL信息	Url所在文件
-------	---------

https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/c.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	e0/x0.java
https://exoplayer.dev/issues/cleartext-not-permitted	b2/b0.java
<a href="https://x</LA_URL>">https://x</LA_URL>	j0/k0.java
https://default.url	j0/k0.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	j0/l0.java
http://dashif.org/guidelines/last-segment-number	l1/d.java
http://dashif.org/guidelines/trickmode	l1/d.java
http://dashif.org/thumbnail_tile	l1/d.java
http://dashif.org/guidelines/thumbnail_tile	l1/d.java
http://ns.adobe.com/xap/1.0/	p0/a.java
https://aomedia.org/emsg/ID3	z0/a.java
https://developer.apple.com/streaming/emsg-id3	z0/a.java
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	摸瓜V2引擎

play.googleapis.com	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
http://www.unicode.org/copyright.html	摸瓜V3引擎
vbwtbv.wehzmsx.com	摸瓜V3引擎
http://scripts.sil.org/OFL http://scripts.sil.org/OFL	摸瓜V3引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V3引擎
h0fr77y9.slt.sched.intlscdn.com	摸瓜V3引擎
https://aomedia.org/emsg/ID3	摸瓜V3引擎
http://dashif.org/thumbnail_tile	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://developer.android.com/guide/topics/permissions/overview	摸瓜V3引擎
https://github.com/flutter/flutter/issues	摸瓜V3引擎
wvsee.jsbacjr.com	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
http://dashif.org/guidelines/trickmode	摸瓜V3引擎
http://dashif.org/guidelines/thumbnail_tile	摸瓜V3引擎
https://github.com/dart-lang/sdk/blob/master/runtime/docs/compiler/aot/entry_point_pragma.md	摸瓜V3引擎
new1.wanzhuoli.top	摸瓜V3引擎

https://github.com/apvarun/toastify-js	摸瓜V3引擎
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	摸瓜V3引擎
http://dashif.org/guidelines/last-segment-number	摸瓜V3引擎
https://exoplayer.dev/issues/cleartext-not-permitted	摸瓜V3引擎
https://default.url	摸瓜V3引擎
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so
https://github.com/flutter/flutter/issues	lib/arm64-v8a/libflutter.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://vbwtbv.wehzmex.com	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://gitee.com/fdsaw/ffewelmexww/raw/master/cg.txt	lib/armeabi-v7a/libapp.so
https://github.com/flutter/flutter/issues/new	lib/armeabi-v7a/libapp.so
https://wvsee.jsbacjr.com/cg.txt	lib/armeabi-v7a/libapp.so
https://raw.githubusercontent.com/little-5/backup/master/cg.txt?t=	lib/armeabi-v7a/libapp.so
https://vbwtbv.uyjwwn.com	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	lib/armeabi-v7a/libapp.so

✉ 邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so
_growablelist@0150898._literal _typeerror@0150898._create _bytebuffer@7027147._new _immutablelist@0150898._uk _double@0150898.fromintege _casterror@0150898._create _assertionerror@0150898._create	lib/armeabi-v7a/libapp.so

☰ 手机线索

手机号	所在文件
17512775099	i2/a.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: CN=Android Debug, O=Android, C=US

签名算法: rsassa_pkcs1v15

有效期自: 2024-02-10 07:12:47+00:00

有效期至: 2054-02-02 07:12:47+00:00

发行人: CN=Android Debug, O=Android, C=US

序列号: 0x1

哈希算法: sha256

md5值: 73e8a618da84833ebd3aed6d63a9ccaf

sha1值: 8cfcf0fea89841747a1bd225f70d99045787e230

sha256值: 3700cee9dcef3c9e696aa51d4ad581b332fbc4040477853f7812ea91c75b75f0

sha512值: b59b74d1370c5509886a41046509857127a0839378b83926a43aa423d1bb45dea901907a9b8f1172ac0430536fa282687ee4c5f256e1e2e49b3dca070457338f

公钥算法: rsa

密钥长度: 2048

指纹: 5a3db976ca130f12887af21ec865966dadfba3e4e6c924570369047e0ede67fe

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.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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_STATE	危	读取电话状	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

	危险	态和身份	码等
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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
	未	Unknown	

com.example.chaguaner2023.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	知	permission	Unknown permission from android reference
--	---	------------	---

应用内通信

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。