MOBSF

ANDROID STATIC ANALYSIS REPORT

Herlife (4.2.3)

File Name:	app.herlife_402030.apk
Package Name:	app.herlife
Scan Date:	Aug. 28, 2025, 10:13 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	21	4	2	1

FILE INFORMATION

File Name: app.herlife_402030.apk
Size: 31.09MB
MD5: a11163a46a27a4edcf118fb90253c3f2
SHA1: 194354a9bcd4a83e89ba1017cd7be3ba741df9d6
SHA256: e67decc97858ede161b3b087c5a0f906302848be512c63cf56d698ab893fc9b4

APP INFORMATION

App Name: Herlife
Package Name: app.herlife
Main Activity: app.herlife.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 4.2.3

Android Version Code: 402030

APP COMPONENTS

Activities: 6
Services: 16
Receivers: 17
Providers: 10
Exported Activities: 2
Exported Services: 2
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
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: 2022-04-27 07:23:13+00:00
Valid To: 2052-04-27 07:23:13+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4d99aae506de46bb9747c813e3151a26b2cab692
Hash Algorithm: sha256
md5: cc30921b80865fb35acc66387456659c
sha1: 1ab919c2ef25e54e3c5ff5a37320f7aca1314da5
sha256: 2f28d2ad21e4d063c1bd2c4d1c63c6de9a334b62e6a0c2ba0b8e0020b68a2022
sha512: 77f7bda4db3d322f3df6d4da25143937c5a177b2c0e658fd975e2ff5ba0b8d1f68540ef094d3db33d3a23ca12d784df7c593b508ce8a7b5de2726037b02a8eb7
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 94d179c846398a058d3ca0f95bb35304c497ba3d7c2e71f34029d3851663a4a8
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
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.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.farsitel.bazaar.permission.REFERRER	unknown	Unknown permission	Unknown permission from android reference
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.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
app.herlife.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.

APKID ANALYSIS

FILE	DETAILS
a11163a46a27a4edcf118fb90253c3f2.apk	FINDINGS: Anti-VM Code — DETAILS: emulator file check possible VM check
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check FINDINGS: Compiler — DETAILS: r8

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check subscriber ID check emulator file check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
app.herlife.MainActivity	Schemes: herlife://, herlifeapp://, herlife.app://, https://, http://, Hosts: app.herlife.app,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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	Activity (app.herlife.FCMActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	Broadcast Receiver (ir.metrix.referrer.cafebazaar.communicators.broadcast.ClientReceiver) is not Protected. [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.
7	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
8	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.
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.
10	Activity (app.notifee.core.NotificationReceiverActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) is not Protected. [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.

</> CODE ANALYSIS

HIGH: 2 | WARNING: 9 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				app/notifee/core/AlarmPermissionBroadcastReceiver.java app/notifee/core/Logger.java app/notifee/core/RebootBroadcastReceiver.java app/notifee/core/b.java com/agontuk/RNFusedLocation/FusedLocationProvider.java com/agontuk/RNFusedLocation/LocationManagerProvider.java com/agontuk/RNFusedLocation/RNFusedLocationModule.java com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/faizal/OtpVerify/AppSignatureHelper.java com/faizal/OtpVerify/OtpBroadcastReceiver.java com/faizal/OtpVerify/OtpVerifyModule.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/FilterView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/learnium/RNDeviceInfo/RNDeviceModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/mapbox/android/gestures/MultiFingerGesture.java com/mapbox/mapboxsdk/location/engine/AndroidLocationEngineImpl.java com/mapbox/mapboxsdk/location/engine/MapboxFusedLocationEngineImpl.java com/mapbox/mapboxsdk/location/permissions/PermissionsManager.java com/mapbox/mapboxsdk/log/Logger.java com/mapbox/mapboxsdk/maps/renderer/egl/EGLContextFactory.java com/mapbox/mapboxsdk/maps/renderer/egl/EGLWindowSurfaceFactory.java com/mapbox/mapboxsdk/maps/renderer/glsurfaceview/MapboxGLSurfaceView.java com/mapbox/rctmgl/components/annotation/MarkerViewManager.java com/mapbox/rctmgl/components/mapview/RCTMGLMapViewManager.java com/mapbox/rctmgl/components/styles/layers/RCTLayer.java com/mapbox/rctmgl/components/styles/sources/RCTMGLImageSource.java com/mapbox/rctmgl/components/styles/sources/RCTMGLShapeSourceManager.java com/mapbox/rctmgl/events/EventEmitter.java com/mapbox/rctmgl/location/LocationManager.java com/mapbox/rctmgl/modules/RCTMGLLogging.java com/mapbox/rctmgl/modules/RCTMGLModule.java com/mapbox/rctmgl/modules/RCTMGLOfflineModule.java com/mapbox/rctmgl/modules/RCTMGLSnapshotModule.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/mapbox/rctmgl/utils/BitmapUtils.java com/mapbox/rctmgl/utils/ConvertUtils.java com/mapbox/rctmgl/utils/DownloadMapImageTask.java com/microsoft/clarity/n/h.java com/microsoft/codepush/react/CodePushUtils.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/webview/RNCWebView.java com/reactnativecommunity/webview/RNCWebViewClient.java com/reactnativecommunity/webview/RNCWebViewManagerImpl.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaView.java com/zmxv/RNSound/RNSoundModule.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/invertase/notifee/NotifeeReactUtils.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/android/core/SentryLogcatAdapter.java io/sentry/android/replay/WindowManagerSpy.java io/sentry/android/replay/WindowSpy.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/sentry/transport/StdoutTransport.java ir/metrix/CoreInitializer.java ir/metrix/analytics/w.java ir/metrix/attribution/h.java ir/metrix/h.java ir/metrix/internal/init/Initializer.java ir/metrix/internal/log/LogcatLogHandler.java org/conscrypt/Platform.java org/conscrypt/ct/CTVerifier.java org/greenrobot/eventbus/Logger.java timber/log/Timber.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/mapbox/mapboxsdk/plugins/annotation/Annotation.java com/mapbox/mapboxsdk/plugins/annotation/SymbolOptions.java com/mapbox/rctmgl/components/styles/RCTMGLStyleFactory.java com/mapbox/turf/TurfMisc.java com/microsoft/codepush/react/CodePushConstants.java com/microsoft/codepush/react/CodePushTelemetryManager.java io/invertase/firebase/common/TaskExecutorService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingHeadlessService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingSerializer.java io/invertase/notifee/NotifeeEventSubscriber.java io/sentry/Baggage.java io/sentry/RequestDetailsResolver.java io/sentry/SpanDataConvention.java io/sentry/TraceContext.java io/sentry/protocol/User.java org/conscrypt/OpenSSLECKeyFactory.java org/conscrypt/OpenSSLRSAKeyFactory.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ir/metrix/network/ServiceGenerator.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/SSLParametersImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nimbusds/jose/jwk/Curve.java org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OidData.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/OpenSSLProvider.java org/conscrypt/OpenSSLSignature.java org/conscrypt/TrustManagerImpl.java org/conscrypt/ct/CTConstants.java
5	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	com/reactnativecommunity/clipboard/ClipboardModule.java
6	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/RNFetchBlob/RNFetchBlobUtils.java com/airbnb/lottie/network/NetworkCache.java com/microsoft/clarity/e/r.java com/microsoft/clarity/i/e0.java com/microsoft/clarity/n/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/RNFetchBlob/RNFetchBlobFS.java com/RNFetchBlob/Utils/PathResolver.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/mapbox/mapboxsdk/storage/FileSource.java com/microsoft/clarity/g/k.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/DeviceInfoUtil.java
8	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/internal/util/RootChecker.java ir/metrix/utils/common/CommonDeviceInfoHelper.java
10	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/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/RNFetchBlob/RNFetchBlobBody.java com/mapbox/rctmgl/components/mapview/RCTMGLMapView.java com/mapbox/rctmgl/modules/RCTMGLSnapshotModule.java com/mapbox/rctmgl/utils/BitmapUtils.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java io/sentry/react/RNSentryModuleImpl.java
12	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/nimbusds/jose/crypto/RSA_OAEP.java io/sentry/util/StringUtils.java
13	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	com/nimbusds/jose/crypto/AESCBC.java com/nimbusds/jose/jca/JCASupport.java
14	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/microsoft/clarity/models/DynamicConfig.java ir/metrix/internal/MetrixStorage.java
15	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	com/agontuk/RNFusedLocation/FusedLocationProvider.java ir/metrix/utils/common/IdGenerator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
16	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	org/conscrypt/Conscrypt.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/RNFetchBlob/Utils/PathResolver.java com/reactnativedocumentpicker/RNDocumentPickerModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/RNFetchBlob/RNFetchBlobFS.java com/RNFetchBlob/RNFetchBlobReq.java com/RNFetchBlob/Utils/PathResolver.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/mapbox/mapboxsdk/offline/OfflineManager.java com/mapbox/mapboxsdk/storage/FileSource.java com/microsoft/codepush/react/CodePush.java com/microsoft/codepush/react/CodePushUpdateUtils.java com/microsoft/codepush/react/CodePushUtils.java com/microsoft/codepush/react/FileUtils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/DirectoryProcessor.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/SentryOptions.java io/sentry/android/core/AndroidOptionsInitializer.java io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/cache/AndroidEnvelopeCache.java io/sentry/android/replay/ReplayCache.java io/sentry/android/replay/capture/BufferCaptureStrategy.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/instrumentation/file/FileIOSpanManager.java io/sentry/react/RNSentryModuleImpl.java
00188	Get the address of a SMS message	sms	com/RNFetchBlob/Utils/PathResolver.java com/reactnativedocumentpicker/RNDocumentPickerModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	com/RNFetchBlob/Utils/PathResolver.java com/reactnativedocumentpicker/RNDocumentPickerModule.java
00201	Query data from the call log	collection calllog	com/RNFetchBlob/Utils/PathResolver.java com/reactnativedocumentpicker/RNDocumentPickerModule.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/RNFetchBlob/Utils/PathResolver.java com/reactnativedocumentpicker/RNDocumentPickerModule.java ir/metrix/referrer/c.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/microsoft/clarity/n/g.java io/sentry/transport/HttpConnection.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java io/sentry/transport/HttpConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/RNFetchBlob/RNFetchBlobBody.java com/RNFetchBlob/RNFetchBlobFS.java com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/mapbox/mapboxsdk/offline/OfflineManager.java com/microsoft/clarity/e/r.java com/microsoft/clarity/g/k.java com/microsoft/clarity/m/a.java com/microsoft/codepush/react/CodePushUpdateUtils.java com/microsoft/codepush/react/FileUtils.java com/nimbusds/jose/util/IOUtils.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/instrumentation/file/FileInputStreamInitData.java io/sentry/instrumentation/file/SentryFileInputStream.java io/sentry/util/FileUtils.java okio/Okio__JvmOkioKt.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/FileClientSessionCache.java org/conscrypt/KeyManagerFactoryImpl.java
00089	Connect to a URL and receive input stream from the server	command network	com/microsoft/clarity/n/g.java com/microsoft/codepush/react/CodePushUpdateManager.java com/nimbusds/jose/util/DefaultResourceRetriever.java io/sentry/transport/HttpConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/microsoft/clarity/n/g.java com/nimbusds/jose/util/DefaultResourceRetriever.java io/sentry/transport/HttpConnection.java
00012	Read data and put it into a buffer stream	file	com/microsoft/codepush/react/FileUtils.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/util/FileUtils.java org/conscrypt/DefaultSSLContextImpl.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/RNFetchBlob/Utils/PathResolver.java ir/metrix/referrer/c.java
00036	Get resource file from res/raw directory	reflection	app/notifee/core/Notifee.java com/mapbox/mapboxsdk/maps/AttributionDialogManager.java com/microsoft/clarity/l/d.java io/invertase/firebase/common/SharedUtils.java ir/metrix/referrer/c.java n/o/t/i/f/e/e/n.java
00034	Query the current data network type	collection network	ir/metrix/q/j.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java ir/metrix/q/j.java
00024	Write file after Base64 decoding	reflection file	com/RNFetchBlob/RNFetchBlobBody.java com/RNFetchBlob/RNFetchBlobFS.java com/airbnb/lottie/LottieCompositionFactory.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java
00163	Create new Socket and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java org/conscrypt/KitKatPlatformOpenSSLSocketImplAdapter.java org/conscrypt/PreKitKatPlatformOpenSSLSocketImplAdapter.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00016	Get location info of the device and put it to JSON object	location collection	com/mapbox/rctmgl/components/mapview/RCTMGLMapView.java
00147	Get the time of current location	collection location	com/agontuk/RNFusedLocation/LocationUtils.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	app/herlife/FCMActivity.java app/notifee/core/Notifee.java com/RNFetchBlob/RNFetchBlobReq.java com/mapbox/mapboxsdk/maps/AttributionDialogManager.java n/o/t/i/f/e/e/m.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	app/herlife/FCMActivity.java app/notifee/core/Notifee.java com/mapbox/mapboxsdk/maps/AttributionDialogManager.java n/o/t/i/f/e/e/m.java
00137	Get last known location of the device	location collection	com/mapbox/mapboxsdk/location/engine/AndroidLocationEngineImpl.java
00123	Save the response to JSON after connecting to the remote server	network command	com/microsoft/clarity/l/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/mapbox/mapboxsdk/utils/BitmapUtils.java com/microsoft/clarity/e/n.java
00191	Get messages in the SMS inbox	sms	com/RNFetchBlob/RNFetchBlobReq.java com/RNFetchBlob/Utils/PathResolver.java ir/metrix/utils/common/DeviceIdHelper.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java com/microsoft/codepush/react/CodePushUtils.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java
00056	Modify voice volume	control	com/zmxv/RNSound/RNSoundModule.java
00033	Query the IMEI number	collection	ir/metrix/q/e.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java ir/metrix/o/d/f.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00146	Get the network operator name and IMSI	telephony collection	ir/metrix/o/d/f.java
00117	Get the IMSI and network operator name	telephony collection	ir/metrix/o/d/f.java
00067	Query the IMSI number	collection	ir/metrix/o/d/f.java
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/CodePushUpdateManager.java
00192	Get messages in the SMS inbox	sms	com/RNFetchBlob/Utils/PathResolver.java
00091	Retrieve data from broadcast	collection	app/herlife/FCMActivity.java
00115	Get last known location of the device	collection location	ir/metrix/o/d/e.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00028	Read file from assets directory	file	com/mapbox/mapboxsdk/http/LocalRequestTask.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://herlife-3b44d-default-rtdb.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/341483758588/namespaces/firebase:fetch?key=AIzaSyBpbCCjma3EsBPLyvC_BGbjksM8TYtGaMw is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'is_subscribed': 'true'}, 'state': 'UPDATE', 'templateVersion': '7'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE
Other Common Permissions	5/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.ACCESS_NOTIFICATION_POLICY

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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.mapbox.com	ok	**IP:** 199.232.192.143 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
codepush.appcenter.ms	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
tracker.metrix.ir	ok	**IP:** 45.94.255.16 **Country:** Iran (Islamic Republic of) **Region:** Azarbayjan-e Gharbi **City:** Salmas **Latitude:** 38.197300 **Longitude:** 44.765301 **View:** Google Map
notifee.app	ok	**IP:** 52.52.192.191 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
herlife-3b44d-default-rtdb.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
apps.mapbox.com	ok	**IP:** 18.238.109.99 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk-sentry.metrix.ir	ok	**IP:** 45.94.255.16 **Country:** Iran (Islamic Republic of) **Region:** Azarbayjan-e Gharbi **City:** Salmas **Latitude:** 38.197300 **Longitude:** 44.765301 **View:** Google Map
docs.swmansion.com	ok	**IP:** 172.67.142.188 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
gateway.metrix.ir	ok	**IP:** 45.94.255.16 **Country:** Iran (Islamic Republic of) **Region:** Azarbayjan-e Gharbi **City:** Salmas **Latitude:** 38.197300 **Longitude:** 44.765301 **View:** Google Map
demotiles.maplibre.org	ok	**IP:** 104.18.12.114 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.clarity.ms	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
analytics.metrix.ir	ok	**IP:** 45.94.255.16 **Country:** Iran (Islamic Republic of) **Region:** Azarbayjan-e Gharbi **City:** Salmas **Latitude:** 38.197300 **Longitude:** 44.765301 **View:** Google Map
shopify.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
clarity.microsoft.com	ok	**IP:** 13.107.6.158 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
entry.metrix.ir	ok	**IP:** 45.94.255.16 **Country:** Iran (Islamic Republic of) **Region:** Azarbayjan-e Gharbi **City:** Salmas **Latitude:** 38.197300 **Longitude:** 44.765301 **View:** Google Map
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Flipper	Analytics	https://reports.exodus-privacy.eu.org/trackers/392
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://herlife-3b44d-default-rtdb.firebaseio.com"
"google_api_key" : "AIzaSyBpbCCjma3EsBPLyvC_BGbjksM8TYtGaMw"
"google_crash_reporting_api_key" : "AIzaSyBpbCCjma3EsBPLyvC_BGbjksM8TYtGaMw"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
41058363725152142129326129780047268409114441015993725554835256314039467401291
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34

POSSIBLE SECRETS
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ae2044fb577e65ee8bb576ca48a2f06e
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
484395612939064517590525852527979142027629495260417479958440807170824046352 86
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434427757837678 4
b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112316
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
5181942b9ebc31ce68dacb56c16fd79f
51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
1ddaa4b892e61b0f7010597ddc582ed3
085c1e6aad7f4d1e992c94412da43557
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
24b2477514809255df232947ce7928c4
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
36134250956749795798585127919587881956611106672985015071877198253568414405109
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

POSSIBLE SECRETS

115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Herlife-هرلایف

Score: 4.52 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** app.herlife

Developer Details: Zarrino, 7907086320236875902, None, https://herlifeapp.com/, herlife@zarrino.io,

Release Date: Apr 27, 2022 **Privacy Policy:** Privacy link

Description:

هِرلایف یک برنامه پریود ترکر (رهگیری قاعدگی) و مدیریت سلامت زنان است. «تقویم پریود، تقویم تخمک گذاری، محاسبه سیکل قاعدگی آنلاین، مشاوره و ویزیت آنلاین با پزشک، مشاهده وضعیت پنجره باروری و تخمک گذاری» از قابلیت‌های مهم نرم افزار هرلایف هستند. در اپلیکیشن هرلایف، حتی می‌توانید شریک عاطفی یا ،(PMS) چرخه قاعدگی، علائم پریود، سندروم پیش از قاعدگی «همراه» خود را در جریان «چرخه پریود، وضعیت روحی و جسمی» خود قرار دهید تا با دریافت پیام‌های سفارشی، بیشتر مراقب شما باشد. ویژگی‌های برنامه پریود هرلایف برای اندروید: امکان مشاوره و ویزیت آنلاین در بخش «کلینیک» با پزشک‌های متخصص وجود دسته بندی‌های متنوع در کلینیک هرلایف مانند: «زنان و زایمان، پوست و مو، تغذیه و داخلی» • ثبت تاریخ پریود، پیش‌بینی و تحلیل عادت ماهانه (تقویم قاعدگی) • امکان پیش بینی زمان دقیق پریود بعدی پیش بینی زمان مناسب باروری و تخمین روز تخمک گذاری • امکان اطلاع از احتمال بروز علائم سندروم پیش از قاعدگی و راه‌های مقابله با آن • ثبت حالات روحی و جسمی، و علائم چرخه پریود به صورت روزانه مانند: «ترشحات واژن، درد پستان و نوسانات خلقی» • امکان مشاهده رشته استوری‌های سفارشی (PMS) پریود و ،(PMS) روزانه، توصیه‌های علمی سفارشی متناسب با وضعیت جسمانی و حال روحی شما و علائم روزانه • اشتراک گذاری اطلاعات چرخه قاعدگی، شروع سندرم پیش از قاعدگی تخمک‌گذاری با شریک عاطفی (همراه) ارسال پیام‌های سفارشی و متناسب با حال و روز شما از طریق ویژگی «همراه» برای شریک عاطفی‌تان • پیشنهاد مقالات علمی و مورد تأیید پزشک، دربارهٔ سلامت زنان با توجه به وضعیت جسمی و روحی شما در هر روز • امکان دریافت گزارش تحلیلی از وضعیت چرخه پریود و علائم جسمی و روحی برای درک بهتر الگوی بدنی منحصر به فرد و ارائه به پزشک خود • امکان پرسش و پاسخ و تبادل تجربه با کاربران دیگر به صورت کاملاً ناشناس در فضای امن «پرس‌وگو» • هرلایف با پشتوانه علمی و با همراهی تیم پزشکی خود، به سؤال‌های پزشکی شما در مورد تغییر «خلق و خو، سطح انرژی، پوست و مو، دستگاه گوارشی و دیگر علائم پریودی» در چرخه قاعدگی پاسخ می‌دهد. پاسخ سؤالات خود را می‌توانید در بخش کلینیک، پرس‌وگو یا در بخش مقالات پیدا کنید. • بخش «پرس‌وگو» در هرلایف، فضایی امن است که به شما این امکان را می‌دهد تا به راحتی و به صورت ناشناس با پزشک گفتگو کنید. همین‌طور با کاربران دیگر اپلیکیشن برای ثبت و بررسی پریود، سندروم پیش از (Period Tracker) تعامل داشته باشید، و تجربیات خود را در مورد پریود و سلامتی با یکدیگر به اشتراک بگذارید. اگر به دنبال نرم افزار رهگیری پریود قاعدگی یا تخمک‌گذاری هستید یا صرفاً می‌خواهید بدن خود را بیشتر بشناسید، هرلایف کنار شماست تا با هم دلی، آگاهی دادن و یادآوری، سبک سلامت زندگی و تعادل را به زندگی شما هدیه دهد.

SCAN LOGS

Timestamp	Event	Error
2025-08-28 22:13:59	Generating Hashes	OK
2025-08-28 22:14:00	Extracting APK	OK
2025-08-28 22:14:00	Unzipping	OK
2025-08-28 22:14:00	Parsing APK with androguard	OK
2025-08-28 22:14:00	Extracting APK features using aapt/aapt2	OK
2025-08-28 22:14:00	Getting Hardcoded Certificates/Keystores	OK
2025-08-28 22:14:02	Parsing AndroidManifest.xml	OK
2025-08-28 22:14:02	Extracting Manifest Data	OK
2025-08-28 22:14:02	Manifest Analysis Started	OK
2025-08-28 22:14:03	Performing Static Analysis on: Herlife (app.herlife)	OK

2025-08-28 22:14:04	Fetching Details from Play Store: app.herlife	OK
2025-08-28 22:14:05	Checking for Malware Permissions	OK
2025-08-28 22:14:05	Fetching icon path	OK
2025-08-28 22:14:05	Library Binary Analysis Started	OK
2025-08-28 22:14:05	Reading Code Signing Certificate	OK
2025-08-28 22:14:05	Running APKiD 2.1.5	OK
2025-08-28 22:14:10	Detecting Trackers	OK
2025-08-28 22:14:14	Decompiling APK to Java with JADX	OK
2025-08-28 22:14:33	Converting DEX to Smali	OK
2025-08-28 22:14:33	Code Analysis Started on - java_source	OK
2025-08-28 22:14:36	Android SBOM Analysis Completed	OK

2025-08-28 22:14:40	Android SAST Completed	OK
2025-08-28 22:14:40	Android API Analysis Started	OK
2025-08-28 22:14:44	Android API Analysis Completed	OK
2025-08-28 22:14:44	Android Permission Mapping Started	OK
2025-08-28 22:14:47	Android Permission Mapping Completed	OK
2025-08-28 22:14:48	Android Behaviour Analysis Started	OK
2025-08-28 22:14:52	Android Behaviour Analysis Completed	OK
2025-08-28 22:14:52	Extracting Emails and URLs from Source Code	OK
2025-08-28 22:14:56	Email and URL Extraction Completed	OK
2025-08-28 22:14:56	Extracting String data from APK	OK
2025-08-28 22:14:56	Extracting String data from Code	OK

2025-08-28 22:14:56	Extracting String values and entropies from Code	OK
2025-08-28 22:14:59	Performing Malware check on extracted domains	OK
2025-08-28 22:15:01	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.