



MoGua

iSeaApp 1.0.0.APK 分析报告



APP名称:

iSeaApp

包名: petrochina.cqsh.dsbztjc

域名线索: 41条

URL线索: 7条

邮箱线索: 2条

分析日期: 2025年7月31日

分析平台: [摸瓜APK反编译平台](#)

文件名: new_isea_cq_dmz_100_jiagu(1).apk
文件大小: 17.46MB
MD5值: 6a74f8767910aaaf8175461deac418c9
SHA1值: cffe7ebb0464adf8739d75fd976e41b0b25d6007
SHA256值: ee5340babf9353962dcfb76d1a56421192ce9ac37242445dec2560adae24e12d

i APP 信息

App名称: iSeaApp
包名: petrochina.cqsh.dsbztjc
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.0
安卓版本: 100

🔍 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
iosoteric.com	没有服务器地理信息.
service.dcloud.net.cn	IP: 110.40.181.119 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

xxx.xxx.xxx	IP: 141.193.213.11 所属国家: United States of America 地区: Texas 城市: Austin 纬度: 30.271158 经度: -97.741699
www.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
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
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
openjsf.org	IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut 纬度: 34.015400 经度: -117.858223
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
pomax.github.io	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
api.bspapp.com	IP: 39.96.249.142 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
caniuse.com	IP: 199.250.214.41 所属国家: United States of America 地区: Virginia 城市: Virginia Beach 纬度: 36.837925 经度: -76.093918
code.google.com	IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
	IP: 104.131.8.164 所属国家: United States of America

bugs.jquery.com	地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
www.google.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
en.wikipedia.org	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
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
www.jacklmoore.com	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
uniapp.dcloud.net.cn	IP: 123.125.244.31 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

franklinta.com	IP: 45.79.104.128 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
jsfiddle.net	IP: 172.67.158.9 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
210.12.193.87	IP: 210.12.193.87 所属国家: China 地区: Guangdong 城市: Zhongshan 纬度: 22.520580 经度: 113.382317
ask.dcloud.net.cn	IP: 123.125.244.28 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
stackoverflow.com	IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
echarts.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
api.next.bspapp.com	IP: 203.107.60.33 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
blogs.adobe.com	IP: 151.101.91.10 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
dribbble.com	IP: 18.245.86.61 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
bugs.webkit.org	IP: 17.33.193.45 所属国家: United States of America 地区: California 城市: Cupertino 纬度: 37.316605 经度: -122.046486
quilljs.com	IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 17.253.85.205 所属国家: Hong Kong 地区: Hong Kong

developer.apple.com	城市: Hong Kong 纬度: 22.285521 经度: 114.157692
graphics.ethz.ch	IP: 129.132.145.103 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
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
sole.github.io	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
lodash.com	IP: 13.215.239.219 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
tc39.github.io	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724

apis.map.qq.com	IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
underscorejs.org	IP: 172.67.134.18 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
momentjs.com	IP: 104.16.32.155 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: 104.18.22.19 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://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎

https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
http://210.12.193.87:20080/miniodown/down?path=	摸瓜V2引擎
">https://lodash.com/>	摸瓜V2引擎
">https://openjsf.org/>	摸瓜V2引擎
">https://lodash.com/license>	摸瓜V2引擎
">http://underscorejs.org/LICENSE>	摸瓜V2引擎
https://npms.io/search?q=ponyfill.	摸瓜V2引擎
http://210.12.193.87:20080	摸瓜V2引擎
https://api.next.bspapp.com	摸瓜V2引擎
https://api.bspapp.com	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/secure-network.html	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/emn178/is-md5	摸瓜V2引擎

https://github.com/chenm170/js-mus	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://caniuse.com/	摸瓜V2引擎
https://github.com/WICG/EventListenerOptions/blob/gh-pages/explainer.md	摸瓜V2引擎
https://code.google.com/p/v8/issues/detail?id=2291	摸瓜V2引擎
https://www.github.com/pissang)	摸瓜V2引擎
https://franklinta.com/2014/09/08/computing-css-matrix3d-transforms/	摸瓜V2引擎
http://www.jacklmoore.com/notes/mouse-position/)	摸瓜V2引擎
https://bugs.jquery.com/ticket/8523	摸瓜V2引擎
https://github.com/jquery/jquery/blob/master/src/event.js	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/MouseEvent/which	摸瓜V2引擎
https://github.com/ecomfe/zrender/pull/536	摸瓜V2引擎
https://github.com/sole/tween.js/blob/master/src/Tween.js	摸瓜V2引擎
http://sole.github.io/tween.js/examples/03_graphs.html	摸瓜V2引擎
https://github.com/mziccard/node-timsort	摸瓜V2引擎
https://jsfiddle.net/pissang/jr4x7mdm/8/	摸瓜V2引擎
http://stackoverflow.com/questions/20883421/sorting-in-javascript-should-every-compare-function-have-a-return-0-statement	摸瓜V2引擎

http://stackoverflow.com/questions/2000542/sorting-in-javascript-should-every-compare-function-have-a-return-statement	摸瓜V2引擎
https://github.com/v8/v8/blob/47cce544a31ed5577ffe2963f67acb4144ee0232/src/js/array.js	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/CanvasRenderingContext2D/globalCompositeOperation	摸瓜V2引擎
https://github.com/ecomfe/zrender/issues/189	摸瓜V2引擎
https://bugs.webkit.org/show_bug.cgi?id=203681	摸瓜V2引擎
https://github.com/pissang	摸瓜V2引擎
http://iosoteric.com/additive-animations-animatewithduration-in-ios-8/	摸瓜V2引擎
https://developer.apple.com/videos/wwdc2014/	摸瓜V2引擎
https://github.com/deltakosh/handjs/blob/master/src/hand.base.js	摸瓜V2引擎
https://msdn.microsoft.com/en-us/library/dn433243(v=vs.85).aspx	摸瓜V2引擎
https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎
http://pomax.github.io/bezierinfo/	摸瓜V2引擎
http://www.github.com/pissang	摸瓜V2引擎
https://en.wikipedia.org/wiki/Largest_remainder_method	摸瓜V2引擎
https://momentjs.com/	摸瓜V2引擎
https://tc39.github.io/ecma262/	摸瓜V2引擎
https://github.com/d3/d3/blob/9cc9a875e636a1dcf36cc1e07bdf77e1ad6e2c74/src/arrays/quantile.js	摸瓜V2引擎
https://dribbble.com/shots/1065060-Infographic-Die-chart-visualization	摸瓜V2引擎

https://dribbble.com/shots/1065960-Infographic-Pie-chart-visualization	摸瓜V2引擎
http://blogs.adobe.com/webplatform/2014/02/24/using-blend-modes-in-html-canvas/	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/SVG/Attribute/fill-rule	摸瓜V2引擎
http://en.wikipedia.org/wiki/Level_of_measurement	摸瓜V2引擎
https://github.com/d3/d3/blob/b516d77fb8566b576088e73410437494717ada26/src/time/scale.js >	摸瓜V2引擎
https://jsperf.com/try-catch-performance-overhead	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/Events/mousewheel),	摸瓜V2引擎
https://github.com/d3/d3-hierarchy)	摸瓜V2引擎
https://github.com/d3/d3-hierarchy/blob/4c1f038f2725d6eae2e49b61d01456400694bac4/src/tree.js >	摸瓜V2引擎
http://xxx.xxx.xxx ,	摸瓜V2引擎
https://graphics.ethz.ch/teaching/scivis_common/Literature/squarifiedTreeMaps.pdf >.	摸瓜V2引擎
https://github.com/d3/d3/blob/9cc9a875e636a1dcf36cc1e07bdf77e1ad6e2c74/src/layout/treemap.js >	摸瓜V2引擎
https://github.com/d3/d3/blob/b516d77fb8566b576088e73410437494717ada26/src/layout/force.js	摸瓜V2引擎
https://en.wikipedia.org/wiki/Parallel_coordinates >	摸瓜V2引擎
https://en.wikipedia.org/wiki/Box_plot >	摸瓜V2引擎
https://echarts.apache.org/examples/en/editor.html?c=custom-gantt-flight	摸瓜V2引擎
http://stackoverflow.com/questions/21125587/css3-transition-not-working-in-chrome-anymore	摸瓜V2引擎
http://msdn.microsoft.com/en-us/library/ms531194%28VS.85%29.aspx	摸瓜V2引擎

https://github.com/kpdecker/jsdiff/blob/master/src/diff/base.js	摸瓜V2引擎
https://html.spec.whatwg.org/multipage/canvas.html	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
emn178@gmail.com	摸瓜V2引擎
errorrik@gmail.com firede@firede.us kener.linfeng@gmail.com	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: CN=datong, OU=datong, O=datong, L=beijing, ST=beijing, C=China
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-11 05:53:15+00:00
有效期至: 2050-06-05 05:53:15+00:00
发行人: CN=datong, OU=datong, O=datong, L=beijing, ST=beijing, C=China
序列号: 0x1
哈希算法: sha256
md5值: e3f7b7cfe6bb6031dcfd894ca5459eea

sha1值: d214138b93f224830d901d148189d10d2ec34be9
sha256值: 15b64152c5c6edb10ce03970a5f99b8ab4eba497de46f99741853108092f8f04
sha512值: 70825b33f79d015c76c3f42939b2290afa6fb6edd979c1f0ec1ced4b7191c6379345b0c1f8bf921101947e4989ebf720b7dbc90475c969e7caf2fbd1e3b2c213
公钥算法: rsa
密钥长度: 2048
指纹: 2c142120cc886683e839e972bc5039e3b75380b033323867b270a2a3507dae68

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_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_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_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

--

向手机申请的权限	是否危险	类型	详细情况
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.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
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
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。

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。