



至尊娱乐 3.0.0.APK 分析报告



APP名称:

至尊娱乐

包名: com.a694880.hccae83

域名线索: 26条

URL线索: 14条

邮箱线索: 0条

分析日期: 2025年8月2日

分析平台: [摸瓜APK反编译平台](#)

文件名: ZhiZunYL-ugjh.apk
文件大小: 13.54MB
MD5值: bcd4591964ad01bff42f690b7887dc83
SHA1值: 220011e9b07240ce7f154d8bfe603fd77e443938
SHA256值: b4cf8bc1aa681bd4c39625b42297bd24d3692b03acf7ea66c8fc6be16b4f3eff

i APP 信息

App名称: 至尊娱乐
包名: com.a694880.hccae83
主活动Activity: com.gpk17.gbrowser.activities.SplashScreenActivity
安卓版本名称: 3.0.0
安卓版本: 2919

🔍 域名线索

域名	服务器信息
drifty.com	IP: 104.21.56.84 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
fontawesome.com	IP: 104.18.23.52 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
checkip.amazonaws.com	IP: 18.142.27.231 所属国家: Singapore 地区: Singapore

	城市: Singapore 纬度: 1.289987 经度: 103.850281
schemas.android.com	没有服务器地理信息.
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
materialdesignicons.com	IP: 34.234.179.93 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
cdn.bvgpkhc.com	IP: 192.142.56.193 所属国家: United States of America 地区: New York 城市: Greenlawn 纬度: 40.868984 经度: -73.365051
lhub.kxdpt.com	没有服务器地理信息.
javax.xml.xmlconstants	没有服务器地理信息.
mikepenz.com	IP: 104.21.27.65 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

scripts.sil.org	IP: 172.67.29.248 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
design.google.com	IP: 172.217.160.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.google.com	IP: 31.13.94.37 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
cdn.fldpknjup.com	IP: 192.142.56.193 所属国家: United States of America 地区: New York 城市: Greenlawn 纬度: 40.868984 经度: -73.365051
3699jg.sdfwf.com	没有服务器地理信息.
5533jg.sdfwf.com	没有服务器地理信息.
9910jg.sdfwf.com	没有服务器地理信息.
ionicons.com	IP: 172.67.145.112 所属国家: United States of America 地区: California 城市: San Francisco

	纬度: 37.775700 经度: -122.395203
cdn.eyfuisr.com	IP: 192.142.56.193 所属国家: United States of America 地区: New York 城市: Greenlawn 纬度: 40.868984 经度: -73.365051
lhdb.dnmwu.com	没有服务器地理信息.
creativecommons.org	IP: 104.20.6.134 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: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
cdn.ptqvdja.com	IP: 192.142.56.193 所属国家: United States of America 地区: New York 城市: Greenlawn 纬度: 40.868984 经度: -73.365051
lhdb.wzhac.com	没有服务器地理信息.
fontawesome.io	IP: 52.207.38.54 所属国家: United States of America 地区: Virginia 城市: Ashburn

	纬度: 39.039474 经度: -77.491806
pd-1.goonycare.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://javax.xml.XMLConstants/feature/secure-processing	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://apache.org/xml/features/disallow-doctype-decl	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	com/fasterxml/jackson/databind/ext/DOMDeserializer.java
http://javax.xml.XMLConstants/feature/secure-processing	com/fasterxml/jackson/databind/ext/DOMSerializer.java
https://lhub.dnmwu.com	com/gpk17/gbrowser/Settings.java
https://lhub.wzhac.com	com/gpk17/gbrowser/Settings.java
https://lhub.kxdpt.com	com/gpk17/gbrowser/Settings.java
https://9910jg.sdfwf.com/apisrv.php	com/gpk17/gbrowser/Settings.java
https://5533jg.sdfwf.com/apisrv.php	com/gpk17/gbrowser/Settings.java
https://3699jg.sdfwf.com/apisrv.php	com/gpk17/gbrowser/Settings.java
https://)?(m.)	com/gpk17/gbrowser/Utils/Utils.java
https://checkip.amazonaws.com/	com/gpk17/gbrowser/activities/GbrowserActivity.java

https://pd-1.goonycare.com:8443/pics/	com/gpk17/gbrowser/misc/BitmapDiskLruCache.java
http://)	com/gpk17/gbrowser/models/ProjectInfo.java
https://))	com/gpk17/gbrowser/models/ProjectInfo.java
http://%s	com/gpk17/gbrowser/models/ProjectInfo.java
http://%s:%d	com/gpk17/gbrowser/models/ProjectInfo.java
http://scripts.sil.org/OFL	com/mikepenz/fontawesome_typeface_library/FontAwesome.java
https://fontawesome.com/	com/mikepenz/fontawesome_typeface_library/FontAwesome.java
http://creativecommons.org/licenses/by/4.0/	com/mikepenz/google_material_typeface_library/GoogleMaterial.java
https://github.com/google/material-design-icons	com/mikepenz/google_material_typeface_library/GoogleMaterial.java
https://github.com/driftyco/ionicons/blob/master/LICENSE	com/mikepenz/ionicons_typeface_library/Ionicons.java
http://ionicons.com/	com/mikepenz/ionicons_typeface_library/Ionicons.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.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
https://cdn.eyfuisr.com/App/	Mogua Engine V1
https://cdn.bvgpkhc.com/App/	Mogua Engine V1
https://cdn.ptqvdja.com/App/	Mogua Engine V1
https://cdn.fldpknjup.com/app/	Mogua Engine V1

http://mikepenz.com/	Mogua Engine V1
https://github.com/mikepenz/Android-Iconics	Mogua Engine V1
https://materialdesignicons.com/	Mogua Engine V1
http://fontawesome.io/icons/	Mogua Engine V1
https://github.com/FortAwesome/Font-Awesome	Mogua Engine V1
https://www.google.com/	Mogua Engine V1
https://design.google.com/icons/	Mogua Engine V1
https://github.com/google/material-design-icons/	Mogua Engine V1
http://drifty.com/	Mogua Engine V1
http://ionicons.com/	Mogua Engine V1
https://github.com/driftyco/ionicons	Mogua Engine V1

 邮箱线索

 手机线索

 签名证书

APK已签名
v1 签名: False

v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=chengdu, ST=chengdu, L=chengdu, O=iw1715913610700, OU=lk1715913610700, CN=rlew
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-17 02:40:10+00:00
有效期至: 2074-05-05 02:40:10+00:00
发行人: C=chengdu, ST=chengdu, L=chengdu, O=iw1715913610700, OU=lk1715913610700, CN=rlew
序列号: 0x21c3c66d
哈希算法: sha1
md5值: 99e473d44a8c8f3cced00f7542f1b23e
sha1值: d1e380f7132f0806852c8bb2bd23fcb3ccbd44fc
sha256值: 3f322f97873fc8438e7988890bd38eec65c9cdad084e97f9d2843ab69626f94c
sha512值: 4781f102b4528dfdc7cdd6b643d27212ade9c410f9329533f1661dad78992b407390a2c40357d9de431642ed0878548e57247b93522bf0573e41917e21eb5cd0
公钥算法: rsa
密钥长度: 1024
指纹: cd9f524a383bc40f71dcc2431f081ab6d36d816a27093469854003fdb95de625

 硬编码敏感信息

可能的敏感信息
"appKey" : "AppKey"
"generateKeyForJWT" : "generateKeyForJWT"
"google_maps_api_key" : "AlzaSyDnSsq8YP8M_l7ln3QHq8sOzCzUVpKmCyo"
"library_AndroidIconics_author" : "Mike Penz"
"library_AndroidIconics_authorWebsite" : "http://mikepenz.com/"
"library_FontAwesome_author" : "Dave Gandy"
"library_FontAwesome_authorWebsite" : "https://materialdesignicons.com/"

"library_GoogleMaterialDesignIcons_author" : "Google Inc."
"library_GoogleMaterialDesignIcons_authorWebsite" : "https://www.google.com/"
"library_Ionicons_author" : "Drifty"
"library_Ionicons_authorWebsite" : "http://drifty.com/"
"sendRequestForJWT" : "sendRequestForJWT"

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云ToDevice消息传递的权限
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信