MoGua

PH 1.1.1.APK 分析报告

APP名称: PH

包名:	com.phppx.ppxone
域名线索:	45条
URL线索:	19条
邮箱线索:	3条
分析日期:	2025年4月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: phyv006_2025.4.7.800.apk
文件大小: 16.12MB
MD5值: e7c961caf662f290b8864986ca25965d
SHA1值: fd936ec6f2cad1dd2e84599c2f2d1429c7f8349e
SHA256值: 78c88aebeab0025ce915c1d69688ae638e0a1c3370bc68db27bca4e3126c51de

APP 信息

App名称: PH
包名: com.phppx.ppxone
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
npms.io	**IP**: 104.21.48.1 **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
vimeo.com	**IP**: 31.13.94.10 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires

	城市: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
cdn.jsdelivr.net	IP: 104.18.187.31 **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.
d3n2vdp1h9ohbb.cloudfront.net	IP: 3.170.230.129 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
html2canvas.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
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
134.122.189.143	IP: 134.122.189.143 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

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
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
aomedia.org	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
cdn.plyr.io	**IP**: 104.26.13.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
swiperjs.comn	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
	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
player.vimeo.com	**IP**: 31.13.94.37 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
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
axios-http.com	**IP**: 52.220.155.145 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
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
imasdk.googleapis.com	**IP**: 114.250.64.33 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

brianleroux.github.com	没有服务器地理信息.
img01.yzcdn.cn	**IP**: 221.15.70.53 **所属国家**: China **地区**: Henan **城市**: Luoyang **纬度**: 34.683289 **经度**: 112.453911
schemas.android.com	没有服务器地理信息.
raw.githubusercontent.com	**IP**: 185.199.108.133 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
www.youtube-nocookie.com	**IP**: 31.13.94.49 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
ldy.nroom10.com	没有服务器地理信息.
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
i.ytimg.com	**IP**: 199.96.63.75 **所属国家**: United States of America **地区**: California **城市**: San Francisco

	纬度: 37.773968 **经度**: -122.410446
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
xk.vvm512.com	IP: 38.182.168.179 **所属国家**: United States of America **地区**: District of Columbia **城市**: Washington **纬度**: 38.901566 **经度**: -77.050781
noembed.com	IP: 151.101.1.91 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
baq.fbafb.cn	没有服务器地理信息.
bk.dlkxi.cc	IP: 118.107.9.147 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
dfe.hapha.cn	没有服务器地理信息.
34.92.95.149	IP: 34.92.95.149 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong

	纬度: 22.285521 **经度**: 114.157692
www.youtube.com	IP: 31.13.94.49 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
bkb.iew91.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
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
hfive.qsxon.com	IP: 104.21.16.1 **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.
go.aniview.com	IP: 104.83.106.30 **所属国家**: Italy **地区**: Lombardia **城市**: Milan **纬度**: 45.464336 **经度**: 9.188547

douyin-api.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
jsperf.com	**IP**: 104.16.228.18 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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

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://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/nhfth001	摸瓜V2引擎
https://cres.rqi564.com	摸瓜V2引擎
https://d3n2vdp1h9ohbb.cloudfront.net/api/v1/	摸瓜V2引擎
https://bkb.iew91.com/api/v1/	摸瓜V2引擎
https://134.122.189.143:19888/api/v1/	摸瓜V2引擎
https://bk.dlkxi.cc/api/v1/	摸瓜V2引擎
https://xk.vvm512.com/api/v1/	摸瓜V2引擎
https://101.132.69.237:16888/api/v1/	摸瓜V2引擎
https://43.231.0.225:19888/api/v1/	摸瓜V2引擎
https://34.92.95.149:19888/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/v3.40.0/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://a	摸瓜V2引擎
https://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	摸瓜V2引擎
https://x	摸瓜V2引擎
https://npms.io/search?q=ponyfill.	摸瓜V2引擎
https://github.com/browserify/crypto-browserify	摸瓜V2引擎
https://img01.yzcdn.cn/vant/share-sheet-	摸瓜V2引擎
https://img01.yzcdn.cn/vant/empty-image-	摸瓜V2引擎
http://swiperjs.com\n	摸瓜V2引擎
https://github.com/indutny/elliptic/issues	摸瓜V2引擎
https://github.com/indutny/elliptic	摸瓜V2引擎
https://github.com/axios/axios.git	摸瓜V2引擎
https://github.com/axios/axios/issues	摸瓜V2引擎
https://axios-http.com	摸瓜V2引擎

https://developer.mozilla.org/fr/docs/Web/API/CustomEvent	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://brianleroux.github.com/lawnchair/),	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	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

tedor@indutny.com	
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: True
找到 1 个唯一证书
主题: C=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-07 06:56:10+00:00
有效期至: 2052-08-23 06:56:10+00:00
发行人: C=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com
序列号: 0x5844abca
哈希算法: sha256
md5值: 9550f88dcecaefbf9755120d1f286beb
sha1值: c9d2b2d9878e2890445a839e8a01572a8f5e4836
sha256值: c96900040ee551ffb046b29ad840064dbfd4e773246d1435fcab6723b9a92af0
sha512值: eaa0e77f93807ab794702cd3e92b5401ca8723180cc9955650e2da34ca56efb57b2389392e6e010eb9b22b2493daa81a88af803f2819fe338645169cdea563d3
公钥算法: rsa
密钥长度: 2048
指纹: 09af32233404d75dbdcd94766928cd79c7962e4b7517ce925a0140488a9a127d

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.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
