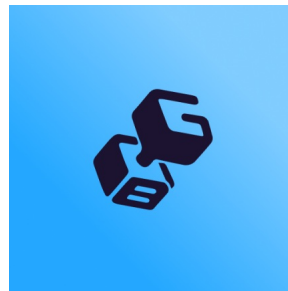




ANDROID STATIC ANALYSIS REPORT



 Liftoff (2.0.2)

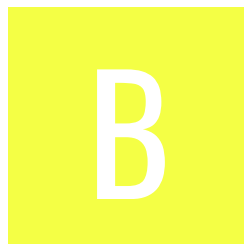
File Name: com.gymbros.app_302.apk

Package Name: com.gymbros.app

Scan Date: Aug. 29, 2025, 11:23 p.m.






App Security Score: 49/100 (MEDIUM RISK)

Grade:



Trackers Detection: 6/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	22	4	2	1

FILE INFORMATION

File Name: com.gymbros.app_302.apk

Size: 124.59MB

MD5: 679599e2e8cc4777ad68166bd2a3f063

SHA1: 760d1a8cc626223eda34aef8a8c4192539978c0f

SHA256: 48caed47ec9745ede3c007261674fe981b6271759417370856ff25c00dfe9010

APP INFORMATION

App Name: Liftoff

Package Name: com.gymbros.app

Main Activity: com.gymbros.app.MainActivity

Target SDK: 34

Min SDK: 23

Max SDK:

Android Version Name: 2.0.2

Android Version Code: 302

APP COMPONENTS

Activities: 11

Services: 19

Receivers: 19

Providers: 13

Exported Activities: 2

Exported Services: 2

Exported Receivers: 5

Exported Providers: 1

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: 2023-04-20 02:43:51+00:00

Valid To: 2053-04-20 02:43:51+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x6aa31cb0f101552a2ff88900aea5668516c5fa57

Hash Algorithm: sha256

md5: 4174af036d6fb13564eb4565b2689236

sha1: 7b45b5f99b43cef56baddac5cae0b920803d0789

sha256: 5fc760275f21c908355419006ad8022187cbf72d7ea701680fc4907cf234bc30

sha512: 3759a45a58cfcc2b8406b9001b7b76543dccee692f4d44e7016c53ea64a7a0d3b721be5c6f1df2e295b12caa1dc1dabea2826568d58252261ea78413d4b9faa3

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 2c019329bd915aa219a61bafae686fe8404d28946ffc12093bc04a9efae4ceda

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.
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_AD SERVICES_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_AD SERVICES_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.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.gymbros.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS
------	---------

FILE	DETAILS	
679599e2e8cc4777ad68166bd2a3f063.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
	Obfuscator	Kiwi encrypter
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible VM check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.TAGS check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check SIM operator check network operator name check
	Obfuscator	Kiwi encrypter
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes4.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes5.dex	FINDINGS	DETAILS
	Anti-VM Code	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 possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)
classes6.dex	FINDINGS	DETAILS
	Compiler	unknown (please file detection issue!)

ACTIVITY	INTENT
com.gymbros.app.MainActivity	Schemes: gymbros://, com.gymbros.app://, exp+gymbros://, https://, Hosts: getgymbros.com, Path Patterns: .*,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

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: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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	App Link assetlinks.json file not found [android:name=com.gymbros.app.MainActivity] [android:host=https://getgymbros.com]	high	App Link asset verification URL (https://getgymbros.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 307). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
3	Content Provider (expo.modules.clipboard.ClipboardFileProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.canhub.cropper.CropImageActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [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	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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	<p>Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.c2dm.permission.SEND [android:exported=true]</p>	warning	<p>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.</p>
9	<p>Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]</p>	warning	<p>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.</p>
10	<p>Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.DUMP [android:exported=true]</p>	warning	<p>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.</p>

NO	ISSUE	SEVERITY	DESCRIPTION
11	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.
12	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: 0 | WARNING: 9 | INFO: 4 | 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 cl/json/RNShareImpl.java cl/json/RNSharePathUtil.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.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/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/lean/PurchasingService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/a/c/b.java com/amazon/device/simplesignin/a/c.java com/amazon/device/simplesignin/a/c/b.java com/amplitude/reactnative/LogcatLogger.java com/brentvatne/common/api/BufferingStrategy.java com/brentvatne/common/api/Source.java com/brentvatne/common/toolbox/DebugLog.java com/brentvatne/exoplayer/ExoPlayerView.java com/brentvatne/exoplayer/FullscreenPlayerView.java com/brentvatne/exoplayer/ReactExoPlayerView.java com/brentvatne/exoplayer/ReactExoPlayerViewManager.java com/brentvatne/exoplayer/VideoPlaybackService.java com/brentvatne/react/ReactNativeVideoManager.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/integration/avif/AvifByteBufferBitmapDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbNailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPrefillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/ResourceUriLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/Bitmap

NO	ISSUE	SEVERITY	STANDARDS	<p>Encoder.java</p> <p>FILES</p> <p>com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java</p>
				<p>com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java</p> <p>com/bumptech/glide/load/resource/bitmap/Downsampler.java</p> <p>com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java</p> <p>com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java</p> <p>com/bumptech/glide/load/resource/bitmap/TransformationUtils.java</p> <p>com/bumptech/glide/load/resource/bitmap/VideoDecoder.java</p> <p>com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java</p> <p>com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java</p> <p>com/bumptech/glide/load/resource/gif/StreamGifDecoder.java</p> <p>com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java</p> <p>com/bumptech/glide/manager/RequestTracker.java</p> <p>com/bumptech/glide/manager/SingletonConnectivityReceiver.java</p> <p>com/bumptech/glide/module/ManifestParser.java</p> <p>com/bumptech/glide/request/SingleRequest.java</p> <p>com/bumptech/glide/request/target/CustomViewTarget.java</p> <p>com/bumptech/glide/request/target/ViewTarget.java</p> <p>com/bumptech/glide/signature/ApplicationVersionSignature.java</p> <p>com/bumptech/glide/util/ContentLengthInputStream.java</p> <p>com/bumptech/glide/util/pool/FactoryPools.java</p> <p>com/canhub/cropper/BitmapUtils.java</p> <p>com/canhub/cropper/CropImageActivity.java</p> <p>com/canhub/cropper/CropOverlayView.java</p>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/canhub/cropper/utils/GetUriForFileKt.java com/caverock/androidsvg/CSSParser.java com/caverock/androidsvg/SVG.java com/caverock/androidsvg/SVGAndroidRenderer.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java com/coremedia/iso/boxes/sampleentry/AudioSampleEntry.java com/github/penfeizhou/animation/FrameAnimationDrawable.java com/github/penfeizhou/animation/apng/decode/APNGDecoder.java com/github/penfeizhou/animation/decode/FrameSeqDecoder.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.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/RNDeviceInfoModule.java com/learnium/RNDeviceInfo/RNDeviceInfoClient.java com/learnium/RNDeviceInfo/resolver/DeviceInfoResolver.java com/mixpanel/android/mpmetrics/AnalyticsMessages.java com/mixpanel/android/mpmetrics/ConfigurationChecker.java com/mixpanel/android/mpmetrics/MPCConfig.java com/mixpanel/android/mpmetrics/MPDbAdapter.java com/mixpanel/android/mpmetrics/MixpanelAPI.java com/mixpanel/android/mpmetrics/PersistentIdent

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	ity.java com/mixpanel/android/mpmetrics/ResourceReader.java com/mixpanel/android/mpmetrics/SessionMetadata.java com/mixpanel/android/mpmetrics/SystemInformation.java com/mixpanel/android/util/HttpService.java com/mixpanel/android/util/MPLog.java com/mrousavy/camera/CameraView\$configureSession\$tryEnableExtension\$1.java com/mrousavy/camera/CameraView\$update\$1\$1.java com/mrousavy/camera/CameraView.java com/mrousavy/camera/CameraViewModule\$getAvailableCameraDevices\$1.java com/mrousavy/camera/CameraViewModule.java com/mrousavy/camera/CameraView_EventsKt.java com/mrousavy/camera/CameraView_TakePhotoKt\$takePhoto\$2\$results\$1.java com/mrousavy/camera/CameraView_TakePhotoKt\$takePhoto\$2\$results\$2.java com/mrousavy/camera/CameraView_TakePhotoKt\$takePhoto\$2.java com/mrousavy/camera/frameprocessor/FrameProcessorRuntimeManager.java com/mrousavy/camera/utils/ImageProxy_saveKt.java com/naman14/androidlame/Mp3AudioRecorder.java com/naman14/androidlame/Mp3Player.java com/reactcommunity/rndatetimepicker/Common.java com/reactcommunity/rndatetimepicker/MinuteIntervalSnappableTimePickerDialog.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/reactnativecommunity/asyncstorage/ReactDa taStoreSupplier.java com/reactnativecompressor/Audio/AudioExtractor. java com/reactnativecompressor/Utils/Downloader.jav a com/reactnativecompressor/Utils/MediaCache.jav a com/reactnativecompressor/Utils/Uploader.java com/reactnativecompressor/Utils/Utils.java com/reactnativecompressor/Video/VideoCompres sor/compressor/Compressor.java com/reactnativecompressor/Video/VideoCompres sor/Utils/CompressorUtils.java com/reactnativecompressor/Video/VideoCompres sor/Utils/StreamableVideo.java com/reactnativecompressor/Video/VideoMain.java com/reactnativemmkv/MmkvModule.java com/revenuecat/purchases/common/DefaultLogH andler.java com/revenuecat/purchases/hybridcommon/Com monKt.java com/revenuecat/purchases/hybridcommon/mapp ers/PurchasesPeriod.java com/revenuecat/purchases/react/RNPurchasesMo dule.java com/sensors/RNSensor.java com/shopify/reactnative/skia/PlatformContext.jav a com/shopify/reactnative/skia/RNSkiaModule.java com/shopify/reactnative/skia/SkiaBaseView.java com/shopify/reactnative/skia/ViewScreenshotServi ce.java com/swmansion/gesturehandler/react/RNGesture HandlerModule.java com/swmansion/gesturehandler/react/RNGesture HandlerRootHelper.java com/swmansion/gesturehandler/react/RNGesture HandlerRootView.java com/swmansion/reanimated/NativeMethodsHelpe r.java

NO	ISSUE	SEVERITY	STANDARDS	com/swmansion/reanimated/ReanimatedModule.j FILES com/swmansion/reanimated/ReanimatedUIManag erFactory.java com/swmansion/reanimated/layoutReanimation/A nimationsManager.java com/swmansion/reanimated/layoutReanimation/R eanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/S haredTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeP roxyCommon.java com/swmansion/reanimated/sensor/ReanimatedS ensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderCo nfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaView.jav a eightbitlab/com/blurview/BlurView.java expo/modules/ExpoModulesPackage.java expo/modules/adapters/react/services/UIManager ModuleWrapper.java expo/modules/apploder/AppLoaderProvider.java expo/modules/av/player/PlayerData.java expo/modules/av/player/SimpleExoPlayerData.jav a expo/modules/av/video/MediaController.java expo/modules/backgroundfetch/BackgroundFetch TaskConsumer.java expo/modules/camera/next/CameraViewNextMod ule.java expo/modules/camera/next/ExpoCameraView.java expo/modules/camera/next/analyzers/BarcodeAn alyzer.java expo/modules/clipboard/ClipboardModule.java expo/modules/constants/ConstantsService.java expo/modules/constants/ExponentInstallationId.ja va expo/modules/core/logging/OSLogHandler.java expo/modules/devlauncher/helpers/DevLauncherI nstallationIDHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				expo/modules/devlauncher/launcher/configurator5/DevLauncherExpoActivityConfigurator.java expo/modules/devmenu/devtools/DevMenuDevToolsDelegate\$openJSInspector\$1\$1.java expo/modules/devmenu/extensions/DevMenuExtension.java expo/modules/devmenu/react/DevMenuPackagerCommandHandlersSwapper\$swapCurrentCommandHandlers\$1.java expo/modules/devmenu/react/DevMenuPackagerCommandHandlersSwapper.java expo/modules/devmenu/react/DevMenuShakeDetectorListenerSwapper.java expo/modules/devmenu/websockets/DevMenuCommandHandlersProvider.java expo/modules/filesystem/FileSystemModule\$definition\$1\$17\$1\$1\$1.java expo/modules/filesystem/FileSystemModule\$definition\$1\$18\$1.java expo/modules/filesystem/FileSystemModule\$definition\$1\$19\$4.java expo/modules/filesystem/FileSystemModule\$downloadResumableTask\$2.java expo/modules/filesystem/FileSystemModule.java expo/modules/image/ExpoImageView.java expo/modules/image/ImageViewWrapperTarget.java expo/modules/image/ThumbnailRequestCoordinatorExtensionKt.java expo/modules/image/events/GlideRequestListener.java expo/modules/imagepicker/ImagePickerUtilsKt.java expo/modules/localization/LocalizationModule.java expo/modules/medialibrary/MediaLibraryModule.java expo/modules/medialibrary/MediaLibraryUtils.java expo/modules/medialibrary/assets/AssetUtilsKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				expo/modules/navigationbar/NavigationBarReactActivityLifecycleListener.java expo/modules/navigationbar/singletons/NavigationBar.java expo/modules/notifications/badge/BadgeHelper.java expo/modules/notifications/notifications/ArgumentsNotificationContentBuilder.java expo/modules/notifications/notifications/JSONNotificationContentBuilder.java expo/modules/notifications/notifications/background/BackgroundRemoteNotificationTaskConsumer.java expo/modules/notifications/notifications/presentation/ExpoNotificationPresentationEffectsManager.java expo/modules/notifications/notifications/presentation/builders/CategoryAwareNotificationBuilder.java expo/modules/notifications/notifications/presentation/builders/ChannelAwareNotificationBuilder.java expo/modules/notifications/notifications/presentation/builders/ExpoNotificationBuilder.java expo/modules/notifications/serverregistration/InstallationId.java expo/modules/notifications/service/NotificationsService.java expo/modules/notifications/service/delegates/ExpoHandlingDelegate.java expo/modules/notifications/service/delegates/ExpoNotificationLifecycleListener.java expo/modules/notifications/service/delegates/ExpoPresentationDelegate.java expo/modules/notifications/service/delegates/ExpoSchedulingDelegate.java expo/modules/securestore/SecureStoreModule.java expo/modules/splashscreen/singletons/SplashScreen.java expo/modules/taskManager/TaskManagerUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				expo/modules/taskManager/TaskService.java expo/modules/taskManager/Utils.java fr/greweb/reactnativeviewshot/RNViewShotModule.java fr/greweb/reactnativeviewshot/ViewShot.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/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 io/sentry/transport/StdoutTransport.java javazoom/jl/converter/jlc.java javazoom/jl/player/PlayerApplet.java javazoom/jl/player/advanced/jlap.java javazoom/jl/player/jlp.java me/leolin/shortcutbadger/ShortcutBadger.java org/greenrobot/eventbus/Logger.java
				com/amplitude/reactnative/AmplitudeReactNativeModule.java com/brentvatne/common/api/DRMProps.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.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	ava com/bumptechnexttech/glide/load/engine/EngineResource.java com/bumptechnexttech/glide/load/engine/ResourceCacheKey.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/av/AVManager.java expo/modules/camera/next/tasks/ResolveTakenPictureKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-14	<div>expo/modules/camera/tasks/ResolveTakenPictureTaskKt.java</div> <div>expo/modules/clipboard/GetImageOptions.java</div> <div>expo/modules/constants/ExponentInstallationId.java</div> <div>expo/modules/image/records/SourceMap.java</div> <div>expo/modules/interfaces/permissions/PermissionsResponse.java</div> <div>expo/modules/notifications/notifications/ArgumentsNotificationContentBuilder.java</div> <div>expo/modules/notifications/notifications/JSONNotificationContentBuilder.java</div> <div>expo/modules/notifications/notifications/background/BackgroundRemoteNotificationTaskConsumer.java</div> <div>expo/modules/notifications/notifications/channels/serializers/NotificationsChannelGroupSerializer.java</div> <div>expo/modules/notifications/notifications/channels/serializers/NotificationsChannelSerializer.java</div> <div>expo/modules/notifications/notifications/presentation/builders/ExpoNotificationBuilder.java</div> <div>expo/modules/notifications/permissions/NotificationPermissionsModuleKt.java</div> <div>expo/modules/notifications/serverregistration/InstallationId.java</div> <div>expo/modules/notifications/service/NotificationsService.java</div> <div>expo/modules/notifications/service/delegates/ExpoPresentationDelegate.java</div> <div>expo/modules/notifications/tokens/PushTokenModuleKt.java</div> <div>expo/modules/taskManager/TaskManagerUtils.java</div> <div>expo/modules/webbrowser/OpenBrowserOptions.java</div> <div>expo/modules/webbrowser/WebBrowserModuleKt.java</div> <div>io/invertase/firebase/common/TaskExecutorService.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/notifee/NotifeeEventSubscriber.java io/sentry/Baggage.java io/sentry/SpanDataConvention.java io/sentry/TraceContext.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	io/sentry/protocol/User.java com/canhub/cropper/BitmapUtils.java com/canhub/cropper/CropImage.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecompressor/Utils/RealPathUtil.java expo/modules/clipboard/ClipboardFileProvider.java expo/modules/medialibrary/MediaLibraryUtils.java io/invertase/firebase/Utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/DeviceInfoUtil.java
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	expo/modules/device/DeviceModule.java io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/internal/util/RootChecker.java
5	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/canhub/cropper/BitmapUtils.java com/canhub/cropper/CropImageActivity.java com/mrousavy/camera/CameraView_RecordVideoKt.java com/mrousavy/camera/CameraView_TakePhotoKt\$takePhoto\$2\$results\$2.java com/mrousavy/camera/CameraView_TakeSnapshotKt\$takeSnapshot\$2.java fr/greweb/reactnativeviewshot/RNViewShotModule.java io/sentry/react/RNSentryModuleImpl.java
6	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java expo/modules/clipboard/ClipboardModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/reactnativemcommunity/clipboard/ClipboardModule.java expo/modules/clipboard/ClipboardModule.java expo/modules/devmenu/modules/DevMenuInternalModule.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/constants/ExponentInstallationId.java expo/modules/devlauncher/launcher/DevLauncherRecentlyOpenedAppsRegistry.java expo/modules/notifications/service/delegates/SharedPreferencesNotificationsStore.java expo/modules/securestore/SecureStoreModule.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/amazon/a/a/o/b/a.java
10	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/amazon/a/a/o/b/a.java
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	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/mixpanel/android/mpmetrics/MPDbAdapter.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
13	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/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java
14	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/airbnb/lottie/network/NetworkCache.java expo/modules/filesystem/FileSystemModule.java
15	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

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	cl/json/RNSharePathUtil.java cl/json/ShareFile.java cl/json/ShareFiles.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/amazon/a/a/b/b.java com/canhub/cropper/Utils/GetUriForFileKt.java com/mrousavy/camera/CameraView_TakePhotoKt\$takePhoto\$2.java com/mrousavy/camera/CameraView_TakeSnapshotKt\$takeSnapshot\$2.java com/reactnativecompressor/Audio/AudioCompressor.java com/reactnativecompressor/Utils/CreateVideoThumbnailClass.java com/reactnativecompressor/Utils/Downloader.java expo/modules/filesystem/FileSystemModule.java expo/modules/image/ExpoImageModule.java expo/modules/imagepicker/exporters/RawImageExporter.java fr/greweb/reactnativeviewshot/RNViewShotModule.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

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/amazon/c/a/a/c.java com/bumptech/glide/disklruCache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/canhub/cropper/Utils/GetUriForFileKt.java com/github/penfeizhou/animation/apng/decode/APNGParser.java com/github/penfeizhou/animation/gif/decode/GifParser.java com/github/penfeizhou/animation/io/FileReader.java com/github/penfeizhou/animation/webp/decode/WebPParser.java com/naman14/androidlame/WaveReader.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecompressor/Video/VideoCompressor/Utils/StreamableVideo.java com/revenuecat/purchases/common/FileHelper.java expo/modules/core/logging/PersistentFileLog.java expo/modules/filesystem/FileSystemModule.java expo/modules/medialibrary/MediaLibraryUtils.java expo/modules/medialibrary/assets/CreateAsset.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/ReplayCache.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 javazoom/jl/converter/Converter.java javazoom/jl/player/advanced/jlap.java

RULE ID	BEHAVIOUR	LABEL	FILES
			javazoom/jl/player/jlp.java okio/Okio_JvmOkioKt.java
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java com/naman14/androidlame/WaveReader.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 javazoom/jl/converter/Converter.java javazoom/jl/player/advanced/jlap.java javazoom/jl/player/jlp.java
00091	Retrieve data from broadcast	collection	com/amazon/device/drm/a/d/c.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/a/c/b.java expo/modules/notifications/service/NotificationsService.java expo/modules/taskManager/TaskManagerUtils.java expo/modules/taskManager/TaskService.java
00046	Method reflection	reflection	org/aspectj/lang/Aspects14.java
00189	Get the content of a SMS message	sms	com/reactnativecompressor/Utils/RealPathUtil.java com/reactnativecompressor/Utils/Utils.java expo/modules/imagepicker/MediaHandler.java expo/modules/medialibrary/MediaLibraryUtils.java expo/modules/medialibrary/albums/migration/CheckIfAlbumShouldBeMigratedKt.java expo/modules/medialibrary/assets/AssetUtilsKt.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	com/reactnativecompressor/Utils/RealPathUtil.java com/reactnativecompressor/Utils/Utils.java expo/modules/imagepicker/MediaHandler.java expo/modules/medialibrary/MediaLibraryUtils.java expo/modules/medialibrary/albums/migration/CheckIfAlbumShouldBeMigratedKt.java expo/modules/medialibrary/assets/AssetUtilsKt.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLOGS)	sms callog collection	com/reactnativecompressor/Utils/RealPathUtil.java com/reactnativecompressor/Utils/Utils.java expo/modules/medialibrary/assets/AssetUtilsKt.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	com/reactnativecompressor/Utils/RealPathUtil.java com/reactnativecompressor/Utils/Utils.java expo/modules/medialibrary/assets/AssetUtilsKt.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	com/reactnativecompressor/Utils/RealPathUtil.java com/reactnativecompressor/Utils/Utils.java expo/modules/imagepicker/MediaHandler.java expo/modules/medialibrary/MediaLibraryUtils.java expo/modules/medialibrary/albums/migration/CheckIfAlbumShouldBeMigratedKt.java expo/modules/medialibrary/assets/AssetUtilsKt.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms callog calendar	expo/modules/medialibrary/MediaLibraryUtils.java expo/modules/medialibrary/albums/migration/CheckIfAlbumShouldBeMigratedKt.java expo/modules/medialibrary/assets/AssetUtilsKt.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00201	Query data from the call log	collection calllog	com/reactnativecompressor/Utils/RealPathUtil.java com/reactnativecompressor/Utils/Utils.java expo/modules/imagepicker/MediaHandler.java expo/modules/medialibrary/MediaLibraryUtils.java expo/modules/medialibrary/albums/migration/CheckIfAlbumShouldBeMigratedKt.java expo/modules/medialibrary/assets/AssetUtilsKt.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/reactnativecompressor/Utils/RealPathUtil.java expo/modules/imagepicker/MediaHandler.java expo/modules/medialibrary/MediaLibraryModule.java expo/modules/medialibrary/MediaLibraryUtils.java expo/modules/medialibrary/albums/migration/CheckIfAlbumShouldBeMigratedKt.java expo/modules/medialibrary/assets/AssetUtilsKt.java expo/modules/medialibrary/assets/GetAssets.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	app/notifee/core/Notifee.java cl/json/RNShareImpl.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/canhub/cropper/CropImageActivity.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/devmenu/devtools/DevMenuDevToolsDelegate.java expo/modules/filesystem/FileSystemModule.java expo/modules/imagepicker/contracts/CameraContract.java expo/modules/imagepicker/contracts/CropImageContract.java expo/modules/notifications/service/NotificationsService.java expo/modules/webbrowser/CustomTabsActivitiesHelperKt.java expo/modules/webbrowser/WebBrowserModule.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.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/notifee/core/Notifee.java cl/json/social/InstagramShare.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/webbrowser/CustomTabsActivitiesHelperKt.java expo/modules/webbrowser/WebBrowserModule.java n/o/t/i/f/e/e/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	app/notifee/core/Notifee.java cl/json/RNSharePathUtil.java com/amazon/a/a/i/g.java com/brentvatne/common/api/Source.java com/canhub/cropper/utils/GetUriForFileKt.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/av/player/MediaPlayerData.java expo/modules/devmenu/devtools/DevMenuDevToolsDelegate.java expo/modules/filesystem/FileSystemModule.java expo/modules/image/records/SourceMap.java expo/modules/notifications/service/NotificationsService.java io/invertase/firebase/common/SharedUtils.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java n/o/t/i/f/e/e/n.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/mrousavy/camera/utils/ImageProxy_saveKt.java com/reactnativecompressor/Image/ImageCompressor.java expo/modules/camera/next/tasks/ResolveTakenPicture.java expo/modules/camera/tasks/ResolveTakenPictureAsyncTask.java expo/modules/clipboard/ClipboardImageKt.java
00192	Get messages in the SMS inbox	sms	cl/json/RNSharePathUtil.java com/reactnativecompressor/Utils/RealPathUtil.java com/reactnativecompressor/Video/VideoCompressor/VideoCompressorClass.java
00175	Get notification manager and cancel notifications	notification	expo/modules/notifications/badge/BadgeHelper.java expo/modules/notifications/service/delegates/ExpoPresentationDelegate.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	cl/json/ShareFile.java cl/json/ShareFiles.java com/airbnb/lottie/LottieCompositionFactory.java expo/modules/filesystem/FileSystemModule.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/mixpanel/android/util/HttpService.java com/reactnativecompressor/Utils/Utils.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/transport/HttpConnection.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/mixpanel/android/util/HttpService.java com/reactnativecompressor/Utils/Utils.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/transport/HttpConnection.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java io/sentry/transport/HttpConnection.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/mixpanel/android/util/HttpService.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/transport/HttpConnection.java
00126	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	expo/modules/medialibrary/MediaLibraryUtils.java
00009	Put data in cursor to JSON object	file	com/amplitude/reactnative/LegacyDatabaseStorage.java com/mixpanel/android/mpmetrics/MPDbAdapter.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/amplitude/reactnative/AndroidContextProvider.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/mixpanel/android/mpmetrics/SystemInformation.java
00132	Query The ISO country code	telephony collection	com/amplitude/reactnative/AndroidContextProvider.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi 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
00080	Save recorded audio/video to a file	record file	expo/modules/av/AVManager.java
00101	Initialize recorder	record	expo/modules/av/AVManager.java
00121	Create a directory	file command	expo/modules/av/AVManager.java expo/modules/filesystem/FileSystemModule.java
00199	Stop recording and release recording resources	record	expo/modules/av/AVManager.java
00198	Initialize the recorder and start recording	record	expo/modules/av/AVManager.java
00136	Stop recording	record command	expo/modules/av/AVManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00194	Set the audio source (MIC) and recorded file format	record	expo/modules/av/AVManager.java
00090	Set recorded audio/video file format	record	expo/modules/av/AVManager.java
00197	Set the audio encoder and initialize the recorder	record	expo/modules/av/AVManager.java
00102	Set the phone speaker on	command	expo/modules/av/AVManager.java
00138	Set the audio source (MIC)	record	expo/modules/av/AVManager.java
00196	Set the recorded file format and output path	record file	expo/modules/av/AVManager.java
00133	Start recording	record command	expo/modules/av/AVManager.java
00104	Check if the given path is directory	file	expo/modules/av/AVManager.java expo/modules/filesystem/FileSystemModule.java
00041	Save recorded audio/video to file	record	expo/modules/av/AVManager.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00094	Connect to a URL and read data from it	command network	com/mixpanel/android/util/HttpService.java com/shopify/reactnative/skia/PlatformContext.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	com/mixpanel/android/util/HttpService.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	expo/modules/medialibrary/assets/CreateAsset.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java com/mixpanel/android/mpmetrics/MPDbAdapter.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java
00125	Check if the given file path exist	file	expo/modules/filesystem/FileSystemModule.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebase-remoteconfig.googleapis.com/v1/projects/578546397835/namespaces/firebase:fetch?key=AlzaSyAoRQ1RSDdNx2aSJazAdJZ6sria77HnqFA is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'test_multiplier': '2.5', 'test_showReviews': 'false', 'test_trial_days': '14'}, 'state': 'UPDATE', 'templateVersion': '6'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.CAMERA, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	6/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.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
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
pinterest.com	ok	IP: 151.101.128.84 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
expo.dev	ok	IP: 104.18.4.104 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
xml.org	ok	IP: 104.239.142.8 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: Google Map
plus.google.com	ok	IP: 64.233.185.113 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	IP: 172.253.124.102 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.w3.org	ok	IP: 104.18.23.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 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
twitter.com	ok	IP: 162.159.140.229 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.smp-te-ra.org	ok	IP: 52.20.185.129 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
react-native-vision-camera.com	ok	IP: 66.33.60.194 Country: Canada Region: Ontario City: Etobicoke Latitude: 43.623768 Longitude: -79.559723 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
notifee.app	ok	IP: 63.176.8.218 Country: United States of America Region: Virginia City: Reston Latitude: 38.925961 Longitude: -77.397331 View: Google Map

DOMAIN	STATUS	GEOLOCATION
docs.swmansion.com	ok	IP: 104.21.27.136 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.server.com	ok	IP: 172.67.196.208 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api.mixpanel.com	ok	IP: 107.178.240.159 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
rev.cat	ok	IP: 52.72.49.79 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api-diagnostics.revenuecat.com	ok	IP: 52.21.13.22 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
expo.fyi	ok	IP: 216.150.16.129 Country: Canada Region: Ontario City: Etobicoke Latitude: 43.623768 Longitude: -79.559723 View: Google Map
api-paywalls.revenuecat.com	ok	IP: 52.21.133.233 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
errors.rev.cat	ok	IP: 67.199.248.13 Country: United States of America Region: New York City: New York City Latitude: 40.739288 Longitude: -73.984955 View: Google Map

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	IP: 18.238.109.116 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
xmlpull.org	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
www.amazon.com	ok	IP: 23.222.206.109 Country: United States of America Region: Minnesota City: Minneapolis Latitude: 44.979969 Longitude: -93.263840 View: Google Map
www.facebook.com	ok	IP: 31.13.70.36 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map
www.shoutcastserver.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.javazoom.net	ok	No Geolocation information available.
api.revenuecat.com	ok	IP: 54.160.110.226 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 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

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

TRACKER	CATEGORIES	URL
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AlzaSyAoRQ1RSDdNx2aSJazAdjZ6sria77HnqFA"
"google_crash_reporting_api_key" : "AlzaSyAoRQ1RSDdNx2aSJazAdjZ6sria77HnqFA"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
9A04F079-9840-4286-AB92-E65BE0885F95

POSSIBLE SECRETS
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZlJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ae2044fb577e65ee8bb576ca48a2f06e
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMIM=
9a04f079-9840-4286-ab92-e65be0885f95
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
e2719d58-a985-b3c9-781a-b030af78d30e
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
01360240043788015936020505
115792089210356248762697446949407573530086143415290314195533631308867097853951

POSSIBLE SECRETS
A2B55680-6F43-11E0-9A3F-0002A5D5C51B
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
5181942b9ebc31ce68dacb56c16fd79f
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
1ddaa4b892e61b0f7010597ddc582ed3
24b2477514809255df232947ce7928c4
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Liftoff - Ranked Gym Workouts

Score: 4.7093596 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [com.gymbros.app](https://play.google.com/store/apps/details?id=com.gymbros.app)

Developer Details: GymBros Inc., GymBros+Inc., None, <https://getgymbros.com>, support@getgymbros.com,

Release Date: Apr 19, 2023 **Privacy Policy:** [Privacy link](#)

Description:

🏋️ Empower Your Fitness Journey with Liftoff 🏋️ Connect and Compete Join a vibrant community of fitness enthusiasts who make every workout count. Liftoff isn't just a fitness app, it's a social platform where you can connect, compete, and share your fitness journey with friends and like-minded gym-goers. - 🏆 Community Engagement: Dive into a fitness community that motivates and inspires. Follow friends, exchange tips, and celebrate each other's successes. - 🌐 Global Leaderboards: See how you stack up against the world. Participate in community challenges and climb the leaderboards by staying active and consistent. 📊 Track and Progress With Liftoff,

monitoring your fitness progress has never been easier or more enjoyable. Utilize advanced visualizations and get detailed insights into your workouts and overall fitness evolution.

- 📊 Comprehensive Tracking: Log workouts seamlessly, noting every exercise, set, and rep. Experience the joy of tracking with our intuitive interface.
- 📈 Progress Visualization: Watch your progress unfold with new charts and bodygraphs. Understand your strengths and areas for improvement at a glance.
- 🎁 Daily Deals and Rewards Stay motivated with daily deals and exclusive bundles available in the Liftoff Shop. Earn rewards by completing daily and weekly quests, adding a gamified layer to your fitness regime.
- 🥚 Earn and Spend: Collect eggs through workouts and challenges. Use them to unlock exciting rewards like new cosmetics, gear, and workout plans.
- 🎟 Exclusive Offers: Access daily deals and special bundles that make your fitness journey rewarding.

🔧 Customization at Your Fingertips Personalize your workout experience with custom exercises and adjustable presets. Tailor everything to fit your needs, from workout duration to intensity, ensuring a truly personalized fitness routine.

- 🏋️ Custom Exercises: Add your exercises, complete with custom images and descriptions, making your workouts truly yours.
- 🔄 Adaptive Workouts: Adjust presets and routines on the fly based on your current fitness level and goals.

👥 Engagement and Motivation Liftoff is designed to keep you engaged and motivated. With features like referral systems for new users and social media integrations, staying committed to your fitness goals is fun and social.

- 🎁 Referral Bonuses: Invite friends and earn rewards together. New users get bonus perks starting their fitness journey on Liftoff.
- 📱 Social Sharing: Share your workout posts stylishly with friends on other platforms, spreading motivation and healthy habits.

👤 Designed for All Whether you're a beginner or a seasoned athlete, Liftoff caters to all levels. With support for various types of exercise tracking—from weightlifting to cardio—every workout counts.

- 🧘 Inclusive Fitness: Track all types of workouts, including strength training, cardio sessions, and more.
- ♿ Accessibility Features: Enjoy a user-friendly interface with accessibility options to ensure everyone can join the Liftoff community.

🔄 Support and Updates Constantly evolving, Liftoff is committed to improving your experience with regular updates and quality of life enhancements. Our team is always ready to assist you in your fitness journey.

- 🔄 Regular Updates: Stay on top of the latest features and enhancements. We continually refine Liftoff based on user feedback and new trends in fitness.
- 🛠 Dedicated Support: Encounter an issue or have a suggestion? Our responsive support team and community on Discord are here to help you keep your workouts on track.

🚀 Join Liftoff Today Ready to elevate your fitness game? Download Liftoff now and transform the way you exercise. Become part of a community that's as passionate about fitness as you are!!

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-29 23:23:06	Generating Hashes	OK
2025-08-29 23:23:06	Extracting APK	OK
2025-08-29 23:23:06	Unzipping	OK

2025-08-29 23:23:07	Parsing APK with androguard	OK
2025-08-29 23:23:07	Extracting APK features using aapt/aapt2	OK
2025-08-29 23:23:07	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 23:23:10	Parsing AndroidManifest.xml	OK
2025-08-29 23:23:10	Extracting Manifest Data	OK
2025-08-29 23:23:10	Manifest Analysis Started	OK
2025-08-29 23:23:10	Performing Static Analysis on: Liftoff (com.gymbros.app)	OK
2025-08-29 23:23:11	Fetching Details from Play Store: com.gymbros.app	OK
2025-08-29 23:23:11	Checking for Malware Permissions	OK
2025-08-29 23:23:11	Fetching icon path	OK
2025-08-29 23:23:11	Library Binary Analysis Started	OK

2025-08-29 23:23:11	Reading Code Signing Certificate	OK
2025-08-29 23:23:13	Running APKID 2.1.5	OK
2025-08-29 23:23:21	Detecting Trackers	OK
2025-08-29 23:23:27	Decompiling APK to Java with JADX	OK
2025-08-29 23:23:57	Converting DEX to Smali	OK
2025-08-29 23:23:57	Code Analysis Started on - java_source	OK
2025-08-29 23:24:04	Android SBOM Analysis Completed	OK
2025-08-29 23:24:14	Android SAST Completed	OK
2025-08-29 23:24:14	Android API Analysis Started	OK
2025-08-29 23:24:24	Android API Analysis Completed	OK
2025-08-29 23:24:24	Android Permission Mapping Started	OK

2025-08-29 23:24:34	Android Permission Mapping Completed	OK
2025-08-29 23:24:36	Android Behaviour Analysis Started	OK
2025-08-29 23:24:45	Android Behaviour Analysis Completed	OK
2025-08-29 23:24:45	Extracting Emails and URLs from Source Code	OK
2025-08-29 23:24:49	Email and URL Extraction Completed	OK
2025-08-29 23:24:49	Extracting String data from APK	OK
2025-08-29 23:24:49	Extracting String data from Code	OK
2025-08-29 23:24:49	Extracting String values and entropies from Code	OK
2025-08-29 23:24:55	Performing Malware check on extracted domains	OK
2025-08-29 23:24:58	Saving to Database	OK

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](#).