



MoGua

JavDB 1.9.11.APK 分析报告



APP名称:

JavDB

包名:	com.example.astarte
域名线索:	19条
URL线索:	23条
邮箱线索:	5条
分析日期:	2025年5月11日
分析平台:	摸瓜APK反编译平台

文件名: jdb_official_v1.9.11.apk
文件大小: 29.75MB
MD5值: d0eb935739fb2e7741bb45362e6d52f2
SHA1值: 1e411867d5db9627b425d71dea801949efda3e68
SHA256值: 4b0fb88de1ff15cf8764aef0de11d6d98bcbc1a97d77c1b83593aad536cb3b9

i APP 信息

App名称: JavDB
包名: com.example.astarte
主活动Activity: com.example.astarte.MainActivity
安卓版本名称: 1.9.11
安卓版本: 1

🔍 域名线索

域名	服务器信息
www.w3.org	IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge 纬度: 42.365078 经度: -71.104523
developer.android.com	IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
fanyi.baidu.com	IP: 110.242.68.186 所属国家: China 地区: Hebei

	城市: Baoding 纬度: 38.851109 经度: 115.490280
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ns.adobe.com	没有服务器地理信息.
api.rollbar.com	IP: 35.201.81.77 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
staging.letidi.com	IP: 162.159.138.85 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.ibm.com	IP: 104.107.215.168 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Dusseldorf 纬度: 51.221722

	经度: 6.776160
flutter.dev	IP: 151.101.1.195 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: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
upload.ffmpeg.org	IP: 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris 纬度: 48.853409 经度: 2.348800
dashif.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
aomedia.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
schemas.android.com	没有服务器地理信息.

jdforrepam.com	IP: 104.21.71.233 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.apple.com	IP: 17.253.83.206 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067
www.sl4j.org	IP: 83.166.144.67 所属国家: Switzerland 地区: Geneve 城市: Carouge 纬度: 46.180962 经度: 6.139210
www.instagram.com	IP: 104.244.46.21 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446

 URL线索

URL信息	Url所在文件
https://api.rollbar.com/api/1/item/	com/rollbar/notifier/sender/SyncSender.java
http://ns.adobe.com/xap/1.0/	d0/a.java

http://www.w3.org/ns/ttml#parameter	g3/c.java
http://schemas.android.com/apk/res/android	o/i.java
http://127.0.0.1:8080	w6/g.java
http://127.0.0.1:8080	y6/d.java
http://ns.adobe.com/xap/1.0/	y1/a.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	m6/c.java
http://www.slf4j.org/codes.html#replay	m6/c.java
http://www.slf4j.org/codes.html#substituteLogger	m6/c.java
http://www.slf4j.org/codes.html#unsuccessfulInit	m6/c.java
http://www.slf4j.org/codes.html#loggerNameMismatch	m6/c.java
http://www.slf4j.org/codes.html#multiple_bindings	m6/c.java
http://www.slf4j.org/codes.html#version_mismatch	m6/c.java
http://dashif.org/guidelines/last-segment-number	v2/d.java
http://dashif.org/guidelines/trickmode	v2/d.java
https://aomedia.org/emsg/ID3	j2/a.java
https://developer.apple.com/streaming/emsg-id3	j2/a.java
https://github.com/flutter/flutter/issues/2897 .It	io/flutter/plugin/platform/PlatformViewsController.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java

https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/videoplayer/VideoPlayerPlugin.java
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libijkplayer.so
http://www.w3.org/XML/1998/namespace	lib/armeabi-v7a/libflutter.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues	lib/armeabi-v7a/libflutter.so
https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/svg	lib/armeabi-v7a/libapp.so
https://jdforrepam.com	lib/armeabi-v7a/libapp.so
http://www.w3.org/1998/Math/MathML	lib/armeabi-v7a/libapp.so
https://staging.letidi.com	lib/armeabi-v7a/libapp.so
http://www.w3.org/2000/xmlns/	lib/armeabi-v7a/libapp.so
https://www.instagram.com/	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://fanyi.baidu.com/#auto/	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android	lib/armeabi-v7a/libapp.so

https://github.com/flutter/flutter/issues/new.	lib/armeabi-v7a/libapp.so
ftp://upload.ffmpeg.org/incoming/	lib/arm64-v8a/libijkplayer.so
http://www.w3.org/XML/1998/namespace	lib/arm64-v8a/libflutter.so
http://www.w3.org/2000/xmlns/	lib/arm64-v8a/libflutter.so
https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so

 邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so
_httpparser@13463476.responsepa _double@0150898.fromintege ._future@4048458.immediate _growablelist@0150898._literal _link@14069316.fromrawpat c_growablelist@0150898.withcapaci _growablelist@0150898._literal6 _receiveportimpl@1026248.fromrawrec z_timer@1026248.periodic m_growablelist@0150898._literal2 g_bigintimpl@0150898.from _list@0150898.empty tzt@paystatusentity.fromjson _directory@14069316.fromrawpat _casterror@0150898._create	

l_invocationmirror@0150898._withtype
r_growablelist@0150898.empty
_colorfilter@16065589.mode
_colorfilter@16065589.srgbtoline
i_rawsocket@14069316._writepipe
lectiontoolbarbutton@812113492.text
4_uri@0150898.file
_growablelist@0150898._literal1
q_imagefilter@16065589.blur
_growablelist@0150898._literal4
storationinformation@1080124995.fromserial
bb_growablelist@0150898._ofgrowabl
x_growablelist@0150898.of
3_list@0150898._ofimmutab
k_colorfilter@16065589.lineartoser
v_utf8encoder@9003594.withbuffer
_nativesocket@14069316.pipe
_growablelist@0150898._ofimmutab
_cookie@13463476.fromsetcoo
authenticationscheme@13463476.fromstring
_list@0150898.of
_growablelist@0150898._withdata
_list@0150898.generate
n_typeerror@0150898._create
_list@0150898._ofgrowabl
_list@0150898._ofefficie
_growablelist@0150898._literal3
lectiontoolbarbutton@695392285.text
u_growablelist@0150898._ofother
_list@0150898._oflist
_timer@1026248._internal
_growablelist@0150898._literal5
_rawsocket@14069316._readpipe
_socket@14069316._readpipe
_list@0150898._ofother
eo_bytebuffer@7027147._new
ngstreamsubscription@4048458.zoned
_assertionerror@0150898._create

av_nativesocket@14069316.normal
j_filestream@14069316.forstdin
_uri@0150898.directory
qd_growablelist@0150898._literal8

lib/armeabi-v7a/libapp.so

v_file@14069316.fromrawpat gh_growablelist@0150898.generate _uri@0150898.notsimple 7u_growablelist@0150898._literal7 _future@4048458.zonevalue __growablelist@0150898._ofefficie _future@4048458.immediatee m_growablelist@0150898._oflist	
ffmpeg-devel@ffmpeg.org	lib/arm64-v8a/libijkplayer.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
appro@openssl.org	lib/arm64-v8a/libijkffmpeg.so

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java
17512775099	p3/a.java

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=us, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-08-04 13:46:01+00:00

Valid To: 2047-12-21 13:46:01+00:00
Issuer: C=us, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x9e409b2
Hash Algorithm: sha256
md5: a8bb12e4d0a930301325d968497ccf7b
sha1: 278ef4b9f8dfe1dbbfc8e63cecba486cddbaf9e9
sha256: 23952c015d33464d547d62e5297f6fae75385ea30f8950adce04899cb5e1252d
sha512: f2eb6d324bbad273b5594a39d91d20ac2514fe04ca8691ae54ddb33b7484ea92f0a057de31223cf930cd060711d0e4f0bf04fdebd372074622609660fd27ac43
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d5e6bc4bbc4e7c76a70f50e199ba7b91cea1ef0020e951bb6b3b11d4eb6d981c

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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.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.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_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.ACCESS_MEDIA_LOCATION	危险	访问的任何地理位置	允许应用程序访问的任何地理位置持久保存在用户的共享集合
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.example.astarte.MainActivity	Schemes: dvkft4://,