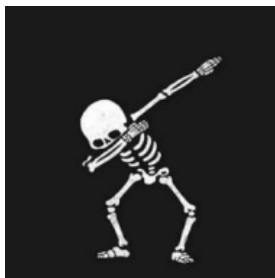




MoGua

欧皇宝典k 1.4.6.APK 分析报告



APP名称:

欧皇宝典k

包名:	plus.H505019C0
域名线索:	26条
URL线索:	21条
邮箱线索:	2条
分析日期:	2025年5月5日
分析平台:	摸瓜APK反编译平台

文件名: 欧皇宝贝v1.4.6.apk
文件大小: 12.12MB
MD5值: 1d168cf125e07ebf6ce0d09b8f6de81f
SHA1值: 8ca2626e1ddd1a9d2e784e559cfe006977c35079
SHA256值: 0b097e108ffda7d0c9a7541fd989852a0d1724ab95d1ca780bc1aa8f306afa11

i APP 信息

App名称: 欧皇宝典k
包名: plus.H505019C0
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.4.6
安卓版本: 100

🔍 域名线索

域名	服务器信息
120.78.205.139	IP: 120.78.205.139 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
m3w.cn	IP: 101.72.254.91 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
bugs.jquery.com	IP: 104.131.8.164 所属国家: United States of America 地区: New Jersey

	城市: Clifton 纬度: 40.858585 经度: -74.163605
support.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
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
dev.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
bugs.webkit.org	IP: 17.33.192.145 所属国家: United States of America 地区: California 城市: Cupertino 纬度: 37.316605 经度: -122.046486
jquery.org	IP: 104.18.159.194 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 34.110.178.183

bugzilla.mozilla.org	所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
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
blindsignals.com	IP: 103.224.182.247 所属国家: Australia 地区: Victoria 城市: Beaumaris 纬度: -37.982201 经度: 145.038940
perfectionkills.com	IP: 192.30.252.153 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
sms.yixinwl.top	IP: 156.241.156.176 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
code.google.com	IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660

	经度: -79.382927
jquery.com	IP: 104.18.155.119 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
103.88.35.202	IP: 103.88.35.202 所属国家: China 地区: Zhejiang 城市: Ningbo 纬度: 29.878410 经度: 121.549767
schemas.android.com	没有服务器地理信息.
dev.dcloud.net.cn	IP: 116.131.57.100 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
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

ns.adobe.com	没有服务器地理信息.
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
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
er.dcloud.io	没有服务器地理信息.
ask.dcloud.net.cn	IP: 101.72.254.86 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
sizzlejs.com	IP: 104.17.98.190 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
-------	---------

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://ask.dcloud.net.cn/article/35627	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.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
http://jquery.com/	摸瓜V2引擎
http://sizzlejs.com/	摸瓜V2引擎

http://jquery.org/license	摸瓜V2引擎
http://jsperf.com/thor-indexof-vs-for/5	摸瓜V2引擎
http://bugs.jquery.com/ticket/13378	摸瓜V2引擎
http://bugs.jquery.com/ticket/12359	摸瓜V2引擎
http://msdn.microsoft.com/en-us/library/ie/hh465388.aspx	摸瓜V2引擎
https://bugs.webkit.org/show_bug.cgi?id=136851	摸瓜V2引擎
https://github.com/jquery/sizzle/pull/225	摸瓜V2引擎
http://msdn.microsoft.com/en-us/library/ms536429%28VS.85%29.aspx	摸瓜V2引擎
http://bugs.jquery.com/ticket/12282	摸瓜V2引擎
http://jsperf.com/getall-vs-sizzle/2	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/CSS/display	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=649285	摸瓜V2引擎
https://bugzilla.mozilla.org/show_bug.cgi?id=491668	摸瓜V2引擎
http://blindsignals.com/index.php/2009/07/jquery-delay/	摸瓜V2引擎
https://support.microsoft.com/kb/2856746	摸瓜V2引擎
https://bugs.webkit.org/show_bug.cgi?id=29084	摸瓜V2引擎
https://code.google.com/p/chromium/issues/detail?id=229280	摸瓜V2引擎

https://github.com/jquery/jquery/pull/764	摸瓜V2引擎
https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries	摸瓜V2引擎
https://github.com/jquery/jquery/pull/557)	摸瓜V2引擎
https://github.com/carhartl/jquery-cookie	摸瓜V2引擎
http://103.88.35.202:88/login?key='+km2+'&uid=222222',	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://sms.yixinwl.top/login?key=WGFZ7e32d2e80681&uid=222	摸瓜V2引擎
http://103.88.35.202:88/login?key='+pwd.value+'&uid=222222',	摸瓜V2引擎
http://120.78.205.139:8001/kk/index.php?key='+pwd.value+'&uid='+uuid,	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
lizhiziyan@qq.com	摸瓜V2引擎
houfeng@dcloud.io	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=, L=, O=Android, OU=Android, CN=pNk%2Ba8bRBaLYgpNV3YfuuTapFhwEkYclfypGRyS7eEHxhDZEdu6iLAd6zcczxhb98HGx55aeNxFr4nwzPpkV8A%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-20 12:46:10+00:00
有效期至: 2125-02-24 12:46:10+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=pNk%2Ba8bRBaLYgpNV3YfuuTapFhwEkYclfypGRyS7eEHxhDZEdu6iLAd6zcczxhb98HGx55aeNxFr4nwzPpkV8A%3D%3D
序列号: 0x42c149bf
哈希算法: sha256
md5值: e5ab562e796e63b6c7cad8ed9c6d4c0c
sha1值: 8500abf19cb92cca92a01f98ef508fe17cc940b1
sha256值: 7ded0c4012283a84ef25ab44cbbb11fcc20f3760447875c0714773aee9e7248
sha512值: 8f99f4c98b4dd42c3f4c795159c16151453e328988633af36ebdec534971c44dc20216461958f30b411932de59dada50f3dfd67777b1ad776787a55c3fa9e11
公钥算法: rsa
密钥长度: 2048
指纹: b8513c2e0873f6b8bdb37eaab170b41c5b09f72ece5b8826ffbdb73b0e79048f

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_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_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
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_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
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。

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h505019c0://,

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。