



## ANDROID 静态分析报告



黑料网 • 1.4.0

分析日期: 2025-07-07 15:26:29

i应用概览

|           |                                                                    |
|-----------|--------------------------------------------------------------------|
| 文件名称:     | hlwapp_1.4.0_250701_6.apk                                          |
| 文件大小:     | 28.37MB                                                            |
| 应用名称:     | 黑料网                                                                |
| 软件包名:     | sg.ixfwr.blukyj                                                    |
| 主活动:      | com.didi.hlw.MainActivity                                          |
| 版本号:      | 1.4.0                                                              |
| 最小SDK:    | 21                                                                 |
| 目标SDK:    | 31                                                                 |
| 加固信息:     | 未加壳                                                                |
| 开发框架:     | Flutter                                                            |
| 应用程序安全分数: | 52/100 (中风险)                                                       |
| 杀软检测:     | AI评估: 可能有安全隐患                                                      |
| MD5:      | 682907dfed45cd78d1a4d0bbe11d9da0                                   |
| SHA1:     | 20ab032ae205350bfecd4ab3609343f181b48ebb                           |
| SHA256:   | 9776a52d608467a5e79e9d154e80e99e86c7fda9518580f98416dcba33324d10b6 |

分析结果严重性分布

|    |    |    |    |    |
|----|----|----|----|----|
| 高危 | 中危 | 信息 | 安全 | 关注 |
| 1  | 5  | 1  | 1  | 0  |

四大组件导出状态统计

|                                |
|--------------------------------|
| Activity组件: 2个, 其中export的有: 0个 |
| Service组件: 1个, 其中export的有: 0个  |
| Receiver组件: 1个, 其中export的有: 1个 |
| Provider组件: 3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=Android Debug, O=Android, C=US

签名算法: rsassa\_pkcs1v15

有效期自: 2022-11-03 10:16:02+00:00

有效期至: 2052-10-26 10:16:02+00:00

发行人: CN=Android Debug, O=Android, C=US

序列号: 0x1

哈希算法: sha1

证书MD5: 7d8a2c0d2493e5d6d85c3865d0918482

证书SHA1: 7682ef35f017d1b3d352557971c295a6885fae4c

证书SHA256: 7b86e6199d7c910d075153a0fe61cf241a4b390dd5f4dd0a74381dab7cf42b6f

证书SHA512: 5d1a8d09f651ee318f3411e559df66a5439dfea5538839f3bc527c6fa3a0671d1326e28949e56f2766e9f716bc9ff5ecb1298370c4bb59b57701a43ef4744178b

公钥算法: rsa

密钥长度: 2048

指纹: a715c81d7c87ff29afca669875aed119aeed1a6f489b5d567f6e4c3922f04e1f

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.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.REQUEST_INSTALL_PACKAGES      | 危险   | 允许安装应用程        | 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.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.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.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.DOWNLOAD_WITHOUT_NOTIFICATION | 普通   | 后台下载文件         | 这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。                       |
| 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.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.RECEIVE_BOOT_COMPLETE<br>D            | 普通 | 开机自启    | 允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。 |
| sg.ixfwr.blukyj.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | 未知 | 未知权限    | 来自 android 引用的未知权限。                                       |

网络通信安全风险分析

| 序号 | 范围 | 严重级别 | 描述 |
|----|----|------|----|
|----|----|------|----|

证书安全合规分析

高危: 1 | 警告: 1 | 信息: 1

| 标题        | 严重程度 | 描述信息                          |
|-----------|------|-------------------------------|
| 已签名应用     | 信息   | 应用已使用代码签名证书进行签名               |
| 检测到调试证书签名 | 高危   | 检测到应用使用调试证书签名。请勿在生产环境中使用调试证书。 |

Manifest 配置安全分析

高危: 0 | 警告: 3 | 信息: 0 | 屏蔽: 0

| 序号 | 问题                                                                                                                                                          | 严重程度 | 描述信息                                                                                                                                     |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 应用已启用明文网络流量<br>[android:usesCleartextTraffic] 属性被设置为 true                                                                                                   | 警告   | 应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 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<br>[android:networkSecurityConfig] 属性被设置为 @7F0C0003                                                                                             | 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<br>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  | Broadcast Receiver (androidx.profileinstaller.ProfileInstallerReceiver) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.DUMP<br>[android:exported=true] | 警告   | 检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。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: 2 | 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<br>OWASP MASVS: MST G-STORAGE-3                                        | <a href="#">升级会员: 解锁高级权限</a> |
| 2  | <a href="#">文件可能包含硬编码的敏感信息,如用户名、密码、密钥等</a>             | 警告 | CWE: CWE-312: 明文存储敏感信息<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MST G-STORAGE-14 | <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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MST G-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/libapp.so       | <p>True<br/><a href="#">info</a></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 she llcode 不可执行。</p> | <p>动态共享对象 (DSO)<br/><a href="#">info</a></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<br/><a href="#">info</a></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>Not Applicable<br/><a href="#">info</a></p> <p>RELRO 检查不适用于 Flutter/Dart 二进制文件</p>                                                                | <p>N<br/>o<br/>n<br/>e<br/><br/><a href="#">info</a></p> <p>二进制文件没有设置运行时搜索路径或 R P A T H</p> | <p>N<br/>o<br/>n<br/>e<br/><br/><a href="#">info</a></p> <p>二进制文件没有设置 R U N P A T H</p> | <p>False<br/><a href="#">info</a></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> | <p>Tr<br/>u<br/>e<br/><br/><a href="#">info</a></p> <p>符号被剥离</p> |
| 2 | arm64-v8a/libwebcrypto.so | <p>True<br/><a href="#">info</a></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 she llcode 不可执行。</p> | <p>动态共享对象 (DSO)<br/><a href="#">info</a></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<br/><a href="#">info</a></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<br/><a href="#">info</a></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> | <p>N<br/>o<br/>n<br/>e<br/><br/><a href="#">info</a></p> <p>二进制文件没有设置运行时搜索路径或 R P A T H</p> | <p>N<br/>o<br/>n<br/>e<br/><br/><a href="#">info</a></p> <p>二进制文件没有设置 R U N P A T H</p> | <p>True<br/><a href="#">info</a></p> <p>二进制文件有以下加固函数: ['_read_chk', '_memset_chk', '_memcpy_chk']</p>                                                                     | <p>Tr<br/>u<br/>e<br/><br/><a href="#">info</a></p> <p>符号被剥离</p> |

应用行为分析

| 编号    | 行为                        | 标签 | 文件                          |
|-------|---------------------------|----|-----------------------------|
| 00054 | 从文件安装其他APK                | 反射 | <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> |
| 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> |
| 00022 | 从给定的文件绝对路径打开文件            | 文件 | <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> |
| 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中                | 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> |
| 00056 | 修改语音音量                    | 控制 | <a href="#">升级会员：解锁高级权限</a> |

敏感权限滥用分析

| 类型       | 匹配   | 权限                                                                                                                                                                                                                                   |
|----------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 恶意软件常用权限 | 6/30 | android.permission.SYSTEM_ALERT_WINDOW<br>android.permission.REQUEST_INSTALL_PACKAGES<br>android.permission.VIBRATE<br>android.permission.READ_PHONE_STATE<br>android.permission.CAMERA<br>android.permission.RECEIVE_BOOT_COMPLETED |
| 其它常用权限   | 5/46 | android.permission.INTERNET<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.ACCESS_WIFI_STATE                              |

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。

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。                                                     |
| IJKPlayer | <a href="#">Bilibili</a> | IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。 |

|                          |                         |                                                                                                                                                                          |
|--------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File Provider            | <a href="#">Android</a> | 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。                                                                              |
| Jetpack App Startup      | <a href="#">Google</a>  | App Startup 库提供了一种直接，高效的方法来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 Start up 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。 |
| Jetpack Media            | <a href="#">Google</a>  | 与其他应用共享媒体内容和控件。已被 media2 取代。                                                                                                                                             |
| Jetpack ProfileInstaller | <a href="#">Google</a>  | 让库能够提前预填充要由 ART 读取的编译轨迹。                                                                                                                                                 |

## 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，深入扫描软件中潜藏的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成