南明离火
移动应用检测平台

ANDROID 静态分析报告

自健身 • v3.3.4

分析日期: 2025-08-29 09:35:36

应用概览

文件名称:	user.apk
文件大小:	32.19MB
应用名称:	自健身
软件包名:	com.coach.mu.gymtrain
主活动:	com.mu.gymtrain.Activity.WelcomeActivity
版本号:	3.3.4
最小SDK:	19
目标SDK:	31
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	53/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	4f461a720aba817d6f140a71ac5251cf
SHA1:	d2a28a5f79e20e79c192b69e6c1a7340c1bf7303
SHA256:	a30d07d7d4c302ac1dbdc2b4f302e4e6f0624f7fb0353701b92e1f4386a6da8

分析结果严重性分布

高危	中危	信息	安全	关注
1	25	2	2	0

四大组件导出状态统计

Activity组件：103个，其中export的有： 8个
Service组件：7个，其中export的有： 1个
Receiver组件：5个，其中export的有： 0个
Provider组件：7个，其中export的有： 1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: C=86, ST=北京, L=北京, O=北京, OU=北京, CN=摩码（北京）科技有限公司
签名算法: rsassa_pkcs1v15
有效期自: 2019-08-05 03:19:11+00:00
有效期至: 2044-07-29 03:19:11+00:00
发行人: C=86, ST=北京, L=北京, O=北京, OU=北京, CN=摩码（北京）科技有限公司
序列号: 0x71f65a05
哈希算法: sha256
证书MD5: a23d12938441e3bf273560b7ae98bb3e
证书SHA1: 8fa69dbee43545926826dc4255b97fe6c3a2f04c
证书SHA256: 2ae4c0d1a039ee10975cc186026419ac6bb24fca8d39fbf18e4f420c1571e8d0
证书SHA512:
ef6fba2bd91d5de475f0ae41c4487460e922d92efe01e002ad14686161fe92a761c8db2a5f7f5a7142be9b4cc368a6e8d8527e156f9d8993d6ed56edb85feab0

公钥算法: rsa
密钥长度: 2048
指纹: 826aa362688a0258e70c1d1d3f77441ea2d2f34d7913bfce6e0e03277dab64cc
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.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
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_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.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.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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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.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_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.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.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
com.coach.mu.gymtrain.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。
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.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
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.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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。

android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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。

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: **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。

Manifest 配置安全分析

高危: **1** | 警告: **13** | 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=@7F140002]	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。
4	Activity (cn.jpush.android.ui.PopWinActivity) 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 (cn.jpush.android.ui.PushActivity) 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。
6	Activity (com.coach.mu.gymtrain.wxapi.WXEntryActivity) 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 (com.coach.mu.gymtrain.wxapi.WXPayEntryActivity) 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	Service (cn.jpush.android.service.DaemonService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
9	Activity (cn.jpush.android.service.DActivity) 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	Content Provider (cn.jpush.android.service.DownloadProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。
11	Activity (cn.jpush.android.service.JNotifyActivity) 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。
12	Activity (cn.android.service.JTransitActivity) 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	Activity (cn.jiguang.share.android.ui.JiguangShellActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
14	Activity (cn.jiguang.share.android.ui.JiguangShellActivity) 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。
15	高优先级 Intent（1000） - {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。

代码安全漏洞检测

高危: **0** | 警告: **10** | 信息: **2** | 安全: **2** | 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，不应记录敏感信息	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	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

3	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
4	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
5	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
6	SHA-1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
7	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
8	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
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
10	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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

11	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
12	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
13	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
14	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	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/librtmp-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。	动态共享对象 (DSO) info 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。	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	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	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
00054	从文件安装其他APK	反射	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
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	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
00121	创建目录	文件 命令	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
00204	获取默认铃声	信息收集	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
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
00191	获取短信收件箱中的消息	短信	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
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00177	检查是否授予权限并请求	权限	升级会员：解锁高级权限
00195	设置录制文件的输出路径	录制音视频 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
00007	Use absolute path of directory for the output media file path	文件	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
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
00041	将录制的音频/视频保存为文件	录制音视频	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	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
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限

00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	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	10/30	android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.SYSTEM_ALERT_WINDOW android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS
其它常用权限	13/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.BROADCAST_STICKY android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.CHANGE_NETWORK_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
www.zijianshen.com	安全	是	**IP地址:** 47.94.88.108 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图

www.pgyer.com	安全	是	**IP地址:** 58.220.52.223 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
paygate-yf.meituan.com	安全	是	**IP地址:** 101.236.69.63 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://www.zijianshen.com/index.php/app/classes/get_sub_classes/	com/mu/gymtrain/Fragment/CourseFragment.java
• http://36.112.61.98:8888/article-api/list	com/mu/gymtrain/Activity/OnlineCoachActivity.java
• https://www.zijianshen.com/index.php/app/classes/get_comment_counts_of_class • https://www.zijianshen.com/index.php/app/classes/get_comment_counts_of_coach	com/mu/gymtrain/Activity/AllCommentActivity.java
• 127.0.0.1 • http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
• http://36.112.61.98:8888	com/mu/gymtrain/Fragment/ArticleFragment.java
• https://www.zijianshen.com/index.php/app/friendship/get_praise_info/ • https://www.zijianshen.com/index.php/app/coach/get_coach_info_detail/ • https://www.zijianshen.com/index.php/app/friendship/praise_cancel/ • https://www.zijianshen.com/index.php/app/classes/get_sub_classes/ • http://www.zijianshen.com:18080/public/privacy_policy.html • https://www.zijianshen.com/index.php/app/friendship/get_praisers/ • https://www.zijianshen.com/ • https://www.zijianshen.com/index.php/ • https://www.zijianshen.com/index.php/app/friendship/get_user_sort_info/ • https://www.zijianshen.com/index.php/app/friendship/praise_friend/ • https://www.zijianshen.com/index.php/app/gym/get_gym_info_detail/	com/mu/gymtrain/Utils/UrlConfig.java
• https://www.zijianshen.com/index.php/ • https://www.zijianshen.com/index.php/app/bulletin/get_recharge_instruction	com/mu/gymtrain/Activity/MainPackage/ChargeActivity.java
• https://www.zijianshen.com/index.php/app/classes/get_class_info_detail/ • https://www.zijianshen.com/	com/mu/gymtrain/Activity/MainPackage/CoachDetailActivity.java
• www.pgyer.com	com/pgyersdk/update/a.java
• https://www.zijianshen.com/index.php/app/classes/get_class_info_detail/ • https://www.zijianshen.com/	com/mu/gymtrain/Activity/MainPackage/CKDetailActivity.java

• http://36.112.61.98:8888/ai-service-api	com/mu/gymtrain/Http/api/AiWelcomeByVideoAPI.java
• https://www.zijianshen.com//public/upload	com/mu/gymtrain/Activity/CoachDetailHtmlActivity.java
• http://36.112.61.98:8888/ai-service-api	com/mu/gymtrain/Http/api/AiWelcomeAPI.java
• http://www.pgyer.com/apiv1/crash/add	com/pgyersdk/crash/f.java
• https://www.zijianshen.com/public/invite_toknow.php	com/mu/gymtrain/Activity/InviteActivity.java
• https://www.zijianshen.com/index.php/	com/mu/gymtrain/Activity/HomeActivity.java
• https://www.zijianshen.com/index.php/app/friendship/get_friend_classes_ck • https://www.zijianshen.com/index.php/app/friendship/get_friend_classes_sk	com/mu/gymtrain/Activity/FriendCourseDetailActivity.java
• https://www.zijianshen.com/index.php/app/home/get_contract	com/mu/gymtrain/Activity/WebViewActivity.java
• http://36.112.61.98:8888/ai-service-api	com/mu/gymtrain/Http/api/SendVideoMsgAPI.java
• http://36.112.61.98:8888/ai-service-api	com/mu/gymtrain/Http/api/SendMsgAPI.java
• http://36.112.61.98:8888	com/mu/gymtrain/Http/easy/api/BaseApi_Port8888.java
• https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple	com/alipay/test/a.java
• https://www.zijianshen.com/index.php/	com/mu/gymtrain/Http/easy/RequestServer.java
• file:///system/media/audio/ui/camera_click.ogg	com/pgyersdk/feedback/m.java
• http://www.pgyer.com/apiv1/feedback/add	com/pgyersdk/feedback/k.java
• https://www.zijianshen.com/	com/mu/gymtrain/Activity/PersonalTrainerDetailActivity.java
• https://www.zijianshen.com/index.php/	com/mu/gymtrain/Fragment/RootFragment.java
• http://36.112.61.98:8888/article-api/attribute/list	com/mu/gymtrain/viewmodel/OnlineViewModel.java
• https://www.zijianshen.com//public/upload	com/mu/gymtrain/Activity/MainPackage/GymHtmlDetailActivity.java
• http://%s:%d/%s	com/danikula/videocache/Pinger.java
• https://www.zijianshen.com/index.php/app/bulletin/get_about_us • http://www.zijianshen.com:18080/public/appdownload4.html	com/mu/gymtrain/Fragment/MineFragment.java

• https://github.com/vinc3m1/roundedimageview.git • https://github.com/vinc3m1 • https://github.com/vinc3m1/roundedimageview	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
IJKPlayer	Bilibili	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。
极光推送	极光	JPush 是经过考验的大规模 App 推送平台，每天推送消息数超过 5 亿条。开发者集成 SDK 后，可以通过调用 API 推送消息。同时，JPush 提供可视化的 web 端控制台发送通知，统计分析推送效果。 JPush 全面支持 Android, iOS, Winphone 三大手机平台。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
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。
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。
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

敏感凭证泄露检测

可能的密钥
极光推送的=> "JPUSH_APPKEY" : "e004f2eebd488a73bc013022"
极光推送的=> "JPUSH_CHANNEL" : "developer-default"

"app_wx_key" : "wx0f041dee24e86737"
"Umeng_key" : "585b51c2ae1bf87e7d0019b1"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"app_wx_secret" : "9a944bf42c3c9306a9bfbd1c467db152"
mGUKhyCYw/1FnPEZQ8FGeDB7QaATHkNbkLAeBpLvF9wgj9s6oNsH009dx4vTHELt
MRENxMTbGBgaiCAGIiIGipFgIhgIHmAx8f97sE962t6ZRpwJHjXVVfXqg53eKV66
KWW8fk8BbD0IWIJAB45UN8WU/vc8a1G1bENVGJm5dCbimQqMa5kIyHIMKnBkslJo
3aJFDbBrHy3229k2zCEgX+gdLaeg2gIaYvkxEowlqA4qMZSSuPhP+TA+p8ggYfzg
433de5ec495dec624c30472f139d3482ae885318e7f30980019a9439ae8c7c0b
6pvzapYwMmuaPlp3GAhAC7WmXhHBrPgKvGMor8cMtWJfzhoknPcNJP1vsAEJtYQS
2FDgvkGVlKtvyo6NX8HbSycCiDHWR2gaqJRI3JrAqT9lGxZAxTnmUE8MNnhRWfoNZJHX2
2FsPONw4QOqEQkzYvoiuVATWxbyQmsCJ
WL3iUbjMezB9f1hL3Vh/gLiCJ9nAZHpnjHbNMOBZNjBoy+LlnmHAllkOAQa91b6o
fC3c0zTQKMvO+8AY7JP6hqGaBBpjyWUNTAi1LaimgCYwv86EMZTibhXQAg0HSFeA
GjAOCOpEZE0DxlVqJKiORQPGvbE6EVnTgGsv46xBogEzEhaCRAPG6w+rSjXtaMD6
vv9TVn7j3F1aoNKETK9fmMLQERG5O4WUUsxDrXLLBr5kAx+vgTfZwKts4Hk28Dgb
RAkWEcRCBLEQi1RWaaxSWvl2PoWNYBEIBILKKv4gmu8WC7PLnXVm17X42Jk7955z
39280363481451541647
-39280363481451541647
305092bc73c180b55c26012a94809131
56aAMXWxLr+BzP2uGeC9gD4rYZtQeCWQJwdQnQGpEcYWc3OETa0w1mvvDJsWGMou
b37d93b6a7651920a3820a80bf57900c
9a944bf42c3c9306a9bfbd1c467db152
bUn1+2yaHj0K53Ke9VJv2dtmjqsUYhlbnIEb8WAUZ8gfkHtzY+mGydMgiutIDVVm
AZsSGGvWexrr+k0J7JmgSlB9TpW0sPWoY0vVaYCRpDz22alApQG+BKiLYKQAxn/j
2GHAVOyrAToMWK2yyAYGvW6MDpVhwCONfUN0ODBoBotTI3RIMGiK2LEBOiwYNJmu
qi+uTdJ/i8JFuc97sZnzjQxfe6ZHxEHkWlWcou+uN5cL4b4d7UiZr1DQlXSj4gnS
pNFRZ9Sig0GDngUUHXq9PP4B62fQcqx0J7wAAAAASUVORK5CYII=
2FnsLvYQe4m9xbphGMIN43qWjXR2EAMcoH5ZOCwC7FW20tF1AnAM3yQwQOeoOYbF

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。