



MoGua

出发 1.0.APK 分析报告



APP名称:

出发

包名:	com.wzp.android.rpc
域名线索:	10条
URL线索:	9条
邮箱线索:	1条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件名: 出发.apk
文件大小: 5.46MB
MD5值: 342b56476e2f17091c991cb5116c3853
SHA1值: 5ba8e9200999e7bb9fe37533881258d28d25b97e
SHA256值: 6bd47061b535d936c4d511c760e20ce455ad220cef663f6352791d03d3617bac

i APP 信息

App名称: 出发
包名: com.wzp.android.rpc
主活动Activity: com.wzp.android.rpc.MainActivity
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
www.openssl.org	IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
139.9.164.5	IP: 139.9.164.5 所属国家: China 地区: Guangdong

	城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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
www.eclipse.org	IP: 198.41.30.198 所属国家: Canada 地区: Ontario 城市: Brampton 纬度: 43.702347 经度: -79.711548
wzp-obs.obs.cn-east-2.myhuaweicloud.com	IP: 122.112.208.161 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
xml.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
sekiro.virjar.com	IP: 182.92.142.39 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 104.21.3.132

netty.io	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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

 URL线索

URL信息	Url所在文件
http://xml.apache.org/xslt	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/disallow-doctype-decl	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-general-entities	cn/hutool/core/util/XmlUtil.java
http://xml.org/sax/features/external-parameter-entities	cn/hutool/core/util/XmlUtil.java
http://apache.org/xml/features/nonvalidating/load-external-dtd	cn/hutool/core/util/XmlUtil.java
https://sekiro.virjar.com	com/virjar/sekiro/business/api/util/Constants.java
https://www.openssl.org/docs/manmaster/apps/verify.html	com/virjar/sekiro/business/netty/handler/ssl/OpenSslCertificateException.java
http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html	com/virjar/sekiro/business/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java

http://www.eclipse.org/jetty/documentation/current/npn-chapter.html	com/virjar/sekiro/business/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java
http://netty.io/wiki/sslcontextbuilder-and-private-key.html	com/virjar/sekiro/business/netty/handler/ssl/PemReader.java
http://netty.io/wiki/forked-tomcat-native.html	com/virjar/sekiro/business/netty/handler/ssl/OpenSsl.java
http://netty.io/wiki/reference-counted-objects.html	com/virjar/sekiro/business/netty/util/ResourceLeakDetector.java
https://wzp-obs.obs.cn-east-2.myhuaweicloud.com/serverurl.txt	com/wzp/android/rpc/Main.java
http://139.9.164.5:1234/ppmt/receiveEvent	com/wzp/android/rpc/Main.java

 邮箱线索

邮箱地址	所在文件
auth-agent@openssh.com	cn/hutool/extra/ssh/ChannelType.java

 手机线索

 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-30 17:24:50+00:00

有效期至: 2052-06-22 17:24:50+00:00
 发行人: CN=Android Debug, O=Android, C=US
 序列号: 0x1
 哈希算法: sha1
 md5值: a791f38d7878c1e3ad44421645bfbc62
 sha1值: 8c09b3d31c2336686a3f7de7979ee4e7f56b7caa
 sha256值: 1b31f2da171bc3685389a345b8290b9b08377302de002abd16bbf839e8ac72f0
 sha512值: 218fa80efd861c631ad9e10242e5f4f4eb6482ca63f8ba4cdb02c8ba3a3aa966e1aa845aeb77ded497869e0ace2e1a5b6e63e486aee7c02dc74b14e9136398c0
 公钥算法: rsa
 密钥长度: 2048
 指纹: 4e4c867905e6278cfc01b4f8ad2eed608051818d77b886cbf5e05f80575d1fb3

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

应用内通信

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。