南明离火
移动应用检测平台

ANDROID 静态分析报告

Course Demon • v1.0

分析日期: 2025-04-03 16:12:36

应用概览

文件名称:	Course Demon v1.0.apk
文件大小:	4.45MB
应用名称:	Course Demon
软件包名:	com.course.app
主活动:	.MainActivity
版本号:	1.0
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	60/100 (低风险)
杀软检测:	21 个杀毒软件报毒
MD5:	b4f2ff6a8abef3aec0c83e53c9f1dc28
SHA1:	12e1b888c07ea586ac2875c4aeab[illegible]e9e9ea78e1
SHA256:	ddd2bb8e7959842b4993889[illegible]0e7ae092802e3ed134[illegible]bae4[illegible]f39543dd5c3709

分析结果严重性

高危	中危	信息	安全	关注
0	6	1	1	0

四大组件信息

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

证书信息

二进制文件已签名
v1 签名: True

v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d7958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
找到 1 个唯一证书

应用权限

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.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.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.INTERNAL_SYSTEM_WINDOW	签名	显示未授权的窗口	允许创建专用于内部系统用户界面的窗口。普通应用程序不能使用此权限。
android.permission.CONNECTIVITY_INTERNAL	未知	未知权限	来自 android 引用的未知权限。
huawei.permission.ACCESS_LOCATION_SERVICE	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_MOCK_LOCATION	危险	获取模拟定位信息	获取模拟定位信息，一般用于帮助开发者调试应用。恶意程序可以用它来覆盖真实位置信息源。
android.permission.LOCATION_HARDWARE	普通	允许使用硬件中的定位功能	允许应用程序在硬件中使用位置功能，例如：geofencing api。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.READ_CONTACTS	危险	读取联系人信息	允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.READ_CONTENT_RATING_SYSTEMS	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST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。
2	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
3	Broadcast Receiver (.AlarmReceiver) 未被保护。存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

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	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

2	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
3	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

行为分析

编号	行为	标签	文件
00192	获取短信收件箱中的消息	短信	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
00080	将录制的音频/视频保存到文件	录制音视频 文件	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
00101	初始化录音机	录制音视频	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	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
00136	停止录音	录制音视频 命令	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
00090	设置录制的音频/视频文件格式	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
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00006	安排录制任务	录制音视频	升级会员：解锁高级权限
00138	设置音频源（MIC）	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
00133	开始录音	录制音视频 命令	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
00041	将录制的音频/视频保存到文件	录制音视频	升级会员：解锁高级权限

00128	查询用户账户信息	信息收集 账号	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.RECORD_AUDIO android.permission.ACCESS_FINE_LOCATION android.permission.READ_SMS android.permission.SEND_SMS android.permission.READ_CONTACTS android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_MOCK_LOCATION

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。

域名检测

域名	状态	中国境内	位置信息
api.db-ip.com	安全	否	**IP地址:** 172.67.75.166 **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:** Google 地图
api.telegram.org	安全	否	**IP地址:** 149.154.167.220 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://api.db-ip.com/v2/free/self • https://drive.google.com/uc?id= • https://script.google.com/macros/s/akfycbwjdauzuauj3prxql6yjucs_dcltofcd2cvvfojddhurauuqyry-9mkyxlxxoruunzt/exec • https://api.telegram.org/bot	com/course/app/MainActivity.java

第三方SDK

SDK名称	开发者	描述信息
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。

密钥凭证

可能的密钥
Telegram_Bot_API_Key: 6771091056:AAFu9RVkIwKQtLDNpOFZXTrD2DCKhTMJTJQ
qwertyuiopasdfghjklzxcvbnm1234567890

GooglePlay应用信息

标题: FableDuo

评分: 0 **安装:** 10+ **价格:** 0 **Android版本支持:** **分类:** 教育 **Play Store URL:** com.course.app

开发者信息: FableDuo, FableDuo, None, None, fableduo.dev@gmail.com,

发布日期: 2024年7月10日 **隐私政策:** Privacy link

关于此应用:

FableDuo：有趣的互动语言学习体验 学习语言最有效的方法是积极使用它并定期练习。FableDuo 为用户提供了通过语音和文本学习快速有效提高语言技能的机会。 特征： 语音对话： FableDuo 通过现实生活中的对话为用户提供练习机会。这有助于学习者自然而流利地讲语言。语音对话可增强发音和听力技能。 基于文本的练习： 为了提高语法和词汇量，FableDuo 提供了各种基于文本的练习。用户可以在学习新单词的同时增强阅读和写作技能。 个性化学习之旅： FableDuo 提供根据每个用户的语言水平和目标量身定制的个性化学习旅程。这允许用户按照自己的节奏和水平进步。 每日任务和目标： 为了保持用户的积极性，FableDuo 提供了日常任务和目标。这些任务鼓励定期练习并使学习过程变得有趣。 社区支持： 加入 FableDuo 社区，与其他语言学习者联系、分享经验并结交新朋友。这种社交学习环境使语言学习过程更加愉快和富有成效。 高级跟踪和分析： 详细跟踪您的进度，分析您的优势和劣势。这可以帮助您确定需要更多关注的领域并优化您的语言学习策略。 通过 FableDuo 实现您的目标： FableDuo 旨在让语言学习过程既有趣又有效。通过语音对话和基于文本的练习，您可以通过个性化的学习之旅提高语言技能并更快地实现您的目标。 为什么选择两者双核？ 互动学习：通过现实生活中的对话和场景提高您的语言技能。 综合内容：通过各种练习培养语法、词汇、听力和口语技能。 灵活性和个性化：按照您自己的节奏和水平进步，通过个性化的学习旅程实现您的语言目标。 动机和跟踪：通过日常任务、目标和进度跟踪保持积极性。 使用 FableDuo 开始您的语言学习之旅，享受掌握一门新语言的乐趣！立即下载以提高您的语言技能并打开全球有效沟通的大门。

免责声明及风险提示: