



# ANDROID 静态分析报告



Reqable • v2.33.5

本报告由南明离火移动安全分析平台生成  
本报告由南明离火移动安全分析平台生成

分析日期: 2025-05-31 15:44:16

## i应用概览

文件名称:	reqable-app-android-arm64.apk
文件大小:	29.24MB
应用名称:	Reqable
软件包名:	com.reqable.android
主活动:	com.reqable.android.MainActivity
版本号:	2.33.5
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	47/100 (中风险)
杀软检测:	AI评估: 安全
MD5:	b4bcb3f00f9dbb8be51bdf1d1ddcbe43
SHA1:	bfae81de5b8b95a0087fed3bb9390afffa0d0b17
SHA256:	6ccdfdbc4eb48202c1f06be5a9b11380a9b5d6381d76c2cb40cb5649eb02c0b4

## 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
2	11	1	1	0

## 四大组件导出状态统计

Activity组件: 4个, 其中export的有: 0个
Service组件: 1个, 其中export的有: 1个
Receiver组件: 2个, 其中export的有: 0个
Provider组件: 2个, 其中export的有: 0个

## 应用签名证书信息

APK已签名

v1 签名: True

v2 签名: True

v3 签名: False

v4 签名: False

主题: CN=Reqable, OU=Reqable, O=Reqable, L=Shanghai, ST=Shanghai, C=CN

签名算法: rsassa\_pkcs1v15

有效期自: 2023-11-14 09:55:15+00:00

有效期至: 2073-11-01 09:55:15+00:00

发行人: CN=Reqable, OU=Reqable, O=Reqable, L=Shanghai, ST=Shanghai, C=CN

序列号: 0x1

哈希算法: sha256

证书MD5: 3a9d359c6e1147198f2c9dab400538bf

证书SHA1: 8058feea694f6b5cb5f215bc95657101db7f7b77

证书SHA256: d6b41bee1dc0e39335e1f3171684920bcd192d09bd58fb509a14ef6486d2b666

证书SHA512:

7b8c56de57a60beb0c2bed45a937d1f099a5b3be332d7df789ce61676f6b8ec8d7a4696c56b93e1f93e8e1f4540ccd0b82df3bd9fa5fe786d8c11381212365f

公钥算法: rsa

密钥长度: 2048

指纹: dcb5112c28936af15332ce83b9af706c6cc17bba4b4286cd3e5e6b6c51f43d14

共检测到 1 个唯一证书

## 权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	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.READ_EXTERNAL_STORAGE	危险	读取 SD 卡内容	允许应用程序从 SD 卡读取信息。
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.FOREGROUND_SERVICE	普通	创建前台 Service	Android 9.0 以上允许常规应用程序使用 Service.startForeground，用于 podcast 播放（推送悬浮播放，锁屏播放）
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	普通	启用特殊用途的前台服务	允许常规应用程序使用类型为“specialUse”的 Service.startForeground。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11 引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
com.android.permission.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时代权限	允许应用发布通知，Android 13 引入的新权限。
com.reqable.android.BIND_CORE_SERVICE	未知	未知权限	来自 android 引用的未知权限。



1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、Media Player 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
4	Service (com.reqable.android.NetbareVpnService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_VPN_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处检查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

## </> 代码安全漏洞检测

高危: 0 | 警告: 6 | 信息: 1 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	<a href="#">应用程序记录日志信息,不得记录敏感信息</a>	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MST G-STORAGE-3	<a href="#">升级会员: 解锁高级权限</a>
2	<a href="#">应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密写入数据库</a>	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当 (SQL注入) OWASP Top 10: M7: Client Code Quality	<a href="#">升级会员: 解锁高级权限</a>
3	<a href="#">应用程序可以读取/写入外部存储器。任何应用程序都可以读取写入外部存储器的数据</a>	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MST G-STORAGE-2	<a href="#">升级会员: 解锁高级权限</a>
4	<a href="#">应用程序使用不安全的随机数生成器</a>	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MST G-CRYPTO-6	<a href="#">升级会员: 解锁高级权限</a>

5	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	<a href="#">升级会员: 解锁高级权限</a>
6	<a href="#">SHA-1是已知存在哈希冲突的弱哈希</a>	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	<a href="#">升级会员: 解锁高级权限</a>
7	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	<a href="#">升级会员: 解锁高级权限</a>

## Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈边界)	RELRO	RPATH (指定SO搜索路径)	RUNPATH (指定SO搜索路径)	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED (裁剪符号表)
----	-----	------------	-----	-------------------	-------	------------------	--------------------	-------------------	--------------------------

1	arm64-v8a/libapp.so	<p><b>True info</b> 二进制文件设置了NX位。这标志着内存页面不可执行，使得攻击者注入的shellcode不可执行。</p>	<p>动态共享对象 (DSO) <b>info</b> 共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p><b>True info</b> 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p><b>Not Applicable info</b> RELRO 检查不适用于 Flutter/Dart 二进制文件</p>	None info	None info	<p><b>False info</b> 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数 (如 strcpy, gets 等) 的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用</p>	True info
2	arm64-v8a/libflutter_aviin.so	<p><b>True info</b> 二进制文件设置了NX位。这标志着内存页面不可执行，使得攻击者注入的shellcode不可执行。</p>	<p>动态共享对象 (DSO) <b>info</b> 共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p><b>False info</b> 这个二进制文件没有在线上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。不适用于 Dart/Flutter 库不适用，除非使用了 Dart FFI</p>	<p><b>Full RELRO info</b> 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None info	None info	<p><b>False warning</b> 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数 (如 strcpy, gets 等) 的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用</p>	True info

3	arm64-v8a/libnetbare-jni.so	<p>True <b>info</b></p> <p>二进制文件设置了NX位。这标志着内存页面不可执行，使得攻击者注入的shellcode不可执行。</p>	<p>动态共享对象 (DSO) <b>info</b></p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p>True <b>info</b></p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p>Full RELRO <b>info</b></p> <p>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None	None	<p>False <b>warning</b></p> <p>二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数 (如 strcpy, gets 等) 的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Darwin/Flutter 库不适用</p>	False <b>warning</b> <p>符号可用</p>
4	arm64-v8a/libobjectbox-jni.so	<p>True <b>info</b></p> <p>二进制文件设置了NX位。这标志着内存页面不可执行，使得攻击者注入的shellcode不可执行。</p>	<p>动态共享对象 (DSO) <b>info</b></p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p>True <b>info</b></p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p>Full RELRO <b>info</b></p> <p>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None	None	<p>True <b>info</b></p> <p>二进制文件有以下加固函数: ['_strlen_chk', '_memcpy_chk', '_read_chk', '_vsprintf_chk', '_memmove_chk', '_vsnprintf_chk']</p>	True <b>info</b> <p>符号被剥离</p>

5	arm64-v8a/libreqable_br otli.so	<p>True <b>info</b></p> <p>二进制文件设置了NX位。这标志着内存页面不可执行，使得攻击者注入的shellcode不可执行。</p>	<p>动态共享对象 (DSO) <b>info</b></p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p>True <b>info</b></p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p>Full RELRO <b>info</b></p> <p>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None <b>info</b>	None <b>info</b>	<p>True <b>info</b></p> <p>二进制文件有以下加固函数: ['__memset_chk']</p>	True <b>info</b>
6	arm64-v8a/libreqable_ch ardet.so	<p>True <b>info</b></p> <p>二进制文件设置了NX位。这标志着内存页面不可执行，使得攻击者注入的shellcode不可执行。</p>	<p>动态共享对象 (DSO) <b>info</b></p> <p>共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p>True <b>info</b></p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p>Full RELRO <b>info</b></p> <p>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None <b>info</b>	None <b>info</b>	<p>True <b>info</b></p> <p>二进制文件有以下加固函数: ['__memmove_chk', '__strlen_chk', '__vsprintf_chk']</p>	True <b>info</b>

7	arm64-v8a/libreqable_cronet.so	<p>True info</p> <p>二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。</p>	<p>动态共享对象 (DSO)</p> <p>info</p> <p>共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p>True info</p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p>Full RELRO info</p> <p>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['_FD_SET_chk', '_FD_CLR_chk', '_FD_ISSET_chk']</p>	True info
8	arm64-v8a/libreqable_http.so	<p>True info</p> <p>二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。</p>	<p>动态共享对象 (DSO)</p> <p>info</p> <p>共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p>True info</p> <p>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p>Full RELRO info</p> <p>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['_vsprintf_chk', '_strlen_chk', '_memmove_chk']</p>	True info

9	arm64-v8a/libreqable_nbtbare.so	<p><b>True info</b> 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。</p>	<p>动态共享对象 (DSO) <b>info</b> 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p><b>True info</b> 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p><b>Full RELRO info</b> 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None info	None info	<p><b>True info</b> 二进制文件有以下加固函数: ['_vsprintf_chk', '_memcpy_chk', '_strlen_chk', '_strchr_chk', '_memset_chk', '_read_chk', '_memmove_chk', '_strcat_chk', '_vsnprintf_chk']</p>	True info
10	arm64-v8a/libreqable_zstd.so	<p><b>True info</b> 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。</p>	<p>动态共享对象 (DSO) <b>info</b> 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p><b>True info</b> 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出</p>	<p><b>Full RELRO info</b> 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None info	None info	<p><b>False warning</b> 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数 (如 strcpy, gets 等) 的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用</p>	True info

11	arm64-v8a/libtun2proxy.so	<p><b>True info</b></p> <p>二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。</p>	<p>动态共享对象 (DSO)</p> <p><b>info</b></p> <p>共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。</p>	<p><b>False high</b></p> <p>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于 Dart/Flutter 库不适用，除非使用了 Dart FFI</p>	<p><b>Full RELRO info</b></p> <p>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。</p>	None info	None info	<p><b>False warning</b></p> <p>二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数 (如 strcpy, gets 等) 的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用。</p>	True info
----	---------------------------	--	--	---	---	-----------	-----------	--	-----------

## 应用行为分析

编号	行为	标签	文件
00202	打电话	控制	<a href="#">升级会员：解锁高级权限</a>
00203	将电话号码放入意图	控制	<a href="#">升级会员：解锁高级权限</a>
00063	隐式意图 (查看网页、拨打电话等)	控制	<a href="#">升级会员：解锁高级权限</a>
00051	通过 setData 隐式意图 (查看网页、拨打电话等)	控制	<a href="#">升级会员：解锁高级权限</a>
00013	读取文件并将其放入流中	文件	<a href="#">升级会员：解锁高级权限</a>
00147	获取当前位置的时间	信息收集位置	<a href="#">升级会员：解锁高级权限</a>
00075	获取设备的位置	信息收集位置	<a href="#">升级会员：解锁高级权限</a>
00115	获取设备的最后已知位置	信息收集位置	<a href="#">升级会员：解锁高级权限</a>
00191	获取短信收件箱中的消息	短信	<a href="#">升级会员：解锁高级权限</a>
00036	从 res/raw 目录获取资源文件	反射	<a href="#">升级会员：解锁高级权限</a>

00023	从当前应用程序启动另一个应用程序	反射控制	升级会员: 解锁高级权限
00096	连接到 URL 并设置请求方法	命令网络	升级会员: 解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令网络	升级会员: 解锁高级权限
00109	连接到 URL 并获取响应代码	网络命令	升级会员: 解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员: 解锁高级权限
00209	从最新渲染图像中获取像素	信息收集	升级会员: 解锁高级权限
00210	将最新渲染图像中的像素复制到位图中	信息收集	升级会员: 解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员: 解锁高级权限
00091	从广播中检索数据	信息收集	升级会员: 解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员: 解锁高级权限
00189	获取短信内容	短信	升级会员: 解锁高级权限
00188	获取短信地址	短信	升级会员: 解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员: 解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员: 解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员: 解锁高级权限
00077	读取敏感数据 (短信、通话记录等)	信息收集 短信 通话记录 日历	升级会员: 解锁高级权限

### 敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.CAMERA
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

## 🔍 恶意域名威胁检测

域名	状态	中国境内	位置信息
doh.familyshield.opendns.com	安全	否	IP地址: 75.75.77.197 国家: 美国 地区: 华盛顿 城市: 温哥华 纬度: 45.638634 经度: -122.861453 查看: <a href="#">Google 地图</a>
dns.sb	安全	否	IP地址: 75.75.77.197 国家: 比利时 地区: 布鲁塞尔首都大区市镇 城市: 布鲁塞尔 纬度: 50.850477 经度: 4.348789 查看: <a href="#">Google 地图</a>
doh.dns.sb	安全	否	IP地址: 104.128.62.173 国家: 美国 地区: 伊利诺伊州 城市: 芝加哥 纬度: 41.886875 经度: -88.198830 查看: <a href="#">Google 地图</a>
nextdns.io	安全	否	IP地址: 104.26.11.186 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: <a href="#">Google 地图</a>
dns.google	安全	否	IP地址: 75.75.77.197 国家: 美国 地区: 加利福尼亚 城市: 山景城 纬度: 37.386051 经度: -122.083847 查看: <a href="#">Google 地图</a>
doh.xfinity.com	安全	否	IP地址: 75.75.77.197 国家: 美国 地区: 马萨诸塞州 城市: 切姆斯福德 纬度: 42.599144 经度: -71.366005 查看: <a href="#">Google 地图</a>

www.cisco.com	安全	否	<p>IP地址: 23.222.206.179                      国家: 美国                      地区: 加利福尼亚                      城市: 埃尔塞贡多                      纬度: 33.919201                      经度: -118.416580                      查看: <a href="#">Google 地图</a></p>
odvr.nic.cz	安全	否	<p>IP地址: 193.17.47.1                      国家: 捷克                      地区: 布拉格                      城市: 布拉格                      纬度: 50.087936                      经度: 14.420706                      查看: <a href="#">Google 地图</a></p>
doh-02.spectrum.com	安全	否	<p>IP地址: 193.17.47.1                      国家: 美国                      地区: 伊利诺伊州                      城市: 内珀维尔                      纬度: 41.771000                      经度: -88.153046                      查看: <a href="#">Google 地图</a></p>
dns11.quad9.net	安全	否	<p>IP地址: 193.17.47.1                      国家: 美国                      地区: 加利福尼亚                      城市: 伯克利                      纬度: 37.879318                      经度: -122.265205                      查看: <a href="#">Google 地图</a></p>
cleanbrowsing.org	安全	否	<p>IP地址: 193.17.47.1                      国家: 美国                      地区: 加利福尼亚                      城市: 洛杉矶                      纬度: 34.060734                      经度: -118.239738                      查看: <a href="#">Google 地图</a></p>
dnsnl.alekberg.net	安全	否	No Geolocation information available.
dns10.quad9.net	安全	否	<p>IP地址: 193.17.47.1                      国家: 美国                      地区: 加利福尼亚                      城市: 伯克利                      纬度: 37.879318                      经度: -122.265205                      查看: <a href="#">Google 地图</a></p>
doh-01.spectrum.com	安全	否	<p>IP地址: 193.17.47.1                      国家: 美国                      地区: 伊利诺伊州                      城市: 内珀维尔                      纬度: 41.771000                      经度: -88.153046                      查看: <a href="#">Google 地图</a></p>

www.nic.cz	安全	否	<p>IP地址: 217.31.205.50                      国家: 捷克                      地区: 布拉格                      城市: 布拉格                      纬度: 50.087936                      经度: 14.420798                      查看: <a href="#">Google 地图</a></p>
alekberg.net	安全	否	No Geolocation information available.
www.quad9.net	安全	否	<p>IP地址: 216.21.3.77                      国家: 美国                      地区: 加利福尼亚                      城市: 伯克利                      纬度: 37.879318                      经度: -122.265205                      查看: <a href="#">Google 地图</a></p>
doh.opendns.com	安全	否	<p>IP地址: 209.209.59.227                      国家: 美国                      地区: 华盛顿                      城市: 温哥华                      纬度: 45.638634                      经度: -122.661453                      查看: <a href="#">Google 地图</a></p>
dns.quad9.net	安全	否	<p>IP地址: 149.112.112.112                      国家: 美国                      地区: 加利福尼亚                      城市: 伯克利                      纬度: 37.879318                      经度: -122.265205                      查看: <a href="#">Google 地图</a></p>
docs.rs	安全	否	<p>IP地址: 13.226.225.25                      国家: 美国                      地区: 加利福尼亚                      城市: 洛杉矶                      纬度: 34.052570                      经度: -118.243904                      查看: <a href="#">Google 地图</a></p>
doh.cox.net	安全	否	<p>IP地址: 149.112.112.112                      国家: 美国                      地区: 伊利诺伊州                      城市: 内珀维尔                      纬度: 41.771000                      经度: -88.153046                      查看: <a href="#">Google 地图</a></p>
doh.cleanbrowsing.org	安全	否	<p>IP地址: 149.112.112.112                      国家: 美国                      地区: 加利福尼亚                      城市: 蒂梅丘拉                      纬度: 33.530987                      经度: -117.103394                      查看: <a href="#">Google 地图</a></p>

developers.cloudflare.com	安全	否	<p>IP地址: 209.209.59.227                      国家: 美国                      地区: 加利福尼亚                      城市: 旧金山                      纬度: 37.775700                      经度: -122.395203                      查看: <a href="#">Google 地图</a></p>
objectbox.io	安全	否	<p>IP地址: 149.112.112.112                      国家: 德国                      地区: 图林根                      城市: 弗里德斯多夫                      纬度: 50.604910                      经度: 11.035770                      查看: <a href="#">Google 地图</a></p>
public.dns.ijj.jp	安全	否	<p>IP地址: 149.112.112.112                      国家: 日本                      地区: 东京                      城市: 东京                      纬度: 35.689499                      经度: 139.692872                      查看: <a href="#">Google 地图</a></p>
chromium.dns.nextdns.io	安全	否	<p>IP地址: 209.209.59.227                      国家: 美国                      地区: 加利福尼亚                      城市: 洛杉矶                      纬度: 34.060734                      经度: -118.239738                      查看: <a href="#">Google 地图</a></p>
dns64.dns.google	安全	否	No Geolocation information available.
journeyapps.com	安全	否	<p>IP地址: 216.137.39.6                      国家: 美国                      地区: 加利福尼亚                      城市: 洛杉矶                      纬度: 34.052570                      经度: -118.243904                      查看: <a href="#">Google 地图</a></p>
dns.switch.ch	安全	否	<p>IP地址: 130.59.31.251                      国家: 瑞士                      地区: 苏黎世                      城市: 苏黎世                      纬度: 47.366825                      经度: 8.549790                      查看: <a href="#">Google 地图</a></p>
doh.quickline.ch	安全	否	<p>IP地址: 212.60.63.246                      国家: 瑞士                      地区: 巴塞爾城市州                      城市: 巴塞爾                      纬度: 47.558598                      经度: 7.574011                      查看: <a href="#">Google 地图</a></p>

chrome.cloudflare-dns.com	安全	否	<b>IP地址:</b> 130.59.31.251 <b>国家:</b> 美国 <b>地区:</b> 加利福尼亚 <b>城市:</b> 旧金山 <b>纬度:</b> 37.775700 <b>经度:</b> -122.395203 <b>查看:</b> <a href="#">Google 地图</a>
---------------------------	----	---	---

## 🌐 URL 链接安全分析

URL信息	源码文件
<ul style="list-style-type: none"> <li>10.1.10.1</li> </ul>	v0/c.java
<ul style="list-style-type: none"> <li>8.8.8.8</li> </ul>	v0/d.java
<ul style="list-style-type: none"> <li><a href="https://github.com/flutter/packages/blob/main/packages/in_app_purchase/in_app_purchase/readme.md#loading-products-for-sale">https://github.com/flutter/packages/blob/main/packages/in_app_purchase/in_app_purchase/readme.md#loading-products-for-sale</a></li> </ul>	q4/i.java
<ul style="list-style-type: none"> <li><a href="https://github.com/baseflow/flutter-permission-handler/issues">https://github.com/baseflow/flutter-permission-handler/issues</a></li> </ul>	t0/t.java
<ul style="list-style-type: none"> <li><a href="https://github.com/journeyapps/zxing-android-embedded">https://github.com/journeyapps/zxing-android-embedded</a></li> <li><a href="https://journeyapps.com/">https://journeyapps.com/</a></li> </ul>	自研引擎
<ul style="list-style-type: none"> <li><a href="https://objectbox.io/sync/">https://objectbox.io/sync/</a></li> </ul>	lib/arm64-v8a/libobjectbox-jni.so
<ul style="list-style-type: none"> <li><a href="https://odvr.nic.cz/doh">https://odvr.nic.cz/doh</a></li> <li>185.228.168.9</li> <li><a href="https://doh.dns.sb/dns-query{?dns}">https://doh.dns.sb/dns-query{?dns}</a></li> <li>209.18.47.62</li> <li>208.67.222.222</li> <li>130.59.31.251</li> <li><a href="https://public.dns.iij.jp/dns-query">https://public.dns.iij.jp/dns-query</a></li> <li>185.228.169.11</li> <li>68.105.28.11</li> <li>8.8.8.8</li> <li><a href="https://doh-02.spectrum.com/dns-query{?dns}">https://doh-02.spectrum.com/dns-query{?dns}</a></li> <li><a href="https://dns11.quad9.net/dns-query">https://dns11.quad9.net/dns-query</a></li> <li>193.17.47.1</li> <li>208.67.222.123</li> <li>208.67.220.123</li> <li>www.google.com</li> <li><a href="https://doh.google.com/dns-query">https://doh.google.com/dns-query</a></li> <li>75.75.75.75</li> <li>9.9.9.10</li> <li><a href="https://doh.cleanbrowsing.org/doh/adult-filter{?dns}">https://doh.cleanbrowsing.org/doh/adult-filter{?dns}</a></li> <li>185.228.169.9</li> <li><a href="https://dns.switch.ch/dns-query">https://dns.switch.ch/dns-query</a></li> <li><a href="https://doh.cleanbrowsing.org/doh/security-filter{?dns}">https://doh.cleanbrowsing.org/doh/security-filter{?dns}</a></li> <li>9.9.9.11</li> <li><a href="https://dns.quad9.net/dns-query">https://dns.quad9.net/dns-query</a></li> <li><a href="https://alekberg.net/privacy">https://alekberg.net/privacy</a></li> <li><a href="https://doh-01.spectrum.com/dns-query{?dns}">https://doh-01.spectrum.com/dns-query{?dns}</a></li> <li><a href="https://dns.familyshield.opendns.com/dns-query{?dns}">https://dns.familyshield.opendns.com/dns-query{?dns}</a></li> <li><a href="https://chrome.cloudflare-dns.com/dns-query">https://chrome.cloudflare-dns.com/dns-query</a></li> <li><a href="http://wpad/wpad.dat">http://wpad/wpad.dat</a></li> <li>212.60.61.246</li> <li>185.228.168.10</li> </ul>	

<ul style="list-style-type: none"> <li>• <a href="https://www.quad9.net/home/privacy/">https://www.quad9.net/home/privacy/</a></li> <li>• <a href="https://developers.cloudflare.com/1.1.1.1/privacy/public-dns-resolver/">https://developers.cloudflare.com/1.1.1.1/privacy/public-dns-resolver/</a></li> <li>• 9.9.9.9</li> <li>• <a href="https://public.dns.iij.jp/">https://public.dns.iij.jp/</a></li> <li>• 75.75.76.76</li> <li>• <a href="https://dns64.dns.google/dns-query{?dns}">https://dns64.dns.google/dns-query{?dns}</a></li> <li>• <a href="https://www.nic.cz/odvr/">https://www.nic.cz/odvr/</a></li> <li>• 208.67.220.220</li> <li>• 209.18.47.61</li> <li>• 1.0.0.1</li> <li>• <a href="https://www.cisco.com/c/en/us/about/legal/privacy-full.html">https://www.cisco.com/c/en/us/about/legal/privacy-full.html</a></li> <li>• <a href="https://doh.xfinity.com/dns-query{?dns}">https://doh.xfinity.com/dns-query{?dns}</a></li> <li>• <a href="https://nextdns.io/privacy">https://nextdns.io/privacy</a></li> <li>• <a href="https://cleanbrowsing.org/privacy">https://cleanbrowsing.org/privacy</a></li> <li>• <a href="https://dnsnl.alekberg.net/dns-query{?dns}">https://dnsnl.alekberg.net/dns-query{?dns}</a></li> <li>• 1.2.12.1</li> <li>• 212.60.63.246</li> <li>• 130.59.31.248</li> <li>• 68.105.28.12</li> <li>• <a href="https://doh.cleanbrowsing.org/doh/family-filter{?dns}">https://doh.cleanbrowsing.org/doh/family-filter{?dns}</a></li> <li>• <a href="https://dns.google/dns-query{?dns}">https://dns.google/dns-query{?dns}</a></li> <li>• <a href="https://dns.sb/privacy/">https://dns.sb/privacy/</a></li> <li>• 185.222.222.222</li> <li>• <a href="https://doh.opendns.com/dns-query{?dns}">https://doh.opendns.com/dns-query{?dns}</a></li> <li>• 8.8.4.4</li> <li>• 1.1.1.1</li> <li>• <a href="https://doh.quickline.ch/dns-query{?dns}">https://doh.quickline.ch/dns-query{?dns}</a></li> <li>• 149.112.112.11</li> <li>• <a href="https://chromium.dns.nextdns.io">https://chromium.dns.nextdns.io</a></li> <li>• 185.43.135.1</li> <li>• 45.11.45.11</li> <li>• 185.228.169.168</li> <li>• 149.112.112.112</li> <li>• 185.228.168.168</li> <li>• 149.112.112.10</li> <li>• <a href="https://dns10.quad9.net/dns-query">https://dns10.quad9.net/dns-query</a></li> </ul>	lib/arm64-v8a/libreqable_cronet.so
<ul style="list-style-type: none"> <li>• 127.0.0.1</li> </ul>	lib/arm64-v8a/libreqable_netbare.so
<ul style="list-style-type: none"> <li>• <a href="https://docs.rs/getrandom#nodesjs-module-supportinternal_codedescriptionunknown_code_unknown">https://docs.rs/getrandom#nodesjs-module-supportinternal_codedescriptionunknown_code_unknown</a></li> <li>• data::optmessagelengthcollectedilquidaudhun3usuanetexpirecookiekeepalivepaddingchainunknownclientsubnetaddresssource_prefixscopepolicy</li> <li>• 127.0.0.1</li> <li>• 8.8.8.8</li> </ul>	lib/arm64-v8a/libtun2proxy.so

### 第三方 SDK 组件分析

SDK名称	开发者	描述信息
Flutter	<a href="#">Google</a>	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
Google Play Billing	<a href="#">Google</a>	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。

ZXing Android Embedded	<a href="#">JourneyApps</a>	Barcode scanning library for Android, using ZXing for decoding.
Jetpack App Startup	<a href="#">Google</a>	App Startup 库提供了一种直接、高效的方法在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Firebase	<a href="#">Google</a>	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。

## 🔑 敏感凭证泄露检测

可能的密钥
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy

## ▶ Google Play 应用市场信息

标题: Reqable - 先进API生产力工具

评分: 4.207921 安装: 100,000+ 价格: 0 Android版本支持: 分类: 工具 [Play Store URL: com.reqable.android](#)

开发者信息: Reqable Technology, 5458069517776592710, Shanghai Building 8, No. 251, Liantang Road, Xinghuo Development Zone, Fengxian District, 230000, <https://reqable.com>, [coding@reqable.com](mailto:coding@reqable.com)

发布日期: 2023年12月15日 隐私政策: [Privacy link](#)

关于此应用:

Reqable是新一代API调试 + API测试一站式解决方案，全平台、免登录、轻量级、高性能、无广告，让API更快更简单。Reqable可以抓包应用的HTTP流量，帮助工程师更快更准地定位网络问题。同时，Reqable提供API测试和管理能力，多设备协同工作，让开发和测试更高效。Reqable的之前的版本是HttpCanary，我们重新设计了UI和所有功能，以保持和桌面端的功能一致。

**#1 独立模式** Reqable可以独立地对流量进行监听，无需以来桌面端应用程序。用户可以在手机上直接对应用进行抓包，查看HTTP报文、分析网络请求，方便快捷地定位问题。Reqable手机端提供了各式各样的视图，例如Json视图、Hex视图、图片预览等，方便开发者查看和分析数据。此外，用户还可以对捕获的请求进行重放、编辑、分析和保存等操作。

**#2 协同模式** 如果你觉得手机操作不方便，可以利用App将流量转发到Reqable的桌面端。无需手动配置Wifi代理，只需扫描二维码，即可将手机上的流量转发到桌面端。并且，协同模式下还可以开启增强抓包功能，可以拦截不走系统代理的应用程序的流量，例如Flutter应用程序。协同模式下，用户可以在电脑端直接对请求进行重放、断点、重写和脚本等操作。

**#3 流量抓包** Reqable默认使用VPN技术对应用程序流量进行抓包，目前支持下面这些特性：- HTTP/1.x, HTTP2协议版本。- HTTP/HTTPS/Socks4/Socks4a/Socks5代理协议。- HTTPS, TLSv1.1、TLSv1.2和TLSv1.3加密协议。- 基于HTTP1升级的WebSocket协议。- IPv4 and IPv6。- SSL代理。- HTTP/HTTPS二级代理。- VPN和代理两种模式。- 筛选、搜索和排序。- 编辑API。- 历史记录。- 重放回放。- 颜色高亮。- HAR支持。- 生成代码。

**#4 API测试** Reqable还提供了API测试和管理能力：- HTTP/1.1, HTTP2和HTTP3(QUIC)请求测试。- API集合。- 环境变量。- 参数批量编辑。- 模板设置。- 代理设置。- 性能数据查看。- Cookie管理。- 历史记录。- cURL支持。- 生成代码。用户许可和隐私协议：<https://reqable.com/policy>

## 免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接损失不承担责任。本报告仅用于学习与研究目的，禁止用于任何商业或非法用途。

接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成  
本报告由南明离火移动安全分析平台生成