南明离火
移动应用检测平台

ANDROID 静态分析报告

MomsLab • v0.9.108

分析日期: 2025-04-09 10:40:21

应用概览

文件名称:	MomsLab v0.9.108.apk
文件大小:	40.71MB
应用名称:	MomsLab
软件包名:	com.momslab.app
主活动:	com.momslab.app.MainActivity
版本号:	0.9.108
最小SDK:	23
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:	49/100 (中风险)
跟踪器检测:	10/432
杀软检测:	AI评估：可能有安全隐患
MD5:	282150a8b99529866b09f8a5c544660e
SHA1:	8ca06a26b36813f25784d3b7b8755dbd507dc5b3
SHA256:	e97557a5ae21792bd2fdb40073e772f80faecb0da7d7a91f5d4477da356b5d2a

分析结果严重性分布

高危	中危	信息	安全	关注
3	24	4	2	0

四大组件导出状态统计

Activity组件：21个，其中export的有： 2个
Service组件：20个，其中export的有： 2个
Receiver组件：24个，其中export的有： 5个
Provider组件：12个，其中export的有： 2个

应用签名证书信息

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=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2020-12-08 09:38:03+00:00
有效期至: 2050-12-08 09:38:03+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x9256c68465365ec5a02f70288ab3b40fe6cc4f34
哈希算法: sha256
证书MD5: 5595a9bffdd392a6244d716820e4cfd4
证书SHA1: f37fd4b529e5e17df89019d4b9d637a2c15958fd
证书SHA256: 2a3224ed26901762e7aadb629528d9ff6f25f73eba2ea2073119446e828dc8a9
证书SHA512:
f30e9dd6fd7e6de32edc3fc6edf387d203eaf90e3260fd7fb37aec4e6ac2605d0c4e57dbd45b4e82506fc9c02b630adaf55d96d11618a3ac562ffe2f708df679

公钥算法: rsa
密钥长度: 4096
指纹: 567c53b4320e165c527379c8aea9841e5f7dfefd658125e50a41ec932cdae591
找到 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.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.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_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.ACTION_MANAGE_STORAGE	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_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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。

android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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。
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。
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。
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。
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_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证标记。
com.momslab.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.momslab.app.MainActivity	Schemes: http://, https://, @string/pushwoosh_deep_link_scheme://, Hosts: @string/applink_host, @string/applink_host_alternate, @string/deeplink_scheme,

com.vk.id.internal.auth.AuthActivity	Schemes: vk51837706://, Hosts: vk.com,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.momslab.app,

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **0** | 警告: **11** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (com.vk.id.internal.auth.AuthActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
2	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
3	Activity (com.facebook.CustomTabActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Broadcast Receiver (com.pushwoosh.BootReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.RECEIVE_BOOT_COMPLETED [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
5	Content Provider (com.pushwoosh.PushwooshSharedDataProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

6	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
7	Content Provider (com.yandex.metrica.PreloadInfoContentProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
9	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
10	Broadcast Receiver (com.yandex.metrica.push.core.notification.MetricaPushNotificationStatusChangeHandler) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
11	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

代码安全漏洞检测

高危: **2** | 警告: **11** | 信息: **3** | 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	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
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	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
5	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
6	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
7	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
8	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
9	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
10	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

11	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
12	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-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	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
15	应用程序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
16	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
17	不安全的Web视图实现。WebView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
18	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

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/liblofelt_sdk.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	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。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵，这对于Dart/Flutter库不适用，除非使用了Dart FFI	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
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
00013	读取文件并将其放入流中	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
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
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
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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
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
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
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
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
00192	获取短信收件箱中的消息	短信	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
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	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
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	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
00191	获取短信收件箱中的消息	短信	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

00171	将网络运算符与字符串进行比较	网络	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
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00015	将缓冲流（数据）放入 JSON 对象	文件	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
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
00132	查询ISO国家代码	电话服务 信息收集	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00153	通过 HTTP 发送二进制数据	http	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	9/30	android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	10/46	android.permission.INTERNET android.permission.READ_MEDIA_IMAGES android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.FOREGROUND_SERVICE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
api.eu.amplitude.com	安全	否	**IP地址:** 52.40.23.80 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
api.ipify.org	安全	否	**IP地址:** 104.26.12.205 **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
docs.pushwoosh.com	安全	否	**IP地址:** 18.65.25.35 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052510 **经度:** -118.243904 **查看:** Google 地图
telegram.me	安全	否	**IP地址:** 77.88.44.55 **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
yandex.com	安全	否	**IP地址:** 77.88.44.55 **国家:** 俄罗斯联邦 **地区:** 莫斯科 **城市:** 莫斯科 **纬度:** 55.752258 **经度:** 37.615471 **查看:** Google 地图
api2.amplitude.com	安全	否	**IP地址:** 52.40.23.80 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.676468 **查看:** Google 地图
capacitorjs.com	安全	否	**IP地址:** 104.21.93.31 **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.branch.io	安全	否	**IP地址:** 3.168.147.54 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
api3-eu.branch.io	安全	否	**IP地址:** 3.169.252.24 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
vimeo.com	安全	否	**IP地址:** 162.159.128.61 **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
fallback.adapty.io	安全	否	**IP地址:** 104.22.71.162 **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.rollbar.com	安全	否	**IP地址:** 35.201.81.77 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
icon-icons.com	安全	否	**IP地址:** 104.26.12.212 **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
crisp.chat	安全	否	**IP地址:** 104.18.29.104 **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

stats.rustore.ru	安全	否	**IP地址:** 95.163.61.56 **国家:** 俄罗斯联邦 **地区:** 莫斯科 **城市:** 莫斯科 **纬度:** 55.752258 **经度:** 37.615471 **查看:** Google 地图
appmetrica.yandex.ru	安全	否	**IP地址:** 93.158.134.167 **国家:** 俄罗斯联邦 **地区:** 莫斯科 **城市:** 莫斯科 **纬度:** 55.752258 **经度:** 37.615471 **查看:** Google 地图
trk.mail.ru	安全	否	**IP地址:** 95.163.41.56 **国家:** 俄罗斯联邦 **地区:** 莫斯科 **城市:** 莫斯科 **纬度:** 55.752258 **经度:** 37.615471 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 172.66.0.227 **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
cdn.branch.io	安全	否	**IP地址:** 3.168.147.4 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
settings.crisp.chat	安全	否	**IP地址:** 104.18.29.104 **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
momslab.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

www.dailymotion.com	安全	否	**IP地址:** 195.8.215.137 **国家:** 法国 **地区:** 法兰西岛 **城市:** 巴黎 **纬度:** 48.859077 **经度:** 2.293486 **查看:** Google 地图
android.asset	安全	否	No Geolocation information available.
api.adapty.io	安全	否	**IP地址:** 104.22.71.162 **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
bnc.lt	安全	否	**IP地址:** 3.169.252.77 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
oauth.vk.com	安全	否	**IP地址:** 93.186.237.1 **国家:** 俄罗斯联邦 **地区:** 莫斯科 **城市:** 莫斯科 **纬度:** 55.752258 **经度:** 37.615471 **查看:** Google 地图
s.api.pushwoosh.com	安全	否	**IP地址:** 116.202.214.85 **国家:** 德国 **地区:** 萨克森 **城市:** 法尔肯施泰因 **纬度:** 50.477852 **经度:** 12.371563 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 213.180.204.244 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
api.vk.com	安全	否	**IP地址:** 87.240.129.140 **国家:** 俄罗斯联邦 **地区:** 桑克-彼得堡 **城市:** 圣彼得堡 **纬度:** 59.894440 **经度:** 30.264200 **查看:** Google 地图

api2.branch.io	安全	否	**IP地址:** 18.65.3.119 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
branch.app.link	安全	否	**IP地址:** 18.154.144.86 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
help.branch.io	安全	否	**IP地址:** 104.18.20.218 **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
startup.mobile.yandex.net	安全	否	**IP地址:** 213.180.204.244 **国家:** 俄罗斯联邦 **地区:** 莫斯科 **城市:** 莫斯科 **纬度:** 55.752258 **经度:** 37.615471 **查看:** Google 地图
image.crisp.chat	安全	否	**IP地址:** 104.18.28.104 **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
cp.pushwoosh.com	安全	否	**IP地址:** 46.4.253.88 **国家:** 德国 **地区:** 萨克森 **城市:** 法尔肯施泰因 **纬度:** 50.477852 **经度:** 12.371563 **查看:** Google 地图
appmetrica.yandex.com	安全	否	**IP地址:** 93.158.134.167 **国家:** 俄罗斯联邦 **地区:** 莫斯科 **城市:** 莫斯科 **纬度:** 55.752258 **经度:** 37.615471 **查看:** Google 地图

URL链接安全分析

URL信息	源码文件

- https://mths.be/punycode
- https://github.com/joyent/node/issues/1707
- http://tools.ietf.org/html/rfc3492
- https://openjsf.org/
- https://momslab.app/uploads/paywall/connection.svg
- https://ionic.io
- https://g.co/ng/security
- https://chat.stenciljs.com
- https://www.iubenda.com/privacy-policy/70519719/full-legal
- https://www.iubenda.com/terms-and-conditions/70519719
- http://momentjs.com/guides/
- https://momslab.app/dish-placeholder.png
- https://cdn.momslab.app
- https://github.com/silkimen/cordova-plugin-advanced-http/wiki/Web-APIs-required-for-Multipart-requests
- https://momslab.app/
- https://github.com/tsayen
- https://momslab.app/uploads/paywall/avocado.svg
- http://benng.me
- https://momslab.app.link/tinkoff-pay-success
- https://momslab.app
- https://momslab.app/legal/oferta_na_uslugi.pdf
- https://momslab.app/legal/oferta_regulyarnyh_platezhej.pdf
- https://momslab.app/legal/politika_obrabotki_personal
- http://foo.com
- https://github.com/ChromiumWebApps/chromium/blob/b3d3b4da8bb94c1b2e061600df106d590fda3620/net/cookies/canonical_cookie.cc
- https://momslab.app.link/trainings?videoId=
- https://github.com/joyent/node
- https://tools.ietf.org/html/rfc3492
- https://apis.google.com/js/platform.js
- https://momslab.app/uploads/paywall/meditation.svg
- http://fake.url
- https://github.com/exponentjs/tough-cookie-web-storage-store
- https://github.com/katzer/cordova-plugin-background-mode
- https://github.com/ionic-team/stencil/issues/5457
- https://momslab.app/uploads/paywall/yoga%20.
- http://drifty.com/
- https://mathiasbynens.be/notes/javascript-encoding
- https://docs.sentry.io/platforms/javascript/best-practices/browser-extensions/
- https://capacitorjs.com/docs/web/pwa-elements.
- https://momslab.app.link/joinmomslab
- https://capacitorjs.com/
- http://jsperf.com/b64tests
- https://github.com/silkimen/cordova-plugin-advanced-http
- https://momslab.app/uploads/paywall/paywall_main_picture_v1.jpg
- https://angular.io/license
- https://connect.facebook.net/
- https://momslab.app/ru/actual_programs_new
- https://stackoverflow.com/a/5738254
- https://github.com/ChromiumWebApps/chromium/blob/b3d3b4da8bb94c1b2e061600df106d590fda3620/net/cookies/parsed_cookie.cc
- https://momslab.app/uploads/paywall/paywall_main_picture_dark_v1.jpg
- http://www.iana.org/assignments/character-sets
- https://stenciljs.com/docs/custom-elements
- https://public-media.adapty.io/public/79/ea/79eac879-bcfd-419d-b77d-d592c78e3bf8/img-cover_5b696d83-81bc-4f8b-9474-f0cf6cce1b54.png
- https://stackoverflow.com/questions/29249132/wkwebview-complex-communication-between-javascript-native-code/49474323
- http://paulbakaus.com/
- https://docs.sentry.io/platforms/javascript/guides/angular/
- https://momslab.app/api

自研引擎-A

• http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
• https://appmetrica.yandex.ru/docs/mobile-sdk-dg/push/android-initialize.html	com/yandex/appmetrica/push/firebase/impl/c.java
• 8.1.2.3 • 8.1.2.2 • 8.1.2.1	io/grpc/okhttp/OkHttpServerTransport.java
• https://appmetrica.yandex.ru/docs/mobile-sdk-dg/push/android-initialize.html	com/yandex/metrica/push/common/CoreConstants.java
• https://stats.rustore.ru	ru/rustore/sdk/metrics/BuildConfig.java
• javascript:_pwcallbackhelper.invokecallback	com/pushwoosh/o/c.java
• https://api.branch.io/ • https://api2.branch.io/ • https://api3-eu.branch.io/ • https://cdn.branch.io/	io/branch/referral/PrefHelper.java
• https://%s.api.pushwoosh.com/json/1.3/ • https://cp.pushwoosh.com/json/1.3/	com/pushwoosh/repository/RegistrationPrefs.java
• https://www.dailymotion.com/video/ • https://vimeo.com/ • https://www.dailymotion.com/thumbnail/video/	im/crisp/client/internal/e0/a.java
• https://api2.amplitude.com/2/httpapi • https://api2.amplitude.com/batch • https://api.eu.amplitude.com/2/httpapi • https://api.eu.amplitude.com/batch	com/amplitude/core/Constants.java
• https://yandex.com/dev/appmetrica/doc/mobile-sdk-dg/concepts/android-initialize.html	com/yandex/metrica/impl/ob/Ln.java
• https://api.adapty.io/api/v1/sdk/	com/adapty/internal/data/cloud/Request.java
• https://appmetrica.yandex.ru/docs/mobile-sdk-dg/push/android-initialize.html	com/yandex/appmetrica/push/firebase/impl/e.java
• https://api.ipify.org?format=json • https://fallback.adapty.io/api/v1/sdk/	com/adapty/internal/data/cloud/RequestFactory.java
• https://telegram.me/ • https://twitter.com/	im/crisp/client/internal/c/a.java
• https://api.vk.com • https://oauth.vk.com	com/vk/id/internal/api/VKIDApi.java
• www.dailymotion.com	im/crisp/client/internal/c/h.java
• https://appmetrica.yandex.com/docs/troubleshooting/other.html	com/yandex/metrica/push/service/FakeService.java
• https://appmetrica.yandex.com/docs/troubleshooting/other.html	com/yandex/metrica/push/service/PushJobService.java
• https://appmetrica.yandex.com/docs/troubleshooting/other.html	com/yandex/metrica/push/service/PushService.java

• https://startup.mobile.yandex.net/	com/yandex/metrica/impl/ob/Jg.java
• https://goo.gl/uvjkfp	com/pushwoosh/firebase/internal/checker/FirebaseChecker.java
• https://trk.mail.ru/c/fd4xl1	ru/rustore/sdk/core/Constants.java
• https://capacitorjs.com/docs/apis/splash-screen#hiding-the-splash-screen	com/capacitorjs/plugins/splashscreen/SplashScreen.java
• https://appmetrica.yandex.ru/docs/mobile-sdk-dg/push/android-initialize.html	com/yandex/metrica/push/impl/C0744k.java
• https://docs.pushwoosh.com/platform-docs/pushwoosh-sdk/android-push-notifications	com/pushwoosh/PushwooshInitializer.java
• https://settings.crisp.chat/client/website/	im/crisp/client/internal/l/a.java
• https://appmetrica.yandex.ru/docs/mobile-sdk-dg/push/android-initialize.html	com/yandex/metrica/push/impl/C0805k.java
• https://help.branch.io/developers-hub/docs/android-basic-integration#section-configure-branch-dashboard • https://branch.app.link/link-settings-page • https://help.branch.io/developers-hub/docs/android-basic-integration#section-configure-app • https://help.branch.io/developers-hub/docs/android-basic-integration#section-load-branch • https://help.branch.io/using-branch/docs/android-app-links#section-add-intent-filter-to-manifest	io/branch/referral/validators/IntegrationValidator.java
• https://crisp.chat/en/ • https://www.google.com/	im/crisp/client/internal/u/b.java
• https://api.rollbar.com/api/1/item/	com/pushwoosh/u/b.java
• https://android.asset/	io/noties/markwon/image/destination/ImageDestinationProcessorAssets.java
• https://image.crisp.chat/avatar/operator/ • https://image.crisp.chat/ • https://image.crisp.chat/avatar/website/	im/crisp/client/internal/k/a.java
• https://bnc.lt/a/	io/branch/referral/ServerRequestCreateUrl.java
• https://crisp.chat/	im/crisp/client/internal/j/b.java
• https://help.branch.io/using-branch/docs/adding-test-devices • https://help.branch.io/using-branch/docs/adding-test-devices#section-resetting-your-test-device-data	io/branch/referral/Branch.java
• 127.0.0.1	io/grpc/okhttp/OkHttpClientTransport.java
• https://icon-icons.com/downloadimage.php?id=89781&root=1368/png/512/&file=-avatar_89781.png • https://monisv2b.firebaseio.com	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://momslab.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已启用	警告	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/817694478994/namespaces/firebase:fetch?key=AIzaSyAZbj1vKsmxAtMyCxLxavVaauDS8t0d9hs ） 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": {
		"googlePlayBillingAvailable": "true",
		"launchPlacementId": "launch_placement",
		"liveStream": "{}",
		"mainPlacementId": "test_customsation_v3",
		"onboardingRateAppPaneActive": "true",
		"payOnWebsiteLink": "https://momslab.app/ru/actual_programs_new#tariffs",
		"pushNotificationsRequestLocation": "onboarding-program-selected",
		"surveyFirstHear": "{\"isActive\":false,\"options\":[]}",
		"tinkoffPaymentActive": "false"
		},
		"state": "UPDATE",
		"templateVersion": "111"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Lofelt SDK	Lofelt	Lofelt Studio enables content creators to capitalize on the latest technologies for delivering powerful haptic effects. This suite of tools allows you to automatically generate haptic effects by performing detailed analysis of your audio files. You can avoid the painstaking process of manually programming rich and natural haptic experiences. And importantly, Lofelt Studio enables you to author haptic effects once and then use them on a wide variety of devices. There is no need to create different versions of haptic effects for devices with different capabilities.
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
Sentry	Sentry	Sentry 是一个实时事件日志记录和聚合平台，它专门用于监视错误和提取执行适当的事后操作所需的所有信息。
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
Google Sign-In	Google	提供使用 Google 登录的 API。
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。
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。

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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
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
name@site.ru	自研引擎-S

第三方追踪器检测

名称	类别	网址
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
AppMetrica		https://reports.exodus-privacy.eu.org/trackers/140
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Pushwoosh		https://reports.exodus-privacy.eu.org/trackers/39
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

敏感凭证泄露检测

可能的密钥
凭证信息=> "io.branch.sdk.BranchKey.test" : "@string/branch_test_key"

凭证信息=> "io.branch.sdk.BranchKey" : "@string/branch_key"
凭证信息=> "com.pushwoosh.appid" : "@string/pushwoosh_app_id"
Google_Drive_API_Key: AIzaSyAZkYOg3NmgiXAVC6R8wyiW4VQPP3_MOis
"google_app_id" : "1:817694478994:android:ba1e18386c6ce39b390c4b"
"firebase_database_url" : "https://momslab.firebaseio.com"
"fb_app_id" : "388235655240118"
"facebook_client_token" : "2e000b90b91eca37c49f72999603f259"
"google_api_key" : "AIzaSyAZbj1vKsmxAtMyCxLxavVaauDS8t0d9hs"
"pushwoosh_api_token" : "aHLKAmyNCPY6Nj7U0E6YHbbLQCh6K1ePM9RxLRiK1D"
"appmetrica_api_key" : "fcf1c352-c867-4104-92b9-3f7ae144e732"
"branch_key" : "key_live_oo7jZVi5LzFK2r0QsdPU0hkirue42HGk"
"branch_test_key" : "key_test_leYd7Sp2GztG2F4lAgGJ2hfbEtj1WTVD"
"facebook_app_id" : "388235655240118"
"adapty_sdk_key" : "public_live_jHtUZqYz.XlSoQeOh7UftVzjCxY1P"
"google_crash_reporting_api_key" : "AIzaSyAZbj1vKsmxAtMyCxLxavVaauDS8t0d9hs"
"pushwoosh_app_id" : "C5ADE-68CDF"
"amplitude_api_key" : "2688237e6460ce386c402b7641b[redacted]
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
6c5f504e-8928-47b5-bfb5-73af8d8bf4b4
4e610cd2-753f-4bfc-9b05-772ce8905c5e
9b8f518b086098de3d77736f9458a3d2f6f95a37
sha256/K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q=
67bb016b-be40-[redacted]8a190-96a3f3b503d3
86259288[redacted]43f6c409a922bc3ce40ba[redacted]badb
ABi2fbt8vkzj7SJ8aD5jc4xJFTDF[redacted]dkMrYXL3itsvqY1QIw
0e5e9c33-f8c3-4568-86[redacted]e4f5f523f72
bbf54f5f-e380-46e6-[redacted]506-384200b4448a
c56fb7d[redacted]ba6704df047fd98f535372fea00211
7d962ba4-a392-449a-a02d-6c5be5613928
e4250327-8d3c-4d35-b9e8-3c1720a64b91

dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg==
20799a27-fa80-4b36-b2db-0f8141f24180
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
a72bf6f57701ed3c2b8ed570054febbff4e58c12
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
48761eef50ee53afc4cc9c5f10e6bde7f8f5b82f
cc2751449a350f668590264ed76692694a80308a
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
01528cc0-dd34-494d-9218-24af1317e1ee
7fmduHKTdHHrlMvldlEqAllSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWJnxMDhIfQN0N0K2NDJg==

Google Play 应用市场信息

标题: 孕期瑜伽 / 孕妇孕期食谱 / 孕期运动 / 产后瑜伽

评分: 4.735135 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 健康与健身 **Play Store URL:** com.momslab.app

开发者信息: MomsLab Limited, 5915489605082107932, Unit 1603, 16th Floor, The L. Plaza, 367 - 375 Queen's Road Central, Sheung Wan, Hong Kong, https://momslab.app, support@momslab.app,

发布日期: 2020年12月16日 **隐私政策:** Privacy link

关于此应用:

孕期瑜伽、孕妇孕期食谱, 孕期运动、产前怀孕瑜伽普拉提, 骨盆底锻炼、凯格尔运动, 盆底肌锻炼 — 所有这些都在 Momslab 应用程序中。 Momslab 是一款在产前、孕期和产后孕产之旅中为您提供指导的应用程序。 您将获得一个个性化的、贴心的计划，了解从怀孕计划到分娩乃至一生之后的每个阶段的期望——所有合适的孕期锻炼和产前瑜伽、适合健康妈妈的产前计划和产后锻炼以及安全产后恢复的有用材料。 如果您正在寻找怀孕应用程序，您将在这里与其他准妈妈联系。 您会发现凯格尔运动、孕期伸展运动、骨盆底运动以及带有日记的个性化项目，其中包含不同计划的小任务：训练、心理健康、冥想、营养和孕期食物追踪器。 我们将帮助每位母亲在安全的环境中建立自信和幸福感，无论您是初为人母、怀孕的母亲，还是针对女性的一般计划。 所有生命阶段的锻炼： 所有 15 个程序都包括 500 多个日常锻炼。 他们都是通过在线女性锻炼进行温和改造，产前瑜伽和特殊瑜伽锻炼，让您的身体做好准备。 孕期瑜伽，根据您的孕期为女性提供的孕期锻炼，您还可以在其中找到使用体重追踪器进行的孕期锻炼。 产后或孕后锻炼将帮助您减掉孕肚并恢复您自己的生活：健康的身体、您的女性健康和心理安慰。 该计划为您提供多种锻炼身体的选择，例如凯格尔运动、普拉提锻炼和骨盆底锻炼。 您将获得有关如何通过针对女性的特殊温和安全减肥计划来减肥的信息。 进度跟踪器功能将使您有机会跟踪减肥情况并查看个人体重日记中的统计数据。 定制计划，让所有女性了解产后恢复选择的知识：自然分娩或剖腹产，以便在恢复期间正常愈合。 健康营养库： 您将根据您的个人资料获得个性化的营养计划。 我们有 20 多种适合您阶段和目标的菜单：孕期饮食计划、孕期食物追踪器、孕期营养追踪器和孕期食物指南。 包含营养师的产前营养库可支持您的整体健康。 怀孕期间的健康饮食将包括一个怀孕食物追踪器，以及我们为健康妈妈和宝宝准备的怀孕食物指南。 适合您理想身材的产后营养计划包括针对素食者、母乳喂养者和想要减肥者的饮食计划。 我们的应用程序集成了 Fat Secret 卡路里跟踪器，并提供许多健康和适当饮食的美味食谱。 正念怀孕 准妈妈的冥想和放松技巧可以减少怀孕期间的焦虑、压力和恐惧。 你会发现正念练习，我们会教你如何快速放松。 有用的文章、讲座和播客 该应用程序提供无限数量的有用文献、课程和播客，介绍如何为母亲做准备，以及为有经验的妈妈准备怀孕期间和婴儿出生后的情况。 Momslab 将为您提供健康的产前瑜伽、孕期瑜伽、孕妇孕期食谱, 孕期运动、产前怀孕瑜伽普拉提, 骨盆底锻炼、凯格尔运动, 盆底肌锻炼。 我们的应用程序是一个循序渐进的直线路线图，为女性准备怀孕时会发生什么，在怀孕期间提供舒适怀孕的活动，以及专为女性设计的特殊计划，让她们在产后恢复时感觉最好而无后顾之忧。 在这里您可以找到所有级别的 24/7 全天候帮助。 怀孕应用程序是孕妇的新宠儿。 通过我们的产前、孕期和产后锻炼保持活跃。 通过我们的孕期食品指南和产前营养库保持健康。 如果您有任何问题或疑虑，请联系我们： support@momslab.app momslab.app/en

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