南明离火
移动应用检测平台

ANDROID 静态分析报告

浩瀚钱包 • v2.0.1.17

分析日期: 2024-06-12 14:58:14

应用概览

文件名称:	浩瀚钱包.apk
文件大小:	38.72MB
应用名称:	浩瀚钱包
软件包名:	uni.UNICAB44FD
主活动:	uni.UNICAB44FD.ui.activity.WelcomeActivity
版本号:	2.0.1.17
最小SDK:	21
目标SDK:	30
加固信息:	360加固 加固
应用程序安全分数:	32/100 (高风险)
跟踪器检测:	3/432
杀软检测:	AI评估：可能有安全隐患
MD5:	2adc81aaa4f22f123cfd1503959c6171
SHA1:	fd232b67fe609b42911dbdcb749abf8030e7560e
SHA256:	773e167269594bd387d6197d205bc485a9ad088121619505c0f3fc348a0365a

分析结果严重性分布

高危	中危	信息	安全	关注
7	13	2	0	12

四大组件导出状态统计

Activity组件：66个，其中export的有： 0个
Service组件：2个，其中export的有： 1个
Receiver组件：0个，其中export的有： 0个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

二进制文件已签名

v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=zhongguo, ST=zhejiang, L=hangzhou, O=hhqb, OU=hhqb, CN=hhqb
签名算法: rsassa_pkcs1v15
有效期自: 2022-05-11 02:30:34+00:00
有效期至: 2122-04-17 02:30:34+00:00
发行人: C=zhongguo, ST=zhejiang, L=hangzhou, O=hhqb, OU=hhqb, CN=hhqb
序列号: 0x550fe19a
哈希算法: sha256
证书MD5: 589b5e9fc007c316c1dc4929ac114e61
证书SHA1: 544924898a4cce14f71ee9ba163cf2ea62cf5f36
证书SHA256: 077b416990993a5266006b5fcb08f33f336ffe718aad75bae5246882d084b5b4
证书SHA512:
61355d9688309b6f7954ef7a0d715cedd086e7c02a01646bfe37e91ce27e147d1009bf2d7c45a78abddbbcdf6732a9af82832b00313ceb16ecac218f6f15cc5d

公钥算法: rsa
密钥长度: 2048
指纹: 9eec19240dc2eae9d62c778c50dbbc37a3732e77165e759680712870717f5294
找到 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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。

android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。

可浏览 Activity 组件分析

ACTIVITY	INTENT
uni.UNICAB44FD.ui.activity.WelcomeActivity	Schemes: bnhk://, Hosts: um.659f9eb695b14f5991151fcf, Path Prefixes: /open,

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名

Manifest 配置安全分析

高危: **0** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。

2	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
4	Service (com.blankj.utilcode.util.MessengerUtils$ServerService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。

代码安全漏洞检测

高危: **6** | 警告: **9** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
2	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
3	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
4	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
5	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限

6	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
7	该文件是World Writable。任何应用程序都可以写入文件	高危	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
8	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	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
9	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
10	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
11	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
12	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
13	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。敏感信息也应加密并写入数据库	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	升级会员：解锁高级权限
14	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成

15	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
16	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限
17	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	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/libinteractive_liveness_fortified.so	True info 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。		True info 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	Full RELRO info 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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strchr_chk', '__strrchr_chk', '__snprintf_chk', '__strcpy_chk', '__sprintf_chk', '__vsnprintf_chk', '__strlcpy_chk', '__strcat_chk', '__read_chk', '__strlen_chk']	True info 符号被剥离
2	arm64-v8a/libjni_liveness_interactive.so	True info 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。		True info 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	Full RELRO info 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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__sprintf_chk', '__vsnprintf_chk', '__strlcpy_chk', '__strcat_chk', '__read_chk', '__strlen_chk']	True info 符号被剥离

3	arm64-v8a/libstidinteractive_liveness.so	True info 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。		True info 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	Full RELRO info 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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__sprintf_chk', '__vsnprintf_chk', '__strlcpy_chk', '__strcat_chk', '__read_chk', '__strlen_chk']	True info 符号被剥离
4	arm64-v8a/libstidocr_frame.so	True info 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。		True info 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	Full RELRO info 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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 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	False warning 符号可用

5	arm64-v8a/libstidocr_quality_jni.so	True info 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。		True info 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	Full RELRO info 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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk']	False warning 符号可用
6	arm64-v8a/libstidocr_stream.so	True info 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。		True info 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	Full RELRO info 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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 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	False warning 符号可用

7	arm64-v8a/libstidocr_stream_jni.so	True info 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。		True info 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	Full RELRO info 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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strlcpy_chk', '__strlen_chk']	False warning 符号可用
8	arm64-v8a/libX86Bridge.so	True info 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。		True info 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	Full RELRO info 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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 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	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.SYSTEM_ALERT_WINDOW android.permission.VIBRATE android.permission.READ_CONTACTS android.permission.REQUEST_INSTALL_PACKAGES android.permission.WRITE_SETTINGS

本报告由南明离火移动安全分析平台生成

其它常用权限	9/46	android.permission.INTERNET android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.WRITE_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID

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
auth.wosms.cn	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
wap.cmpassport.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 安徽 **城市:** 合肥 **纬度:** 31.863815 **经度:** 117.280830 **查看:** 高德地图
sy.cl2m.cn	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
fs.cl2009.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
yuntuapi.amap.com	安全	否	No Geolocation information available.
www.cmpassport.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 安徽 **城市:** 合肥 **纬度:** 31.863815 **经度:** 117.280830 **查看:** 高德地图

prod.hhqianbao.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
sysdk.cl2009.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468943 **查看:** 高德地图
yxappclue.yxqiche.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
test.hhqianbao.com	安全	是	**IP地址:** 47.114.177.49 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
aip.baidubce.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
m.hntxxy.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
e.189.cn	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图

URL链接安全分析

URL信息	源码文件

• 2.0.1.17	自研引擎-M
• https://m.hntxxy.com/gj/index.html?txxychannel=mufctdlpuc85q3lcsvzknfj3nu1yzz09&txxysp=1	uni/UNICAB44FD/ui/activity/LenderReviewStateActivity.java
• https://m.hntxxy.com/gj/index.html?txxychannel=mufctdlpuc85q3lcsvzknfj3nu1yzz09&txxysp=1 • https://yxappclue.yxqiche.com/#/newmarketing?clueapi=phneixclueportal&newmarketingtype=1&thirdpartyid=haohan23070302&timestamp=1688370398839&accesstoken=6fdff52dda2c6217a8c00114ffebd008&subthirdpartyid=haohan230703001&timer=1688370398839	o6/j.java
• https://chatbot.aliyuncs.com/intl/index.htm?from=ip4nxuhax8	uni/UNICAB44FD/ui/activity/CustomerServiceCenterActivity.java
• https://e.189.cn/sdk/agreement/detail.do?hidetop=true • https://auth.wosms.cn/html/oauth/protocol2.html • https://wap.cmpassport.com/resources/html/contract.html • 2.3.6.5	t2/f.java
• https://prod.hhqianbao.com/	uo/j.java
• https://test.hhqianbao.com/ • https://prod.hhqianbao.com/	uni/UNICAB44FD/ui/activity/SettingActivity.java
• https://m.hntxxy.com/gj/index.html?txxychannel=mufctdlpuc85q3lcsvzknfj3nu1yzz09&txxysp=1	uni/UNICAB44FD/ui/activity/ProductInfoActivity.java
• www.cmpassport.com	v2/d.java
• https://sysdk.cl2009.com/log/fdr/v3 • 2.3.6.5	com/chuanglan/shanyan_sdk/tool/i.java
• 2.3.6.5	com/chuanglan/shanyan_sdk/tool/k.java
• https://fs.cl2009.com/flash/thin/accountinit/v3 • 2.3.6.5	com/chuanglan/shanyan_sdk/tool/l.java
• https://e.189.cn/sdk/agreement/detail.do?hidetop=true • https://auth.wosms.cn/html/oauth/protocol2.html • https://wap.cmpassport.com/resources/html/contract.html	com/chuanglan/shanyan_sdk/tool/n.java
• 255.255.255.255 • 127.0.0.1 • 224.0.0.1	v2/p.java
• https://m.hntxxy.com/gj/index.html?txxychannel=mufctdlpuc85q3lcsvzknfj3nu1yzz09&txxysp=1	o6/t.java
• https://aip.baidubce.com/oauth/2.0/token?	uni/UNICAB44FD/util/manager/APIService.java
• 2.3.6.5	com/chuanglan/shanyan_sdk/tool/c.java
• https://m.hntxxy.com/gj/index.html?txxychannel=mufctdlpuc85q3lcsvzknfj3nu1yzz09&txxysp=1 • https://chatbot.aliyuncs.com/intl/index.htm?from=ip4nxuhax8	o6/q.java
• https://sy.cl2m.cn/flash/thin/accountinit/v3 • https://sy.cl2m.cn/flash/accountinit/v4	q2/d.java
• https://wap.cmpassport.com/resources/html/contract.html	q2/a.java

• https://yuntuapi.amap.com • http://yuntuapi.amap.com	j1/w1.java
• 2.3.6.5	u2/f.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
Conscrypt	Google	Conscrypt 是一个 Java 安全提供程序 (JSP)，它实现了部分 Java 加密扩展 (JCE) 和 Java 安全套接字扩展 (JSSE)。 它使用 BoringSSL 为 Android 和 OpenJDK 上的 Java 应用程序提供加密原语和传输层安全性 (TLS)。 有关所提供内容的详细信息，请参阅功能文档。
极光认证 SDK	极光	极光认证整合了三大运营商的网关认证能力，为开发者提供一键登录和号码认证功能，优化用户注册/登录、号码验证的体验，提高安全性。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，但串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
闪验 SDK	创蓝云智	闪验整合三大运营商，支持国内三网手机号段，Android/iOS 手机，可通过一键获取用户手机号的 SDK 产品，建立以手机号码作为关键元素的开放账号体系，提升注册转换效率的必备功能。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户与渠道价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
移动号码认证	中国移动	号码认证能力提供一键登录、本机号码校验服务。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView ， 极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案 ， 并且轻量和极度灵活。
XPopup	li-xiaojun	内置几种了常用的弹窗，十几种良好的动画，将弹窗和动画的自定义设计的极其简单。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。

第三方追踪器检测

名称	类别	网址

AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_CHANNEL" : "HHWallet"
高德地图的=> "com.amap.api.v2.apikey" : "42570a888f6f86c3efff7984554096ad"
SWjJuYVh2eEMwSzVmNklFSmh0UXpVb2xtOVM4eU9Ua3E
WY29tLmFuZHJvaWQuaWQuaW1wbC5JZFByb3ZpZGVySW1wbA
C6K+35Zyo6auY5b635byA5pS+5bmz5Y+w5a6Y572R5LiK5Y+R6LW35oqA5pyv5ZKo6K+i5bel5Y2V4oCU5Yi0puWPt+S4jktleemXrumnQ+i3jOWSqOivokl OVkFMSURfVVNFUl9LRVnlpoLkvZXop6PlhrM=
659f9eb695b14f599d151fcf
QImtleSI6IiVzIiwicGxhdGZvcm0iOiJhbmRyb2lkIiwiZGl1IjoiJXMiLCJhZGl1IjoiJXMiLCJwa2diOiIlcyIsIm1vZGVsIjoiJXMiLCJhcHBuYW1lIjoiJXMiLCJhcHB2ZXJzaW9uIjoiJXMiLCJzeXN2ZXJzaW9uIjoiJXMi
6fdff52dda2c6217a8c00114ffebd008
SYW5kcm9pZC5vcy5zdG9yYWdlLlN0b3JhZ2VWb2x1bWU
EYWN0aW9uLmNvbS5oZXl0YXAub3BlbmlkLk9QRU5fSURfUUVSVklDRQ
WYW5kcm9pZC5wZXJtaXNzaW9uLlJFQURfUEhPTkVfU1RBVEU=
SY29tLmhleXRhcC5vcGVuaWQuSWRlbnRpZmllZXJpaWNl
IaHR0cDovL2xvZ3MuYW1hcC5jb20vdXMvbG9hL3VwbG9hZD9wcm9kdWN0PSVzJnR5cGU9JXMmcGxhdGZvcm09JXMmY2hhbm5lbD0lcyZzaWduPSVz
QY29tLnNhbXN1bmcuYW5kcm9pZC5kZXZpY2VpZHNlcnZpY2UuRGVzaWNlSWRTZXJ2aWNl
WYW5kcm9pZC5uZXQuY29ubi5DT05ORUNUSVZJVFlfQ0hBTkdF
WYW5kcm9pZC5wZXJtaXNzaW9uLkFDQ0VTU19XSUZJX1NUQVRF
AYW5kcm9pZC5wZXJtaXNzaW9uLkFDQ0VTU19OVRXT1JLX1NUQVRF
QY29udGVudnovL2NvbS52aXZvLnZtcy5jZFByb3ZpZGVyL0lkZW50aWZpZXJJZC9PQUlE
txxychannel=MUFCTDlpUC85Q3lCSVZkNFJ3NU1yZz09
WYW5kcm9pZC5wZXJtaXNzaW9uLldSSVRFX1NFVFRJTkdT

ADgAJQBdABEAbgAJAHcAFQCMAEEAzQBFARIAIQEzADkBbAA9AakAoQJKASEDawAJA3QADQOBABFLWVc1a2NtOXBaQzV2Y3k1VFpYSjJhV05sVFdGdVlXZGxjZz09UVoyVjBVMlZ5ZG1salpRPT1JY0dodmJtVT1VYVhCb2lyNWxjM1ZpYVc1bWJ3PT1NWTI5dExtRnVaSEp2YVdRdWFXNTBaWEp1WVd3dWRHVnNaWEJvYjl1NUxrbFVaV3hsY0dodmJua2tVM1IxWWc9PVFZMjl0TG1GdVpISnZhV1F1YVc1MFpYSnVZV3d1ZEdWc1pYQm9iMjU1TGtsUWFHOXVaVk4xWWtsdVptOGtVM1IxWWc9PUdWRkpCVGxOQlExUkpUMDVmWjJWMFJHVjJhV05sU1dRPUVZMjl0TG1GdVpISnZhV1F1YVc1MFpYSnVZV3d1ZEdWc1pYQm9iMjU1TGtsVVpXeGxjR2h2Ym5rPUlZMjl0TG1GdVpISnZhV1F1YVc1MFpYSnVZV3d1ZEdWc1pYQm9iMjU1TGtsUWFHOXVaVk4xWWtsdVptOD1FSW10bGVTSTZJaVZ6SWl3aWNHeGhkR1p2Y20waU9pSmhibVJ5YjJsa0lpd2laR2wxSWpvaUpYTWlMQ0p3YTJjaU9pSWxjeUlzSW0xdlpHVnNJam9pSlhNaUxDSmhjSEJ1WVcxbElqb2lKWE1pTENKaGNIQjJaWEp6YVc5dUlqb2lKWE1pTENKemVYTjJaWEp6YVc5dUlqb2lKWE1pTEE9PUNJbXRsZVNJNklpVnpJaXdpY0d4aGRHWnZjbTBpT2lKaGJtUnliMmxrSWl3aVpHbDFJam9pSlhNaUxDSnRZV01pT2lJbGN5SXNJbWJwWkNJNklpVnpJaXdpZFcxcFpIUWlPaUlsY3lJc0ltMWhiblZtWVdOMGRYSmxJam9pSlhNaUxDSmtaWFpwWTJVaU9pSWxjeUlzSW5OcGJTTZJaVZ6SWl3aWNHdG5Jam9pSlhNaUxDSnRiMlJsYkNJNklpVnpJaXdpWVhCd2RtVnljMmx2YmlJNklpVnpJaXdpWVhCd2JtRnRaU0k2SWlWekIpd2liMkZwWkNJNklpVnpJaXdpWVdScGRTSTZJaVZ6SWl3aWIzTmZkbVZ5SWpvaUpYTWlJWVdsa1BRPT1NZkhObGNtbGhiRDA9UVlXNWtjbTlwWkY5cFpBPT0=

WY29tLnVvZGlzLm9wZW5kZXZpY2UuT1BFTklEU19TRVJWSUNF

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，深入扫描软件中中潜在的漏洞和安全隐隐患。