南明离火
移动应用检测平台

ANDROID 静态分析报告

RIGHTHAND - v2.2.2

分析日期: 2025-07-01 05:50:37

应用概览

文件名称:	RIGHTHAND v2.2.2.apk
文件大小:	10.82MB
应用名称:	RIGHTHAND
软件包名:	com.righthandbaseball.righthand
主活动:	com.righthandbaseball.righthand.ui.activity.SplashActivity
版本号:	2.2.2
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	42/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	28eda371658700aae1e508a194c9f5c4
SHA1:	6143e2b6854f6969a3145f4d49fe333660acc6cb
SHA256:	1be41fddf8e90324f487d6eb102b0f734c434f87dce61469a3beb09330997868

分析结果严重性分布

高危	中危	信息	安全	关注
4	12	3	1	0

四大组件导出状态统计

Activity组件：58个，其中export的有： 0个
Service组件：9个，其中export的有： 0个
Receiver组件：3个，其中export的有： 1个
Provider组件：4个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2022-08-30 23:57:57+00:00
有效期至: 2052-08-30 23:57:57+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xb52506bd6069ad0f2defe8fb0d117ff1112a22d2
哈希算法: sha256
证书MD5: 292da70cc537e22cf77d5063b33a6636
证书SHA1: 83fd4f3a80bcb3ccf254aabaceebece5f6169400
证书SHA256: 1e1e2f5a1db3a9f0e6f982e9b53ebfaf11f2baf61c51b4ebc43220f70b8d6b7d
证书SHA512:
6d17bdbcf58229d3b35a6a21c60000b5ff56577ba0fb36c60643d2cc949e7579b888534ddb2bf9bf43a1f5b79bd0b71ac41fd49ed1a33fe6cf72e2c85ce0f8e

公钥算法: rsa
密钥长度: 4096
指纹: 4b53b443b06e33ad3edee5f3c042d8ac2994cbb6e22ce0c4423d0ce10f6afffc
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.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.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.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_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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粗略的经纬度信息，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.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_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.righthandbaseball.righthand.ui.activity.SplashActivity	Schemes: https://, Hosts: righthanddevelop.page.link, righthand.page.link,

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: **0** | 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。

Manifest 配置安全分析

高危: **2** | 警告: **2** | 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 [android:usesCleartextTraffic=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 [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	App 链接 assetlinks.json 文件未找到 [android:name=com.righthandbaseball.righthand.ui.activity.SplashActivity] [android:host=https://righthanddevelop.page.link]	高危	App Link 资产验证 URL（https://righthanddevelop.page.link/.well-known/assetlinks.json）未找到或配置不正确。（状态码：200）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。
4	App 链接 assetlinks.json 文件未找到 [android:name=com.righthandbaseball.righthand.ui.activity.SplashActivity] [android:host=https://righthand.page.link]	高危	App Link 资产验证 URL（https://righthand.page.link/.well-known/assetlinks.json）未找到或配置不正确。（状态码：200）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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: **1** | 警告: **7** | 信息: **3** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用可能可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	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	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
4	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
5	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
6	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
7	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
8	MD5是已知存在哈希冲突的弱哈希	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	升级会员：解锁高级权限
9	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。敏感信息也应加密后写入数据库	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
10	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
11	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

12	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

应用行为分析

编号	行为	标签	文件
00063	隐式意图（查看网页、拨打电话等）	控制	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
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	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
00121	创建目录	文件 命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	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

00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	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
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
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
00012	读取数据并放入缓冲流	文件	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
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00002	打开相机并拍照	相机	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	5/30	android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK

其它常用权限	12/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO android.permission.FLASHLIGHT android.permission.FOREGROUND_SERVICE com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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
righthand-baseball.com	安全	否	IP地址: 35.194.122.208 国家: 日本 地区: 东京 城市: 东京 纬度: 35.689499 经度: 139.692322 查看: Google 地图
righthand.page.link	安全	否	IP地址: 172.217.26.225 国家: 日本 地区: 东京 城市: 东京 纬度: 35.689499 经度: 139.692322 查看: Google 地图
input-righthand-prod.s3.ap-northeast-1.amazonaws.com	安全	否	IP地址: 3.5.158.250 国家: 日本 地区: 东京 城市: 东京 纬度: 35.689499 经度: 139.692322 查看: Google 地图
righthandbaseball.com	安全	否	IP地址: 54.65.129.64 国家: 日本 地区: 东京 城市: 东京 纬度: 35.689499 经度: 139.692322 查看: Google 地图

URL 链接安全分析

URL信息	源码文件
• https://righthandbaseball.com/	com/righthandbaseball/righthand/BuildConfig.java
• https://docs.google.com/viewer?embedded=true&url=	com/righthandbaseball/righthand/ui/activity/PdfActivity.java
• http://%s:%d/%s	com/danikula/videocache/Pinger.java
• https://righthand.page.link	com/righthandbaseball/righthand/other/Constants.java
• https://play.google.com/store/apps/details?id=com.righthandbaseball.righthand • https://input-righthand-prod.s3.ap-northeast-1.amazonaws.com/versioning/android.json	com/righthandbaseball/righthand/ui/dialog/UpdateDialog.java
• file:cropratiox:cropratioy:listener • file:int:int:com.righthandbaseball.righthand.ui.activity.imagecropactivity$oncroplistener	com/righthandbaseball/righthand/ui/activity/ImageCropActivity.java
• www.baidu.com	com/righthandbaseball/righthand/ui/activity/CrashActivity$initData$1.java
• https://righthand-baseball.com/terms-of-service • https://docs.google.com/forms/d/e/1faipqlscnstfi7g9quaruw8fwyyyknfl6ycwwaauxbdin4m-d1arpg/viewform?usp=sf_link • https://righthand-baseball.com/privacypolicy	com/righthandbaseball/righthand/ui/activity/SettingActivity.java
• https://righthand-baseball.com/terms-of-service • https://righthand-baseball.com/privacypolicy	com/righthandbaseball/righthand/ui/activity/ScoutRegisterActivity.java
• https://righthand-baseball.com/terms-of-service • https://righthand-baseball.com/privacypolicy	com/righthandbaseball/righthand/ui/activity/RegisterActivity.java
• https://righthand.page.link	com/righthandbaseball/righthand/ui/fragment/ListFragment$onChildClick$dialog$1.java
• http://%s:%d/%s • 127.0.0.1	com/danikula/videocache/HttpProxyCacheServer.java
• https://righthand.page.link	com/righthandbaseball/righthand/ui/fragment/HomeFragment$onChildClick$dialog$1.java

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已启用	警告	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/149704107565/namespaces/firebase:fetch?key=AIzaSyDzlADNj0CdGU0qTyUvjlds6ja6G2dvk2s ） 已启用。请确保这些配置不包含敏感信息。响应内容如下所示：
		
		{
		"entries": {
		"android_minimum_version": "49",
		"ios_minimum_version": "202212220000"
		},
		"state": "UPDATE",
		"templateVersion": "8"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图 or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架
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。
Jetpack App Startup	Google	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 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	Google	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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

邮箱地址敏感信息提取

EMAIL	源码文件
right-hand@right-hand.jp	自研引擎-S

第三方追踪器检测

名称	类别	网址

本报告由南明离火移动安全分析平台生成

Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyDzlADNj0CdGU0qTyUvjlds6ja6G2dvk2s"
"google_app_id" : "1:149704107565:android:06c1f8b5be7b08ff167aa4"
"google_crash_reporting_api_key" : "AIzaSyDzlADNj0CdGU0qTyUvjlds6ja6G2dvk2s"

Google Play 应用市场信息

标题: RIGHTHAND

评分: None **安装:** 100+ **价格:** 0 **Android版本支持:** **分类:** 体育 **Play Store URL:** com.righthandbaseball.righthand

开发者信息: RIGHTHAND, RIGHTHAND, None, https://righthand-baseball.com, support@righthand-baseball.com,

发布日期: 2022年10月27日 **隐私政策:** Privacy link

关于此应用:

通过集中管理运动员图像和数据，可以实现“运动员可视化”。作为棒球专用的管理应用程序，这项下一代服务在团队强化、球员发展和职业支持方面对球队至关重要。 ▼球员/经理 x 右手： 通过收集和积累分散在团队中的球员信息，我们将为个人和团队提供回顾的机会。在选择职业道路时，它也可以用作投资组合。（您可以在应用程序中执行的操作） □管理播放视频和物理数据 □记录日志和统计数据

免责声明及风险提示: