



MoGua

PH 1.1.1.APK 分析报告



APP名称:

PH

包名:	com.zq.ph
域名线索:	42条
URL线索:	19条
邮箱线索:	3条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件名: phok005_2024.11.9.900.apk
文件大小: 12.76MB
MD5值: 77096d905c07ccd3aa7d4a4ac9ad51cd
SHA1值: 8313bd78737471c6ebd43dfa991f564386bd9471
SHA256值: 0601fe2d54d25755326008e7c28739a3faceb9a66fd7436e12c38ed9d597291f

i APP 信息

App名称: PH
包名: com.zq.ph
主活动Activity: com.zq.douyin.MainActivity
安卓版本名称: 1.1.1
安卓版本: 3

🔍 域名线索

域名	服务器信息
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
douyin-api.ybunx.com	IP: 172.67.139.69 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
ldy.nroom10.com	没有服务器地理信息.
	IP: 104.26.12.19

cdn.plyr.io	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
html2canvas.hertzen.com	IP: 104.21.65.51 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
34.150.33.40	IP: 34.150.33.40 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
bk.dlkxi.cc	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.youtube-nocookie.com	IP: 31.13.73.9 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
noembed.com	IP: 151.101.193.91 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
api.h-gpro.com	没有服务器地理信息.
cres.rqi564.com	IP: 149.104.35.195 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
chen.ybunx.com	IP: 104.21.65.16 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
schemas.android.com	没有服务器地理信息.
aomedia.org	IP: 199.16.156.71 所属国家: United States of America 地区: Georgia 城市: Atlanta 纬度: 33.770844 经度: -84.377632
d3n2vdp1h9ohbb.cloudfront.net	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000

	经度: 0.000000
vimeo.com	IP: 157.240.17.35 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
cdn.jsdelivr.net	IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe 纬度: 32.548328 经度: -92.045235
kk.xcdwt.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
43.231.0.225	IP: 43.231.0.225 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
pan.baidu.com	IP: 110.242.69.174 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
	IP: 52.76.120.174 所属国家: Singapore

axios-http.com	地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
jsperf.com	IP: 104.16.227.18 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
i.ytimg.com	IP: 23.234.30.58 所属国家: United States of America 地区: Delaware 城市: Newark 纬度: 39.707489 经度: -75.734329
img01.yzcdn.cn	IP: 60.25.92.69 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
baq.fbafb.cn	没有服务器地理信息.
hfive.qsxon.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: -

	纬度: 0.000000 经度: 0.000000
dfe.hapha.cn	没有服务器地理信息.
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
swiperjs.comn	没有服务器地理信息.
101.132.69.237	IP: 101.132.69.237 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
brianleroux.github.com	没有服务器地理信息.
go.aniview.com	IP: 104.83.102.21 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
player.vimeo.com	IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
	IP: 168.119.33.54

issues.apache.org	所属国家: Germany 地区: Bayern 城市: Gunzenhausen 纬度: 48.323860 经度: 11.601019
www.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
faw.douying8.com	没有服务器地理信息.
raw.githubusercontent.com	IP: 185.199.110.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
hertzen.com	IP: 172.67.140.170 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
imasdk.googleapis.com	IP: 114.250.69.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 157.240.17.35 所属国家: Switzerland

www.youtube.com	地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
-----------------	---

URL线索

URL信息	Url所在文件
https://chen.ybunx.com/apk/app-1.1.0-3.apk	defpackage/j00.java
https://dfe.hapha.cn	defpackage/l00.java
https://api.h-gpro.com	defpackage/l00.java
https://baq.fbafb.cn	defpackage/l00.java
https://faw.douying8.com	defpackage/l00.java
https://douyin-api.ybunx.com	defpackage/l00.java
http://schemas.android.com/apk/res/android	defpackage/b0.java
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://jsperf.com/b64tests	摸瓜V2引擎
http://server/myapp/index.html	摸瓜V2引擎
https://issues.apache.org/jira/browse/CB-11522)	摸瓜V2引擎
https://html2canvas.hertzen.com>	摸瓜V2引擎

https://hertzen.com >	摸瓜V2引擎
https://cdn.jsdelivr.net/npm/workbox-cdn@5.1.4/workbox	摸瓜V2引擎
https://cdn.plyr.io/3.7.2/plyr.svg	摸瓜V2引擎
https://cdn.plyr.io/static/blank.mp4	摸瓜V2引擎
https://player.vimeo.com/api/player.js	摸瓜V2引擎
https://player.vimeo.com/video/	摸瓜V2引擎
https://vimeo.com/api/oembed.json?url=	摸瓜V2引擎
https://www.youtube.com/iframe_api	摸瓜V2引擎
https://noembed.com/embed?url=https://www.youtube.com/watch?v=	摸瓜V2引擎
https://imasdk.googleapis.com/js/sdkloader/ima3.js	摸瓜V2引擎
https://www.youtube-nocookie.com	摸瓜V2引擎
http://www.youtube.com	摸瓜V2引擎
https://i.ytimg.com/vi/	摸瓜V2引擎
https://go.aniview.com/api/adserver6/vast/	摸瓜V2引擎
https://hfive.qsxon.com	摸瓜V2引擎
https://t.me/	摸瓜V2引擎
https://pan.baidu.com/s/1wPlQE5srd_cGuPVqBWNuxw?pwd=1234	摸瓜V2引擎
https://ldy.nroom10.com:19999/nhft001	摸瓜V2引擎

https://cres.rqi564.com	摸瓜V2引擎
https://kk.xcdwt.com/api/v1/	摸瓜V2引擎
https://43.231.0.225:19888/api/v1/	摸瓜V2引擎
https://34.150.33.40:19888/api/v1/	摸瓜V2引擎
https://bk.dlkxi.cc/api/v1/	摸瓜V2引擎
https://d3n2vdp1h9ohbb.cloudfront.net/api/v1/	摸瓜V2引擎
https://101.132.69.237:16888/api/v1/	摸瓜V2引擎
https://aomedia.org/emsg/ID3	摸瓜V2引擎
https://github.com/mathiasbynens/CSS.escape).	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.37.1/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
http://a	摸瓜V2引擎
http://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	摸瓜V2引擎
http://x	摸瓜V2引擎
https://github.com/crypto-browserify/crypto-browserify	摸瓜V2引擎
https://img01.yzcdn.cn/vant/share-sheet-	摸瓜V2引擎

https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V2引擎
---	--------

邮箱线索

邮箱地址	所在文件
sy12god@gmail.com	摸瓜V2引擎
git@github.com fedor@indutny.com	摸瓜V2引擎
solderzzc@gmail.com stefano.magrassi@gmail.com	摸瓜V2引擎

手机线索

手机号	所在文件
19919152923	摸瓜V2引擎

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: C=a, ST=a, L=a, O=a, OU=a, CN=a

签名算法: rsassa_pkcs1v15
 有效期自: 2022-06-21 05:32:57+00:00
 有效期至: 2049-11-06 05:32:57+00:00
 发行人: C=a, ST=a, L=a, O=a, OU=a, CN=a
 序列号: 0x41772888
 哈希算法: sha256
 md5值: d49d20229d9dab896e21574bc3232c24
 sha1值: 97b79fd8c8827cda42e464328c46dfb462f81b1e
 sha256值: ba05c89d57a24934d976a647b91f733d38eb6f32d0c254b52aaba0ac1cc13b4b
 sha512值: 4cf78e142e057f170c4bab11acec9f775015ff9539379b930d33d62c7587815ea44a53570eaa9b1ac1d1c4688d43d0d0a45c6a70ed86ddffcff7caaac0389fb
 公钥算法: rsa
 密钥长度: 2048
 指纹: a8622d5e2214871f8de1d32546543dce06b23472ccf6ef958be849992a5043d9

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.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.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.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.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

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。