

### ANDROID STATIC ANALYSIS REPORT



**#** Fig (4.92.1)

File Name:	com.fig_11803.apk
Package Name:	com.fig
Scan Date:	Aug. 29, 2025, 10:13 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	8/432

### FINDINGS SEVERITY

<b>≟</b> HIGH	▲ MEDIUM	i INFO	✓ SECURE	<b>◎</b> HOTSPOT
3	30	3	2	1

#### FILE INFORMATION

File Name: com.fig\_11803.apk

**Size:** 70.31MB

MD5: 34536202aed9309144cf7992fab1ffaf

**SHA1**: ccce2295a0810807c7002643f87c9abcd4954a55

**SHA256**: 04167380c69858ddffe3e848d82c6e6b194e0413686cb79f0a3c36f7922110da

# **i** APP INFORMATION

App Name: Fig

Package Name: com.fig

Main Activity: com.fig.MainActivity

Target SDK: 34 Min SDK: 26 Max SDK:

**Android Version Name:** 4.92.1

**Android Version Code: 11803** 

#### **APP COMPONENTS**

Activities: 20 Services: 17 Receivers: 20 Providers: 10

Exported Activities: 6 Exported Services: 2 Exported Receivers: 8 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: 2021-04-28 17:24:42+00:00 Valid To: 2051-04-28 17:24:42+00:00

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

Serial Number: 0xf2bcc43ed8198b8945b1f100c8196760f7d4090b

Hash Algorithm: sha256

md5: f02a62ab86468da686e1f063ba30d164

sha1: 37e4630a4eafe15a2b60d67d9c723b4a4724039a

sha256: 34deac6204409acaa57e0f9c423bc58e16156d8dcaf55fa287850d51a43c40e6

sha512: 0af6acee2c6981ed6fd484a8c8cb7d87247cec80fe36da0cd5b80b7500699176337c3921871f51362db169c44bcb4cee173b325de4f783326a7455f15ec4c725

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: baab19af20f8d68c7f655165830f7a15223790ae99500dd2387cdc03d371a577

Found 1 unique certificates

# **⋮** APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.android.vending.AD_ID	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.

PERMISSION STATUS INFO	D DESCRIPTION
------------------------	---------------

android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.fig.permission.C2D_MESSAGE	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.
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.
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
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.fig.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

# **M** APKID ANALYSIS

FILE	DETAILS		
	FINDINGS		DETAILS
34536202aed9309144cf7992fab1ffaf.apk	Anti-VM Code		possible VM check
	Obfuscator		Kiwi encrypter
	FINDINGS	DETA	ILS
classes.dex	Anti-VM Code	Build.M Build.M Build.P Build.H	INGERPRINT check  MODEL check  MANUFACTURER check  RODUCT check  IARDWARE check  e VM check
	Compiler	r8 with	out marker (suspicious)

FILE	DETAILS		
	FINDINGS	DETAILS	
classes2.dex	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes3.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check	
	Compiler	r8 without marker (suspicious)	

FILE	DETAILS		
	FINDINGS	DETAILS	
classes4.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check possible VM check	
	Anti Debug Code	Debug.isDebuggerConnected() check	
	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes5.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible VM check	
	Obfuscator	Kiwi encrypter	
	Compiler	r8 without marker (suspicious)	

FILE	DETAILS		
	FINDINGS	DETAILS	
classes6.dex	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 network operator name check ro.kernel.qemu check possible VM check	
	Compiler	r8 without marker (suspicious)	
classes7.dex	FINDINGS	DETAILS	
	Compiler	r8 without marker (suspicious)	

# BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.fig.MainActivity	Schemes: com.foodisgood.app://, branchfoodisgood://, https://, http://, Hosts: open, fig.app.link, fig.test-app.link, foodisgood.page.link, figapp.page.link, fig-react-dev.firebaseapp.com, ahara-react.firebaseapp.com,

ACTIVITY	INTENT
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.fig,

# **△** 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

# **Q** MANIFEST ANALYSIS

HIGH: 0 | WARNING: 18 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) 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.
3	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) 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 (com.onesignal.notifications.receivers.NotificationDismissReceiver) 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.
5	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) 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.
6	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) 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.
8	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) 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.
9	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.
10	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
11	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.
12	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
13	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
14	Activity (com.facebook.CustomTabActivity) 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
15	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.
16	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.

NO	ISSUE	SEVERITY	DESCRIPTION
17	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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.
18	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

# </> CODE ANALYSIS

HIGH: 2 | WARNING: 10 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/airbnb/android/react/lottie/LottieAnimati onViewPropertyManager.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.jav a

1				
NO	ISSUE	SEVERITY	STANDARDS	FILES va
				com/amazon/device/iap/internal/c/e.java
				com/amazon/device/simplesignin/BroadcastH
				andler.java
				com/amazon/device/simplesignin/SimpleSignI
				nService.java
				com/amazon/device/simplesignin/a/a/c/b.jav
				a
				com/amazon/device/simplesignin/a/c.java
				com/amazon/device/simplesignin/a/c/b.java
				com/brentvatne/react/ReactVideoView.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/ibits/react_native_in_app_review/AppRev
				iewModule.java
				com/imagepicker/ImageMetadata.java
				com/imagepicker/Metadata.java
				com/learnium/RNDeviceInfo/RNDeviceModul
				e.java
				com/learnium/RNDeviceInfo/RNInstallReferrer
				Client.java
				com/learnium/RNDeviceInfo/resolver/DeviceI
				dResolver.java
				com/mapbox/android/gestures/MultiFingerG
				esture.java
				com/mapbox/common/BaseMapboxInitializer
				.java
				com/mapbox/common/CoreInitializer.java
				com/mapbox/common/LifecycleMonitorAndr
				oid.java
				com/mapbox/common/LifecycleService.java
				com/mapbox/common/LifecycleUtils.java
				com/mapbox/common/LogBackend.java

NO	ISSUE	SEVERITY	STANDARDS	com/mapbox/common/Logger.java eam/mapbox/common/MapboxMapsAndroid Logger.java
				com/mapbox/common/MmeTelemetryProper
				ties.java
				com/mapbox/common/RunloopErrorHandler.
				java
				com/mapbox/common/SettingsServiceHelper. java
				com/mapbox/common/ValueUtilsKt.java
				com/mapbox/common/location/compat/per
				missions/PermissionsManager.java
				com/mapbox/common/logger/MapboxLogger .java
				com/mapbox/common/module/okhttp/Down loadGetCallback.java
				com/mapbox/common/module/okhttp/Netw
				orkUsageListener.java
				com/mapbox/common/module/provider/Ma
				pboxModuleProvider.java
				com/mapbox/maps/FontUtils.java
				com/mapbox/maps/extension/style/atmosph
				ere/generated/Atmosphere.java
				com/mapbox/maps/extension/style/layers/La
				yer.java
				com/mapbox/maps/extension/style/layers/ge
				nerated/BackgroundLayer.java
				com/mapbox/maps/extension/style/layers/ge
				nerated/CircleLayer.java
				com/mapbox/maps/extension/style/layers/ge
				nerated/FillExtrusionLayer.java
				com/mapbox/maps/extension/style/layers/ge
				nerated/FillLayer.java
				com/mapbox/maps/extension/style/layers/ge
				nerated/HeatmapLayer.java
				com/mapbox/maps/extension/style/layers/ge
				nerated/HillshadeLayer.java
				com/mapbox/maps/extension/style/layers/ge
				nerated/LineLayer.java
				com/mapbox/maps/extension/style/layers/ge
				nerated/LocationIndicatorLayer.java

	1			com/mapbox/maps/extension/style/layers/ge
NO	ISSUE	SEVERITY	STANDARDS	reratsd/ModelLayer.java
	·			com/mapbox/maps/extension/style/layers/ge
	1			nerated/RasterLayer.java
	l			com/mapbox/maps/extension/style/layers/ge
	l			nerated/SkyLayer.java
	l			com/mapbox/maps/extension/style/layers/ge
	l			nerated/SymbolLayer.java
	' 			com/mapbox/maps/extension/style/layers/pr
	' 			operties/PropertyValue.java
	' 			com/mapbox/maps/extension/style/light/gen
	' 			erated/Light.java
	' 			com/mapbox/maps/extension/style/sources/
	' 			Source.java
	' 			com/mapbox/maps/extension/style/sources/
	' 			generated/GeoJsonSource.java
	' 			com/mapbox/maps/extension/style/sources/
	' 			generated/ImageSource.java
	' 			com/mapbox/maps/extension/style/sources/
	' 			generated/RasterDemSource.java
	' 			com/mapbox/maps/extension/style/sources/
	' 			generated/RasterSource.java
	' 			com/mapbox/maps/extension/style/sources/
	' 			generated/VectorSource.java
	' 			com/mapbox/maps/extension/style/terrain/g
	' 			enerated/Terrain.java
	' 			com/mapbox/maps/extension/style/utils/Colo
	' 			rUtils.java
	' 			com/mapbox/maps/plugin/locationcompone
	' 			nt/ModelSourceWrapper.java
	' 			com/microsoft/codepush/react/CodePushUtil
	' 			s.java
	' 			com/mrousavy/camera/core/CameraSession.j
	' 			ava
	' 			com/mrousavy/camera/core/CameraSession_
	' 			ConfigurationKt.java
	' 			com/mrousavy/camera/core/CameraSession_
	l			FocusKt.java
	' 			com/mrousavy/camera/core/CameraSession_
	l			PhotoKt.java
	' 			com/mrousavy/camera/core/CameraSession_

				VideoKt.java
NO	ISSUE	SEVERITY	STANDARDS	Type Grousavy/camera/core/CodeScannerPip
				eline.java
				com/mrousavy/camera/core/MetadataProvid
				er.java
				com/mrousavy/camera/core/OrientationMan
				ager.java
				com/mrousavy/camera/core/extensions/Cam
				eraSelector_withExtensionKt.java
				com/mrousavy/camera/core/extensions/Imag
				eCapture_takePictureKt.java
				com/mrousavy/camera/core/types/PixelForm
				at.java
				com/mrousavy/camera/frameprocessors/Fra
				meProcessorPluginRegistry.java
				com/mrousavy/camera/frameprocessors/Visi
				onCameraProxy.java
				com/mrousavy/camera/react/CameraDevices
				Manager\$initialize\$1.java
				com/mrousavy/camera/react/CameraDevices
				Manager.java
				com/mrousavy/camera/react/CameraView\$u
				pdate\$1.java
				com/mrousavy/camera/react/CameraView.jav
				a
				com/mrousavy/camera/react/CameraViewMo
				dule.java
				com/mrousavy/camera/react/CameraView_Ev
				entsKt.java
				com/mrousavy/camera/react/CameraView_Ta
				kePhotoKt.java
				com/mrousavy/camera/react/CameraView_Ta
				keSnapshotKt.java
				com/onesignal/common/AndroidSupportV4C
				ompat.java
				com/onesignal/debug/internal/logging/Loggin
			CWE: CWE-532: Insertion of Sensitive	
1	The App logs information. Sensitive	info		g.java
1	information should never be logged.	info	Information into Log File	com/onesignal/notifications/internal/badges/i
			OWASP MASVS: MSTG-STORAGE-3	mpl/shortcutbadger/ShortcutBadger.java
				com/onesignal/rnonesignalandroid/RNOneSig
				nal.java

10	ICCLIE	CEVEDITY	CTANDADDC	com/proyecto26/inappbrowser/RNInAppBrow
NO	ISSUE	SEVERITY	STANDARDS	F4LJESa
				com/reactnativecommunity/asyncstorage/Asy
				ncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/Asy
				ncStorageExpoMigration.java
				com/reactnativecommunity/asyncstorage/Asy
				ncStorageModule.java com/reactnativecommunity/asyncstorage/Rea
				ctDatabaseSupplier.java
				com/reactnativecommunity/geolocation/Andr
				oidLocationManager.java
				com/reactnativecommunity/geolocation/PlayS
				ervicesLocationManager.java
				com/reactnativegooglesignin/PromiseWrappe
				r.java
				com/reactnativegooglesignin/RNGoogleSignin
				Module.java
				com/revenuecat/purchases/common/DefaultL
				ogHandler.java
				com/revenuecat/purchases/hybridcommon/C
				ommonKt.java
				com/revenuecat/purchases/hybridcommon/
				mappers/PurchasesPeriod.java
				com/revenuecat/purchases/react/RNPurchase
				sModule.java
				com/rnmapbox/rnmbx/components/mapvie
				w/RNMBXLifeCycle.java
				com/rnmapbox/rnmbx/components/styles/la
				yers/RNMBXLayer.java
				com/rnmapbox/rnmbx/components/styles/so
				urces/RNMBXImageSource.java
				com/rnmapbox/rnmbx/events/EventEmitter.j
				ava
				com/rnmapbox/rnmbx/location/LocationMan
				ager.java
				com/rnmapbox/rnmbx/modules/RNMBXLogg
				ing.java
				com/rnmapbox/rnmbx/modules/RNMBXOffli
				neModule.java
				com/rnmapbox/rnmbx/modules/RNMBXOffli

NO	ISSUE	SEVERITY	STANDARDS	neModuleLegacy.java Folk 5 mapbox/rnmbx/modules/RNMBXSnap shotModule.java
				com/rnmapbox/rnmbx/shapeAnimators/Shap eAnimatorCommon.java com/rnmapbox/rnmbx/utils/BitmapUtils.java com/rnmapbox/rnmbx/utils/ConvertUtils.java com/rnmapbox/rnmbx/utils/DownloadMapI mageTask\$downloadImage\$1\$1.java com/rnmapbox/rnmbx/utils/DownloadMapI mageTask.java com/rnmapbox/rnmbx/utils/DownloadMapI mageTask.java com/scandit/datacapture/core/C0579a5.java com/scandit/datacapture/core/C0579a5.java com/scandit/datacapture/core/C0638h1.java com/scandit/datacapture/core/J3.java com/scandit/datacapture/core/J6.java com/scandit/datacapture/core/N0.java com/scandit/datacapture/core/N0.java com/scandit/datacapture/core/extensions/a.ja va com/scandit/datacapture/core/extensions/a.ja va com/scandit/datacapture/core/internal/modul e/source/m.java com/scandit/datacapture/core/source/serializ ation/FrameSourceDeserializerHelperReverse dAdapter.java com/scandit/datacapture/frameworks/barcod e/count/BarcodeCountModule.java com/scandit/datacapture/frameworks/barcod e/find/data/BarcodeFindItemsData.java com/scandit/datacapture/frameworks/barcod e/find/data/BarcodeFindItemsData.java com/scandit/datacapture/frameworks/barcod e/tracking/utils/AdvancedOverlayViewPool.jav a com/scandit/datacapture/frameworks/core/ut ils/DefaultFrameworksLog.java com/scandit/datacapture/frameworks/core/ut ils/DefaultFrameworksLog.java com/segmentanalyticsreactnative/AnalyticsRe actNativeModule.java com/snapchat/djinni/NativeObjectManager.ja va

NO	ISSUE	SEVERITY	STANDARDS	com/sovranreactnative/Sovran.java  Folia Superwall/sdk/logger/Loggable.java  com/swmansion/gesturehandler/react/RNGes
				tureHandlerModule.java
				com/swmansion/gesturehandler/react/RNGes
				tureHandlerRootHelper.java
				com/swmansion/gesturehandler/react/RNGes
				tureHandlerRootView.java
				com/swmansion/reanimated/NativeMethods
				Helper.java
				com/swmansion/reanimated/ReanimatedMod
				ule.java
				com/swmansion/reanimated/ReanimatedUIM
				anagerFactory.java
				com/swmansion/reanimated/keyboard/Wind
				owsInsetsManager.java
				com/swmansion/reanimated/layoutReanimati
				on/AnimationsManager.java
				com/swmansion/reanimated/layoutReanimati
				on/ReanimatedNativeHierarchyManager.java
				com/swmansion/reanimated/layoutReanimati
				on/ScreensHelper.java
				com/swmansion/reanimated/layoutReanimati
				on/SharedTransitionManager.java
				com/swmansion/reanimated/layoutReanimati
				on/TabNavigatorObserver.java
				com/swmansion/reanimated/nativeProxy/Nat
				iveProxyCommon.java
				com/swmansion/reanimated/sensor/Reanima
				tedSensorContainer.java
				com/swmansion/rnscreens/ScreenStackHeade
				rConfigViewManager.java
				com/swmansion/rnscreens/ScreensModule.ja
				va
				com/swmansion/rnscreens/SearchBarManage
				r.java
				com/swmansion/rnscreens/utils/ScreenDum
				myLayoutHelper.java
				com/th3rdwave/safeareacontext/SafeAreaVie
				w.java
				com/zoontek/rnpermissions/RNPermissionsM

NO	ISSUE	SEVERITY	STANDARDS	odulelmpl.java  Fr/banalab/rnimageresizer/lmageResizer.java  fr/bamlab/rnimageresizer/lmageResizerModul
				org/greenrobot/eventbus/util/ErrorDialogMan ager.java org/greenrobot/eventbus/util/ExceptionToRes

NO	ISSUE	SEVERITY	STANDARDS	ourceMapping.java  FILES  org/threeten/bp/zone/TzdbZoneRulesCompile  r.java
2	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/onesignal/core/internal/database/impl/O SDatabase.java com/onesignal/session/internal/outcomes/im pl/OutcomeTableProvider.java com/reactnativecommunity/asyncstorage/Asy ncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/Rea ctDatabaseSupplier.java
3	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/RNAppleAuthentication/webview/SignIn WebViewDialogFragment.java com/onesignal/inAppMessages/internal/displ ay/impl/WebViewManager.java com/superwall/sdk/paywall/vc/web_view/SW WebView.java com/superwall/sdk/view/SWWebViewOld.java
4	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/inAppMessages/internal/displ ay/impl/WebViewManager.java com/superwall/sdk/view/SWWebViewOld.java
				com/RNAppleAuthentication/webview/SignIn WebViewDialogFragment.java com/mapbox/common/MmeTelemetryProper ties.java com/mapbox/common/location/GoogleLiveTr ackingClient.java com/mapbox/maps/ThreadChecker.java com/mapbox/maps/plugin/animation/MapAn imationOwnerRegistry.java com/mapbox/maps/plugin/annotation/genera ted/CircleAnnotation.java com/mapbox/maps/plugin/annotation/genera ted/CircleAnnotationOptions.java

NO	ISSUE	SEVERITY	STANDARDS	com/mapbox/maps/plugin/annotation/genera
				com/mapbox/maps/plugin/annotation/genera ted/PointAnnotationOptions.java com/mapbox/maps/plugin/annotation/genera ted/PolygonAnnotation.java com/mapbox/maps/plugin/annotation/genera ted/PolygonAnnotationOptions.java com/mapbox/maps/plugin/annotation/genera ted/PolylineAnnotation.java com/mapbox/maps/plugin/annotation/genera ted/PolylineAnnotationOptions.java com/mapbox/turf/TurfMisc.java com/microsoft/codepush/react/CodePushCon stants.java com/microsoft/codepush/react/CodePushTele metryManager.java com/nimbusds/jose/jwk/JWKParameterNames. java com/nimbusds/jose/jwk/JWKParameterName s.java com/onesignal/inAppMessages/internal/displ ay/impl/WebViewManager.java com/onesignal/inAppMessages/internal/prom pt/InAppMessagePromptTypes.java com/onesignal/inAppMessages/internal/prom pt/impl/InAppMessagePrompt.java com/onesignal/notifications/bridges/OneSign alHmsEventBridge.java com/onesignal/notifications/internal/Notificati on.java com/onesignal/notifications/internal/bundle/i mpl/NotificationBundleProcessor.java com/onesignal/notifications/internal/common /NotificationConstants.java com/onesignal/notifications/internal/common /NotificationHelper.java com/onesignal/notifications/internal/common /NotificationHelper.java com/onesignal/notifications/receivers/FCMBr oadcastReceiver.java com/revenuecat/purchases/amazon/Amazon

NO	ISSUE	SEVERITY	STANDARDS	BillingKt.java  Ght Svenuecat/purchases/amazon/AmazonC  acheKt.java
5	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/revenuecat/purchases/common/Backen dKt.java com/revenuecat/purchases/common/Backgro undAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnos tics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnos tics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnos tics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlinee ntitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verificat ion/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verificat ion/Signature.java com/revenuecat/purchases/common/verificat ion/SigningManager.java com/revenuecat/purchases/subscriberattribut es/SubscriberAttribute.java com/revenuecat/purchases/subscriberattribut es/SubscriberAttribute.java com/revenuecat/purchases/subscriberattribut es/SubscriberAttributeKt.java com/revenuecat/purchases/subscriberattributeKt.java com/revenuecat/purchases/subscriberattributeKt.java com/revenuecat/purchas

NO	ISSUE	SEVERITY	STANDARDS	e/find/data/BarcodeFindViewCreationData.jav <b>FILES</b>
				com/scandit/datacapture/frameworks/barcod
				e/pick/data/BarcodePickViewCreationData.jav
				a
				com/scandit/datacapture/frameworks/barcod
				e/spark/data/SparkScanViewCreationData.java
				com/scandit/datacapture/reactnative/barcode
				/ScanditDataCaptureBarcodeCaptureModule.j
				ava
				com/scandit/datacapture/reactnative/barcode
				/ScanditDataCaptureBarcodeModule.java
				com/scandit/datacapture/reactnative/barcode
				/ScanditDataCaptureBarcodeSelectionModule.
				java
				com/scandit/datacapture/reactnative/barcode
				/ScanditDataCaptureBarcodeTrackingModule.j
				ava
				com/scandit/datacapture/reactnative/barcode
				/ScanditDataCaptureSparkScanModule.java
				com/scandit/datacapture/reactnative/core/Sca
				nditDataCaptureCoreModule.java
				com/superwall/sdk/config/models/Survey.jav
				a
				com/superwall/sdk/debug/DebugViewActivity.
				java
				com/superwall/sdk/models/config/RawFeatur
				eFlag.java
				com/superwall/sdk/models/paywall/Paywall.j
				ava
				com/superwall/sdk/models/triggers/TriggerRu
				leOccurrence.java
				com/superwall/sdk/paywall/presentation/Pay
				wallInfo.java
				com/superwall/sdk/paywall/vc/SuperwallPay
				wallActivity.java
				com/superwall/sdk/storage/core_data/entities
				/ManagedTriggerRuleOccurrence.java
				io/branch/referral/Branch.java
				io/branch/referral/BranchPreinstall.java
				1

NO	ISSUE	SEVERITY	STANDARDS	io/branch/referral/PrefHelper.java <b>FolioEs</b> nch/referral/ServerRequest.java  io/branch/referral/ServerRequestQueue.java
				io/branch/referral/UniversalResourceAnalyser .java io/branch/referral/validators/DeepLinkRoutin gValidator.java io/grpc/PersistentHashArrayMappedTrie.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/TransportFrameUtil.java io/invertase/firebase/common/TaskExecutorS ervice.java io/sentry/Baggage.java io/sentry/RequestDetailsResolver.java io/sentry/SpanDataConvention.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/sentry/TraceContext.java com/amazon/device/drm/LicensingService.jav io/sentry/protocol/Oser.java a com/amazon/device/iap/PurchasingService.ja va com/nimbusds/jose/jwk/Curve.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.java
7	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 com/onesignal/common/AndroidUtils.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/OutlierDetectionLoadBalancer.jav a io/grpc/util/RoundRobinLoadBalancer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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.jav a com/superwall/sdk/storage/CacheKeysKt.java
9	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 com/revenuecat/purchases/common/UtilsKt.j ava com/scandit/datacapture/core/N6.java io/sentry/util/StringUtils.java
10	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/learnium/RNDeviceInfo/RNDeviceModul e.java io/invertase/firebase/utils/ReactNativeFirebas eUtilsModule.java io/sentry/android/core/DeviceInfoUtil.java
11	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/RootChec ker.java
12	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/mrousavy/camera/core/utils/OutputFile.j ava com/rnmapbox/rnmbx/components/mapvie w/RNMBXMapView.java com/rnmapbox/rnmbx/utils/BitmapUtils.java io/sentry/react/RNSentryModuleImpl.java
13	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 com/scandit/datacapture/core/S4.java io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.ja va

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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/impl/AESCBC.java com/nimbusds/jose/jca/JCASupport.java
15	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/branch/referral/ShareLinkManager.java
16	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/RootChec ker.java

# ■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

# **BEHAVIOUR ANALYSIS**

RULE ID	BEHAVIOUR	LABEL	FILES
------------	-----------	-------	-------

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java com/mapbox/maps/module/telemetry/PhoneState.java com/onesignal/common/DeviceUtils.java io/branch/referral/SystemObserver.java
00183	Get current camera parameters and change the setting.	camera	com/scandit/datacapture/core/C0771w.java
00022	Open a file from given absolute path of the file	file	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/mapbox/common/Corelnitializer.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/microsoft/codepush/react/FileUtils.java com/microsoft/codepush/react/FileUtils.java com/mrousavy/camera/core/utils/OutputFile.java com/mrousavy/camera/react/CameraView_TakeSnapshotKt.java com/mrousavy/camera/react/CameraView_TakeSnapshotKt.java com/oblador/vectoricons/VectorlconsModule.java com/oblador/vectoricons/VectorlonsModule.java com/rnmapbox/rnmbx/modules/RNMBXOfflineModuleLegacy.java com/scandit/datacapture/core/AbstractC0590b7.java com/scandit/datacapture/core/B3.java com/scandit/datacapture/core/I3.java com/scandit/datacapture/core/M3.java com/scandit/datacapture/core/M3.java com/scandit/datacapture/core/framesave/BurstFrameSaveSession.java com/scandit/datacapture/core/framesave/BurstFrameSaveSession.java com/scandit/datacapture/core/framesave/CameraSequenceFrameSaveSession.java com/scandit/datacapture/core/framesave/CameraSequenceFrameSaveSession.java fr/bamlab/rnimageresizer/ImageResizer.java fr/bamlab/rnimageresizer/ImageResizer.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/DirectoryProcessor.java

RULE ID	BEHAVIOUR	LABEL	io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java FILES 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/microsoft/codepush/react/CodePushUpdateUtils.java com/microsoft/codepush/react/FileUtils.java io/grpc/util/AdvancedTlsxSo9TextManager.java io/grpc/util/AdvancedTlsxSo9TrustManager.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/PreviousSessionFinalizer.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/instrumentation/file/FileInputStreamInitData.java io/sentry/til/FileUtils.java ois/sentry/til/FileUtils.java ois/sentry/til/FileUtils.java ois/sentry/til/FileUtils.java ois/sentry/til/FileUtils.java okio/OkiolvmOkioKt.java org/threeten/bp/chrono/HijrahDate.java

RULE ID	BEHAVIOUR LABEL		FILES	
00012	Read data and put it into a buffer stream		com/amazon/c/a/a/c.java 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	
00189	Get the content of a SMS message sms		com/imagepicker/Utils.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java	
00188	Get the address of a SMS message sms		com/imagepicker/Utils.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java	
00200	Query data from the contact list collection contact		com/imagepicker/Utils.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java	
00201	Query data from the call log collection calllog co		com/imagepicker/Utils.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java	
00077	Read sensitive data(SMS, CALLLOG, etc) collection sms calllog calendar		com/imagepicker/Utils.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java	

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/amazon/device/iap/internal/a/a.java com/mapbox/maps/plugin/attribution/AttributionDialogManagerImpl.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/NavigateToAndroidSettingsForLocatio n.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHom eBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHome Badger.java com/onesignal/
00147	Get the time of current location collection location		com/reactnativecommunity/geolocation/AndroidLocationManager.java com/reactnativecommunity/geolocation/PlayServicesLocationManager.java
00075	Get location of the device collection location		com/reactnativecommunity/geolocation/AndroidLocationManager.java

RULE ID	BEHAVIOUR	LABEL	FILES	
00036	Get resource file from res/raw directory	reflection	com/amazon/a/a/i/g.java com/mapbox/maps/plugin/MapAttributionDelegateImpl.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/NavigateToAndroidSettingsForLocatio n.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/Everything MeHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/HuaweiHo meBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/NovaHome Badger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHom eBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHome Badger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHome Badger.java com/onesignal/notifications/internal/common/NotificationHelper.java com/onesignal/notifications/internal/common/NotificationHelper.java com/onesignal/notifications/internal/common/NotificationHelper.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/rnmapbox/rnmbx/utils/DownloadMapImageTask.java com/zoontek/rnpermissions/RNPermissionsModuleImpl.java io/branch/referral/Branch.java io/invertase/firebase/common/SharedUtils.java	
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/CodePushUpdateManager.java fr/bamlab/rnimageresizer/ImageResizer.java	
00089	Connect to a URL and receive input stream from the server		com/microsoft/codepush/react/CodePushUpdateManager.java com/nimbusds/jose/util/DefaultResourceRetriever.java com/revenuecat/purchases/common/HTTPClient.java com/superwall/sdk/network/RequestExecutor.java fr/bamlab/rnimageresizer/ImageResizer.java io/sentry/transport/HttpConnection.java	

RULE ID	BEHAVIOUR LABEL		FILES	
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/revenuecat/purchases/common/HTTPClient.java com/superwall/sdk/network/RequestExecutor.java io/sentry/transport/HttpConnection.java	
00030	Connect to the remote server through the given URL network		com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java fr/bamlab/rnimageresizer/ImageResizer.java io/sentry/transport/HttpConnection.java	
00011	Query data from URI (SMS, CALLLOGS)  sms calllog collection		com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java	
00191	Get messages in the SMS inbox	sms	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java io/branch/coroutines/InstallReferrersKt.java	
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungH omeBadger.java	
00162	Create InetSocketAddress object and connecting to it	socket	io/grpc/okhttp/internal/Platform.java	
00163	Create new Socket and connecting to it socket		io/grpc/okhttp/internal/Platform.java	
00091	091 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 com/onesignal/core/activities/PermissionsActivity.java com/onesignal/notifications/internal/common/NotificationFormatHelper.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java io/branch/referral/Branch.java	

RULE ID	BEHAVIOUR LABEL		FILES	
00034	Query the current data network type	collection network	com/mapbox/common/TelemetrySystemUtils.java	
00109	Connect to a URL and get the response code network command		com/nimbusds/jose/util/DefaultResourceRetriever.java com/revenuecat/purchases/common/HTTPClient.java com/superwall/sdk/network/RequestExecutor.java io/sentry/transport/HttpConnection.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 com/rnmapbox/rnmbx/modules/RNMBXOfflineModule.java	
00003	Put the compressed bitmap data into JSON object camera		io/branch/referral/network/BranchRemoteInterfaceUrlConnection.java	
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object		com/scandit/datacapture/core/internal/sdk/extensions/BitmapExtensionsKt.java fr/bamlab/rnimageresizer/ImageResizer.java	
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/mapbox/maps/plugin/attribution/AttributionDialogManagerImpl.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/NavigateToAndroidSettingsForLocatio n.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/zoontek/rnpermissions/RNPermissionsModuleImpl.java io/branch/referral/Branch.java io/branch/rnbranch/RNBranchModule.java	
00004	Get filename and put it to JSON object file collection		com/airbnb/lottie/LottieCompositionFactory.java com/rnmapbox/rnmbx/modules/RNMBXOfflineModule.java	
00062	Query WiFi information and WiFi Mac Address wifi collection		com/learnium/RNDeviceInfo/RNDeviceModule.java	

RULE ID	BEHAVIOUR	LABEL	FILES	
00038	Query the phone number	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	
00092	Send broadcast	command	io/branch/rnbranch/RNBranchModule.java	
00177	Check if permission is granted and request it	permission com/onesignal/common/AndroidSupportV4Compat.java		
00029	Initialize class object dynamically	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java	
00157	Instantiate new object using reflection, possibly used for dexClassLoader		com/mapbox/common/module/provider/MapboxModuleProvider.java	
00046	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java	
00026	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java	
00024	Write file after Base64 decoding reflection file		com/airbnb/lottie/LottieCompositionFactory.java fr/bamlab/rnimageresizer/ImageResizer.java	
00009	Put data in cursor to JSON object file		com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java	
00094	Connect to a URL and read data from it	command network	fr/bamlab/rnimageresizer/lmageResizer.java	

RULE ID	BEHAVIOUR LABEL		FILES	
00108	Read the input stream from given URL network command		fr/bamlab/rnimageresizer/ImageResizer.java	
00031	Check the list of currently running applications	reflection collection	com/mapbox/common/LifecycleUtils.java	
00043	Calculate WiFi signal strength collection wifi		com/reactnativecommunity/netinfo/ConnectivityReceiver.java	
00115	Get last known location of the device collection location		com/mrousavy/camera/core/MetadataProvider.java	

# FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://ahara-react.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/606858370097/namespaces/firebase.fetch? key=AlzaSyAnAwAgCxbFQzaUxgkssnfwNAFxkoBhZlU is enabled. Ensure that the configurations are not sensitive. This is indicated by the responses: {'entries': ('androidMinSupportedVersion': '4.3.0', 'disableIngredientLoadingScreen': 'false', 'enableAnonymousSignup': 'true', 'enableDemoinOnboarding': 'true', 'enableBeforceryFeed': 'false', 'enableGroceryWhatsNew': 'false', 'enableGoidedTour': 'false', 'enableHowDidYouHearAboutFig': 'true', 'enableIngredientNotifications: 'false', 'enableProfileGreationBeforceryWhatsNew': 'false', 'enableBonboardingPaywallRedesignDemoi': 'false', 'enableProfileGreationBeforeati

## **SECOND SECOND PERMISSIONS**

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.INTERNET, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

#### **Malware Permissions:**

Top permissions that are widely abused by known malware.

#### **Other Common Permissions:**

Permissions that are commonly abused by known malware.

## • OFAC SANCTIONED COUNTRIES

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

DOMAIN COUNTRY/REGION
-----------------------

## **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
config.mapbox.com	ok	IP: 44.228.251.40 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
api.mapbox.com	ok	IP: 18.238.109.16 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
help.branch.io	ok	IP: 104.18.21.218 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
appleid.apple.com	ok	IP: 17.111.105.242 Country: United States of America Region: California City: Cupertino Latitude: 37.316605 Longitude: -122.046486 View: Google Map
codepush.appcenter.ms	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ahara-react.firebaseio.com	ok	IP: 34.120.160.131 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
play.google.com	ok	IP: 172.253.124.101 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
api-events-config-staging.tilestream.net	ok	IP: 44.206.17.171 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
github.com	ok	IP: 140.82.114.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
cloudfront-staging.tilestream.net	ok	IP: 18.155.173.110 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 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
api-events-staging.tilestream.net	ok	IP: 35.164.22.88 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
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

DOMAIN	STATUS	GEOLOCATION
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
branch.app.link	ok	IP: 18.238.109.80 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
docs.mapbox.com	ok	IP: 18.238.96.51 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
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

DOMAIN	STATUS	GEOLOCATION
api3-eu.branch.io	ok	IP: 18.155.173.118  Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
superwall.com	ok	IP: 172.67.74.93 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api.branch.io	ok	IP: 18.238.109.24 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
bnc.lt	ok	IP: 18.238.109.60 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api-diagnostics.revenuecat.com	ok	IP: 3.226.164.55 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
cdn.branch.io	ok	IP: 18.238.109.80 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
api.onesignal.com	ok	IP: 104.16.160.145 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api-paywalls.revenuecat.com	ok	IP: 54.158.163.245 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
events.mapbox.com	ok	IP: 44.241.67.103  Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
errors.rev.cat	ok	IP: 67.199.248.12 Country: United States of America Region: New York City: New York City Latitude: 40.739288 Longitude: -73.984955 View: Google Map
docs.revenuecat.com	ok	IP: 18.238.109.13 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
apps.mapbox.com	ok	IP: 18.238.109.101 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	IP: 142.250.9.138  Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
api2.branch.io	ok	IP: 18.238.109.69 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.amazon.com	ok	IP: 18.155.172.176 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
api.revenuecat.com	ok	IP: 3.226.164.55 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map



EMAIL	FILE
support@scandit.com	com/scandit/datacapture/core/extensions/a.java

## **A** TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193
Scandit	Analytics	https://reports.exodus-privacy.eu.org/trackers/84
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447



POSSIBLE SECRETS
"CodePushDeploymentKey" : "dont_set_here_set_in_app_code"
"facebook_client_token" : "b5718bf1952aa7bf85951a5a85c3167d"
"firebase_database_url" : "https://ahara-react.firebaseio.com"
"google_api_key" : "AlzaSyAnAwAgCxbFQzaUxgkssnfwNAFxkoBhZIU"
"google_crash_reporting_api_key" : "AlzaSyAnAwAgCxbFQzaUxgkssnfwNAFxkoBhZIU"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
115792089237316195423570985008687907853269984665640564039457584007908834671663
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057151
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
41058363725152142129326129780047268409114441015993725554835256314039467401291
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
32670510020758816978083085130507043184471273380659243275938904335757337482424

#### **POSSIBLE SECRETS**

c56fb7d591ba6704df047fd98f535372fea00211

68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057148

 $10938490380737342745111123907668055699362075989516837489945863944959531161507350160137087375737596232485921322967063133094384525315910\\12912142327488478985984$ 

UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=

39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

55066263022277343669578718895168534326250603453777594175500187360389116729240

48439561293906451759052585252797914202762949526041747995844080717082404635286

9b8f518b086098de3d77736f9458a3d2f6f95a37

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

37571800257700204635455072244911836035944551347697624866945677796155444774405563166912344050129455395621444445372894285225856667291965

POSSIBLE SECRETS
c682b8144a8dd52bc1ad63
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
115792089237316195423570985008687907852837564279074904382605163141518161494337
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
11f00dc53be30cfe213781d453297cf1
115792089210356248762697446949407573530086143415290314195533631308867097853951
ee4655b3ec0d2ace448aa481008538b7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
26617408020502170632287687167233609607298591687569731477066713684188029449964278084915450806277719023520942412250655586621571135455709 16814161637315895999846
cc2751449a350f668590264ed76692694a80308a
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb

#### POSSIBLE SECRETS

68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403 80340372808892707005449

115792089210356248762697446949407573530086143415290314195533631308867097853948

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871

26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087

36134250956749795798585127919587881956611106672985015071877198253568414405109

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

115792089210356248762697446949407573529996955224135760342422259061068512044369



### > PLAYSTORE INFORMATION

Title: Fig: Food Scanner & Discovery

Score: 4.5576925 Installs: 500,000+ Price: 0 Android Version Support: Category: Health & Fitness Play Store URL: com.fig

Developer Details: Fig - Food Is Good, Fig+-+Food+Is+Good, None, https://foodisgood.com, support@foodisgood.com,

Release Date: Nov 30, 2021 Privacy Policy: Privacy link

#### **Description:**

With 1M+ satisfied members, Fig is the only app that supports EVERY dietary restriction and allergy, helping you find food you CAN eat and avoid reactions. Whether you have food allergies or follow a specialized diet like Low FODMAP, Gluten-Free, Vegan, Low Histamine, Alpha-Gal, or any of our 2,800+ other options, Fig empowers you to navigate grocery aisles and restaurants with confidence and reclaim your love for food. No more second-guessing or tedious label reading—simply scan, discover, and enjoy a wide range of foods that align with your specific dietary needs and help you hit your nutrition goals. CUSTOMER REVIEWS "This app is an ABSOLUTE GODSEND

and I cannot recommend it enough. It works amazingly, is so easy to use, scans things super quickly and allows you to put in so many different things (I've got allergies, intolerances, and OAS [yay me, right!])" -Karina C. ["Fig has changed my life. Being able to easily scan labels and quickly see if a product is safe for me to eat has been a game changer. I used to cry almost every time I went to the store. My eyesight is terrible, so reading labels is difficult. Now I can get in and out easily. Thank you!!" -Allegra K. | "I have never felt more liberated, supported, seen and represented by an app and its founders. I am better able to manage my allergies and food intolerances through Fig and it has made an immense impact in my everyday life." -Rachel S. "Food allergies had turned grocery shopping into a nightmare for me. I was having so much trouble finding foods that I could eat that I started having panic attacks. A friend told me about the Fig app & I immediately downloaded it. My life changed again, only this time for the better! Wow, not only was I able to find new foods to eat, but I also discovered many foods that I thought were okay-weren't. My health improved. I'm so thankful for Fig. -Raella T. [] "Finally, an app that understands the needs of families with dietary restrictions. The Multiple Figs feature is a game-changer for managing my kids' allergies. Thank you, Fig!" - Jason M. 🛮 KEY FEATURES 🖰 - Check if a product's ingredients are compatible with your diet in under a second using the barcode scanner -Discover a comprehensive list of foods that work for you at 100+ grocery stores and restaurants. -Learn about ingredients and follow complex diets with confidence. -Make a profile for everyone you care about and find food that works for everyone at once. -Create shopping lists and save hours at the grocery store. I Fig goes beyond basic ingredient analysis. Our powerful technology is powered by millions of ingredient ratings and notes from our team of 11+ expert dietitians, to help you find what you CAN eat at grocery stores and restaurants. No matter how unique your dietary needs are, Fig has got you covered. ☐ Join the Fig Movement ☐ Our small team consists of individuals with dietary restrictions, just like you. We understand the struggles and challenges you face, and we're committed to continually improving Fig to meet your evolving needs and fighting for causes that matter to us. Together, we're building the app we've all dreamed of and fostering a community where you feel represented and welcomed. Download Fig Today! Save yourself from the pain of reading every label, researching every ingredient, and wasting money on products you can't actually eat. Start using Fig and experience the joy of finding food that makes you feel your best. We respect your privacy. For more information, please read our privacy policy at http://foodisgood.com/privacy. By using Fig, you agree to our terms of service. Read them at http://foodisgood.com/terms-of-service. Fig is free to download and use. However, we offer an additional subscription (Fig+) that unlocks additional features, including Restaurants, Multiple Figs, Unlimited Scans and more. Want something added to the app? Email support@foodisgood.com and we'll be happy to help you!

### **∷** SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:13:23	Generating Hashes	ОК
2025-08-29 22:13:24	Extracting APK	ОК
2025-08-29 22:13:24	Unzipping	ОК

2025-08-29 22:13:24	Parsing APK with androguard	ОК
2025-08-29 22:13:24	Extracting APK features using aapt/aapt2	ОК
2025-08-29 22:13:24	Getting Hardcoded Certificates/Keystores	ОК
2025-08-29 22:13:26	Parsing AndroidManifest.xml	ОК
2025-08-29 22:13:26	Extracting Manifest Data	ОК
2025-08-29 22:13:26	Manifest Analysis Started	ОК
2025-08-29 22:13:27	Performing Static Analysis on: Fig (com.fig)	ОК
2025-08-29 22:13:28	Fetching Details from Play Store: com.fig	ОК
2025-08-29 22:13:29	Checking for Malware Permissions	ОК
2025-08-29 22:13:29	Fetching icon path	ОК

2025-08-29 22:13:29	Library Binary Analysis Started	ОК
2025-08-29 22:13:29	Reading Code Signing Certificate	OK
2025-08-29 22:13:30	Running APKiD 2.1.5	ОК
2025-08-29 22:13:39	Detecting Trackers	ОК
2025-08-29 22:13:47	Decompiling APK to Java with JADX	ОК
2025-08-29 22:14:19	Converting DEX to Smali	ОК
2025-08-29 22:14:19	Code Analysis Started on - java_source	ОК
2025-08-29 22:14:26	Android SBOM Analysis Completed	ОК
2025-08-29 22:14:40	Android SAST Completed	ОК
2025-08-29 22:14:40	Android API Analysis Started	ОК
2025-08-29 22:14:53	Android API Analysis Completed	ОК

2025-08-29 22:14:54	Android Permission Mapping Started	ОК
2025-08-29 22:15:06	Android Permission Mapping Completed	ОК
2025-08-29 22:15:07	Android Behaviour Analysis Started	ОК
2025-08-29 22:15:23	Android Behaviour Analysis Completed	ОК
2025-08-29 22:15:23	Extracting Emails and URLs from Source Code	ОК
2025-08-29 22:15:31	Email and URL Extraction Completed	ОК
2025-08-29 22:15:31	Extracting String data from APK	ОК
2025-08-29 22:15:31	Extracting String data from Code	ОК
2025-08-29 22:15:31	Extracting String values and entropies from Code	ОК
2025-08-29 22:15:40	Performing Malware check on extracted domains	ОК
2025-08-29 22:15:42	Saving to Database	ОК

### Report Generated by - MobSF v4.4.0

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

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