MoGua

G头条 3.4.0.APK 分析报告

APP名称:	G头条

包名:	info.eprb.xvpeb.nay
域名线索:	29条
URL线索:	25条
邮箱线索:	1条
分析日期:	2025年6月11日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: gtt_3.4.0.apk
文件大小: 21.65MB
MD5值: 32c6540c9adba43acc436264a781e7ad
SHA1值: 659d8731b0a8b8d3118b631e3d766be55d8e4903
SHA256值: 67787b2153746347730236a463b4f7eefb66977e152f973827574d7c26fec58c

APP 信息

App名称: G头条
包名: info.eprb.xvpeb.nay
主活动Activity:
安卓版本名称: 3.4.0
安卓版本: 340

域名线索

域名	服务器信息
opentelemetry.io	**IP**: 3.33.186.135 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
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
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
wpk-auth.ucweb.com	**IP**: 157.185.188.1 **所属国家**: Canada **地区**: Ontario **城市**: North York **纬度**: 43.771862 **经度**: -79.331528
woodpecker.uc.cn	**IP**: 116.132.219.154 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
applog.uc.cn	**IP**: 116.132.217.44 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
oss.aliyuncs.com	**IP**: 118.178.29.5 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
d3n1ffjuidexxy.cloudfront.net	**IP**: 13.33.100.206 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

up4.ucweb.com	**IP**: 116.132.216.194 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
gttd6.cc	**IP**: 176.113.70.106 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
dashif.org	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
up4-intl.ucweb.com	**IP**: 157.185.188.1 **所属国家**: Canada **地区**: Ontario **城市**: North York **纬度**: 43.771862 **经度**: -79.331528
oss-cn-.aliyuncs.comor	没有服务器地理信息.
txap1105.workshard.cn	没有服务器地理信息.
image.cnamedomain.com	没有服务器地理信息.
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
gtymm.bvds29x.top	没有服务器地理信息.
storage.googleapis.com	**IP**: 172.217.14.219 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
oss-cn-hangzhou.aliyuncs.com	**IP**: 118.31.219.250 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
inter1017-2691760-1317946434.ap-shanghai.run.tcloudbase.com	**IP**: 124.223.146.85 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ccqgap1212o.gbk15c.top	没有服务器地理信息.
gcttgwo-1325757273.cos.ap-guangzhou.myqcloud.com	**IP**: 36.248.13.182 **所属国家**: China **地区**: Fujian **城市**: Fuzhou **纬度**: 26.061390 **经度**: 119.306107
gjapplog.ucweb.com	**IP**: 157.185.189.158 **所属国家**: Canada **地区**: Ontario **城市**: North York **纬度**: 43.771862

	经度: -79.331528
ccqgap12122.gbk29f.top	没有服务器地理信息.
ccqgap0130p.gsk812.top	**IP**: 156.251.50.180 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
ns.adobe.com	没有服务器地理信息.
ap-southeast-1.log.aliyuncs.com	**IP**: 161.117.125.35 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
t.me	**IP**: 149.154.167.99 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: Warrington **纬度**: 52.184460 **经度**: -0.687590
gtxztgo.oss-cn-guangzhou.aliyuncs.com	**IP**: 8.134.41.206 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572

URL线索

URL信息	Url所在文件
https://ip.	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSImpl.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
http://oss.aliyuncs.com	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://127.0.0.1	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://ccqgap12122.gbk29f.top/	ha/a.java
http://ccqgap1212o.gbk15c.top/	ha/a.java
http://txap1105.workshard.cn/	ha/a.java
http://inter1017-2691760-1317946434.ap-shanghai.run.tcloudbase.com/	ha/a.java
https://opentelemetry.io/schemas/1.20.0	io/opentelemetry/semconv/resource/attributes/ResourceAttributes.java
https://opentelemetry.io/schemas/1.20.0	io/opentelemetry/semconv/trace/attributes/SemanticAttributes.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/danikula/AndroidVideoCache/issues/88.	nc/h.java

https://github.com/danikula/AndroidVideoCache/issues/43.	nc/h.java
https://github.com/danikula/AndroidVideoCache/issues.	nc/h.java
http://%s:%d/%s	nc/j.java
https://github.com/danikula/AndroidVideoCache/issues/134.	nc/j.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	l7/d.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	l7/f.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	l7/i.java
http://dashif.org/guidelines/last-segment-number	v3/d.java
http://dashif.org/guidelines/trickmode	v3/d.java
http://%s:%d/%s	xyz/gqjts/lqpb/dty/HttpProxyCacheServer.java
http://ns.adobe.com/xap/1.0/	b3/a.java
https://gjapplog.ucweb.com/collect	x5/h.java
https://applog.uc.cn/collect	x5/h.java
https://wpk-auth.ucweb.com	x5/d.java
https://woodpecker.uc.cn	x5/d.java
https://up4-intl.ucweb.com/upload	w5/e.java
https://up4.ucweb.com/upload	w5/e.java

http://gtymm.bvds29x.top	gb/f.java
http://ccqgap0130p.gsk812.top/	gb/d.java
http://ccqgap0130p.gsk812.top/	gb/e.java
https://gtxztgo.oss-cn-guangzhou.aliyuncs.com/host.jsonb	t/CG.java
https://gcttgwo-1325757273.cos.ap-guangzhou.myqcloud.com/host.jsonb	t/CG.java
https://storage.googleapis.com/gtgole03/host.jsonb	t/CG.java
https://d3n1ffjuidexxy.cloudfront.net/host.jsonb	t/CG.java
http://gttd6.cc	t/CG.java
https://t.me/xiaoxiao_66666	t/CG.java
https://ap-southeast-1.log.aliyuncs.com	wa/c.java
https://applog.uc.cn/collect	lib/arm64-v8a/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/arm64-v8a/libcrashsdk.so
https://woodpecker.uc.cn	lib/arm64-v8a/libcrashsdk.so
https://wpk-auth.ucweb.com	lib/arm64-v8a/libcrashsdk.so

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	nc/h.java

[illegible]	[illegible]

手机线索

手机号	所在文件
17512775099	t4/a.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java
13516237631	x4/d.java
17882652114	x4/d.java
18914945834	x4/d.java
16832995016	x4/d.java
13846158196	x4/d.java
17471680261	x4/d.java
18826691036	x4/d.java
14159265359	x4/d.java
13446589358	x4/d.java
19870156017	x4/d.java
19846674381	x4/d.java
17387749012	x4/d.java

17222222222	c3/e.java

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: C=howhw, ST=howhw, L=howhw, O=howhw, OU=howhw, CN=howhw
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-05 05:52:12+00:00
有效期至: 2123-07-31 05:52:12+00:00
发行人: C=howhw, ST=howhw, L=howhw, O=howhw, OU=howhw, CN=howhw
序列号: 0x33a5c1fb
哈希算法: sha256
md5值: 5266283c023dc2271ec743ea51ce51ee
sha1值: b42f5b2304750daed25d0276ccf19964ec1fffbc
sha256值: 4a6ff4cb01de0d219fa0c60244c540a0ceb067108e47034b6c62a5dad99976f7
sha512值: 34f1ff51fb2a5ab62d07ee9e1c29a399df0f2888a2cdcf7a8223a01808d9be8960a373fa221d22637cec82446e98c5237a68f1e96351b23f7f1f1fb43be06a61
公钥算法: rsa
密钥长度: 3072
指纹: 34f34724141817325b000a01dfeabb5021ac40ce0df89db00a6e28c3a0e2b6ce

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.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
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.LOCAL_MAC_ADDRESS	未知	Unknown permission	Unknown permission from android reference
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.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.DETECT_SCREEN_CAPTURE	未知	Unknown permission	Unknown permission from android reference

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.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。
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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.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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低

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

应用内通信
