MOBSF

ANDROID STATIC ANALYSIS REPORT

MyGEHA (1.0.0)

File Name:	com.bob.geha_9.apk
Package Name:	com.bob.geha
Scan Date:	Aug. 29, 2025, 8:26 p.m.
App Security Score:	57/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	16	2	3	1

FILE INFORMATION

File Name: com.bob.geha_9.apk
Size: 15.09MB
MD5: 8bae9e8cc73544036459d0fc66406b5c
SHA1: d056d45d9f782a72d24aa2f75919a0291208a759
SHA256: c3155da50519c0e9b37b0bad66b293ce217a433f6271a74595c1a179a0212bb6

APP INFORMATION

App Name: MyGEHA
Package Name: com.bob.geha

Main Activity: com.apmobileapp.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 9

APP COMPONENTS

Activities: 8
Services: 8
Receivers: 4
Providers: 10
Exported Activities: 1
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
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: 2024-11-22 15:29:55+00:00
Valid To: 2054-11-22 15:29:55+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x9dfca01ef76916c0ab30f25f9fba6b7fa4172e61
Hash Algorithm: sha256
md5: 503fda880acad7343041c5cf287b0fbf
sha1: 7768d18b43561148dfeedc3350f2ffffb5e5b40b
sha256: 41fcf7dddf6aa2471ab77df0cf02d8ee06a960030a23e1f092837dc1c2cb69c7
sha512: b4a33f8fee098ebae90e893ea50f6ff661943b5f50876588f57edd17b18ef967ca142433a5fc4e55c0c53aed517b7fb7e6a0bdb137f1d2e00dc1d9bb7b1e01d2
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 49f20b635e020ac9a3e42caac2efb90e10f490d8f94dfba156c3ce17ba8521a8
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.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.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
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.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.bob.geha.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
8bae9e8cc73544036459d0fc66406b5c.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.apmobileapp.MainActivity	Schemes: http://, @string/hsidPrefix://, Hosts: umr.app,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	umr.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	App Link assetlinks.json file not found [android:name=com.apmobileapp.MainActivity] [android:host=http://umr.app]	high	App Link asset verification URL (http://umr.app/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). 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.
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.
5	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.
6	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.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/adobe/marketing/mobile/reactnative/target/RCTACPTargetModule.java com/apmobileapp/BuildConfig.java com/appmattus/certificatetransparency/internal/loglist/model/v3/Log.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/image/records/SourceMap.java expo/modules/webbrowser/OpenBrowserOptions.java io/invertase/firebase/common/TaskExecutorService.java l5/g.java p2/e.java sb/b.java tb/e.java tb/w.java tc/b.java u2/g.java w2/d.java w2/p.java w2/x.java
				a3/c.java a3/d.java a3/g.java a3/s.java a3/t.java a3/u.java ab/i.java b0/c.java b1/a.java c1/l0.java c3/a.java c8/a.java cg/i.java com/adobe/marketing/mobile/AbstractHitsDatabase.java com/adobe/marketing/mobile/Analytics.java com/adobe/marketing/mobile/AnalyticsDispatcherAnalyticsResponseContent.java com/adobe/marketing/mobile/AnalyticsDispatcherAnalyticsResponseIdentity.java com/adobe/marketing/mobile/AnalyticsExtension.java com/adobe/marketing/mobile/AnalyticsHitsDatabase.java com/adobe/marketing/mobile/AnalyticsListenerAcquisitionResponseContent.java com/adobe/marketing/mobile/AnalyticsListenerAnalyticsRequestContent.java com/adobe/marketing/mobile/AnalyticsListenerAnalyticsRequestIdentity.java com/adobe/marketing/mobile/AnalyticsListenerConfigurationResponseContent.java com/adobe/marketing/mobile/AnalyticsListenerGenericRequestReset.java com/adobe/marketing/mobile/AnalyticsListenerGenericTrackRequestContent.java com/adobe/marketing/mobile/AnalyticsListenerHubBooted.java com/adobe/marketing/mobile/AnalyticsListenerHubSharedState.java com/adobe/marketing/mobile/AnalyticsListenerLifecycleRequestContent.java com/adobe/marketing/mobile/AnalyticsListenerLifecycleResponseContent.java com/adobe/marketing/mobile/AnalyticsListenerRulesEngineResponseContent.java com/adobe/marketing/mobile/AnalyticsState.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/AndroidDatabase.java com/adobe/marketing/mobile/AndroidEventHistoryDatabase.java com/adobe/marketing/mobile/AndroidLoggingService.java com/adobe/marketing/mobile/AndroidNetworkServiceOverrider.java com/adobe/marketing/mobile/AssuranceConnectionStatusUI.java com/adobe/marketing/mobile/AssuranceExtension.java com/adobe/marketing/mobile/AssuranceFloatingButton.java com/adobe/marketing/mobile/AssuranceFullScreenTakeover.java com/adobe/marketing/mobile/AssurancePinCodeEntryURLProvider.java com/adobe/marketing/mobile/AssuranceSession.java com/adobe/marketing/mobile/AssuranceWebViewSocket.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/CacheManager.java com/adobe/marketing/mobile/ConfigurationDownloader.java com/adobe/marketing/mobile/ConfigurationExtension.java com/adobe/marketing/mobile/Core.java com/adobe/marketing/mobile/DataMarshaller.java com/adobe/marketing/mobile/DispatcherAnalyticsRequestContentIdentity.java com/adobe/marketing/mobile/DispatcherConfigurationRequestContentIdentity.java com/adobe/marketing/mobile/DispatcherIdentityResponseIdentityIdentity.java com/adobe/marketing/mobile/EventBus.java com/adobe/marketing/mobile/EventHub.java com/adobe/marketing/mobile/ExtensionApi.java com/adobe/marketing/mobile/HitQueue.java com/adobe/marketing/mobile/Identity.java com/adobe/marketing/mobile/IdentityCore.java com/adobe/marketing/mobile/IdentityExtension.java com/adobe/marketing/mobile/IdentityHitSchema.java com/adobe/marketing/mobile/IdentityHitsDatabase.java com/adobe/marketing/mobile/LifecycleCore.java com/adobe/marketing/mobile/LifecycleExtension.java com/adobe/marketing/mobile/LifecycleMetricsBuilder.java com/adobe/marketing/mobile/LifecycleSession.java com/adobe/marketing/mobile/LifecycleV2DataStoreCache.java com/adobe/marketing/mobile/LifecycleV2DispatcherApplicationState.java com/adobe/marketing/mobile/LifecycleV2StateManager.java com/adobe/marketing/mobile/Matcher.java com/adobe/marketing/mobile/MobileCore.java com/adobe/marketing/mobile/MobileIdentities.java com/adobe/marketing/mobile/PersistentProfileData.java com/adobe/marketing/mobile/RuleConditionHistorical.java com/adobe/marketing/mobile/RulesEngine.java com/adobe/marketing/mobile/RulesRemoteDownloader.java com/adobe/marketing/mobile/SignalCore.java com/adobe/marketing/mobile/SignalExtension.java com/adobe/marketing/mobile/StringEncoder.java com/adobe/marketing/mobile/TargetCore.java com/adobe/marketing/mobile/TargetEventDispatcher.java com/adobe/marketing/mobile/TargetExtension.java com/adobe/marketing/mobile/TargetListenerRequestContent.java com/adobe/marketing/mobile/TargetListenerRequestIdentity.java com/adobe/marketing/mobile/TimerState.java com/adobe/marketing/mobile/UserProfileCore.java com/adobe/marketing/mobile/ZipBundleHandler.java com/adobe/marketing/mobile/reactnative/target/RCTACPTargetModule.java com/apmobileapp/MainApplication.java com/appmattus/certificatetransparency/internal/loglist/model/v3/Log$$serializer.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/q.java com/canhub/cropper/CropImageActivity.java com/canhub/cropper/CropOverlayView.java com/github/barteksc/pdfviewer/e.java com/github/barteksc/pdfviewer/h.java com/github/penfeizhou/animation/decode/b.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/d.java com/lugg/RNCConfig/RNCConfigModule.java com/reactcommunity/rndatetimepicker/d.java com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/cookies/CookieManagerModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/reactnativecommunity/webview/e.java com/reactnativecommunity/webview/i.java com/reactnativecommunity/webview/k.java com/rnfs/c.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/i.java com/swmansion/gesturehandler/react/j.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/th3rdwave/safeareacontext/k.java d3/c.java d3/d.java d3/h.java d3/j.java d3/k.java d3/n.java d3/x.java e5/d.java e8/b.java ee/e.java fd/a.java ff/e.java fr/greweb/reactnativeviewshot/RNViewShotModule.java fr/greweb/reactnativeviewshot/a.java g9/a.java g9/d.java gb/f.java h0/b.java h0/d.java h3/a.java h3/d.java h3/j.java hf/i.java i1/a.java i1/d.java ia/a.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/legere/pdfiumandroid/DefaultLogger.java io/legere/pdfiumandroid/PdfiumCore.java j1/h.java j3/c.java k9/g.java ke/m.java l3/h.java la/c.java lb/f.java lb/n.java lc/b.java m9/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m9/e0.java m9/i.java m9/j.java m9/j0.java m9/m.java m9/v.java m9/z.java mc/c.java me/f.java me/t.java me/z.java mk/e.java n0/c.java o3/a.java o9/x.java ob/g.java org/wonday/pdf/a.java p0/a.java p9/a.java p9/a0.java p9/a1.java p9/b1.java p9/c.java p9/c1.java p9/d0.java p9/e1.java p9/k1.java p9/o1.java p9/x0.java q2/a.java q3/a.java r/f.java r2/d.java r2/e.java r3/c.java rb/s.java rc/a.java rc/e.java re/a.java s0/d.java s2/a.java s9/a.java t2/a.java t9/b.java u3/a.java u9/g.java u9/n.java ua/d.java uc/b0.java uc/d0.java uc/g.java uc/g0.java uc/k.java uc/x.java ud/b.java v2/c.java v2/e.java v3/b.java v3/h.java v3/k.java v4/f.java v5/a.java v5/g.java v8/k.java vc/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w0/n.java w2/e.java w2/i.java w2/k.java w2/q.java w2/z.java w7/a.java wc/c.java wc/f.java we/l.java wk/e.java x2/i.java x2/j.java x9/b.java xa/g.java y/c.java y2/e.java y2/i.java y8/a.java yd/b.java z1/a.java z2/a.java
3	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	ah/a.java ah/b.java bh/a.java hf/i.java lk/z.java zk/d.java zk/h.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	d2/l.java n2/d.java vk/c.java vk/d.java vk/i.java vk/j.java
5	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/ReactNativeBlobUtil/i.java xd/a.java
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	ab/w.java rb/i.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/appmattus/certificatetransparency/internal/verifier/CertificateTransparencyTrustManager.java h2/d.java h2/j.java h2/m.java n2/j.java y6/a.java
8	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/ReactNativeBlobUtil/a.java com/canhub/cropper/CropImageActivity.java com/reactnativecommunity/webview/k.java fr/greweb/reactnativeviewshot/RNViewShotModule.java lc/c.java r3/c.java y3/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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/ReactNativeBlobUtil/c.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/k.java com/rnfs/RNFSManager.java i4/a.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java m1/c.java r3/c.java y3/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	l4/c.java lc/b.java yf/b.java
11	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	c9/m0.java c9/v0.java com/adobe/marketing/mobile/AndroidDatabase.java com/adobe/marketing/mobile/AndroidEventHistoryDatabase.java com/reactnativecommunity/asyncstorage/f.java
12	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	ie/a.java
13	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/adobe/marketing/mobile/AssuranceWebViewSocket.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	c4/c.java com/ReactNativeBlobUtil/c.java com/ReactNativeBlobUtil/g.java com/adobe/marketing/mobile/AbstractHitsDatabase.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/CacheManager.java com/adobe/marketing/mobile/ConfigurationExtension.java com/adobe/marketing/mobile/RemoteDownloader.java com/rnfs/RNFSManager.java d0/m.java fr/greweb/reactnativeviewshot/RNViewShotModule.java i1/d.java i1/e.java i1/f.java i4/a.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java ke/m.java m1/c.java me/e.java sb/f.java u3/a.java uf/c0.java y3/f.java ye/d.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ReactNativeBlobUtil/d.java com/ReactNativeBlobUtil/g.java com/adobe/marketing/mobile/AssuranceSession.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/services/ui/a.java com/canhub/cropper/CropImageActivity.java fg/b.java fg/k.java i1/a.java j1/h.java j1/o.java ke/m.java m9/f.java vd/e.java w7/a.java xe/a.java xe/c.java
00091	Retrieve data from broadcast	collection	com/ReactNativeBlobUtil/g.java com/adobe/marketing/mobile/LocalNotificationHandler.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ReactNativeBlobUtil/g.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/services/ui/a.java fg/b.java fg/k.java j1/h.java m9/f.java vd/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a3/g.java al/q.java com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/c.java com/ReactNativeBlobUtil/e.java com/ReactNativeBlobUtil/h.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/ConfigurationExtension.java com/adobe/marketing/mobile/FileUtil.java com/bumptech/glide/load/a.java com/christopherdro/RNPrint/RNPrintModule.java com/reactnativecommunity/asyncstorage/c.java com/rnfs/RNFSManager.java com/rnfs/i.java d0/m.java fl/b.java ke/m.java lc/c.java q2/a.java rb/b0.java sb/f.java tg/f.java u3/a.java w3/b.java wb/e.java xd/a.java yb/a.java
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/AssuranceClientInfo.java com/learnium/RNDeviceInfo/RNDeviceModule.java u1/c.java
00014	Read file into a stream and put it into a JSON object	file	lc/c.java sb/f.java yb/a.java
00005	Get absolute path of file and put it to JSON object	file	sb/f.java
00026	Method reflection	reflection	sh/a.java sh/b.java
00121	Create a directory	file command	ke/m.java
00024	Write file after Base64 decoding	reflection file	com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/g.java i1/e.java i1/f.java ke/m.java
00012	Read data and put it into a buffer stream	file	com/rnfs/i.java ke/m.java
00125	Check if the given file path exist	file	com/ReactNativeBlobUtil/g.java ke/m.java
00104	Check if the given path is directory	file	ke/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	expo/modules/image/records/SourceMap.java i1/d.java io/invertase/firebase/common/SharedUtils.java ke/m.java m9/f.java u3/a.java vd/e.java
00109	Connect to a URL and get the response code	network command	com/adobe/marketing/mobile/AssuranceBlob.java com/bumptech/glide/load/data/j.java com/rnfs/c.java g9/d.java k9/f.java mc/c.java
00192	Get messages in the SMS inbox	sms	com/rnfs/RNFSManager.java i1/d.java m1/c.java
00162	Create InetSocketAddress object and connecting to it	socket	vk/b.java vk/j.java
00163	Create new Socket and connecting to it	socket	u1/g.java vk/b.java vk/j.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
00028	Read file from assets directory	file	com/rnfs/RNFSManager.java
00043	Calculate WiFi signal strength	collection wifi	hd/e.java
00096	Connect to a URL and set request method	command network	com/adobe/marketing/mobile/AssuranceBlob.java mc/c.java
00089	Connect to a URL and receive input stream from the server	command network	com/adobe/marketing/mobile/AssuranceBlob.java com/bumptech/glide/load/data/j.java com/rnfs/c.java mc/c.java
00153	Send binary data over HTTP	http	com/adobe/marketing/mobile/AssuranceBlob.java
00187	Query a URI and check the result	collection sms calllog calendar	h0/d.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	h0/b.java h0/d.java m1/c.java v2/c.java we/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/ReactNativeBlobUtil/g.java m1/c.java
00189	Get the content of a SMS message	sms	l4/f.java m1/c.java we/m.java
00188	Get the address of a SMS message	sms	l4/f.java m1/c.java we/m.java
00200	Query data from the contact list	collection contact	l4/f.java m1/c.java we/m.java
00201	Query data from the call log	collection calllog	l4/f.java m1/c.java we/m.java
00072	Write HTTP input stream into a file	command network file	com/rnfs/c.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java com/rnfs/c.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	m1/c.java
00114	Create a secure socket connection to the proxy address	network command	qk/f.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java
00094	Connect to a URL and read data from it	command network	vb/a.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/106305343195/namespaces/firebase:fetch?key=AIzaSyAeUin3SL-s-0e-Oh3tkt45fZa4lq1gEsk is enabled. Ensure that the configurations are not sensitive. Th hsid","secureMessengerTheme":"geha","website":"https://www.umr.com","apiGatewayBaseUrl":"https://gateway.optum.com/api/cel/gateway/v1","hsidClientId":"63b07f149ec48e4bb65d26ccf6067390242890902b03b572","omniChatBaseUrl":"ht id.com/oidc/token","secureMessengerUrl":"https://www.tpa.com/app-secure-messaging?token=","hsidSettingsUrl":"https://identity.healthsafe-id.com/web/redirect?to=manage-profile","hsidRevokeServer":"https://identity.healthsafe-id.com/oidc response_type=code&client_id=63b07f149ec48e4bb65d26ccf6067390242890902b03b572&response_type=code&scope=openid+profile+email+phone&redirect_uri=geha://geha/login","providerDocType":"docProviderEcho","enableAppealClaim" app","statusBarStyle":"light"}}', 'minAppVersion': '1.0.0'}, 'state': 'UPDATE', 'templateVersion': '23'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	3/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
pinterest.com	ok	**IP:** 151.101.64.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
expo.dev	ok	**IP:** 104.18.5.104 **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:** 64.233.185.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 64.233.177.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
blobs.griffon.adobe.com	ok	No Geolocation information available.
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:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 74.125.136.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
developer.android.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
pagead2.googlesyndication.com	ok	**IP:** 142.250.9.156 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
aep-sdks.gitbook.io	ok	**IP:** 172.64.147.209 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
accounts.google.com	ok	**IP:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.gstatic.com	ok	**IP:** 142.250.72.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.9.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
assets.adobedtm.com	ok	**IP:** 23.3.85.32 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **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
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

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	m9/u.java

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"ADOBE_ANALYTICS_KEY" : "512027f42d3c/0a32cd3d13e2/launch-0218f4ec3762"
"ANDROID_FIREBASE_APP_ID" : "1:106305343195:android:bbaee40307ffef412c06fe"
"FIREBASE_PROJECT_ID" : "ymstqpgx-movf-f364-pbog-dz539v"
"IOS_FIREBASE_APP_ID" : "1:106305343195:ios:5dcbe3e8f7924a332c06fe"
"IOS_FIREBASE_APP_ID_INTERNAL" : "1:106305343195:ios:d2b0c62d705286aa2c06fe"
"com.google.firebase.crashlytics.mapping_file_id" : "27fe4df8a0874b148ce5000e5ae02d90"
"google_api_key" : "AIzaSyAeUin3SL-s-0e-Oh3tkt45fZa4lq1gEsk"
"google_crash_reporting_api_key" : "AIzaSyAeUin3SL-s-0e-Oh3tkt45fZa4lq1gEsk"
bbaee40307ffef412c06fe
d2b0c62d705286aa2c06fe
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
5dcbe3e8f7924a332c06fe
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa

PLAYSTORE INFORMATION

Title: MyGEHA

Score: 4.178218 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.bob.geha

Developer Details: G.E.H.A, G.E.H.A, None, https://www.geha.com, editor@geha.com,

Release Date: Dec 8, 2024 **Privacy Policy:** Privacy link

Description:

An upgraded app experience for federal employees, retirees and military retirees who are members of G.E.H.A medical and dental plans. With the MyGEHA app, you can easily access your medical or dental health information, including: - Instant access: Access your digital ID card. - Plan details & Claims: View your plan details on-demand (view or upload claims, balances, including deductibles and out-of-pocket maximums). - Find a Provider: Search for in-network medical or dental providers, hospitals, and clinics. - Single Sign On: One tap access to important resources like HSA Bank and Caremark so no need to login again. - Live chat: Connect with G.E.H.A Customer Care by chat, call, or secure messaging. - Personalization: See a personalized list of things to do – Stay on top of your health and keep your benefits up to date.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:26:37	Generating Hashes	OK
2025-08-29 20:26:37	Extracting APK	OK
2025-08-29 20:26:37	Unzipping	OK
2025-08-29 20:26:37	Parsing APK with androguard	OK
2025-08-29 20:26:37	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:26:37	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:26:39	Parsing AndroidManifest.xml	OK
2025-08-29 20:26:39	Extracting Manifest Data	OK
2025-08-29 20:26:39	Manifest Analysis Started	OK
2025-08-29 20:26:40	Reading Network Security config from network_security_config.xml	OK
2025-08-29 20:26:40	Parsing Network Security config	OK
2025-08-29 20:26:40	Performing Static Analysis on: MyGEHA (com.bob.geha)	OK
2025-08-29 20:26:41	Fetching Details from Play Store: com.bob.geha	OK
2025-08-29 20:26:41	Checking for Malware Permissions	OK
2025-08-29 20:26:41	Fetching icon path	OK
2025-08-29 20:26:41	Library Binary Analysis Started	OK
2025-08-29 20:26:41	Reading Code Signing Certificate	OK

2025-08-29 20:26:41	Running APKiD 2.1.5	OK
2025-08-29 20:26:43	Detecting Trackers	OK
2025-08-29 20:26:45	Decompiling APK to Java with JADX	OK
2025-08-29 20:26:56	Converting DEX to Smali	OK
2025-08-29 20:26:56	Code Analysis Started on - java_source	OK
2025-08-29 20:26:58	Android SBOM Analysis Completed	OK
2025-08-29 20:27:05	Android SAST Completed	OK
2025-08-29 20:27:05	Android API Analysis Started	OK
2025-08-29 20:27:11	Android API Analysis Completed	OK
2025-08-29 20:27:12	Android Permission Mapping Started	OK
2025-08-29 20:27:18	Android Permission Mapping Completed	OK
2025-08-29 20:27:18	Android Behaviour Analysis Started	OK
2025-08-29 20:27:26	Android Behaviour Analysis Completed	OK
2025-08-29 20:27:26	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:27:29	Email and URL Extraction Completed	OK
2025-08-29 20:27:29	Extracting String data from APK	OK
2025-08-29 20:27:29	Extracting String data from Code	OK

2025-08-29 20:27:29	Extracting String values and entropies from Code	OK
2025-08-29 20:27:30	Performing Malware check on extracted domains	OK
2025-08-29 20:27:32	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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