南明离火
移动应用检测平台

ANDROID 静态分析报告

Engineering Physics 2 • v13.0

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: 2025-08-04 10:48:35

应用概览

文件名称:	Engineering Physics 2 v13.0.apk
文件大小:	12.14MB
应用名称:	Engineering Physics 2
软件包名:	engg.hub.engg.physics.two
主活动:	engg.hub.engg.physics.two.SplashScreen
版本号:	13.0
最小SDK:	24
目标SDK:	35
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	48/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	ab493b5b19d1c03a8321543521fc6e0e
SHA1:	47fcff8c8b9d6b196a3183862606a659bf0d91a2
SHA256:	b610514777a3ad74d66e6c6981fbe8a18090361563eca96d9639a255a6d24897

分析结果严重性分布

高危	中危	信息	安全	关注
1	25	1	0	0

四大组件导出状态统计

Activity组件：17个，其中export的有： 11个
Service组件：12个，其中export的有： 1个
Receiver组件：14个，其中export的有： 7个

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

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: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: CN=Engg Hub
签名算法: rsassa_pkcs1v15
有效期自: 2015-10-05 07:00:10+00:00
有效期至: 2040-09-28 07:00:10+00:00
发行人: CN=Engg Hub
序列号: 0x56121ffa
哈希算法: sha1
证书MD5: 0e9d7f46b36de0092099bb98f788f646
证书SHA1: 47998e1d0877e06811f99b90221760cf79e3c9d1
证书SHA256: e9a6c3a89a6cd949f8b6bb7ead4e58a4f7b788b8cd8f9e8aa64378384b3d63e9
证书SHA512:
9d6806a02c1b38f902fc0a3fbbcd454cc5ba8a0c6264d5842c5232cb97f3a8fcdcd8a16ec49d72e[illegible]f72a[illegible]f8cfddc33819a010375b2a[illegible]c1a7e37f01889ab29ab

公钥算法: rsa
密钥长度: 1024
指纹: 55af23fd2cbe518974c78215a4f89b54579b315a2373631125a47c21772ce54b
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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
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。
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。
engg.hub.enggphysics.two.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。
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。
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.RECEIVE_BOOT_COMPLETED	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。

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

com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。

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

android.permission.ACCESS_ADSERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。
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）
engg.hub.engg.physics.two.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: **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: **0** | 警告: **21** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F140004]	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。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Activity (engg.hub.engg.physics.two.Start_Activity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
4	Activity (engg.hub.engg.physics.two.FirstActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
5	Activity (engg.hub.engg.physics.two.AboutAct) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

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

6	Activity (engg.hub.engg.physics.two.FeedBackAct) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (engg.hub.engg.physics.two.Exiter) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
8	Activity (engg.hub.engg.physics.two.MainActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
9	Activity (engg.hub.engg.physics.two.Three) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
10	Activity (engg.hub.engg.physics.two.Four) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
11	Broadcast Receiver (com.onesignal.FCMBroadcastReceiver) 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。
12	Activity (com.onesignal.NotificationOpenedActivityHMS) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
13	Broadcast Receiver (com.onesignal.NotificationDismissReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
14	Broadcast Receiver (com.onesignal.BootUpReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
15	Broadcast Receiver (com.onesignal.UpgradeReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
16	Activity (com.onesignal.NotificationOpenedReceiver) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

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

17	Activity (com.onesignal.NotificationOpenedReceiverAndroid22AndOlder) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
18	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。
19	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_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。
20	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [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。
21	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [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。
22	高优先级 Intent（999）-{1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

高危: **1** | 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	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

2	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
3	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
4	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

应用行为分析

编号	行为	标签	文件
00036	从 res/raw 目录获取资源文件	反射	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
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
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
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
00078	获取网络运营商名称	信息收集 电话服务	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
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

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

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
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
00009	将游标中的数据放入JSON对象	文件	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	3/30	android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	5/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET com.google.android.gms.permission.AD_ID com.google.android.c2dm.permission.RECEIVE 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。

URL 链接安全分析

URL信息	源码文件
• https://play.google.com/store/apps/developer?id=engineering+wale+baba	engg/hub/engg/physics/two/FirstActivity.java
• http://play.google.com/store/apps/details?id=	engg/hub/engg/physics/two/j.java
• http://play.google.com/store/apps/details?id=	engg/hub/engg/physics/two/FeedBackAct.java

第三方 SDK 组件分析

本报告由南明离火移动安全分析平台生成

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。
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

邮箱地址敏感信息提取

EMAIL	源码文件
georgydoki@gmail.com	自研引擎分

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

敏感凭证泄露检测

可能的密钥
AdMob广告平台的=>"com.google.android.gms.ads.APPLICATION_ID" : "@7F11001C"
"ad_app_id" : "ca-app-pub-6826768390532214~3894156682"
5eb5a37e-b458-11e3-ac11-000c2940e62c
SAPfS6+H98U1C0ANBreIJc5ptiyOYFNSHyBHAhVJyQg=
b2f7f966-d8cc-11e4-bed1-df8f05be55ba

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

o67bbrxK96j6mNouS6gRPl9+GTzx8JOi3tOGIto7FR0=
ghhbpmGyL49K3SA/toagHlFG7fjqknyz6LmyHBjbfiuAtv3WNusjbqa9cLYjKRKjFv3wHbWwZzmIo99q66qbacxuvabdQ5hrNBOetaXg8YM
ylDuICebUCywfmcaa1QU3mVEIhw1XkPyHHrcd1RnCxs=
2a3aa9e0-de43-44a6-8659-31056c8bc54e

Google Play 应用市场信息

标题: Engineering Physics - II

评分: 3.29 **安装:** 5,000+ **价格:** 0 **Android版本支持:** **分类:** 教育 **Play Store URL:** engg.hub.engg.physics.two

开发者信息: Engineering Wale Baba, Engineering+Wale+Baba, None, https://engineeringappsinfo.blogspot.com/app-ads.txt, georgydoki@gmail.com,

发布日期: 2015年10月25日 **隐私政策:** Privacy link

关于此应用:

工程物理2： 该应用程序是一本完整的免费工程物理第一年工程手册，其中涵盖了课程中的重要主题、笔记和材料。 该应用程序列出了 60 个主题，包括详细的注释、图表、方程式、公式和课程资料，主题分为 4 个章节。 该应用程序专为考试和面试时的快速学习、修订、参考而设计。 这个应用程序涵盖了大部分相关主题和所有基础主题的详细解释。 该应用程序中涵盖的一些主题是： 1. 波动学概论 2. 德布罗意物质波 3. 薛定谔方程 4. 波粒二象性 5. 相位和群速度 6. Davisson-Germer 实验 7. 波函数的物理意义 8. 一维盒子中的粒子 9. X射线衍射原理 10.布拉格光谱仪 11.康普顿效应 12. 实验验证：康普顿效应 13. 超声波生产 14. 压电效应 15. 压电发电机 16. 超声波检测 17. 吸声光栅 18. 超声波的应用 19. 超声波清洗应用 20. 介电常数 21. 磁场中的运动 22. 介电常数和极化率 23. 极化率来源 24. 压电 25. 铁电 26. 介电损耗 27. 抗磁性材料的量子力理论 28. Langevins 顺磁性理论 29. 磁场 30. 洛伦兹力 31. 交叉电场和磁场中的运动 32. 载流导体上的力 33. 均匀磁场中电流回路上的转矩 34. 磁偶极子的势能 35. Biot-萨伐尔定律 36. 安培定律 37. 矢量势 38. 电磁感应 39. 运动电动势 40. 时变场 41. 互感 42. 自感 43. 物质中的磁性 44. 铁磁体 45. 抗磁性：位移电流 46.麦克斯韦方程组 47. 电磁波 48. 电磁波的产生 49.坡印亭向量 50. 引言：相变的证据 51. 迈斯纳效应 52. 超导体的磁性 53. I型和II型超导体 54. 超导机理 55. BCS 理论和库珀对 56. 高温超导体 57. 超导体的应用 58. 纳米尺度的重要性 59. 巴基球 60. 正在进行的研发活动 61. 纳米技术的应用 由于字数限制，未列出所有主题。 特征： *章节明智的完整主题 * 丰富的 UI 布局 * 舒适的阅读模式 * 重要的考试题目 * 非常简单的用户界面 *涵盖大部分主题 * 一键获取相关全书 * 移动优化内容 *移动优化图像 这个应用程序将有助于快速参考。使用这个应用程序可以在几个小时内完成所有概念的修改。 请不要给我们较低的评级，而是将您的疑问、问题邮寄给我们，并给我们有价值的评级和建议，以便我们在以后的更新中考虑它。我们很乐意为您解决这些问题。

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。

© 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