



ANDROID STATIC ANALYSIS REPORT



 DocMorris (5.13.0)

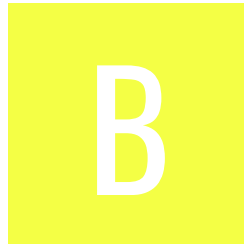
File Name: de.docmorris.pharmacyapp_6370000.apk

Package Name: de.docmorris.pharmacyapp

Scan Date: Sept. 1, 2025, 12:58 p.m.






App Security Score: 50/100 (MEDIUM RISK)

Grade:



Trackers Detection: 6/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	21	4	3	7

FILE INFORMATION

File Name: de.docmorris.pharmacyapp_6370000.apk

Size: 31.08MB

MD5: 0cdc7af49ae4baf216a006bedae4f310

SHA1: 7fa92643c0a7ef06b1918b18b6f4b8a9fb114707

SHA256: 7f488b5af56ada8af2eca755fe8ef9ac282d1305edc71f421ffd6f3532ad2971

APP INFORMATION

App Name: DocMorris

Package Name: de.docmorris.pharmacyapp

Main Activity: de.comventure.commerce.MainActivity

Target SDK: 34

Min SDK: 24

Max SDK:

Android Version Name: 5.13.0

Android Version Code: 6370000

APP COMPONENTS

Activities: 11

Services: 23

Receivers: 17

Providers: 11

Exported Activities: 3

Exported Services: 3

Exported Receivers: 5

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: True

v3 signature: True

v4 signature: False

X.509 Subject: C=Unknown, ST=Unknown, L=Unknown, O=DocMorris N.V., OU=Unknown, CN=Unknown

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2016-04-25 09:14:18+00:00

Valid To: 2290-02-08 09:14:18+00:00

Issuer: C=Unknown, ST=Unknown, L=Unknown, O=DocMorris N.V., OU=Unknown, CN=Unknown

Serial Number: 0x706ca9c1

Hash Algorithm: sha256

md5: f2b7939ad602f5d8207fef6cf4127b65

sha1: 77c4f8cd1ce2d4845dc2dc0516e31d8b7636b83a

sha256: 40e8eee974b9078da898d36fe6bd9d1e1c4db3cd82d2365e2d322ba28ad11cea

sha512: 2d66a4a719b590b940d823380933e6ff3ddc76ee37e833cabb5ca5d8b9ca4bd40e01e28b0839a7aaa6ccb9bf5dec449578e7fcf1bf9098e27d645cdd4c9f5f39

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: ade62cc3aafb8f0b398ffa683c45d9464bdbda7910c66451dc0ee3ac48e464f5

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.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
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.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference

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

FILE	DETAILS	
0cdc7af49ae4baf216a006bedae4f310.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check Build.TAGS check SIM operator check network operator name check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)
classes4.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

ACTIVITY	INTENT
de.comventure.commerce.MainActivity	Schemes: adyencheckout://, https://, docmorris://, Hosts: checkout, www.docmorris.de, Paths: /, Path Prefixes: /angebote, /express, /e-rezept-einloesen, /host/erx/addtocart, /produkte, /rezepteinloesen, /search, /service/infos/e-rezept, /rezepte/rezept-einloesen, /rezepte/rezept- einloesen/e-rezept, /eingeladen, Path Patterns: /..*/..*,
com.adyen.checkout.dropin.internal.ui.DropInActivity	Schemes: adyencheckout://, Hosts: de.docmorris.pharmacyapp, Paths: /,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.de.docmorris.pharmacyapp://,
com.adyen.threeds2.internal.ui.activity.ChallengeActivity	Schemes: adyen3ds2://, Hosts: de.docmorris.pharmacyapp,

NETWORK SECURITY

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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

🔍 MANIFEST ANALYSIS

HIGH: 2 | WARNING: 11 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Service (com.wix.reactnativenotifications.fcm.FcmInstanceIdListenerService) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Activity (com.adyen.checkout.dropin.internal.ui.DropInActivity) 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.
7	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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
8	<p>Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]</p>	warning	<p>A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.</p>
9	<p>Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.DUMP [android:exported=true]</p>	warning	<p>A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.</p>
10	<p>Activity (com.adyen.threeds2.internal.ui.activity.ChallengeActivity) is not Protected.</p> <p>[android:exported=true]</p>	warning	<p>An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.</p>
11	<p>Broadcast Receiver (com.adyen.threeds2.internal.AppUpgradeBroadcastReceiver) is not Protected.</p> <p>[android:exported=true]</p>	warning	<p>A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.</p>

NO	ISSUE	SEVERITY	DESCRIPTION
12	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.
13	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: 1 | WARNING: 9 | INFO: 4 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A6/m.java B0/h.java B6/C0671c.java B6/C0672c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				B6/C0073e.java B6/C1226c.java B6/C1228e.java B6/G.java B6/J.java B6/m.java B6/t.java B6/u.java B6/y.java Cj/b.java De/f.java Df/a.java Df/e.java E/d.java F6/a.java F6/d.java F6/j.java Fg/a.java G/A.java Gf/B.java Gf/C0222g.java Gf/C1360g.java Gf/D.java Gf/F.java Gf/k.java Gf/x.java H6/e.java H6/f.java H6/o.java H6/p.java H6/r.java H6/s.java H8/d.java H8/g.java H8/h.java H8/j.java H8/l.java H8/m.java H8/y.java H9/e.java Hf/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t17b.java le/d.java ld/h.java le/C0230f.java le/C1373f.java le/n.java lf/c.java lf/f.java J/e.java J1/g.java K0/b.java K6/h.java K8/d.java L6/d.java L6/k.java Le/g.java Mb/d.java N/c.java N0/b.java N6/a.java O9/a.java Oe/r.java P6/a.java Qn/j.java R7/m.java Sj/a.java U5/a.java Vd/a.java Vf/i.java Xd/d.java Xf/f.java Xf/n.java Xf/p.java Xn/g.java Y5/d.java Y5/e.java Yd/b.java Yi/b.java Z/c.java a6/C0759a.java a6/C0763e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a6/C1641a.java a6/C1645e.java ae/C0293g.java ae/C1736g.java af/C0307g.java af/C1750g.java ap/j.java b0/AbstractC1037a.java b0/AbstractC1968a.java b1/d.java b6/C1074h.java b6/C2005h.java ba/c.java bo/g.java ch/C0664c.java ch/C2131c.java cl/json/RNShareModule.java com/adjust/nativemodule/Adjust.java com/adjust/sdk/Logger.java com/adyen/checkout/components/core/internal/data/model/AnalyticsTrackLog.java com/adyenreactnativesdk/component/dropin/AdvancedCheckoutService.java com/adyenreactnativesdk/component/dropin/DropInModule.java com/agontuk/RNFusedLocation/RNFusedLocationModule.java com/airbnb/android/react/lottie/LottieAnimationViewManager.java com/bumptechnology/glide/GeneratedAppGlideModuleImpl.java com/bumptechnology/glide/c.java com/bumptechnology/glide/load/data/b.java com/bumptechnology/glide/load/data/j.java com/bumptechnology/glide/load/data/l.java com/datadog/android/rum/DdRumContentProvider.java com/emarsys/geofence/RegisterGeofencesOnBootCompletedReceiver.java com/emarsys/rnwrapper/RNEmarsysPredictWrapperModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/gevorg/reactlibrary/RNQRGeneratorMod com/github/barteksc/pdfviewer/e.java com/github/barteksc/pdfviewer/h.java com/ibits/react_native_in_app_review/AppRe viewModule.java com/imagepicker/b.java com/imagepicker/h.java com/learnium/RNDeviceInfo/RNDeviceModul e.java com/learnium/RNDeviceInfo/d.java com/lugg/ReactNativeConfig/ReactNativeConf igModule.java com/microsoft/codepush/react/k.java com/oblador/storereview/b.java com/pusherman/networkinfo/RNNetworkInfo .java com/reactcommunity/rndatetimepicker/b.jav a com/reactnativecommunity/asyncstorage/c.ja va com/reactnativecommunity/webview/RNCWe bViewManager.java com/reactnativecommunity/webview/RNCWe bViewModule.java com/reactnativedocumentpicker/RNDocumen tPickerModule.java com/rnfs/c.java com/rnmaps/maps/MapModule.java com/rnmaps/maps/MapTileWorker.java com/rnmaps/maps/i.java com/rnmaps/maps/p.java com/rnmaps/maps/q.java com/shockwave/pdfium/PdfiumCore.java com/swmansion/gesturehandler/react/RNGes tureHandlerModule.java com/swmansion/gesturehandler/react/j.java com/swmansion/gesturehandler/react/k.java com/swmansion/reanimated/NativeMethods Helper.java com/swmansion/reanimated/ReanimatedMo

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	dule.java Files com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/keyboard/WindowsInsetsManager.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/ScreensHelper.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/layoutReanimation/TabNavigatorObserver.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/tencent/mm/opensdk/channel/MMessageActV2.java com/tencent/mm/opensdk/channel/a/a.java com/tencent/mm/opensdk/diffdev/DiffDevOAuthFactory.java com/tencent/mm/opensdk/diffdev/a/a.java com/tencent/mm/opensdk/diffdev/a/b.java com/tencent/mm/opensdk/diffdev/a/c.java com/tencent/mm/opensdk/modelbiz/AddCardToWXCardPackage.java com/tencent/mm/opensdk/modelbiz/ChooseCardFromWXCardPackage.java com/tencent/mm/opensdk/modelbiz/SubscribeMessage.java com/tencent/mm/opensdk/modelbiz/SubscribeMiniProgramMsg.java com/tencent/mm/opensdk/modelbiz/WXChannelBaseJumpInfo.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com.tencent.mm.opensdk.modelbiz/WXChannelJumpMiniProgramInfo.java com.tencent.mm.opensdk.modelbiz/WXChannelJumpUrlInfo.java com.tencent.mm.opensdk.modelbiz/WXChannelOpenFeed.java com.tencent.mm.opensdk.modelbiz/WXChannelOpenLive.java com.tencent.mm.opensdk.modelbiz/WXChannelOpenProfile.java com.tencent.mm.opensdk.modelbiz/WXChannelShareVideo.java com.tencent.mm.opensdk.modelbiz/WXInvoiceAuthInsert.java com.tencent.mm.opensdk.modelbiz/WXLaunchMiniProgram.java com.tencent.mm.opensdk.modelbiz/WXLaunchMiniProgramWithToken.java com.tencent.mm.opensdk.modelbiz/WXNonTaxPay.java com.tencent.mm.opensdk.modelbiz/WXOpenBusinessView.java com.tencent.mm.opensdk.modelbiz/WXPayInsurance.java com.tencent.mm.opensdk.modelbiz/WXPreloadMiniProgram.java com.tencent.mm.opensdk.modelmsg/GetMessageFromWX.java com.tencent.mm.opensdk.modelmsg/LaunchFromWX.java com.tencent.mm.opensdk.modelmsg/SendAuth.java com.tencent.mm.opensdk.modelmsg/SendMessageToWX.java com.tencent.mm.opensdk.modelmsg/WXAppExtendObject.java com.tencent.mm.opensdk.modelmsg/WXDesignerSharedObject.java com.tencent.mm.opensdk.modelmsg/WXDynamicVideoMiniProgramObject.java com.tencent.mm.opensdk.modelmsg/WXEm

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>ojiObject.java</div> <div>com.tencent/mm/opensdk/modelmsg/WXEm</div> <div>ojiPageSharedObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXEm</div> <div>ojiSharedObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXEnt</div> <div>erpriseCardObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXFil</div> <div>eObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXGa</div> <div>meVideoFileObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXIm</div> <div>ageObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXLit</div> <div>eAppObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXMe</div> <div>diaMessage.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXMi</div> <div>niProgramObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXMu</div> <div>sicObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXMu</div> <div>sicVideoObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXSta</div> <div>teJumpChannelProfileInfo.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXSta</div> <div>teJumpMiniProgramInfo.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXSta</div> <div>teJumpUrlInfo.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXSta</div> <div>teSceneDataObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXTe</div> <div>xtObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXVid</div> <div>eoFileObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXVid</div> <div>eoObject.java</div> <div>com/tencent/mm/opensdk/modelmsg/WXWe</div> <div>bpageObject.java</div> <div>com/tencent/mm/opensdk/modelpay/PayRe</div> <div>q.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tencent/mm/opensdk/openapi/BaseWX ApplmV10.java com/tencent/mm/opensdk/openapi/MMShar edPreferences.java com/tencent/mm/opensdk/openapi/WXAPIFa ctory.java com/tencent/mm/opensdk/openapi/WXApiIm plComm.java com/tencent/mm/opensdk/utls/Log.java com/tencent/mm/opensdk/utls/b.java com/th3rdwave/safeareacontext/k.java com/wix/reactnativenotifications/RNNotificati onsModule.java e/AbstractC1190f.java e/AbstractC2511f.java ep/a.java hc/f.java hc/l.java he/i.java io/invertase/firebase/app/ReactNativeFirebas eApp.java io/invertase/firebase/app/ReactNativeFirebas eAppModule.java io/invertase/firebase/common/RCTConvertFir ebase.java io/invertase/firebase/common/ReactNativeFir ebaseEventEmitter.java io/invertase/firebase/common/SharedUtils.ja va io/invertase/firebase/crashlytics/ReactNativeF irebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeF irebaseCrashlyticsModule.java io/invertase/firebase/dynamiclinks/ReactNati veFirebaseDynamicLinksModule.java io/invertase/firebase/perf/ScreenTrace.java io/invertase/firebase/utls/ReactNativeFirebas eUtilsModule.java j0/n.java l/MenuItemC1458c.java l/MenuItemC3173c.iava

NO	ISSUE	SEVERITY	STANDARDS	FILES
				l0/o.java l0/r.java l0/u.java l0/y.java ld/C0711a.java ld/C3236a.java lf/C0716b.java lf/C3241b.java mf/C0734c.java mf/C3435c.java n0/AbstractC1539a.java n0/AbstractC3520a.java n6/e.java o3/e.java org/wonday/orientation/a.java p0/h.java p6/C1604b.java p6/C3720b.java pi/K2.java q/c.java q0/d.java q6/C1642d.java q6/C3957d.java q6/e.java qk/C1488d.java qk/C4011d.java r0/C1660a.java r0/C4040a.java r6/C1676a.java r6/C4056a.java rf/e.java t/d.java t6/C1738c.java t6/C1740e.java t6/C4222c.java t6/C4224e.java tb/f.java u/c.java u/o.java u0/C1758a.java u0/C4293a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u6/h.java u6/i.java u6/k.java u6/q.java u6/z.java ue/C0850a.java ue/C0851b.java ue/C0852c.java ue/C4331a.java ue/C4332b.java ue/C4333c.java uf/C0856c.java uf/C4337c.java uj/b.java v0/AbstractC1792a.java v0/AbstractC4376a.java v6/i.java v6/k.java vd/k.java w/f.java w6/e.java w6/i.java x6/ExecutorServiceC1867a.java x6/ExecutorServiceC4543a.java y/AbstractC1881a.java y/AbstractC1883c.java y/AbstractC4618a.java y/AbstractC4620c.java y/d.java y/f.java y6/c.java y6/d.java y6/f.java y6/r.java y6/s.java yd/AbstractC0914a.java yd/AbstractC4646a.java
				Ff/b.java G0/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	N2/e.java N2/e.java Pe/b.java Qe/C0268e.java Qe/C1550e.java Qe/w.java R7/e.java R7/k.java Xb/C0278h.java Xb/C1598h.java app/cash/paykit/core/models/request/CreateCustomerRequest.java com/adjust/sdk/Constants.java com/adyen/checkout/adyen3ds2/internal/data/model/FingerprintToken.java com/adyen/checkout/components/core/internal/data/model/PublicKeyResponse.java com/adyen/checkout/components/core/paymentmethod/CardPaymentMethod.java com/adyenreactnativesdk/component/base/BaseModule.java com/adyenreactnativesdk/cse/AdyenCSEModule.java com/scandit/datacapture/reactnative/barcode/ScanditDataCaptureBarcodeCaptureModule.java com/scandit/datacapture/reactnative/barcode/ScanditDataCaptureBarcodeModule.java com/scandit/datacapture/reactnative/barcode/ScanditDataCaptureBarcodeSelectionModule.java com/scandit/datacapture/reactnative/barcode/ScanditDataCaptureBarcodeTrackingModule.java com/scandit/datacapture/reactnative/barcode/ScanditDataCaptureSparkScanModule.java com/scandit/datacapture/reactnative/core/ScanditDataCaptureCoreModule.java com/tencent/mm/opensdk/constants/ConstantsAPI.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f3/C1250b.java f3/C1250b.java f3/g.java f3/r.java io/invertase/firebase/common/TaskExecutorService.java k5/C1434a.java k5/C3036a.java n5/C1548a.java n5/C3529a.java q3/k.java s6/C1713g.java s6/C4151g.java u6/d.java u6/p.java u6/x.java w8/C1831a.java w8/C4466a.java y3/AbstractC1890a.java y3/AbstractC4627a.java y3/d.java
3	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/ClipboardModule.java g3/AbstractC1291d.java g3/AbstractC2692d.java la/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	C8/c.java C8/h.java Fo/d.java Fo/e.java Lo/b.java Vk/a.java Vk/b.java Wk/a.java Xf/o.java a6/C0759a.java a6/C1641a.java com/adjust/sdk/Util.java com/adyen/threeds2/internal/dispatchDisplayHint.java com/adyen/threeds2/internal/jose/jwa/contentEncryption/ContentEncryptionAlgorithm.java com/adyen/threeds2/internal/util/StringObfuscator.java de/gematik/ti/healthcard/control/common/pace/TrustedChannelPaceKeyExchange.java f8/C1258a.java f8/C2602a.java org/songsterq/pdfthumbnail/PdfThumbnailModule.java zf/d.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	a9/C0833a.java a9/C1715a.java hb/c.java lf/C0716b.java lf/C3241b.java pi/E2.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	E5/f.java L1/c.java Ua/a.java com/ReactNativeBlobUtil/d.java com/adyen/threeds2/internal/deviceinfo/parameter/environment/GetExternalStorageState.java com/learnium/RNDeviceInfo/RNDeviceInfoModule.java com/reactnativecommunity/webview/RNCWebViewModule.java com/rnfs/RNFSManager.java eb/C1225a.java eb/C2546a.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
7	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	Ua/a.java com/ReactNativeBlobUtil/a.java com/reactnativecommunity/webview/RNCWebViewModule.java com/rnmaps/maps/MapModule.java com/rnmaps/maps/a.java l0/y.java lf/C0717c.java lf/C3242c.java org/songsterq/pdfthumbnail/PdfThumbnailModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	Lc/a.java Lm/a.java Mm/a.java Mo/e.java Nm/a.java Om/a.java Pg/a.java Pm/a.java Qm/c.java com/pusherman/networkinfo/RNNetworkInfo.java en/C0738a.java en/C2567a.java fo/C0782c.java fo/C2666c.java fo/InterfaceC0783d.java fo/InterfaceC2667d.java hn/h.java ho/InterfaceC0851b.java ho/InterfaceC2853b.java io/InterfaceC0882a.java io/InterfaceC2915a.java ko/InterfaceC0979b.java ko/InterfaceC3170b.java lo/InterfaceC1137b.java lo/InterfaceC3402b.java no/j.java p000do/InterfaceC0722b.java p002do/InterfaceC2505b.java yn/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	Cd/M.java Cd/W.java N0/a.java N0/b.java b9/c.java c9/C1113b.java c9/C2101b.java com/reactnativecommunity/asyncstorage/f.java q0/c.java
10	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	de/gematik/ti/cardreader/provider/nfc/security/SecureMessaging.java qk/C1488d.java qk/C4011d.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	Oe/AbstractC0248i.java Oe/AbstractC1530i.java com/adyen/threeds2/internal/security/checker/SecurityCheckerImpl.java he/w.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	pi/AbstractC1427w.java pi/AbstractC3883w.java
13	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/k.java com/tencent/mm/opensdk/channel/a/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativemcommunity/clipboard/ClipboardModule.java
15	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	ra/C1688a.java ra/C4068a.java
16	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	Hg/a.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	I1/b.java I1/c.java I1/d.java J7/c.java L1/c.java P/m.java Pe/f.java Ua/f.java Ya/c.java com/ReactNativeBlobUtil/d.java com/ReactNativeBlobUtil/i.java com/microsoft/codepush/react/a.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/k.java com/microsoft/codepush/react/n.java com/oblador/vectoricons/VectorIconsModule.java com/reactnatedocumentpicker/RNDocumentPickerModule.java com/rnfs/RNFSManager.java eb/C1225a.java eb/C2546a.java i7/f.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java k6/C1445g.java k6/C1446h.java k6/C3047g.java k6/C3048h.java l0/y.java q0/d.java r0/C1660a.java r0/C4040a.java si/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	Mk/k.java Oe/A.java P/m.java Pe/f.java Sa/b.java Te/e.java Ve/a.java com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/d.java com/ReactNativeBlobUtil/f.java com/ReactNativeBlobUtil/j.java com/adjust/sdk/PreinstallUtil.java com/adyen/threeds2/internal/jose/util/PRNGFixes.java com/bumptech/glide/load/a.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/n.java com/reactnativeaesgcmcrypto/AesGcmCryptoModule.java com/reactnativecommunity/asyncstorage/c.java com/rnfs/RNFSManager.java com/rnfs/i.java com/rnmaps/maps/a.java com/rnmaps/maps/k.java com/rnmaps/maps/p.java j\$/desugar/sun/nio/fs/m.java k6/C1445g.java k6/C1446h.java k6/C3047g.java k6/C3048h.java l0/y.java l7/C1512e.java l7/C3227e.java lf/C0717c.java lf/C3242c.java n0/AbstractC1540b.java n0/AbstractC3521b.java okio/r.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	p6/C1604b.java p6/C3720b.java y6/f.java com/microsoft/codepush/react/n.java com/rnfs/i.java l7/C1512e.java l7/C3227e.java
00036	Get resource file from res/raw directory	reflection	l1/b.java ch/C0664c.java ch/C2131c.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/InstallReferrerHuawei.java com/adjust/sdk/c.java com/dylanvann/fastimage/f.java com/rnmaps/maps/d.java com/rnmaps/maps/l.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java ik/o.java io/invertase/firebase/common/SharedUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	E5/i.java J1/g.java J1/n.java S0/d.java af/C0307g.java af/C1750g.java ch/C0664c.java ch/C2131c.java cl/json/RNShareModule.java com/ReactNativeBlobUtil/ReactNativeBlobUtil.java com/ReactNativeBlobUtil/i.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/PreinstallUtil.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java io/invertase/firebase/dynamiclinks/ReactNativeFirebaseDynamicLinksModule.java la/d.java ld/C0711a.java ld/C3236a.java q/c.java ta/C1752a.java ta/C4236a.java y5/C1895a.java y5/C4632a.java
00026	Method reflection	reflection	nl/C1229a.java nl/C1230b.java nl/C3562a.java nl/C3563b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	E5/i.java J1/g.java S0/d.java ch/C0664c.java ch/C2131c.java com/ReactNativeBlobUtil/i.java y5/C1895a.java y5/C4632a.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java
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
00024	Write file after Base64 decoding	reflection file	l1/c.java l1/d.java com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/i.java com/gevorg/reactlibrary/RNQRGeneratorModule.java com/reactnativeaesgcmcrypto/AesGcmCryptoModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	L1/c.java com/adjust/sdk/c.java com/imagepicker/k.java com/reactnatedocumentpicker/RNDocumentPickerModule.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java hb/f.java
00188	Get the address of a SMS message	sms	L1/c.java com/adjust/sdk/c.java com/imagepicker/k.java com/reactnatedocumentpicker/RNDocumentPickerModule.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java hb/f.java
00200	Query data from the contact list	collection contact	L1/c.java com/adjust/sdk/c.java com/imagepicker/k.java com/reactnatedocumentpicker/RNDocumentPickerModule.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java hb/f.java
00201	Query data from the call log	collection callog	L1/c.java com/adjust/sdk/c.java com/imagepicker/k.java com/reactnatedocumentpicker/RNDocumentPickerModule.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java hb/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/rnfs/i.java com/tencent/mm/opensdk/channel/a/a.java k6/C1440b.java k6/C3042b.java mf/C0734c.java mf/C3435c.java
00089	Connect to a URL and receive input stream from the server	command network	F9/e.java Xf/n.java com/bumptech/glide/load/data/j.java com/microsoft/codepush/react/h.java com/rnfs/c.java com/rnfs/i.java com/tencent/mm/opensdk/channel/a/a.java mf/C0734c.java mf/C3435c.java
00109	Connect to a URL and get the response code	network command	Xf/n.java com/bumptech/glide/load/data/j.java com/rnfs/c.java com/rnfs/i.java com/tencent/mm/opensdk/channel/a/a.java mf/C0734c.java mf/C3435c.java
00094	Connect to a URL and read data from it	command network	F9/e.java Se/a.java com/rnmaps/maps/p.java com/tencent/mm/opensdk/channel/a/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms callog calendar	L1/c.java com/adjust/sdk/c.java com/imagepicker/k.java com/reactnatedocumentpicker/RNDocumentPickerModule.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java t6/C1738c.java t6/C4222c.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	Mi/b.java com/gevorg/reactlibrary/RNQRGeneratorModule.java com/rnmaps/maps/p.java
00192	Get messages in the SMS inbox	sms	l1/b.java L1/c.java com/rnfs/RNFSManager.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/rnfs/RNFSManager.java
00028	Read file from assets directory	file	com/rnfs/RNFSManager.java
00011	Query data from URI (SMS, CALLLOGS)	sms callog collection	L1/c.java com/adjust/sdk/c.java com/rnfs/RNFSManager.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00191	Get messages in the SMS inbox	sms	L1/c.java com/ReactNativeBlobUtil/i.java com/adjust/sdk/InstallReferrerMeta.java com/adjust/sdk/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00072	Write HTTP input stream into a file	command network file	F9/e.java com/microsoft/codepush/react/h.java com/rnfs/c.java
00030	Connect to the remote server through the given URL	network	F9/e.java com/adjust/sdk/AdjustLinkResolution.java com/bumptechnology/glide/load/data/j.java com/rnfs/c.java com/rnfs/i.java k6/C1440b.java k6/C3042b.java
00108	Read the input stream from given URL	network command	F9/e.java com/adyen/threeds2/internal/api/Api.java com/tencent/mm/opensdk/channel/a/a.java
00209	Get pixels from the latest rendered image	collection	com/scandit/datacapture/core/internal/module/source/CameraApi2Delegate.java
00014	Read file into a stream and put it into a JSON object	file	Pe/f.java Ve/a.java lf/C0717c.java lf/C3242c.java
00005	Get absolute path of file and put it to JSON object	file	Pe/f.java com/microsoft/codepush/react/k.java
00147	Get the time of current location	collection location	a6/AbstractC0767i.java a6/AbstractC1649i.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	pi/C1325e4.java pi/C3781e4.java
00091	Retrieve data from broadcast	collection	b8/b.java com/ReactNativeBlobUtil/i.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java hk/f.java
00175	Get notification manager and cancel notifications	notification	jk/C0892b.java jk/C3015b.java
00187	Query a URI and check the result	collection sms callog calendar	com/tencent/mm/opensdk/openapi/MMSharedPreferences.java
00125	Check if the given file path exist	file	com/ReactNativeBlobUtil/i.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms callog collection	com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java
00079	Hide the current app's icon	evasion	H0/p.java
00161	Perform accessibility service action on accessibility node info	accessibility service	G/A.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	G/A.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	com/adjust/sdk/network/ActivityPackageSender.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/863344085397/namespaces/firebase:fetch?key=AlzaSyBWVobzXufCySXu4y8ZMVGofGL-WZnOgVk . This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, 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
app.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
subscription.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
gdpr.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
open.weixin.qq.com	IP: 203.205.232.110 Country: China Region: Guangdong City: Shenzhen
ssrv.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou

DOMAIN	COUNTRY/REGION
long.open.weixin.qq.com	IP: 43.154.252.67 Country: China Region: Beijing City: Beijing

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
pinterest.com	ok	IP: 151.101.128.84 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
app.adjust.cn	ok	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map

DOMAIN	STATUS	GEOLOCATION
app.eu.adjust.com	ok	IP: 185.151.204.60 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
checkoutshopper-live-in.adyen.com	ok	IP: 147.12.21.133 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
play.google.com	ok	IP: 142.250.74.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
gdpr.tr.adjust.com	ok	IP: 195.244.54.44 Country: Turkey Region: Izmir City: Izmir Latitude: 38.412731 Longitude: 27.138380 View: Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.adjust.world	ok	IP: 185.151.204.40 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
codepush.appcenter.ms	ok	No Geolocation information available.
app.adjust.com	ok	IP: 185.151.204.15 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
log-dealer.eservice.emarsys.net	ok	IP: 35.198.176.244 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
plus.google.com	ok	IP: 216.58.211.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
checkoutanalytics-live-us.adyen.com	ok	IP: 135.84.151.167 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
gdpr.adjust.com	ok	IP: 185.151.204.50 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
subscription.tr.adjust.com	ok	IP: 195.244.54.6 Country: Turkey Region: Izmir City: Izmir Latitude: 38.412731 Longitude: 27.138380 View: Google Map
ssrv.us.adjust.com	ok	IP: 185.151.204.70 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
sandbox.api.cash.app	ok	IP: 151.101.66.133 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api.cash.app	ok	IP: 151.101.130.133 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
checkoutanalytics-live.adyen.com	ok	IP: 147.12.19.92 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
issuetracker.google.com	ok	IP: 142.250.74.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
checkoutshopper-live-us.adyen.com	ok	IP: 185.101.198.192 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
subscription.adjust.world	ok	IP: 185.151.204.44 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
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
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

DOMAIN	STATUS	GEOLOCATION
ssrv.adjust.world	ok	IP: 185.151.204.206 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
twitter.com	ok	IP: 172.66.0.227 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
firebase.google.com	ok	IP: 142.250.74.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	ok	IP: 142.250.74.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mobile-sdk-config.gservice.emarsys.net	ok	IP: 34.95.90.26 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
checkoutanalytics-test.adyen.com	ok	IP: 147.12.18.127 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
checkoutanalytics-live-in.adyen.com	ok	IP: 147.12.21.148 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
static.payu.com	ok	IP: 18.155.173.44 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	IP: 31.97.181.89 Country: United Kingdom of Great Britain and Northern Ireland Region: England City: Bowness-on-Windermere Latitude: 54.363312 Longitude: -2.918590 View: Google Map
ssrv.adjust.com	ok	IP: 185.151.204.2 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 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
ssrv.adjust.net.in	ok	IP: 185.151.204.207 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.eu.adjust.com	ok	IP: 185.151.204.60 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
subscription.eu.adjust.com	ok	IP: 185.151.204.60 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
checkoutshopper-live.adyen.com	ok	IP: 62.146.255.10 Country: Germany Region: Bayern City: Nuremberg Latitude: 49.447781 Longitude: 11.068330 View: Google Map
deep-link.eservice.emarsys.net	ok	IP: 35.242.204.238 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.us.adjust.com	ok	IP: 185.151.204.70 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
checkoutshopper-live-apse.adyen.com	ok	IP: 85.184.228.203 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
checkoutanalytics-live-apse.adyen.com	ok	IP: 85.184.229.219 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
subscription.adjust.cn	ok	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.adjust.net.in	ok	IP: 185.151.204.34 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
gdpr.adjust.cn	ok	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
app.adjust.world	ok	IP: 185.151.204.43 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
me-inbox.eservice.emarsys.net	ok	IP: 34.89.192.150 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map

DOMAIN	STATUS	GEOLOCATION
checkoutshopper-test.adyen.com	ok	IP: 62.146.255.5 Country: Germany Region: Bayern City: Nuremberg Latitude: 49.447781 Longitude: 11.068330 View: Google Map
mobile-events.eservice.emarsys.net	ok	IP: 34.102.218.62 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
ssrv.tr.adjust.com	ok	IP: 195.244.54.44 Country: Turkey Region: Izmir City: Izmir Latitude: 38.412731 Longitude: 27.138380 View: Google Map
ssrv.eu.adjust.com	ok	IP: 185.151.204.60 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.us.adjust.com	ok	IP: 185.151.204.70 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
open.weixin.qq.com	ok	IP: 203.205.232.110 Country: China Region: Guangdong City: Shenzhen Latitude: 22.545540 Longitude: 114.068298 View: Google Map
app.tr.adjust.com	ok	IP: 195.244.54.5 Country: Turkey Region: Izmir City: Izmir Latitude: 38.412731 Longitude: 27.138380 View: Google Map
gdpr.adjust.net.in	ok	IP: 185.151.204.33 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
app.us.adjust.com	ok	IP: 185.151.204.70 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
ssrv.adjust.cn	ok	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
me-client.eservice.emarsys.net	ok	IP: 34.96.123.93 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
long.open.weixin.qq.com	ok	IP: 43.154.252.67 Country: China Region: Beijing City: Beijing Latitude: 39.907501 Longitude: 116.397232 View: Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	IP: 216.58.207.195 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
subscription.adjust.com	ok	IP: 185.151.204.52 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
api.squareup.com	ok	IP: 162.159.136.66 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
checkoutshopper-live-au.adyen.com	ok	IP: 147.12.23.70 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
recommender.scarabresearch.com	ok	IP: 54.213.50.244 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
checkoutanalytics-live-au.adyen.com	ok	IP: 85.184.230.95 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
console.firebase.google.com	ok	IP: 142.250.74.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
app.adjust.net.in	ok	IP: 185.151.204.33 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Scandit	Analytics	https://reports.exodus-privacy.eu.org/trackers/84

HARDCODED SECRETS

POSSIBLE SECRETS
"CodePushDeploymentKey" : "gflKRtkkkjCI7J80yVh7ZixeFvnXJWd2rMYddY"
"google_api_key" : "AlzaSyBWVobzXufCySXu4y8ZMVGofGL-WZnOgVk"
"google_crash_reporting_api_key" : "AlzaSyBWVobzXufCySXu4y8ZMVGofGL-WZnOgVk"
"google_maps_key" : "AlzaSyBWVobzXufCySXu4y8ZMVGofGL-WZnOgVk"
DB7C2ABF62E35E668076BEAD2088
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
41058363725152142129326129780047268409114441015993725554835256314039467401291
0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C
E95E4A5F737059DC60DFC7AD95B3D8139515620F
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
74D59FF07F6B413D0EA14B344B20A2DB049B50C3
26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92
046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C

POSSIBLE SECRETS
VFM0cERYUUpFM0paTkQ1TFdESW9PRDRzQnhsQk1GRUBZbDFRZmdCc2ZsMDdYVkJrUGxOQIZFMU5ZWHh1UXIR
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
1E589A8595423412134FAA2DBDEC95C8D8675E58
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
04B8266A46C55657AC734CE38F018F2192
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03
883423532389192164791648750360308885314476597252960362792450860609699839
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
RTFGeVkmWNjQU5EU2c0V1pRZERkQ0JHQmhwY0NRQGR6UmNFUkktQmkwaUpHcGtDbTRuV2xnMmFXazViUQ
115792089210356248762697446949407573529996955224135760342422259061068512044369
2866537B676752636A68F56554E12640276B649EF7526267
00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
3045AE6FC8422F64ED579528D38120EAE12196D5

POSSIBLE SECRETS

04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
07A526C63D3E25A256A007699F5447E32AE456B50E
0307AF69989546103D79329FCC3D74880F33BBE803CB
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
3045AE6FC8422f64ED579528D38120EAE12196D5
00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A

POSSIBLE SECRETS
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
Wmw4SWNsVWhQMjvUZTN3bkxDtkpPQ014YlJsMU1tZEVMQUBTU3h4QVNGRVrRXIDd3dJzjFZNVhWRkVlbndISEFZMFJ3
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
0479BE667EF9DCBBAC55A06295CE870B07029BFCDDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
00F50B028E4D696E676875615175290472783FB1
ffffffff00000000fffffffffffffbce6faada7179e84f3b9cac2fc632551
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04
B4E134D3FB59EB8BAB57274904664D5AF50388BA
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883

POSSIBLE SECRETS
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
2AA058F73A0E33AB486B0F610410C53A7F132310
4099B5A457F9D69F79213D094C4BCD4D4262210B
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
7d7374168ffe3471b60a857686a19475d3bfa2ff
985BD3ADBAD4D696E676875615175A21B43A97E3
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
3086d221a7d46bcde86c90e49284eb15
b8adf1378a6eb73409fa6c9c637ba7f5
9760508f15230bccb292b982a2eb840bf0581cf5
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
010092537397ECA4F6145799D62B0A19CE06FE26AD

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
E95E4A5F737059DC60DF5991D45029409E60FC09
10E723AB14D696E6768756151756FEBF8FCB49A9
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
6b8cf07d4ca75c88957d9d670591
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
R0JseFhCWW9XaDRKYUc5bU1WUUhCU0ZxYWtWeU53QGuzWWNjbhnlUDJkaUdnWUxleVpvYWxVSkFpQVJYQQ
3086d221a7d46bcde86c90e49284eb153dab
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11

POSSIBLE SECRETS

26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087

5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297

4D696E676875615175985BD3ADBADA21B43A97E2

A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7

0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA

D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311

020A601907B8C953CA1481EB10512F78744A3205FD

71169be7330b3038edb025f1

040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259

00E8BEE4D3E2260744188BE0E9C723

POSSIBLE SECRETS

VnlkU0FYQW9JUTFTQUNRYmJuRVIZVzBjWjM1NIF3d3BIM01GSW10S1JVNTBIRjhFwHsUmZnd3hXaW9NY1I4bGNpOHJOVTFqYjBwa0ZoTjVMSGtwYmxZQUFVRTdSQU5TS
UFZZFB4UXFBMEpxT2pjLUNCsmlMVDhCUERWOWZDRkdQdzlmWXdCbGVBNFvUilzV21aUU55UVJlaEkzTWlkOEx4SWtGWDR3YTBZa1BpRTZhQVV5SUVKNFkxeHNheEjt
VkvZdWFTcEFLWElwQ0JNQmZEWTRkd0ZrY21sSEZXTWhTMUIOSiZaUilJHdG5YeUz0UEFGeERqNFJEU29xV0hZQ1B6Y1RlaGh2Q3pjSEYyb0tkeEINWIZJTEkxc1JLaXN3QWtFc
WFXVkNabElvSVFNaUNDOHFVbHhVWEsdWNSRkhUakk5TUEwb0VEUkZFMFpLQlYwZE1UeGVBaUjXYmhwR0I3UmVHM2tqVEFFSE5XWTFMV1prZVZRTIhVd2FYd1Y2TFF
CSUd4Vk1Pd2cyWkNzWkNRQjhIUteZSVRNWGUzQThBVDfRwKhKTFRVb1BhRklwUG0wZkxna01DMHcxWjNFNGRsVVEakFuYnlRMUpnZ2taaVo2RGIScFV4aGZGSGhDQlJ
nUWUxTUZCVnNhWmlRTGRUUIFWVzIVVNOOfhGSWRkU1FIYkQ1b2NtRVZIMTFNY3o1LVZFMWJWREIMUWtaRVFERVRGd3RIVXhzaEZGQXILanR4YWpVdkwza2RTbWR1S
0NNVFVGWVphMEl6T2tKs55UUJQbXBuTEJKQmNla2NSQmtqRkZaaEdoOWNSVIZnRWtNU0xGQUNLQnRDWGS5GQk5SOUxhRU14ZFhGMUdsaGtEMEJzTHk1SEVpd29EQ
IUzYVdabUExSWJOVDVYVYwTkxGb2hHekFHQ3hRUlHxZFKaXNER0VzRUVINTHJaWNaSXIRUGFBVmxRUzI0VXlJRVr6OWHkQklhTIR0Z0dFUmhjQjUzQUhWSIQwQmRMa
m8xVkvobkoySVNSUVPlZkY5TVISNHNFRnNyS2d3dVdnaDVOeEetVEZ4ekd3SUxUVEU3R3dNREFCWS1KeFpZTHpKME0zUmxPbDFqQUFaYlBnTU9ZMU1JWTFGLUN5SjZN
QlktZGxrbIBBc2tMRG81Q2pKN2RuZGZRZ2RkS3ISbkixOWZBVDWdoTVZRV1MxWVJHaFFMSFVCQkRGdzVUQIFpTVFFYUloWlIGQnRmWm0xVUzoMGpIMlJ4S1dsMWF3STFQ
Z3hoTIM5S0ttVvdQeDh3ZVjvWfVsVJjVFI5S1E4QlJYUkNVQmNOTEJrcWNRZ3Zjd1FKWDNaSlZ3QXRhVnhqWm1vOVh5QlJNek03SjNkdE1CUTNHsFk0WUM5QVW4NFRmb
FUxVHIBMIVRMERJMHM4ZTNrWklGMUtMa0pxUWIKN01FSmtPZ0pPV2hJMFZSWjZUUVpIVVsdIzTlliaWtSVXIRQkVWQTJiUmdVSzBvRVJ5RVIMenQ1TndWUEZRQUNMUX
hkZGhFLWR3dDFMVVizSGtWeWRRRINQMUIJzQlCxdGjTGLIEGd1TDNaRE4yeHVZV1I5WFQ0akVSOUpPV29PUnlOSIQxQjNhVIVxVENCcURWNFVUak1BWHICNE5Fa0FSVn
N5SHg1YlhHeGRHenBFRVRGRmJSMXJBWHDZUWDGREFEaE5SeGgxY2pjTfJsRlpYVWNjVke4WUGxNXRYaTVKQ1RBRVEyczZQaDvkQUR3ZGRWSnFBRVVoSIN0NE9FUKINVF
pqZHdjY056aHBGa0k5ZIFCWlpGdEVCUjRaQ1hjQVhuc09ER3dwSFU5VdnVmxkMHhYTzNOY2V4c3pOVmRoTUQ1akUzTkxmZ1Z1SUJGa2ZGOTZiMVVwSndCvEtYqTFLbT
FsRHdaVUJ4eGxjVXh1RXINQ1doRWxQZ0BHbTRiUIQxQ1lrNFRjR3Q4THdaUkl5eDdMaXm0QIZaRmZFdHdaaTBvYwKwN0xoTU5leU0zTzNsNGJteGJGSHhTTVvOeWZBWU1
OUU1IZkNNOGJRNdHVEZaVkrSfNBrsVIZbUZUYVZacldoWxjVUU6pUIVNUIdueFFaWEVYTFhBUGUwNFZMRk1oUFYxWkwxVxdHMMWNGY21abWFWaG1aUIIHUzFWeWJ
DUjNMVEpwYkd4TxxWUnJaQIFwTWhjb0ttQWtEzZVDQIVncGF6MWxaRXAwTVdSTEFFWTFLeTBSUkRKdER4Qkhad3daS0FjRk5tTThYa1kzUG1SOE5GTklDeJlYUkFkNEFSRV
ZTbDIGY0NSY05WTkJLQIZnWIRCMGZYMUZTd2RvR2p3YU5EOUtFa2xXUVdwoEZnMHRlamNNUXlOM0IzZHpa0JyVvd3QlJ3OHpTQmxNNum5JMFF4UWJPa014YIRVeFFqMV
pCWFPkKWM5Q1ICd3RUQmxKT2pSVU5VUKplbW9MV1gwWWZrUjdKVUJlU0RfCBFOGZiSEJERIFkRVfY2xMakFzQXh4TktUYzVmd1lxWjBSZVFqdHdKaWg4SUFsRlJuUm1
BMlpYZmtZVVBINHdaWDAtWTJBYWJqa1FSMzlITfJGRWFoWlPEV0pnRUdNR0pDWVJaVllxTldabE1sNWZObndQUERkWE9pNEJObFU0UHlnTUFrZENCQVEzR1dsQmVtbDB
HVzlvVWhKLWVXODBBSGhzYWo1Y2V6SXjhVlJrTVFkT09YZHBiWF1WW1ONVZnNGdkbVFPsfVsN0ZreHRVQjhuVUdrLWRnUUhRM05YV3pkWVcyd0hleWdKZm5BUklUbGJ
SVEkwU3dFaVJIUXBhbThFWDJoUFZVeDjLeWNqUJ3cEFWSXhNUlJsVGdOTVIsaC1hbHRtR3dGbVhud3hRQnBSYWhZdWNoVjZaM001V1RVZ2Jrd25PMTFISzBvd0VIZFhCb
UVoWEJBYkUxVWtjRDFtTEE4TWRBbHdiUWxTzmdwMU5VRXhMRGNyT1hWSVvtMTZiMWthRW0wUUVHSnFkVGtqYnpWb2ZsNW9iMmhpYUVKRWZTOFBZVksQWt3M2N
UVlJhSFpwZVhKZVZTVk9DamhiYUV3T1IWNudBQ3gyVG1COVhWRKjPRjVMT2pFdUpIQTRBSEltY1JvWVJdDE1DQVpWQUdaUWUxdEpjQIFDVGpCVERYQmdWazINyWtkc1V
WMDROemdZUIV4UGFGSVFSUUVYUG5oU2lyY29CMGtwVHlweFNfDfPDRtInR2IKSU5XSXZHV1ZEQnhNMUZuaE1IVIY1SudSWUZxVmxOeFFjTFdkOEfoVlJBQWxZRUVjbV
oxcEtjZ0FwUjAxeIRpUUIORzRSR3pGUIB3QkNEbGR6RXIKNvInUi1IRGRQYUF4eWJBTU1IbWM1Y1E4bmUxc1hMVnBEREZJc0h6WTRGd29ZSVFneUwwWi1FRVZtV3hskdJlb
GNIWHBUrDJ3dVkwSkFYMTThIzVd4Z1JEazNGQ01PQVZKR1p6YzdmUTHfRnpjRFNnbGZUeDRoQUUNVT2JVeHZaRFFRVUlwR0NnNHIEVzI5VIY0dWRPaGtCbUktS0FrUUtUk5
DVUpCT1IxdUtIWkRHMGS5QWlaR0NXtJFTMXBwRWOWMVRYVvVZU1jSFNvaWVEUK1jMjRnWkFFbUNGZE1RRjFJTUNrZUVqWnBCamRLZEc4b0hXWi1PWEV5SkNZVIDN
G5iSGN1TzJbDWVRNVjImkVYV1hNSFZud2dOazR6Y0dBdmNoZE9PVU55RDJRqk1YMXdSejl0YXlsX09RUjdjd2NTRj3SIRoZ1JWMFU1UTM4RVpnMG9XMHM1YVFZRIJtUNT
VDR3S3dnd0RneFBFVThyV2dwZmZ3OG9IVGNYZIZkU1FBNGpkbUpuS0V0MIJb

B99B99B099B323E02709A4D696E6768756151751

5181942b9ebc31ce68dacb56c16fd79f

POSSIBLE SECRETS
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECD A12AE6A380E62881FF2F2D82C68528AA6056583A48F3
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
UzF4YIFTUXFWaFVFSVWwVZBRjFHMVlzQUFAS0RNMmlwVKNbWRYU0NGSUItUWJmejIDWnc
D6031998D1B3BBFEBF59CC9BBFF9AEE1
b3fb3400dec5c4adceb8655d4c94
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
24B7B137C8A14D696E6768756151756FD0DA2E5C
S1FoU0tEWndWQ0IQVUFkN0tYUTJhMUZHUIJBQFRIMThTMTRSUFV4cE9YVWVCd2RER3pRME5tVQ
ae2044fb577e65ee8bb576ca48a2f06e
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
10B7B4D696E676875615175137C8A16FD0DA2211
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4

POSSIBLE SECRETS

30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303932353231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d0101040500038181005ee9be8bcb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2

D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24

3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784

03F7061798EB99E238FD6F1BF95B48FEEB4854252B

6b8cf07d4ca75c88957d9d67059037a4

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069

962eddcc369cba8ebb260ee6b6a126d9346e38c5

0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB

bb85691939b869c1d087f601554b96b80cb4f55b35f433c2

115792089210356248762697446949407573530086143415290314195533631308867097853948

VGtJaUZnWUVFRFjyWnIWRWFGaGtDaUo5TEVvUkNVUmFjMFI2UjFvRUtRSXdhMjlkUWlacWFRMU5AR2lwSE5rbFhNRnNaUjFFc0RYZ3JXUUIMU1RoaVIDczBBeTBKWnpScIhTSkRlaDh0TFZRZURHbGo

POSSIBLE SECRETS
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
401028774D7777C7B7666D1366EA432071274F89FF01E718
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
115792089237316195423570985008687907853269984665640564039457584007908834671663
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
6277101735386680763835789423207666416083908700390324961279
659EF8BA043916EEDE8911702B22
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFAFFEF2E331F296E071FA0DF9982CFEA7D43F2E
T1ZKbFZDNTVDaUZRWkZVSkR5c0BGallFSUU5V1prNHpCVGttZkY0
03E5A88919D7CAFCBF415F07C2176573B2
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3
D2C0FB15760860DEF1EEF4D696E6768756151754
UEVFU0gwNHBaMElrZHgwTERUaHZHVGHsQEV5VnpheThHQ3kxSEZuRWtiMUVCTmtzaw

POSSIBLE SECRETS
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
V3pkVEdHZ3hWSGN5VzFKaE1saEZQRzBzQ0RJQE9GZy1OaHRRSVFWYk1Id1NSem8yU0I5TmZGYw
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
85E25BFE5C86226CDB12016F7553F9D0E693A268
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
RXdOWklIRTZIR2s4ZmhnNVNWVndEUVIORVVnc1RSVWRleGNfZkRnRmVIUUBkMlozVWg1WWFrZGRFSHhMSmp3VUkzNTlmanRKS1R0MGNXUkxIVJjwSFFZ
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985
D09E8800291CB85396CC6717393284AAA0DA64BA
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xILmFuZHIjaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

POSSIBLE SECRETS
005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
8d5155894229d5e689ee01e6018a237e2cae64cd
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
e43bb460f0b80cc0c0b075798e948060f8321b7d
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
32670510020758816978083085130507043184471273380659243275938904335757337482424
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffc3d03e6dfc8ada5934242dd6d3bccca2a406cb0b
0217C05610884B63B9C6C7291678F9D341

POSSIBLE SECRETS
VnpSaVBRd2hUQlpZSFVzQ0ZnVUJjRHRMTHIFUUNGdDhGUzR0VmtOUkFFTVJAT0VZRkUycFRLWE01Y3k5d2VXeGxCRIFrUTFJLWVqUVRZWEZPUGIZeWF5Wmo
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
6C01074756099122221056911C77D77E77A777E7E7E77FCB
115792089210356248762697446949407573530086143415290314195533631308867097853951
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEFE8C2701C307E8E4C9E183115A1554062CFB
TEhwRU5qVUNhM3BoSmpOMkVFNEFSbHdJYmh0VUBIQkloRmxGbkhSTUNReE1mWTI1eUtUTjhDMzk2
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
7fffffffffffffffffffff800000cfa7e8594377d414c03821bc582063
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F

POSSIBLE SECRETS
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
c469684435deb378c4b65ca9591e2a5763059a2e
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
RINSSE1WQIJRVzIKY2tZeFNCb3NLRDVEQUFAT2tBbVJURi1MUUFxRXlvZU1laEzSaEV3ZFE
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACB F04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B
000E0D4D696E6768756151750CC03A4473D03679
470fa2b4ae81cd56ecbcda9735803434cec591fa
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
ZVR4Q1ZnTkFNUU5UWWpsQUZUUUBWazg3SIhjbFhDd3hDMWR2WmtF
3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1
6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057148

POSSIBLE SECRETS

114ca50f7a8e2f3f657c1108d9d44cfd8

48439561293906451759052585252797914202762949526041747995844080717082404635286

04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886

DB7C2ABF62E35E7628DFAC6561C5

07A11B09A76B562144418FF3FF8C2570B8

1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F

072546B5435234A422E0789675F432C89435DE5242

TVhzN0pqa29XVjh3T204aFNRWm5ZeDR4Zkr4YkFtbG9YUUZrVJGdlZVOGhVUU1oRVFAWGdsY0NGOWFQRHBSVkF0VEptOERGM0ZIRUU5MWNBWUhLVjRIZVhRTVBpcFREbk5UZmc

047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44

00BDDb97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE

0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0

22123dc2395a05caa7423daecc94760a7d462256bd56916

SmtsYUFCWIRjem9VSFVzRIhSUVILUjRZUG5JNkwzWVpma0ZZQWtkUFFoRIVAUIINZM0xtVW1BMTItYVNOcU1IVnJSWDk2RUFCVIFBSjhEVEk5YkRNbUkzMG4

04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34

POSSIBLE SECRETS

0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B

03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012

1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1

04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035D
A5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332

04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83

DB7C2ABF62E35E668076BEAD208B

0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D

12511cfe811d0f4e6bc688b4d

002757A1114D696E6768756151755316C05E0BD4

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294

31a92ee2029fd10d901b113e990710f0d21ac6b6

027d29778100c65a1da1783716588dce2b8b4aee8e228f1896

7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826

EE353FCA5428A9300D4ABA754A44C00FD FEC0C9AE4B1A1803075ED967B7BB73F

POSSIBLE SECRETS
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
127971af8721782ecffa3
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
51DEF1815DB5ED74FCC34C85D709
TzFwWUhHaHRmSGw1UkdCZEJRNDVARKNraGj4d0IFVIlCSmdrektuMU0
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27

POSSIBLE SECRETS
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
55066263022277343669578718895168534326250603453777594175500187360389116729240
003088250CA6E7C7FE649CE85820F7
FFFFFFFFE0000000075A30D1B9038A115
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
5EEEFCA380D02919DC2C6558BB6D8A5D
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3
MFkwEwYHKoZlZjOCAQYIKoZlZj0DAQcDQgAELjWEUIBX9zlm1OI4gF1hMCBLzpaBwgs9HlmSIBaQp4MDGy4ibOOV3FVDrnAY0Q34LZTbPBlp3gRNZJ19UoSy2Q==
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
308202eb30820254a00302010202044d36f7a4300d06092a864886f70d01010505003081b9310b300906035504061302383631123010060355040813094775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f7520526573656172636820616e6420446576656c6f706d656e742043656e7465723110300e0603550403130754656e63656e74301e170d3131303131393134333933325a170d3431303131313134333933325a3081b9310b300906035504061302383631123010060355040813094775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f7520526573656172636820616e6420446576656c6f706d656e742043656e7465723110300e0603550403130754656e63656e7430819f300d06092a864886f70d010101050003818d0030818902818100c05f34b231b083fb1323670bfbe7bdab40c0c0a6efc87ef2072a1ff0d60cc67c8edb0d0847f210bea6cbfaa241be70c86daf56be08b723c859e52428a064555d80db448cdacc1aea2501eba06f8bad12a4fa49d85cacd7abeb68945a5cb5e061629b52e3254c373550ee4e40cb7c8ae6f7a8151ccd8df582d446f39ae0c5e930203010001300d06092a864886f70d0101050500038181009c8d9d7f2f908c42081b4c764c377109a8b2c70582422125ce545842d5f520aea69550b6bd8bfd94e987b75a3077eb04ad341f481aac266e89d3864456e69fba13df018acdc168b9a19dfd7ad9d9cc6f6ace57c746515f71234df3a053e33ba93ece5cd0fc15f3e389a3f365588a9fcb439e069d3629cd7732a13fff7b891499

POSSIBLE SECRETS
115792089237316195423570985008687907852837564279074904382605163141518161494337
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
c49d360886e704936a6678e1139d26b7819f7e90
71169be7330b3038edb025f1d0f9
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
7167EFC92BB2E3CE7C8AAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
1243ae1b4d71613bc9f780a03690e
YVRzR1N6Sk1NM0VPQVZaUkZEb1hTQzl6TUJrQENsUnJaVUFqWEFWdmj6SWplMU56WmwwwY1gyMA
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614

POSSIBLE SECRETS
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
9162fbe73984472a0a9d0590
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7F FEFF7F2955727A
004D696E67687561517512D8F03431FCE63B88F4
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b5 47c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
e8b4011604095303ca3b8099982be09fcb9ae616
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5B D66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD1 6650
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677

POSSIBLE SECRETS
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
6127C24C05F38A0AAAF65C0EF02C
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
07B6882CAAFA84F9554FF8428BD88E246D2782AE2
00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
4E13CA542744D696E67687561517552F279A8C84
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
YXhVMEZRRmpjeEpwU0h4eU1rdE9UekINT2xvZFNuQmjWejhhY0J0Z1R5UndCRDRIR0QxbIhCY0BLbnNVY0d3V0gzTWRKdzVTV3podUxWZGxWRDA5UHdNLU14OXVlenNTT2twUWNGWjdPSHdYTERr
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5
10C0FB15760860DEF1EEF4D696E676875615175D
103FAEC74D696E676875615175777FC5B191EF30
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316

POSSIBLE SECRETS
1053CDE42C14D696E67687561517533BF3F83345
C49D360886E704936A6678E1139D26B7819F7E90
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F
e4437ed6010e88286f547fa90abfe4c42212
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
0108B39E77C4B108BED981ED0E890E117C511CF072
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
026108BABBB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
36134250956749795798585127919587881956611106672985015071877198253568414405109
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
E87579C11079F43DD824993C2CEE5ED3
36DF0AAFD8B8D7597CA10520D04B

POSSIBLE SECRETS

00689918DBEC7E5A0DD6DFC0AA55C7
036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
E95E4A5F737059DC60DFC7AD95B3D8139515620C
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
Y1JnV1IxVnlhZ1k5Wm0wTU9tOGJTeVZzQFhtdHZOQ0VYQnlsT0FrSjBXQVoxWkZZWg

POSSIBLE SECRETS
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4
040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F

PLAYSTORE INFORMATION


Title: DocMorris Pharmacy

Score: 4.5079365 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** [de.docmorris.pharmacyapp](https://play.google.com/store/apps/details?id=de.docmorris.pharmacyapp)

Developer Details: Versandapotheke DocMorris, 6501443598430079239, None, <https://www.docmorris.de>, service@docmorris.de,

Release Date: Aug 3, 2021 **Privacy Policy:** [Privacy link](#)

Description:

New: Prescription Benefit in the DocMorris App! From now on, you'll receive up to €10 credit for every e-prescription medication. The amount will be credited 14 days after your redemption and will be visible in your customer account. You can use it for payment or receive it automatically via bank transfer. For over 20 years, we have been reliably delivering a wide range of pharmacy products directly to our customers' homes. You receive over-the-counter products at particularly favourable prices. And of course, you can also redeem prescriptions with us: simply send us a classic paper prescription by mail or redeem your e-prescriptions effortlessly digitally in the app with our e-prescription scanner. THE ADVANTAGES OF THE DOCMORRIS APP - Benefit from numerous exclusive app offers, such as discounts on selected products and categories. - Redeem e-prescriptions quickly and conveniently with the e-prescription scanner. Just scan your health insurance card, order your medication and done! - ¹Order medicines and prescription drugs in the app from our partner pharmacies with DocMorris Express Delivery and receive same-day delivery (A service of DocMorris Services B.V.). The express service is currently available in selected cities and will be further expanded. - With the Online Doctor function, you can get your doctor at home conveniently and contactless via video call using the DocMorris app. Our range of over 150,000 pharmacy products offers a wide selection in the following areas: - Allergies & Intolerances - Cold & flu - Skin diseases & injuries - Smoking cessation - Painkillers - Pregnancy & Infertility - Vitamins & Minerals - Diabetic supplies - Cosmetics and much more. And that's just the beginning, because many more innovative features and promotions are planned for our app to make your experience with DocMorris even better. In the process, your well-being is important to us. That's why, if you have any questions about your orders or need pharmaceutical advice for your pharmacy shopping, you can contact our discreet and competent support team by phone or contact form. DocMorris  If you have any questions, suggestions or problems, you can contact us at any time at service@docmorris.de. _____ *The voucher can only be used as part of a digital redemption of a valid health insurance prescription in the DocMorris app (does not apply to private prescriptions, compositions and free text prescriptions). A customer account with DocMorris and a smartphone with the DocMorris app are required to redeem the voucher. Redeemable once on the entire product range (excluding infant formula and price-linked items, e.g. books) including discounted goods. Not redeemable when purchasing products from other providers via the

DocMorris online marketplace or Same Day Delivery orders. The voucher amount will first be offset against the statutory co-payment during the ordering process and then against the price of any non-prescription products ordered. Validity of the voucher promotion and code: Until 31.12.2024. Cannot be combined with other promotions or price advantages, e.g. special prices advertised exclusively via third parties. If a voucher (code) is entered, a higher price than the special price may be applied. Any voucher value exceeding the invoice amount shall be forfeited. Payment of the voucher value is excluded.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 12:58:11	Generating Hashes	OK
2025-09-01 12:58:11	Extracting APK	OK
2025-09-01 12:58:11	Unzipping	OK
2025-09-01 12:58:11	Parsing APK with androguard	OK
2025-09-01 12:58:11	Extracting APK features using aapt/aapt2	OK
2025-09-01 12:58:11	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 12:58:13	Parsing AndroidManifest.xml	OK

2025-09-01 12:58:13	Extracting Manifest Data	OK
2025-09-01 12:58:13	Manifest Analysis Started	OK
2025-09-01 12:58:14	Performing Static Analysis on: DocMorris (de.docmorris.pharmacyapp)	OK
2025-09-01 12:58:15	Fetching Details from Play Store: de.docmorris.pharmacyapp	OK
2025-09-01 12:58:17	Checking for Malware Permissions	OK
2025-09-01 12:58:17	Fetching icon path	OK
2025-09-01 12:58:17	Library Binary Analysis Started	OK
2025-09-01 12:58:17	Reading Code Signing Certificate	OK
2025-09-01 12:58:17	Running APKiD 2.1.5	OK
2025-09-01 12:58:22	Detecting Trackers	OK
2025-09-01 12:58:25	Decompiling APK to Java with JADX	OK

2025-09-01 12:58:49	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 12:58:49	Decompiling classes2.dex with JADX	OK
2025-09-01 12:58:56	Decompiling classes4.dex with JADX	OK
2025-09-01 12:58:58	Decompiling classes.dex with JADX	OK
2025-09-01 12:59:08	Decompiling classes3.dex with JADX	OK
2025-09-01 12:59:17	Decompiling classes2.dex with JADX	OK
2025-09-01 12:59:24	Decompiling classes4.dex with JADX	OK
2025-09-01 12:59:26	Decompiling classes.dex with JADX	OK
2025-09-01 12:59:35	Decompiling classes3.dex with JADX	OK
2025-09-01 12:59:44	Converting DEX to Smali	OK
2025-09-01 12:59:44	Code Analysis Started on - java_source	OK

2025-09-01 12:59:50	Android SBOM Analysis Completed	OK
2025-09-01 13:00:01	Android SAST Completed	OK
2025-09-01 13:00:01	Android API Analysis Started	OK
2025-09-01 13:00:12	Android API Analysis Completed	OK
2025-09-01 13:00:12	Android Permission Mapping Started	OK
2025-09-01 13:00:20	Android Permission Mapping Completed	OK
2025-09-01 13:00:20	Android Behaviour Analysis Started	OK
2025-09-01 13:00:34	Android Behaviour Analysis Completed	OK
2025-09-01 13:00:34	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:00:40	Email and URL Extraction Completed	OK
2025-09-01 13:00:40	Extracting String data from APK	OK

2025-09-01 13:00:40	Extracting String data from Code	OK
2025-09-01 13:00:40	Extracting String values and entropies from Code	OK
2025-09-01 13:00:45	Performing Malware check on extracted domains	OK
2025-09-01 13:01:00	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).