ANDROID STATIC ANALYSIS REPORT

app_icon

🤖 DanceFitme (4.19.0)

File Name:	dance.fit.zumba.weightloss.danceburn_102.apk
Package Name:	dance.fit.zumba.weightloss.danceburn
Scan Date:	Sept. 1, 2025, 12:57 p.m.
App Security Score:	**42/100 (MEDIUM RISK)**
Grade:	**B**
Trackers Detection:	4/432

🥧 FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
5	18	2	1	4

📦 FILE INFORMATION

File Name: dance.fit.zumba.weightloss.danceburn_102.apk
Size: 36.57MB
MD5: 6bdf5f1a25de83561ce0241f98f2448d
SHA1: d308b12cc474ef7b6ce58631d1ddd830c761ebd5
SHA256: cf690f06fba6c9df33b760000319b0e8f538a66e2cf31db999edce9c6478a4a4

ℹ APP INFORMATION

App Name: DanceFitme
Package Name: dance.fit.zumba.weightloss.danceburn
Main Activity: dance.fit.zumba.weightloss.danceburn.maintab.SplashActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 4.19.0

Android Version Code: 102

▦ APP COMPONENTS

Activities: 79
Services: 14
Receivers: 12
Providers: 5
Exported Activities: 0
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

✤ CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-03-15 05:58:38+00:00
Valid To: 2052-03-15 05:58:38+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x8c046821fd199ac78bbeb86625d93a53d96f3661
Hash Algorithm: sha256
md5: c69517eb9e2a949a701239bad0fb3480
sha1: 44bd2f35fc74a49403263c8c8c4a9d050d9ab829
sha256: 899a1f5af2634df0ed9644e76a2ca19933df8c8c5a7c57b2dd61dc7d1a6d271d
sha512: 68adcaaac0bf7f593c4cd3812a271ec7822338b440f2304f0b5e6ae1e3e14e1bc40daf4db3cb4a31ef4f45702f676fcb4a1c0e159168c228d036654246daf09d
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 7e7632bd7aabdb2dfbe3d14d2f5f934ebda47eac32a09560b9ee8173d8b276ac
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
dance.fit.zumba.weightloss.danceburn.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

🔲 APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS	
classes.dex	**FINDINGS**	**DETAILS**
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check
	Compiler	r8 without marker (suspicious)
classes2.dex	**FINDINGS**	**DETAILS**
	Anti Debug Code	Debug.isDebuggerConnected() check
	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check possible VM check
	Compiler	r8 without marker (suspicious)

📑 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
dance.fit.zumba.weightloss.danceburn.maintab.SplashActivity	Schemes: dancefitmeh2o://, Hosts: www.dancefitme.com,

🔒 NETWORK SECURITY

HIGH: **1** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

📇 CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

🔍 MANIFEST ANALYSIS

HIGH: **2** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (dance.fit.zumba.weightloss.danceburn.receiver.InstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Service (androidx.work.impl.background.gcm.WorkManagerGcmService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
9	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **8** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/a.java
				a0/c.java
				a0/h.java
				b2/c.java
				b2/m0.java
				b2/n1.java
				b2/y.java
				b5/a.java
				c0/e.java
				c0/o.java
				c2/t0.java
				c3/n.java
				c4/c.java
				c4/e.java
				c4/g.java
				cc/d.java
				com/adjust/sdk/Logger.java
				com/alibaba/android/vlayout/VirtualLayout Manager.java
				com/alibaba/android/vlayout/a.java
				com/alibaba/android/vlayout/extend/InnerR ecycledViewPool.java
				com/bumptech/glide/GeneratedAppGlideM oduleImpl.java
				com/bumptech/glide/c.java
				com/bumptech/glide/gifdecoder/a.java
				com/bumptech/glide/h.java
				com/bumptech/glide/i.java
				com/bumptech/glide/integration/webp/Web pBitmapFactory.java
				com/bumptech/glide/load/data/b.java
				com/bumptech/glide/load/data/j.java
				com/bumptech/glide/load/data/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/f.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/e.java com/bumptech/glide/load/engine/f.java com/bumptech/glide/load/engine/k.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/bitmap/a.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/request/SingleRequest.java com/connectsdk/core/ChannelInfo.java com/connectsdk/device/ConnectableDevice.java com/connectsdk/device/SimpleDevicePicker.java com/connectsdk/discovery/DiscoveryManager.java com/connectsdk/discovery/provider/CastDiscoveryProvider.java com/connectsdk/discovery/provider/SSDPDiscoveryProvider.java com/connectsdk/service/CastService.java com/connectsdk/service/DIALService.java com/connectsdk/service/DLNAService.java com/connectsdk/service/NetcastTVService.java com/connectsdk/service/RokuService.java com/connectsdk/service/WebOSTVService.java com/connectsdk/service/netcast/NetcastHttpServer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/connectsdk/service/netcast/NetcastPOSTRequestParser.java com/connectsdk/service/sessions/CastWebAppSession.java com/connectsdk/service/webos/WebOSTVMouseSocketConnection.java com/connectsdk/service/webos/WebOSTVServiceSocketClient.java com/connectsdk/service/webos/WebOSTVTrustManager.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/a.java com/pili/pldroid/player/PLMediaPlayer.java com/pili/pldroid/player/SharedLibraryNameHelper.java com/pili/pldroid/player/network/a.java com/pili/pldroid/player/report/a.java com/pili/pldroid/player/report/core/e.java com/sensorsdata/analytics/android/autotrack/core/AutoTrackContextHelper.java com/sensorsdata/analytics/android/autotrack/core/autotrack/ActivityLifecycleCallbacks.java com/sensorsdata/analytics/android/autotrack/core/autotrack/FragmentViewScreenCallbacks.java com/sensorsdata/analytics/android/autotra

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ck/core/impl/AutoTrackProtocolImpl.java com/sensorsdata/analytics/android/autotrack/core/pageleave/FragmentPageLeaveCallbacks.java com/sensorsdata/analytics/android/sdk/AbstractSensorsDataAPI.java com/sensorsdata/analytics/android/sdk/AnalyticsMessages.java com/sensorsdata/analytics/android/sdk/SALog.java com/sensorsdata/analytics/android/sdk/SensorsDataAPI.java com/sensorsdata/analytics/android/sdk/advert/deeplink/ChannelDeepLink.java com/sensorsdata/analytics/android/sdk/advert/deeplink/DeepLinkManager.java com/sensorsdata/analytics/android/sdk/advert/impl/SAAdvertProtocolImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/OAIDRom.java com/sensorsdata/analytics/android/sdk/advert/oaid/SAOaidHelper.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/AsusImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/CoolpadImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/HuaweiImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/LenovoImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/MeizuImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/NubiaImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/OAIDFactory.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/OppoImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/SamsungImpl.java com/sensorsdata/analytics/android/sdk/adv

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ert/oaid/impl/VivoImpl.java
				com/sensorsdata/analytics/android/sdk/adv ert/oaid/impl/XiaomiImpl.java
				com/sensorsdata/analytics/android/sdk/adv ert/oaid/impl/ZTEImpl.java
				com/sensorsdata/analytics/android/sdk/adv ert/scan/ChannelDebugScanHelper.java
				com/sensorsdata/analytics/android/sdk/adv ert/utils/SAAdvertUtils.java
				com/sensorsdata/analytics/android/sdk/aop /push/PushAutoTrackHelper.java
				com/sensorsdata/analytics/android/sdk/cor e/business/SAPluginVersion.java
				com/sensorsdata/analytics/android/sdk/cor e/event/imp/BaseEventAssemble.java
				com/sensorsdata/analytics/android/sdk/cor e/event/imp/H5TrackAssemble.java
				com/sensorsdata/analytics/android/sdk/cor e/event/imp/ItemEventAssemble.java
				com/sensorsdata/analytics/android/sdk/cor e/event/imp/StoreDataImpl.java
				com/sensorsdata/analytics/android/sdk/cor e/event/imp/TrackEventAssemble.java
				com/sensorsdata/analytics/android/sdk/cor e/mediator/SAModuleManager.java
				com/sensorsdata/analytics/android/sdk/dat a/SAProviderHelper.java
				com/sensorsdata/analytics/android/sdk/dat a/SensorsDataDBHelper.java
				com/sensorsdata/analytics/android/sdk/dat a/adapter/DataOperation.java
				com/sensorsdata/analytics/android/sdk/dat a/adapter/EncryptDataOperation.java
				com/sensorsdata/analytics/android/sdk/dat a/adapter/EventDataOperation.java
				com/sensorsdata/analytics/android/sdk/dat a/adapter/TransportEncryption.java
				com/sensorsdata/analytics/android/sdk/dat a/persistent/PersistentSuperProperties.java
				com/sensorsdata/analytics/android/sdk/dial og/SchemeActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/sensorsdata/analytics/android/sdk/dialog/SensorsDataDialogUtils.java com/sensorsdata/analytics/android/sdk/encrypt/AESSecretManager.java com/sensorsdata/analytics/android/sdk/encrypt/biz/SecretKeyManager.java com/sensorsdata/analytics/android/sdk/encrypt/encryptor/SAECEncrypt.java com/sensorsdata/analytics/android/sdk/encrypt/impl/SAEncryptAPIImpl.java com/sensorsdata/analytics/android/sdk/encrypt/utils/EncryptUtils.java com/sensorsdata/analytics/android/sdk/exposure/AppPageChange.java com/sensorsdata/analytics/android/sdk/exposure/ExposedPage.java com/sensorsdata/analytics/android/sdk/exposure/ExposedTransform.java com/sensorsdata/analytics/android/sdk/exposure/ExposureVisible.java com/sensorsdata/analytics/android/sdk/exposure/SAExposedProcess.java com/sensorsdata/analytics/android/sdk/exposure/StayDurationRunnable.java com/sensorsdata/analytics/android/sdk/jsbridge/AppWebViewInterface.java com/sensorsdata/analytics/android/sdk/jsbridge/JSHookAop.java com/sensorsdata/analytics/android/sdk/network/HttpConfig.java com/sensorsdata/analytics/android/sdk/network/RealRequest.java com/sensorsdata/analytics/android/sdk/plugin/encrypt/AbstractStoreManager.java com/sensorsdata/analytics/android/sdk/plugin/property/PropertyPluginManager.java com/sensorsdata/analytics/android/sdk/push/core/PushProcess.java com/sensorsdata/analytics/android/sdk/remote/BaseSensorsDataSDKRemoteManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	[The App logs information. Sensitive information should never be logged.](#)	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/sensorsdata/analytics/android/sdk/remote/SensorsDataRemoteManager.java com/sensorsdata/analytics/android/sdk/remote/SensorsDataRemoteManagerDebug.java com/sensorsdata/analytics/android/sdk/useridentity/Identities.java com/sensorsdata/analytics/android/sdk/useridentity/LoginIDAndKey.java com/sensorsdata/analytics/android/sdk/useridentity/UserIdentityAPI.java com/sensorsdata/analytics/android/sdk/util/AppInfoUtils.java com/sensorsdata/analytics/android/sdk/util/AppStateTools.java com/sensorsdata/analytics/android/sdk/util/DeviceUtils.java com/sensorsdata/analytics/android/sdk/util/NetworkUtils.java com/sensorsdata/analytics/android/sdk/util/Pathfinder.java com/sensorsdata/analytics/android/sdk/util/PermissionUtils.java com/sensorsdata/analytics/android/sdk/util/SADataHelper.java com/sensorsdata/analytics/android/sdk/util/SASchemeHelper.java com/sensorsdata/analytics/android/sdk/util/SASpUtils.java com/sensorsdata/analytics/android/sdk/util/SAViewUtils.java com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java com/sensorsdata/analytics/android/sdk/util/ThreadUtils.java com/sensorsdata/analytics/android/sdk/util/ToastUtil.java com/sensorsdata/analytics/android/sdk/util/WebUtils.java com/sensorsdata/analytics/android/sdk/visual/AbstractNodesManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/sensorsdata/analytics/android/sdk/visual/AbstractViewCrawler.java com/sensorsdata/analytics/android/sdk/visual/ViewSnapshot.java com/sensorsdata/analytics/android/sdk/visual/VisualDebugHelper.java com/sensorsdata/analytics/android/sdk/visual/VisualizedAutoTrackService.java com/sensorsdata/analytics/android/sdk/visual/WebViewVisualInterface.java com/sensorsdata/analytics/android/sdk/visual/impl/VisualProtocolImpl.java com/sensorsdata/analytics/android/sdk/visual/property/VisualConfigRequestHelper.java com/sensorsdata/analytics/android/sdk/visual/property/VisualPropertiesCache.java com/sensorsdata/analytics/android/sdk/visual/property/VisualPropertiesManager.java com/sensorsdata/analytics/android/sdk/visual/snap/Caller.java com/sensorsdata/analytics/android/sdk/visual/snap/ResourceReader.java com/sensorsdata/analytics/android/sdk/visual/utils/AlertMessageUtils.java com/sensorsdata/analytics/android/sdk/visual/view/PairingCodeEditDialog.java com/sensorsdata/analytics/android/sdk/visual/view/PairingCodeRequestHelper.java com/tencent/mmkv/MMKV.java com/tencent/mmkv/MMKVContentProvider.java com/zhouyou/http/body/UploadProgressRequestBody.java com/zhouyou/http/request/DownloadRequest.java com/zhouyou/http/utils/RetryWithDelay.java com/zhouyou/http/utils/ZipTool.java d1/b.java d4/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d4/d.java d4/e.java d4/f.java d5/a0.java d5/b0.java d5/d0.java d5/e.java d5/g.java d5/g0.java d5/h0.java d5/i0.java d5/j.java d5/j0.java d5/m.java d5/m0.java d5/n0.java d5/o.java d5/r0.java d5/t0.java d5/w.java d5/y.java d5/z.java dance/fit/zumba/weightloss/danceburn/maintab/DanceMainActivity.java dance/fit/zumba/weightloss/danceburn/maintab/ProfileFragment.java dance/fit/zumba/weightloss/danceburn/maintab/fragment/StatsMonthFragment.java dance/fit/zumba/weightloss/danceburn/push/MyFirebaseMessagingService.java dance/fit/zumba/weightloss/danceburn/session/adapter/NewFilterLabelAdapter.java dance/fit/zumba/weightloss/danceburn/session/model/MediaController.java dance/fit/zumba/weightloss/danceburn/view/picker/PickerLayoutManager.java e4/c.java e4/d.java e4/f.java f3/a.java f3/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f4/c.java
				g0/j.java
				g2/v.java
				g4/a0.java
				g4/c0.java
				g4/g.java
				g4/h.java
				g4/h0.java
				g4/n.java
				g4/o.java
				g4/r.java
				g4/w.java
				g4/x.java
				g4/y.java
				g5/j.java
				h/a.java
				h4/d.java
				h4/g.java
				h4/j.java
				h4/l.java
				h5/m.java
				i/a.java
				i2/a.java
				i5/a.java
				io/flutter/app/FlutterFragmentActivity.java
				io/flutter/embedding/android/FlutterActivity.java
				io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java
				io/flutter/embedding/android/FlutterFragment.java
				io/flutter/embedding/android/FlutterFragmentActivity.java
				io/flutter/embedding/android/FlutterImageView.java
				io/flutter/embedding/android/FlutterSurfaceView.java
				io/flutter/embedding/android/FlutterTextureView.java
				io/flutter/embedding/android/FlutterView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/embedding/android/KeyEmbedderResponder.java
				io/flutter/embedding/android/KeyboardManager.java
				io/flutter/embedding/engine/FlutterEngineConnectionRegistry.java
				io/flutter/embedding/engine/FlutterJNI.java
				io/flutter/embedding/engine/dart/DartExecutor.java
				io/flutter/embedding/engine/dart/DartMessenger.java
				io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java
				io/flutter/embedding/engine/loader/FlutterLoader.java
				io/flutter/embedding/engine/loader/ResourceExtractor.java
				io/flutter/embedding/engine/plugins/util/GeneratedPluginRegister.java
				io/flutter/embedding/engine/renderer/FlutterRenderer.java
				io/flutter/embedding/engine/systemchannels/KeyEventChannel.java
				io/flutter/embedding/engine/systemchannels/RestorationChannel.java
				io/flutter/embedding/engine/systemchannels/SettingsChannel.java
				io/flutter/embedding/engine/systemchannels/TextInputChannel.java
				io/flutter/plugin/editing/c.java
				io/flutter/plugin/platform/PlatformViewWrapper.java
				io/flutter/plugin/platform/SingleViewPresentation.java
				io/flutter/plugin/platform/b.java
				io/flutter/plugin/platform/p.java
				io/flutter/plugin/platform/q.java
				io/flutter/view/AccessibilityViewEmbedder.java
				io/flutter/view/FlutterView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/view/FlutterView.java
				j/c.java
				j1/p.java
				jc/h.java
				k/a.java
				k0/a.java
				k2/a.java
				k3/a.java
				k4/a.java
				k9/b.java
				kc/d.java
				l1/i.java
				l3/b.java
				l3/c.java
				l4/d.java
				l4/e.java
				l5/y.java
				m/h.java
				m/i.java
				m3/a.java
				m4/c.java
				m9/a.java
				n2/d.java
				n2/f.java
				n2/i.java
				n3/c.java
				n3/f.java
				n4/b.java
				n4/d.java
				n4/e.java
				n6/a.java
				o/a.java
				o1/c.java
				o2/j.java
				org/extra/tools/a.java
				org/extra/tools/b.java
				org/libpag/HardwareDecoder.java
				org/libpag/PAGAnimator.java
				org/libpag/TraceImage.java
				org/libpag/b.java
				org/slf4j/helpers/Util.java
				p2/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p3/n.java p3/o.java p7/a.java q/i.java q/j.java q2/a.java q2/c.java q3/c0.java q9/a.java r/e.java r/j.java r1/j.java r3/f.java r3/i.java r3/j.java s/a.java t/c.java t/d.java t/f.java t/t.java t/u.java t6/a.java t9/b.java t9/j.java tv/danmaku/ijk/media/player/IjkMediaCodecInfo.java tv/danmaku/ijk/media/player/IjkMediaPlayer.java tv/danmaku/ijk/media/player/pragma/DebugLog.java u1/a.java v/a.java v3/e.java w/c.java w/d.java w/j.java w/k.java w/o.java w/t.java w0/a.java w2/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x17a0.java x4/b.java y0/a.java y0/c.java z4/a.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/connectsdk/discovery/provider/ssdp/SSDPClient.java com/pili/pldroid/player/network/a.java com/pili/pldroid/player/report/common/a.java dance/fit/zumba/weightloss/danceburn/MyApp.java
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/zhouyou/http/request/DownloadRequest.java com/zhouyou/http/utils/RxUtil.java dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java org/libpag/PAGDiskCache.java u6/e.java
4	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/sensorsdata/analytics/android/sdk/visual/ViewSnapshot.java com/zhouyou/http/interceptor/CustomSignInterceptor.java com/zhouyou/http/utils/HttpUtil.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/sensorsdata/analytics/android/sdk/advert/oaid/impl/OppoImpl.java d5/w.java org/java_websocket/drafts/Draft_6455.java z4/a.java
				com/bumptech/glide/load/engine/h.java com/connectsdk/device/DefaultConnectableDeviceStore.java com/connectsdk/service/capability/KeyControl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/connectsdk/service/config/WebOSTVSe rviceConfig.java com/connectsdk/service/sessions/WebOSW ebAppSession.java com/sensorsdata/analytics/android/sdk/adv ert/utils/ChannelUtils.java com/sensorsdata/analytics/android/sdk/cor e/mediator/Modules.java com/sensorsdata/analytics/android/sdk/dat a/adapter/DbParams.java com/sensorsdata/analytics/android/sdk/enc rypt/biz/SecretKeyManager.java com/sensorsdata/analytics/android/sdk/enc rypt/impl/SAEncryptAPIImpl.java com/sensorsdata/analytics/android/sdk/plu gin/encrypt/AbstractStoreManager.java com/sensorsdata/analytics/android/sdk/plu gin/encrypt/SAStoreManager.java com/sensorsdata/analytics/android/sdk/use ridentity/Identities.java com/sensorsdata/analytics/android/sdk/util /SADataHelper.java com/zhouyou/http/interceptor/CustomSignl nterceptor.java io/flutter/embedding/android/FlutterActivity AndFragmentDelegate.java io/flutter/embedding/android/FlutterActivity LaunchConfigs.java io/flutter/embedding/engine/loader/Applica tionInfoLoader.java io/flutter/embedding/engine/loader/FlutterL oader.java io/flutter/embedding/engine/systemchannel s/SettingsChannel.java org/java_websocket/drafts/Draft_6455.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/sensorsdata/analytics/android/sdk/data/OldBDatabaseHelper.java com/sensorsdata/analytics/android/sdk/data/SensorsDataDBHelper.java x1/j0.java x1/q0.java x1/t.java
8	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	a3/y.java com/adjust/sdk/Util.java com/pili/pldroid/player/report/common/a.java dance/fit/zumba/weightloss/danceburn/push/MyFirebaseMessagingService.java dance/fit/zumba/weightloss/danceburn/session/activity/BaseSessionPlayActivity.java dance/fit/zumba/weightloss/danceburn/session/activity/SessionCompleteActivity.java dance/fit/zumba/weightloss/danceburn/tools/notice/a.java g5/j.java jb/a.java jb/b.java kb/a.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/zhouyou/http/EasyHttp.java com/zhouyou/http/request/BaseRequest.java jc/c.java jc/d.java jc/g.java jc/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/b.java io/flutter/plugin/platform/c.java
11	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	c3/a.java
12	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/connectsdk/BuildConfig.java
13	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/sensorsdata/analytics/android/webview/impl/SAWebViewProtocolImpl.java

🔲 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

🔲 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/pili/pldroid/player/report/core/b.java com/zhouyou/http/utils/RxUtil.java com/zhouyou/http/utils/ZipTool.java dance/fit/zumba/weightloss/danceburn/maintab/ClassesFragment.java dance/fit/zumba/weightloss/danceburn/maintab/DanceMainActivity.java dance/fit/zumba/weightloss/danceburn/maintab/InAppPurchaseActivity.java dance/fit/zumba/weightloss/danceburn/maintab/activity/ForcedPurchaseActivity.java dance/fit/zumba/weightloss/danceburn/maintab/activity/ForcedPurchaseActivity2.java dance/fit/zumba/weightloss/danceburn/maintab/activity/ForcedPurchaseActivity3.java dance/fit/zumba/weightloss/danceburn/maintab/activity/ForcedPurchaseActivity4.java dance/fit/zumba/weightloss/danceburn/maintab/activity/ForcedPurchaseActivity8.java dance/fit/zumba/weightloss/danceburn/maintab/activity/FundamentalPurchaseActivity.java dance/fit/zumba/weightloss/danceburn/maintab/view/VideoSplashView.java dance/fit/zumba/weightloss/danceburn/ob/view/ObNewStyleView.java dance/fit/zumba/weightloss/danceburn/onboarding/activity/NewPurchaseVideoActivity.java dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java dance/fit/zumba/weightloss/danceburn/tools/s.java dance/fit/zumba/weightloss/danceburn/view/ResizableImageView.java h4/g.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java org/extra/relinker/d.java u6/e.java z8/b.java z8/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	com/adjust/sdk/network/ActivityPackageSender.java jc/b.java jc/h.java org/java_websocket/SSLSocketChannel2.java org/java_websocket/client/WebSocketClient.java
00191	Get messages in the SMS inbox	sms	com/adjust/sdk/a.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/MeizuImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/VivoImpl.java dance/fit/zumba/weightloss/danceburn/tools/c.java
00036	Get resource file from res/raw directory	reflection	com/adjust/sdk/ActivityHandler.java com/adjust/sdk/InstallReferrerHuawei.java com/adjust/sdk/a.java com/pili/pldroid/player/common/Util.java com/pili/pldroid/player/network/a.java d5/e.java dance/fit/zumba/weightloss/danceburn/tools/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a3/v.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/PreinstallUtil.java com/pili/pldroid/player/network/a.java com/sensorsdata/analytics/android/sdk/util/NetworkUtils.java com/sensorsdata/analytics/android/sdk/visual/view/PairingCodeRequestHelper.java d5/e.java dance/fit/zumba/weightloss/danceburn/maintab/EditInfoActivity.java dance/fit/zumba/weightloss/danceburn/maintab/activity/SettingNotificationActivity.java dance/fit/zumba/weightloss/danceburn/maintab/fragment/BaseStatsFragment.java dance/fit/zumba/weightloss/danceburn/session/activity/SessionCompleteActivity.java dance/fit/zumba/weightloss/danceburn/tools/LinkJumpToPageManage.java dance/fit/zumba/weightloss/danceburn/tools/e.java dance/fit/zumba/weightloss/danceburn/tools/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	bc/z.java com/adjust/sdk/PreinstallUtil.java com/bumptech/glide/integration/webp/WebpBitmapFactory.java com/bumptech/glide/load/a.java com/bumptech/glide/load/b.java com/sensorsdata/analytics/android/sdk/util/AppInfoUtils.java com/sensorsdata/analytics/android/sdk/util/FileUtils.java dance/fit/zumba/weightloss/danceburn/tools/w.java h4/g.java h5/e.java i/a.java l4/d.java org/extra/relinker/elf/i.java org/libpag/PAGFont.java t/f.java x6/g.java y0/c.java
00003	Put the compressed bitmap data into JSON object	camera	com/connectsdk/service/webos/WebOSTVDeviceService.java com/sensorsdata/analytics/android/sdk/visual/ViewSnapshot.java d5/r.java dance/fit/zumba/weightloss/danceburn/maintab/fragment/BaseStatsFragment.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/FlutterImageView.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/FlutterImageView.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/sensorsdata/analytics/android/sdk/data/SAProviderHelper.java com/sensorsdata/analytics/android/sdk/data/adapter/DataOperation.java o/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a3/v.java com/sensorsdata/analytics/android/sdk/visual/view/PairingCodeRequestHelper.java d5/e.java dance/fit/zumba/weightloss/danceburn/maintab/activity/SettingNotificationActivity.java dance/fit/zumba/weightloss/danceburn/tools/LinkJumpToPageManage.java dance/fit/zumba/weightloss/danceburn/tools/e.java dance/fit/zumba/weightloss/danceburn/tools/j.java
00005	Get absolute path of file and put it to JSON object	file	com/pili/pldroid/player/report/core/b.java dance/fit/zumba/weightloss/danceburn/maintab/DanceMainActivity.java h4/g.java
00096	Connect to a URL and set request method	command network	com/pili/pldroid/player/report/core/e.java com/sensorsdata/analytics/android/sdk/AnalyticsMessages.java com/sensorsdata/analytics/android/sdk/advert/utils/SAAdvertUtils.java com/sensorsdata/analytics/android/sdk/dialog/SensorsDataDialogUtils.java com/sensorsdata/analytics/android/sdk/network/RealRequest.java com/sensorsdata/analytics/android/sdk/visual/AbstractViewCrawler.java o1/c.java org/libpag/b.java p3/o.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/j.java com/pili/pldroid/player/report/core/e.java com/sensorsdata/analytics/android/sdk/AnalyticsMessages.java com/sensorsdata/analytics/android/sdk/advert/utils/SAAdvertUtils.java com/sensorsdata/analytics/android/sdk/network/RealRequest.java com/sensorsdata/analytics/android/sdk/visual/AbstractViewCrawler.java o1/c.java org/libpag/b.java p3/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/j.java com/pili/pldroid/player/report/core/e.java com/sensorsdata/analytics/android/sdk/AnalyticsMessages.java com/sensorsdata/analytics/android/sdk/advert/utils/SAAdvertUtils.java com/sensorsdata/analytics/android/sdk/dialog/SensorsDataDialogUtils.java com/sensorsdata/analytics/android/sdk/network/RealRequest.java com/sensorsdata/analytics/android/sdk/visual/AbstractViewCrawler.java o1/c.java org/libpag/b.java p3/o.java
00091	Retrieve data from broadcast	collection	com/sensorsdata/analytics/android/sdk/aop/push/PushAutoTrackHelper.java d5/o.java d5/z.java
00009	Put data in cursor to JSON object	file	com/sensorsdata/analytics/android/sdk/data/adapter/EncryptDataOperation.java com/sensorsdata/analytics/android/sdk/data/adapter/EventDataOperation.java com/sensorsdata/analytics/android/sdk/data/adapter/PersistentDataOperation.java
00094	Connect to a URL and read data from it	command network	com/pili/pldroid/player/report/core/e.java com/sensorsdata/analytics/android/sdk/visual/AbstractViewCrawler.java k4/a.java org/libpag/b.java p3/o.java
00108	Read the input stream from given URL	network command	com/pili/pldroid/player/report/core/e.java com/sensorsdata/analytics/android/sdk/visual/AbstractViewCrawler.java org/libpag/b.java p3/o.java
00012	Read data and put it into a buffer stream	file	com/bumptech/glide/integration/webp/WebpBitmapFactory.java com/sensorsdata/analytics/android/sdk/util/FileUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/adjust/sdk/AdjustLinkResolution.java com/bumptech/glide/load/data/j.java com/sensorsdata/analytics/android/sdk/network/RealRequest.java org/libpag/b.java p3/o.java
00130	Get the current WIFI information	wifi collection	com/connectsdk/core/Util.java com/pili/pldroid/player/report/common/a.java com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java
00112	Get the date of the calendar event	collection calendar	dance/fit/zumba/weightloss/danceburn/tools/m.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00104	Check if the given path is directory	file	io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java
00078	Get the network operator name	collection telephony	com/pili/pldroid/player/report/common/a.java
00076	Get the current WiFi information and put it into JSON	collection wifi	com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java dance/fit/zumba/weightloss/danceburn/MyApp.java
00162	Create InetSocketAddress object and connecting to it	socket	jc/b.java jc/h.java org/java_websocket/client/WebSocketClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00034	Query the current data network type	collection network	com/sensorsdata/analytics/android/sdk/util/NetworkUtils.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java
00033	Query the IMEI number	collection	com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java
00116	Get the current WiFi MAC address and put it into JSON	wifi collection	com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java
00083	Query the IMEI number	collection telephony	com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java
00082	Get the current WiFi MAC address	collection wifi	com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java
00132	Query The ISO country code	telephony collection	p3/m.java
00014	Read file into a stream and put it into a JSON object	file	h4/g.java
00189	Get the content of a SMS message	sms	dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java
00188	Get the address of a SMS message	sms	dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java
00121	Create a directory	file command	dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	dance/fit/zumba/weightloss/danceburn/maintab/DanceMainActivity.java dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java
00200	Query data from the contact list	collection contact	dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java
00187	Query a URI and check the result	collection sms calllog calendar	dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java
00201	Query data from the call log	collection calllog	dance/fit/zumba/weightloss/danceburn/tools/crop/CoachSelectImagesActivity.java
00028	Read file from assets directory	file	io/flutter/embedding/engine/loader/ResourceExtractor.java

🛢 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/460765977729/namespaces/firebase:fetch?key=AIzaSyBZe-0Q2mE07KqYutza3GZNP3pMeadq-9M is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'country_code': '1'}, 'state': 'UPDATE', 'templateVersion': '2'}

⣿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_PHONE_STATE
Other Common Permissions	5/44	com.google.android.gms.permission.AD_ID, android.permission.READ_CALENDAR, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

❗OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION
play-pili-qos-report.qiniuapi.com	IP: 110.242.48.56 Country: China Region: Hebei City: Baoding
otheve.beacon.qq.com	IP: 129.226.103.123 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN	COUNTRY/REGION
misc-pili-qos-report.qiniuapi.com	IP: 110.242.48.56 Country: China Region: Hebei City: Baoding

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
app.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gdpr.adjust.world	ok	**IP:** 185.151.204.40 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.tr.adjust.com	ok	**IP:** 195.244.54.7 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
img.dailyyoga.com	ok	**IP:** 54.80.100.196 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
play-pili-qos-report.qiniuapi.com	ok	**IP:** 110.242.48.56 **Country:** China **Region:** Hebei **City:** Baoding **Latitude:** 38.851109 **Longitude:** 115.490280 **View:** Google Map
www.dancefit.me	ok	**IP:** 18.238.96.7 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
otheve.beacon.qq.com	ok	**IP:** 129.226.103.123 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
app.adjust.com	ok	**IP:** 185.151.204.13 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.sec.co.kr	ok	**IP:** 112.106.187.200 **Country:** Korea (Republic of) **Region:** Seoul-teukbyeolsi **City:** Seoul **Latitude:** 37.568260 **Longitude:** 126.977829 **View:** Google Map
subscription.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.adjust.com	ok	**IP:** 185.151.204.51 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.adjust.world	ok	**IP:** 185.151.204.44 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.xmlsoap.org	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
manual.sensorsdata.cn	ok	**IP:** 47.246.23.178 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
gdpr.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api.dancefit.me	ok	**IP:** 18.238.109.86 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
misc-pili-qos-report.qiniuapi.com	ok	**IP:** 110.242.48.56 **Country:** China **Region:** Hebei **City:** Baoding **Latitude:** 38.851109 **Longitude:** 115.490280 **View:** Google Map
subscription.adjust.net.in	ok	**IP:** 185.151.204.34 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.adjust.world	ok	**IP:** 185.151.204.42 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.pv.com	ok	**IP:** 86.105.245.69 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
subscription.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.tr.adjust.com	ok	**IP:** 195.244.54.44 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
gdpr.adjust.net.in	ok	**IP:** 185.151.204.30 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
dev.dailyyoga.com	ok	**IP:** 34.193.83.103 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
purl.org	ok	**IP:** 207.241.225.157 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map

| DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
subscription.adjust.com	ok	**IP:** 185.151.204.52 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
en.wikipedia.org	ok	**IP:** 198.35.26.96 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.791256 **Longitude:** -122.400810 **View:** Google Map
app.adjust.net.in	ok	**IP:** 185.151.204.32 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

✉ EMAILS
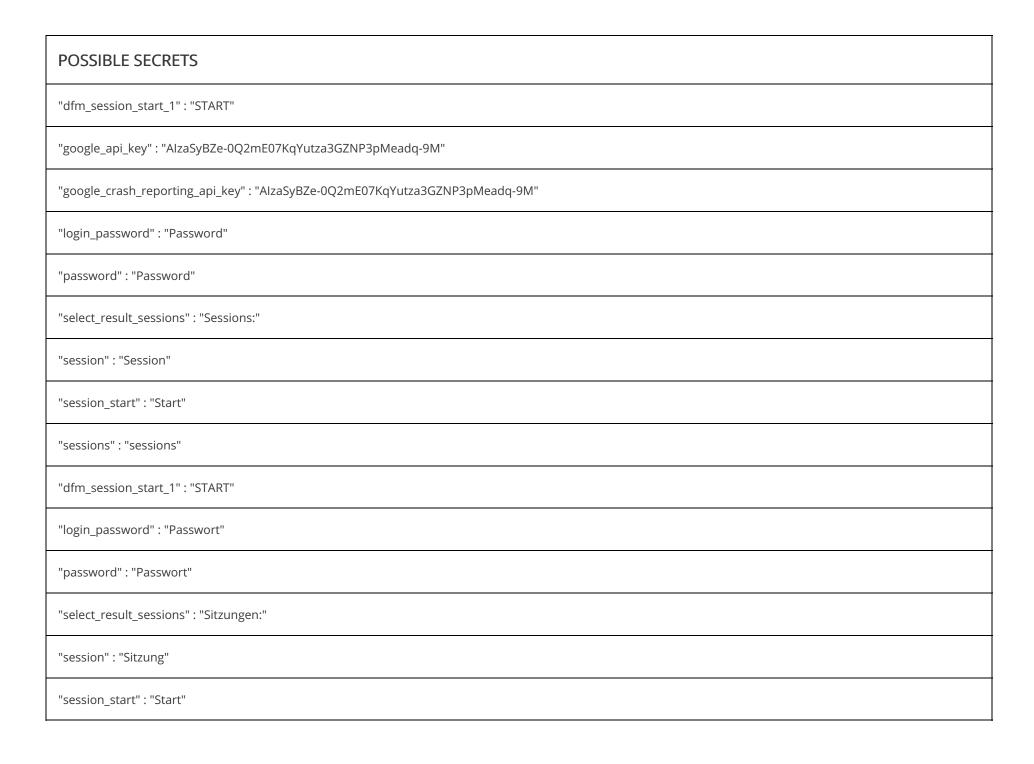
EMAIL	FILE
□□□□□support@dancefit.me□□□□□□□□□ support@dancefit.me □□□□□□□□□□□□support@dancefit.me□□□□□	Android String Resource
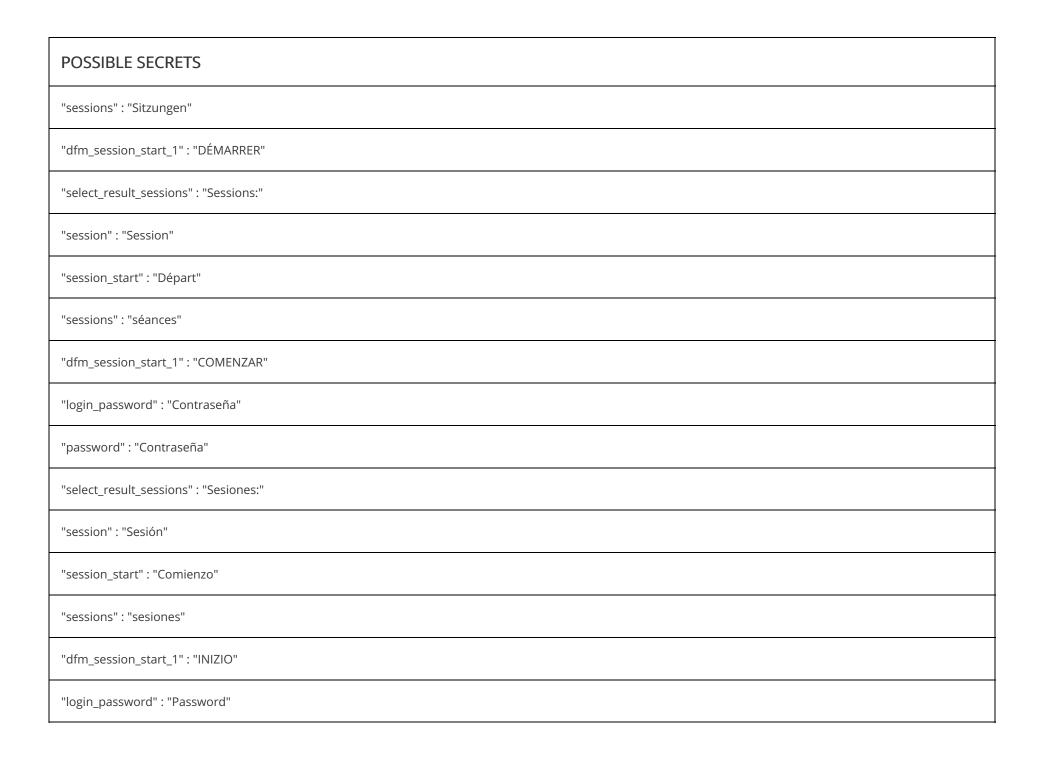
🕵 TRACKERS
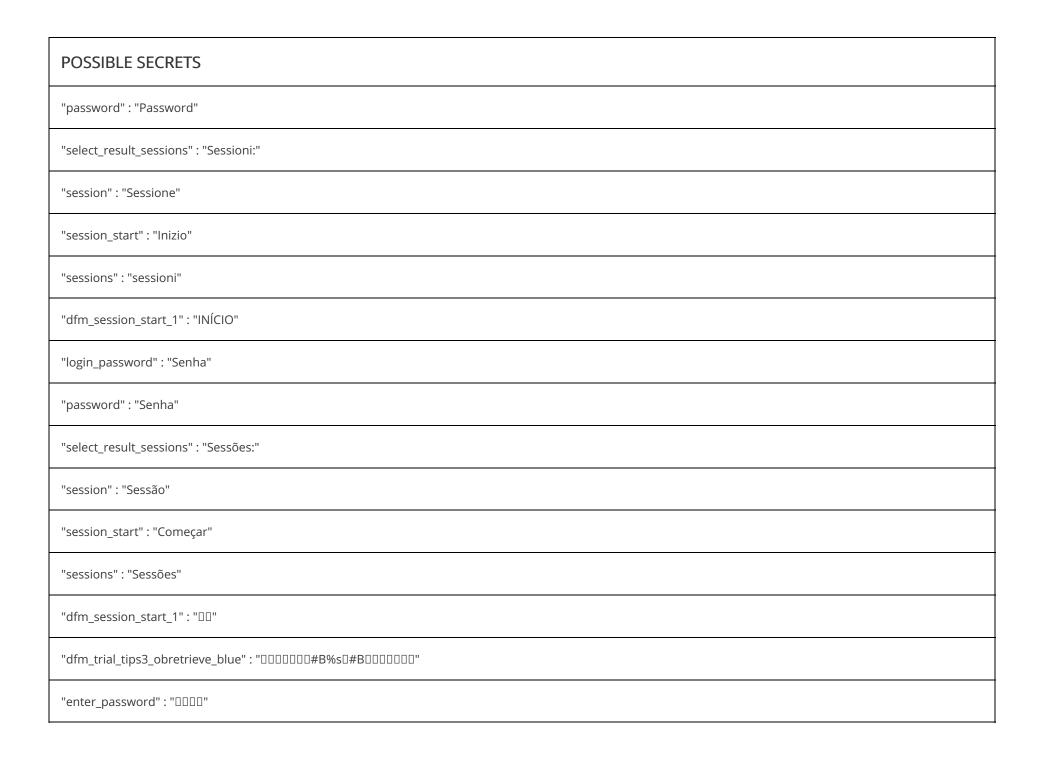
TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248
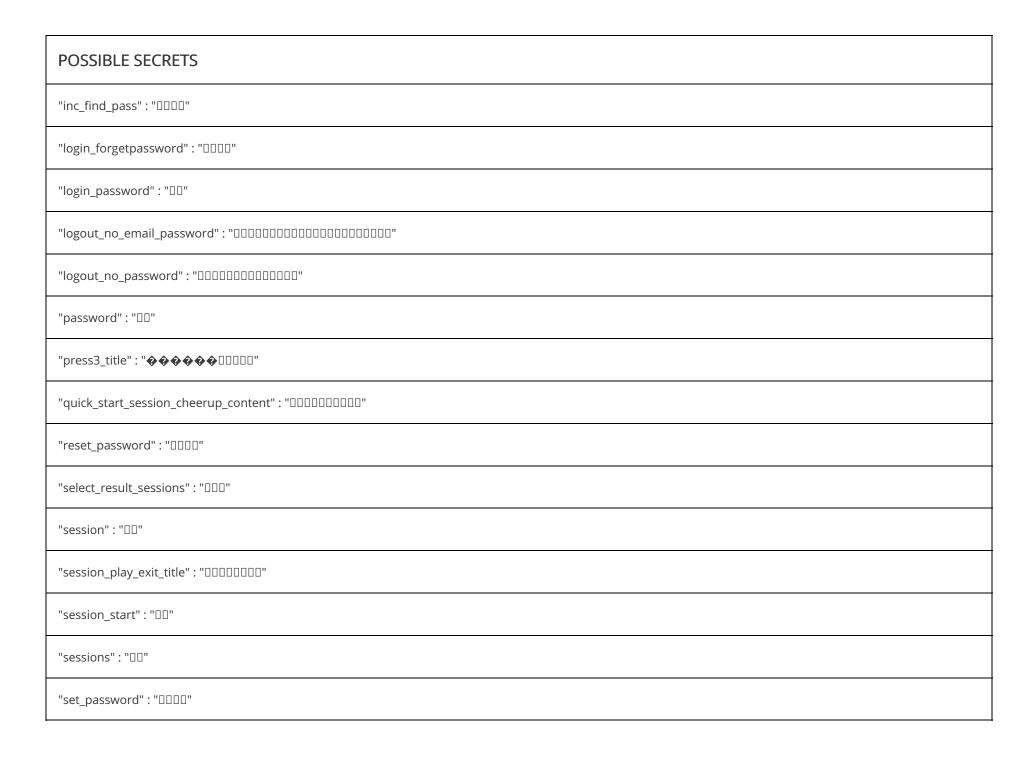
🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "0000000000000000000000000000000"

POSSIBLE SECRETS

"dfm_session_start_1" : "START"

"google_api_key" : "AIzaSyBZe-0Q2mE07KqYutza3GZNP3pMeadq-9M"

"google_crash_reporting_api_key" : "AIzaSyBZe-0Q2mE07KqYutza3GZNP3pMeadq-9M"

"login_password" : "Password"

"password" : "Password"

"select_result_sessions" : "Sessions:"

"session" : "Session"

"session_start" : "Start"

"sessions" : "sessions"

"dfm_session_start_1" : "START"

"login_password" : "Passwort"

"password" : "Passwort"

"select_result_sessions" : "Sitzungen:"

"session" : "Sitzung"

"session_start" : "Start"

POSSIBLE SECRETS

"sessions" : "Sitzungen"

"dfm_session_start_1" : "DÉMARRER"

"select_result_sessions" : "Sessions:"

"session" : "Session"

"session_start" : "Départ"

"sessions" : "séances"

"dfm_session_start_1" : "COMENZAR"

"login_password" : "Contraseña"

"password" : "Contraseña"

"select_result_sessions" : "Sesiones:"

"session" : "Sesión"

"session_start" : "Comienzo"

"sessions" : "sesiones"

"dfm_session_start_1" : "INIZIO"

"login_password" : "Password"

POSSIBLE SECRETS
"password" : "Password"
"select_result_sessions" : "Sessioni:"
"session" : "Sessione"
"session_start" : "Inizio"
"sessions" : "sessioni"
"dfm_session_start_1" : "INÍCIO"
"login_password" : "Senha"
"password" : "Senha"
"select_result_sessions" : "Sessões:"
"session" : "Sessão"
"session_start" : "Começar"
"sessions" : "Sessões"
"dfm_session_start_1" : "□□"
"dfm_trial_tips3_obretrieve_blue" : "□□□□□□□□#B%s□#B□□□□□□□□"
"enter_password" : "□□□□"

POSSIBLE SECRETS
"inc_find_pass" : "□□□□"
"login_forgetpassword" : "□□□□"
"login_password" : "□□"
"logout_no_email_password" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"logout_no_password" : "□□□□□□□□□□□□□□□"
"password" : "□□"
"press3_title" : "�����□□□□□"
"quick_start_session_cheerup_content" : "□□□□□□□□□□□"
"reset_password" : "□□□□"
"select_result_sessions" : "□□□"
"session" : "□□"
"session_play_exit_title" : "□□□□□□□□"
"session_start" : "□□"
"sessions" : "□□"
"set_password" : "□□□□"

POSSIBLE SECRETS

5181942b9ebc31ce68dacb56c16fd79f

8e8c69d523213083d856bb24d9022b91

6d85ce851054c1455f23aa8285c4c970

ChNjb20uYW5kcm9pZC52ZW5kaW5nCibjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

ae2044fb577e65ee8bb576ca48a2f06e

edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

470fa2b4ae81cd56ecbcda9735803434cec591fa

n6uU8wPBqzMdqFpPcubedIOmh4nNa2sNkfvMkbR4Pk/YupsDpic56dMxX0Twvg6SiaKGjv8NO9Lcv

30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e3020170d303930383331323135323136325a180f32303530303930323353231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d01010405000381810005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2At7fSUHuMw6bm/z3Q+X4oY9KpDa1s06

2f57cc785fa56cff2449de2938f2dec2

▶ PLAYSTORE INFORMATION

Title: Dancefitme: Fun Workouts

Score: 4.2828946 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support: Category:** Health & Fitness **Play Store URL:** dance.fit.zumba.weightloss.danceburn

Developer Details: TechPionners Team, 8429985153700026319, None, http://dancefit.me, support@dancefit.me,

Release Date: Apr 13, 2022 **Privacy Policy:** Privacy link

Description:

DanceFitme provides energetic dance workouts and cardio for weight loss everywhere! Get motivated with hip-hop-inspired fitness and our exclusive 4-week workout plans. Sweat and have fun with Dancefitme which contains workouts from beginner to advanced with popular music! WITH DanecFitme YOU'LL GET: - Get an exclusive 28-day personalized dance challenge, start anywhere and anytime - Connect your dance workouts directly to your TV Experience to enjoy a higher-quality experience - Hip-hop, aerobics, jazz, Latin, salsa, Kpop, walking dance, and other dance styles, make exercising easy and enjoyable - Become slim, sexy, and happy all in just one app Dance Workouts Styles include: >> Aerobics >> Dance Fitness >> Hiphop >> Salsa >> K-pop >> Jazz >> Latin >> Walking Dance and more to be explored... Every small step counts for transforming your body, so start moving by downloading the DanceFitme app! - A dance workouts app for weight loss - Numerous beginner dance workouts for choosing freely - Professional dancer team creates dance workouts and customizes the 28-day plan based on your fitness level - Break a sweat with dance workouts at home ⬜DanceFitme provides a new fashionable and efficient way to lose weight in 2025. As DanceFitme knows the traditional workout is boring and hard to commit to, you will say goodbye to boring routines and follow us to lose weight efficiently and joyfully. ⬜DanceFitme took more than 2 years to continuously develop programs with the right intensity, music, dance styles, and movements aimed at weight loss and burning calories. Whether you have danced before, DanceFitme will help you lose weight more energetically and efficiently. You never need to be skilled at dance, cause each workout is easy to follow. ⬜Follow the popular music DanceFitme selected and move your body with the dance bit. Just in a song, you can burn about 100 calories while having fun with the pumped-up tunes and energetic moves. 5 MAJOR BENEFITS YOU'LL GET: - POPULAR QUICK WEIGHT LOSS DANCE STYLES Aerobics, salsa, Kpop, walking dance, and more specially designed dance &fitness workouts. Over 300+ songs and programs in the DanceFitme app. - PERSONALIZED DANCE WORKOUTS PLAN DanceFitme tailors your dance workout plan according to your current body status, weight loss goals, and the areas where you want to improve. With our 4-week dance plan, you are more likely to keep on track. - FOR ANY LEVEL Whether you're a newbie or a pro, you will find suitable programs or workouts in this Dance app with simple and clear instructions. Everyone may be at a different level, the great thing is that you are working out. - FOR ALL BODY PARTS Dance workouts are designed by fitness and dance experts to help you achieve your goals. You can select the full body, or specific parts such as abs, butt, back, or legs, to make your practice more targeted. - AUTOMATED DATA TRACKING Track your progress to motivate yourself and reach new fitness goals. You can view calories burned and total practice time in DanceFitme. Progress tracking can motivate you to reach new dance fitness levels and get your dream body! * All payments will be made through your Google Account and may be managed under Account Settings after the initial payment. Subscription payments will automatically renew unless deactivated at least 24 hours before the end of the current cycle. Your account will be charged for renewal at least 24 hours before the end of the current cycle. Any unused portion of your free trial will be forfeited upon payment. Cancellations are incurred by disabling auto-renewal. CONTACT & INFO Email: support@dancefit.me Privacy Policy: https://www.dancefit.me/privacy-policy.html Terms of Use Agreement: https://www.dancefit.me/terms-of-use.html FOLLOW US Facebook: https://www.facebook.com/profile.php?id=100081953393070 Instagram: https://www.instagram.com/dancefitme

☰ SCAN LOGS

Timestamp	Event	Error
2025-09-01 12:57:05	Generating Hashes	OK
2025-09-01 12:57:05	Extracting APK	OK
2025-09-01 12:57:05	Unzipping	OK
2025-09-01 12:57:06	Parsing APK with androguard	OK
2025-09-01 12:57:06	Extracting APK features using aapt/aapt2	OK
2025-09-01 12:57:06	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 12:57:10	Parsing AndroidManifest.xml	OK
2025-09-01 12:57:10	Extracting Manifest Data	OK
2025-09-01 12:57:10	Manifest Analysis Started	OK
2025-09-01 12:57:10	Reading Network Security config from network_security_config.xml	OK

2025-09-01 12:57:10	Parsing Network Security config	OK
2025-09-01 12:57:10	Performing Static Analysis on: DanceFitme (dance.fit.zumba.weightloss.danceburn)	OK
2025-09-01 12:57:12	Fetching Details from Play Store: dance.fit.zumba.weightloss.danceburn	OK
2025-09-01 12:57:13	Checking for Malware Permissions	OK
2025-09-01 12:57:13	Fetching icon path	OK
2025-09-01 12:57:13	Library Binary Analysis Started	OK
2025-09-01 12:57:13	Reading Code Signing Certificate	OK
2025-09-01 12:57:14	Running APKiD 2.1.5	OK
2025-09-01 12:57:19	Detecting Trackers	OK
2025-09-01 12:57:21	Decompiling APK to Java with JADX	OK
2025-09-01 12:57:36	Converting DEX to Smali	OK

2025-09-01 12:57:36	Code Analysis Started on - java_source	OK
2025-09-01 12:57:40	Android SBOM Analysis Completed	OK
2025-09-01 12:57:44	Android SAST Completed	OK
2025-09-01 12:57:44	Android API Analysis Started	OK
2025-09-01 12:57:47	Android API Analysis Completed	OK
2025-09-01 12:57:48	Android Permission Mapping Started	OK
2025-09-01 12:57:51	Android Permission Mapping Completed	OK
2025-09-01 12:57:52	Android Behaviour Analysis Started	OK
2025-09-01 12:57:57	Android Behaviour Analysis Completed	OK
2025-09-01 12:57:57	Extracting Emails and URLs from Source Code	OK
2025-09-01 12:58:00	Email and URL Extraction Completed	OK

2025-09-01 12:58:00	Extracting String data from APK	OK
2025-09-01 12:58:01	Extracting String data from Code	OK
2025-09-01 12:58:01	Extracting String values and entropies from Code	OK
2025-09-01 12:58:04	Performing Malware check on extracted domains	OK
2025-09-01 12:58:08	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.