



MoGua

ProjectChat 2.02.03.APK 分析报告



APP名称:

ProjectChat

包名:	plus.H5ACE11EE
域名线索:	39条
URL线索:	29条
邮箱线索:	8条
分析日期:	2025年5月29日
分析平台:	摸瓜APK反编译平台

文件名: projectchat.apk
文件大小: 11.06MB
MD5值: e75eb4527e603c16ee08c36315624bda
SHA1值: 960f73f8ce775ce6f4033300829ca1314c33d14f
SHA256值: 1d334a61aa7f89850c54f872bf3033c0bbb88d82d01c02bc441a9f6ac3423cfa

i APP 信息

App名称: ProjectChat
包名: plus.H5ACE11EE
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 2.02.03
安卓版本: 192

🔍 域名线索

域名	服务器信息
fontawesome.comthe	没有服务器地理信息.
sdk.api.oaid.wocloud.cn	没有服务器地理信息.
fontawesome.comhttps	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
s1.dcloud.net.cn	IP: 150.158.3.107 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

html.spec.whatwg.org	IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
edgedl.me.gvt1.com	IP: 34.104.35.123 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
zi.artx.cn	IP: 208.98.43.15 所属国家: United States of America 地区: Illinois 城市: Chicago 纬度: 41.867199 经度: -87.625900
msdn.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
android.googlesource.com	IP: 142.250.107.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
perfectionkills.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: -

	纬度: 0.000000 经度: 0.000000
greensock.com	IP: 50.28.34.250 所属国家: United States of America 地区: Michigan 城市: Lansing 纬度: 42.733280 经度: -84.637764
vuejs.org	IP: 15.197.167.90 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
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
sdk.api.oaid.wocloud.cn.local	没有服务器地理信息.
app.visionsic.com	IP: 124.70.189.146 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
gac2.dcloud.net.cn	IP: 124.222.75.101 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

www.jsdelivr.com	IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.dcloud.io	IP: 124.163.195.101 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
popper.js.org	IP: 172.67.73.64 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
cli.vuejs.org	IP: 15.197.167.90 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
dev.dcloud.net.cn	IP: 119.188.180.230 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
opencollective.com	IP: 104.26.13.145 所属国家: United States of America 地区: California 城市: San Francisco

	纬度: 37.775700 经度: -122.395203
cdn.bootcdn.net	IP: 121.22.232.162 所属国家: China 地区: Hebei 城市: Qinhuangdao 纬度: 39.932541 经度: 119.588226
tidelift.com	IP: 54.144.237.174 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
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
m3w.cn	IP: 124.163.195.65 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
fontawesome.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 121.4.61.130

cdn.dcloud.net.cn	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
getbootstrap.com	IP: 104.22.59.100 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
er.dcloud.io	没有服务器地理信息.
registry.npmjs.org	IP: 104.16.29.34 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.
bgac.dcloud.net.cn	IP: 170.106.67.149 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
er.dcloud.net.cn	IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

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
gac1.dcloud.net.cn	IP: 122.51.46.227 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.webkaka.com	IP: 211.149.147.36 所属国家: China 地区: Sichuan 城市: Chengdu 纬度: 30.666670 经度: 104.066269
ask.dcloud.net.cn	IP: 116.136.188.184 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665

 URL线索

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java

https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/c.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/c.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://registry.npmjs.org/@babel/parser/-/parser-7.23.6.tgz	摸瓜V2引擎
https://registry.npmjs.org/@jridgewell/sourcemap-codec/-/sourcemap-codec-1.4.15.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/compiler-core/-/compiler-core-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/compiler-dom/-/compiler-dom-3.3.12.tgz	摸瓜V2引擎

https://registry.npmjs.org/@vue/compiler-sfc/-/compiler-sfc-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/compiler-ssr/-/compiler-ssr-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/reactivity/-/reactivity-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/reactivity-transform/-/reactivity-transform-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/runtime-core/-/runtime-core-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/runtime-dom/-/runtime-dom-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/server-renderer/-/server-renderer-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/@vue/shared/-/shared-3.3.12.tgz	摸瓜V2引擎
https://registry.npmjs.org/base64-arraybuffer/-/base64-arraybuffer-1.0.2.tgz	摸瓜V2引擎
https://registry.npmjs.org/css-line-break/-/css-line-break-2.1.0.tgz	摸瓜V2引擎
https://registry.npmjs.org/csstype/-/csstype-3.1.3.tgz	摸瓜V2引擎
https://registry.npmjs.org/estree-walker/-/estree-walker-2.0.2.tgz	摸瓜V2引擎
https://registry.npmjs.org/file-saver/-/file-saver-2.0.5.tgz	摸瓜V2引擎
https://registry.npmjs.org/html2canvas/-/html2canvas-1.4.1.tgz	摸瓜V2引擎
https://registry.npmjs.org/magic-string/-/magic-string-0.30.5.tgz	摸瓜V2引擎
https://registry.npmjs.org/nanoid/-/nanoid-3.3.7.tgz	摸瓜V2引擎
https://github.com/sponsors/ai	摸瓜V2引擎

https://registry.npmjs.org/picocolors/-/picocolors-1.0.0.tgz	摸瓜V2引擎
https://registry.npmjs.org/postcss/-/postcss-8.4.32.tgz	摸瓜V2引擎
https://opencollective.com/postcss/	摸瓜V2引擎
https://tidelift.com/funding/github/npm/postcss	摸瓜V2引擎
https://registry.npmjs.org/source-map-js/-/source-map-js-1.0.2.tgz	摸瓜V2引擎
https://registry.npmjs.org/text-segmentation/-/text-segmentation-1.0.3.tgz	摸瓜V2引擎
https://registry.npmjs.org/utrie/-/utrie-1.0.2.tgz	摸瓜V2引擎
https://registry.npmjs.org/vue/-/vue-3.3.12.tgz	摸瓜V2引擎
http://www.dcloud.io/hellomui/	摸瓜V2引擎
https://github.com/ftlabs/fastclick/issues/251	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=922896	摸瓜V2引擎
http://msdn.microsoft.com/en-us/library/windows/apps/Hh767313.aspx	摸瓜V2引擎
https://github.com/highlightjs/highlight.js/issues/2277	摸瓜V2引擎
https://github.com/highlightjs/highlight.js/issues/2886	摸瓜V2引擎
http://dev.dcloud.net.cn/mui	摸瓜V2引擎
http://ask.dcloud.net.cn/article/113 ;	摸瓜V2引擎
http://perfectionkills.com/global-eval-what-are-the-options/	摸瓜V2引擎
http://dev.dcloud.net.cn/mui	摸瓜V2引擎

http://zi.artx.cn/zi/)	摸瓜V2引擎
http://www.dcloud.io/helloh5p/HelloH5.apk	摸瓜V2引擎
http://www.dcloud.io/helloh5/update.json	摸瓜V2引擎
https://vuejs.org/guide/essentials/computed.html	摸瓜V2引擎
https://github.com/vuejs/core	摸瓜V2引擎
https://cli.vuejs.org/guide/webpack.html	摸瓜V2引擎
https://github.com/vitejs/vite-plugin-vue/tree/main/packages/plugin-vue	摸瓜V2引擎
https://html.spec.whatwg.org/multipage/parsing.html	摸瓜V2引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/vuejs/core	摸瓜V2引擎
https://cli.vuejs.org/guide/webpack.html	摸瓜V2引擎
https://github.com/vitejs/vite-plugin-vue/tree/main/packages/plugin-vue	摸瓜V2引擎
https://github.com/andreasgal/pdf.js	摸瓜V2引擎
http://greensock.com	摸瓜V2引擎
http://greensock.com/standard-license	摸瓜V2引擎
https://getbootstrap.com/)	摸瓜V2引擎
https://github.com/twbs/bootstrap/graphs/contributors)	摸瓜V2引擎

https://github.com/twbs/bootstrap/blob/main/LICENSE)	摸瓜V2引擎
https://popper.js.org)	摸瓜V2引擎
https://github.com/richttr/NoSleep.js/issues/15	摸瓜V2引擎
https://registry.npmjs.org/magic-string/-/magic-string-0.30.5.tgz	摸瓜V3引擎
sdk.api.oaid.wocloud.cn	摸瓜V3引擎
https://registry.npmjs.org/estree-walker/-/estree-walker-2.0.2.tgz	摸瓜V3引擎
https://registry.npmjs.org/html2canvas/-/html2canvas-1.4.1.tgz	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
s1.dcloud.net.cn	摸瓜V3引擎
https://cdn.bootcdn.net/ajax/libs/vue/2.7.0-beta.5/vue.min.js	摸瓜V3引擎
https://cdn.bootcdn.net/ajax/libs/element-ui/2.15.9/index.js	摸瓜V3引擎
https://registry.npmjs.org/text-segmentation/-/text-segmentation-1.0.3.tgz	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://github.com/highlightjs/highlight.js/issues/2277	摸瓜V3引擎
https://registry.npmjs.org/base64-arraybuffer/-/base64-arraybuffer-1.0.2.tgz	摸瓜V3引擎
edgedl.me.gvt1.com	摸瓜V3引擎
http://dev.dcloud.net.cn/mui	摸瓜V3引擎
https://cdn.bootcdn.net/ajax/libs/vue/3.3.4/vue.global.min.js	摸瓜V3引擎

https://ask.dcloud.net.cn/article/35058	摸瓜V3引擎
https://registry.npmjs.org/postcss/-/postcss-8.4.32.tgz	摸瓜V3引擎
https://er.dcloud.io/rv	摸瓜V3引擎
https://fontawesome.com/license/free	摸瓜V3引擎
https://er.dcloud.net.cn/rv	摸瓜V3引擎
https://registry.npmjs.org/picocolors/-/picocolors-1.0.0.tgz	摸瓜V3引擎
https://github.com/sponsors/ai	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
gac2.dcloud.net.cn	摸瓜V3引擎
sdk.api.oaid.wocloud.cn.local	摸瓜V3引擎
https://github.com/highlightjs/highlight.js/issues/2886	摸瓜V3引擎
app.visionsic.com	摸瓜V3引擎
https://registry.npmjs.org/nanoid/-/nanoid-3.3.7.tgz	摸瓜V3引擎
http://schemas.android.com/apk/res-auto((androidx.appcompat.widget.ActionMenuView	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://tidelift.com/funding/github/npm/postcss	摸瓜V3引擎
http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout((androi	摸瓜V3引擎

https://registry.npmjs.org/file-saver/-/file-saver-2.0.5.tgz	摸瓜V3引擎
https://registry.npmjs.org/source-map-js/-/source-map-js-1.0.2.tgz	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35877	摸瓜V3引擎
https://fontawesome.com The	摸瓜V3引擎
https://er.dcloud.io/sc	摸瓜V3引擎
http://schemas.android.com/apk/res-auto 00androidx.appcompat.widget.ActionBarOverlayLayout	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
https://registry.npmjs.org/	摸瓜V3引擎
https://ask.dcloud.net.cn/article/283	摸瓜V3引擎
https://ask.dcloud.net.cn/article/282	摸瓜V3引擎
https://fontawesome.com https://fontawesome.com Font	摸瓜V3引擎
https://m3w.cn/s/	摸瓜V3引擎
https://registry.npmjs.org/utrie/-/utrie-1.0.2.tgz	摸瓜V3引擎
https://cdn.dcloud.net.cn/img/mui-shadow-grey.png);	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35627	摸瓜V3引擎
bgac.dcloud.net.cn	摸瓜V3引擎
https://fontawesome.com	摸瓜V3引擎
http://www.webkaka.com/tutorial/html/2023/0407372/	摸瓜V3引擎

er.dcloud.net.cn	摸瓜V3引擎
https://opencollective.com/postcss/	摸瓜V3引擎
https://registry.npmjs.org/css-line-break/-/css-line-break-2.1.0.tgz	摸瓜V3引擎
https://registry.npmjs.org/csstype/-/csstype-3.1.3.tgz	摸瓜V3引擎
gac1.dcloud.net.cn	摸瓜V3引擎
https://registry.npmjs.org/vue/-/vue-3.3.12.tgz	摸瓜V3引擎
https://er.dcloud.net.cn/sc	摸瓜V3引擎

 邮箱线索

邮箱地址	所在文件
7wb1fnu@gc96h.al	摸瓜V2引擎
admin@imuboy.cn	摸瓜V2引擎
houfeng@dcloud.io	摸瓜V2引擎
yanyilin@dcloud.io	摸瓜V2引擎
hilogjw@gmail.com	摸瓜V2引擎
gal@mozilla.com cjones@mozilla.com shaon.barman@gmail.com 31@inspiration.org	摸瓜V2引擎

z1@vingtetun.org justindarc@gmail.com	
jack@greensock.com	摸瓜V2引擎
h@p5w.بئسii	摸瓜V2引擎

手机线索

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=CN, ST=shanghai, L=shanghai, O=null, OU=null, CN=fang
签名算法: rsassa_pkcs1v15
有效期自: 2024-03-30 16:05:33+00:00
有效期至: 2124-03-06 16:05:33+00:00
发行人: C=CN, ST=shanghai, L=shanghai, O=null, OU=null, CN=fang
序列号: 0x26b70560
哈希算法: sha256
md5值: 8607b04846c0199763a6205ffc21b45b
sha1值: d5ea81b41725b27ecb7508397a865a277fee86b4
sha256值: 3e4a83edbb6379bf54b4ed21da2a1053af627362e34a0cdaf7f6ce7a1f9cb5a5
sha512值: 00703fd009a0ff552f0dc3896b5a4bedb4315913df8f33c76174d4fae6f97b05cc51387efb0b4e3996443fc6225745c43f4a6208983951d5331e6a62df728643
公钥算法: rsa
密钥长度: 2048
指纹: b6174b698f2a795b1be6d6812d2faec43ce2f8de7b231650e2aca6c308ba16f5

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_feature_confusion_exception_no_private_key_input" : "no private key input"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_feature_confusion_exception_no_private_key_input" : "私钥数据为空"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"

"dcloud_oauth_token_failed": "获取token失败"
"dcloud_permissions_reauthorization": "重新授权"
"dcloud_tips_certificate": "证书"

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