



MoGua

桔多多 1.0.APK 分析报告



APP名称:

桔多多

包名:

域名线索: 30条

URL线索: 5条

邮箱线索: 0条

分析日期: 2025年6月26日

分析平台: [摸瓜APK反编译平台](#)

文件信息

文件名: base(3).apk

文件大小: 84.35MB
MD5值: 4bf7e361fd30edbb4db04ccc57a72ddf
SHA1值: 544806aa37aaa0841b22bf3237e0ca5e4ac6b656
SHA256值: 0c418bd14455ab3d1eabd4f224839c38d2507df759c37a9cf9b832a81b00ca91

i APP 信息

App名称: 桔多多
包名:
主活动Activity: []
安卓版本名称: 1.0
安卓版本: []

🔍 域名线索

域名	服务器信息
www.wolframalpha.com	IP: 140.177.50.12 所属国家: United States of America 地区: Illinois 城市: Champaign 纬度: 40.112537 经度: -88.246277
grs.dbankcloud.com	IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
en.wikipedia.org	IP: 199.16.158.9 所属国家: United States of America 地区: California 城市: San Francisco

	纬度: 37.773968 经度: -122.410446
www.math.ubc.ca	IP: 137.82.155.105 所属国家: Canada 地区: British Columbia 城市: Vancouver 纬度: 49.265823 经度: -123.256630
www.color.org	IP: 172.67.70.181 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
data-dra.push.dbankcloud.com	IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
code.google.com	IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660 经度: -79.382927
www.brucelindbloom.com	IP: 66.175.58.9 所属国家: Canada 地区: Ontario 城市: Waterloo 纬度: 43.505604 经度: -80.545486
	IP: 151.101.2.132

www.apache.org	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.w3.org	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
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
www.poynton.com	IP: 15.235.66.161 所属国家: Canada 地区: Quebec 城市: Montreal 纬度: 45.508839 经度: -73.587807
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
grs.dbankcloud.asia	IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572

grs.dbankcloud.cn	IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
metrics5.dt.dbankcloud.ru	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
metrics5.data.hicloud.com	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
developer.apple.com	IP: 17.253.85.201 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.jpeg.org	IP: 176.58.118.251 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London 纬度: 51.508530 经度: -0.125740
metrics1-drcn.dt.dbankcloud.cn	IP: 111.202.16.252 所属国家: China 地区: Beijing

	城市: Beijing 纬度: 39.907501 经度: 116.397102
www.adobe.com	IP: 221.194.158.143 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
tools.ietf.org	IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
rjwagner49.com	IP: 67.20.98.29 所属国家: United States of America 地区: Utah 城市: Provo 纬度: 40.213909 经度: -111.634071
data-dre.push.dbankcloud.com	IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
data-drcn.push.dbankcloud.com	IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572

data-drru.push.dbankcloud.com	IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
grs.dbankcloud.eu	没有服务器地理信息.
grs.platform.dbankcloud.ru	没有服务器地理信息.
metrics2.data.hicloud.com	IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
bugzilla.mozilla.org	IP: 34.110.178.183 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568

URL线索

URL信息	Url所在文件
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎

https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1-drcn.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://tools.ietf.org/html/rfc3986	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=810490	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=683280	摸瓜V2引擎
http://www.wolframalpha.com/input/	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=726227	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=664884	摸瓜V2引擎

https://bugzilla.mozilla.org/show_bug.cgi?id=904007	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=972126	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://tools.ietf.org/html/rfc3986	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=810490	摸瓜V2引擎
http://	摸瓜V2引擎
http://rjwagner49.com/Mathematics/Interpolation.pdf	摸瓜V2引擎
http://www.poynton.com/notes/colour_and_gamma/ColorFAQ.html ,	摸瓜V2引擎
http://www.brucelindbloom.com/index.html?Eqn_ChromAdapt.html	摸瓜V2引擎
http://www.brucelindbloom.com/index.html?Eqn_RGB_XYZ_Matrix.html .	摸瓜V2引擎
http://en.wikipedia.org/wiki/SRGB .	摸瓜V2引擎
http://www.adobe.com/content/dam/Adobe/en/devnet/photoshop/sdk/	摸瓜V2引擎
http://www.color.org/srgb.pdf	摸瓜V2引擎
https://developer.apple.com/fonts/TTRefMan/RM05/Chap5.html	摸瓜V2引擎
https://github.com/mozilla/pdf.js/pull/2127	摸瓜V2引擎
http://www.math.ubc.ca/	摸瓜V2引擎
http://code.google.com/p/chromium/issues/detail?id=122465	摸瓜V2引擎
https://github.com/mozilla/pdf.js/issues/1689	摸瓜V2引擎

https://github.com/mozmar/patjs/issues/1009	摸瓜V2引擎
http://www.jpeg.org/public/fcd15444-1.pdf	摸瓜V2引擎
https://code.google.com/p/smhasher/wiki/MurmurHash3.	摸瓜V2引擎

邮箱线索

手机线索

手机号	所在文件
15695978492	摸瓜V2引擎
16563550634	摸瓜V2引擎

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: CN=jz
签名算法: rsassa_pkcs1v15
有效期自: 2016-06-17 08:05:08+00:00
有效期至: 2041-06-11 08:05:08+00:00
发行人: CN=jz
序列号: 0x53abc425
哈希算法: sha256
md5值: 7d49e69bf277a66656e55601b58579b0
sha1值: 1d48b09a6e0e8aecab38e6b0f7bddbaa14cad047

sha256值: 8dc25c2bf209350fed05cbe9ae91ded96473b62e8ad0be26223836e6b7b99721
sha512值: 752d2722f98c51b61abcb0309898de20346d4a240951bf4dbf48891e70953168d9531ff6b90502e7fc05b61006d9bb62173d98d2abfafb3be8bb6dca5a1c348f
公钥算法: rsa
密钥长度: 2048
指纹: d391308a462ed280731fe0fec00c97bd37311e150adfeb733692a81ff0a37d70

硬编码敏感信息

可能的敏感信息
"auth_goto_auth" : "去认证"
"commit_auth" : "已提交"
"commit_auth_add_btn" : "确认"
"des_freeze_auth" : "很抱歉，您的账户已冻结，暂无信用额度"
"face_auth_result_tips" : "要达到%d分才可通过认证哦～"
"forget_password" : "忘记密码"
"reset_password" : "重置密码"
"security_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyls7JWKm4py9KcldJsZRh9onknVeAVIU++jnrGFGYfQb8iKzCIN059gYeejBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fjQIDAQAB"
"str_authing_btn" : "认证中..."
"udesk_no_sdktoken" : "sdktoken为空,请传入合法的值"
"user_authorization_agree_tips" : "同意 （%ss） "
"user_authorize_idcard_tips" : "%s秒后授权书信息将自动失效"

"wallet_quota_no_auth" : "50000.00"

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

应用内通信