



MoGua

XV 1.1.1.APK 分析报告



APP名称:

XV

包名:	com.xxv.xxvone
域名线索:	44条
URL线索:	19条
邮箱线索:	3条
分析日期:	2025年10月5日
分析平台:	摸瓜APK反编译平台

文件名: xvtanh001_2025.2.25.400.apk
文件大小: 15.11MB
MD5值: 95659e222ccd2a70f5c217b258cc99ca
SHA1值: 30bc18b4d690216f022758e586db267b601c9685
SHA256值: 0af0f76d8c4bfd008ece4836eced8785d3bad62a9df9906bfe58c4955d1b6219

i APP 信息

App名称: XV
包名: com.xxv.xxvone
主活动Activity: com.zq.douyin.MainActivity
安卓版本名称: 1.1.1
安卓版本: 2

🔍 域名线索

域名	服务器信息
raw.githubusercontent.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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
d3n2vdp1h9ohbb.cloudfront.net	IP: 3.165.16.198 所属国家: United States of America 地区: Washington

	城市: Seattle 纬度: 47.627499 经度: -122.346199
aomedia.org	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
noembed.com	IP: 151.101.129.91 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
bk.dlkxi.cc	IP: 149.104.35.34 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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
faw.douying8.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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
cres.rqi564.com	IP: 149.104.35.45 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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
baq.fbafb.cn	没有服务器地理信息.
i.ytimg.com	IP: 128.242.240.155 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
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
	IP: 110.242.69.174

pan.baidu.com	所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
www.youtube.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
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
dfe.hapha.cn	没有服务器地理信息.
player.vimeo.com	IP: 31.13.106.4 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
www.youtube-nocookie.com	IP: 31.13.73.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
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
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
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
jsperf.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
35.241.80.232	IP: 35.241.80.232 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
ldy.nroom10.com	IP: 106.74.25.198 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
	IP: 127.0.0.1 所属国家: -

vimeo.com	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
schemas.android.com	没有服务器地理信息.
hfive.qsxon.com	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
xk.vvm512.com	IP: 149.104.35.45 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
npms.io	IP: 104.21.96.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
axios-http.com	IP: 52.76.120.174 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
api.h-gpro.com	没有服务器地理信息.
go.aniview.com	IP: 104.103.88.235 所属国家: Austria 地区: Wien 城市: Vienna 纬度: 48.208889 经度: 16.372080
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
chen.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
brianleroux.github.com	没有服务器地理信息.
imasdk.googleapis.com	IP: 114.250.63.33 所属国家: China 地区: Beijing 城市: Beijing

	纬度: 39.907501 经度: 116.397102
issues.apache.org	IP: 168.119.33.54 所属国家: Germany 地区: Bayern 城市: Gunzenhausen 纬度: 48.323860 经度: 11.601019
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
cdn.jsdelivr.net	IP: 151.101.89.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

 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/1wPIQE5srd_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://34.92.95.149:19888/api/v1/	摸瓜V2引擎
https://d3n2vdp1h9ohbb.cloudfront.net/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://43.231.0.225:19888/api/v1/	摸瓜V2引擎
https://101.132.69.237:16888/api/v1/	摸瓜V2引擎
https://35.241.80.232:19888/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/v3.39.0/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
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	...

o-c-g-m----- 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: 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: 2025-02-24 21:26:02+00:00
有效期至: 2052-07-12 21:26:02+00:00
发行人: C=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com
序列号: 0x15cf234
哈希算法: sha256
md5值: ea1a6d970702a76953983b1d6f8c9c49
sha1值: 3496802332e899b559231be2ff0f74e770d9ab11
sha256值: 254989188f5356462ac57219240728e0b6a2273708a83dae16a4fa6a7ea40ef3
sha512值: ef43fae879fd917bbaa79b86e30c54eab95f02d98bb4badff4d8d8c61922d26fa4f9319cc6d55f5c8099ec64364db73d5ba9d9b82d00735c4f4b3396a7caede6
公钥算法: rsa
密钥长度: 2048
指纹: 1fd7126cc8ec23ddcc56e41e309c17055f3c706841791018d231f1a9ebf57ec

 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应用。	恶意应用程序可以利用它来安装恶意应用并安装其他恶意软件。
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。