ANDROID STATIC ANALYSIS REPORT

Baritastic (1.9.4)

File Name:	com.baritastic.view_384.apk
Package Name:	com.baritastic.view
Scan Date:	Aug. 29, 2025, 8:05 p.m.
App Security Score:	41/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	6/432

◐ FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
6	21	2	1	1

📦 FILE INFORMATION

File Name: com.baritastic.view_384.apk
Size: 97.86MB
MD5: 22df5fa507d72382eb6be233eb1630b8
SHA1: a984af119035f47be11ff3bf9b03f6f70a9be0fc
SHA256: 42a6f20e74c6e0ec7fa8180071d815909de5688ed1be88dc4fdaee6139933e18

ℹ APP INFORMATION

App Name: Baritastic
Package Name: com.baritastic.view
Main Activity: com.baritastic.view.activity.AppIntroActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 1.9.4
Android Version Code: 384

⬛ APP COMPONENTS

Activities: 24
Services: 21
Receivers: 22
Providers: 6
Exported Activities: 1
Exported Services: 2
Exported Receivers: 6
Exported Providers: 1

✸ CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Baritastic
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-07-26 12:52:59+00:00
Valid To: 2039-07-20 12:52:59+00:00
Issuer: CN=Baritastic
Serial Number: 0x487d495
Hash Algorithm: sha256
md5: e0b5badc16582ce9ab3bd89656f91e5c
sha1: 770e1fbdb6ca13841a44f40df9d6b4d05356ec51
sha256: b82c08114067264b43bd2a5caa727f7bff11f1bc00d429ee31d3b0e97235735a
sha512: bef0bdf24aa4fac5d765693426384982f38816a7d005a1f831f5c41d363bd6824226495690f650d4edd1b8a9f92cc21f5d7f7606a168fd23d38f9a9d3557f197
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 0d4ccf4df8be25ec9d5d3846741ee797615459ce02cc8fdc3555c9d495a4cf78
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.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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
com.alarm.permission.SET_ALARM	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.

PERMISSION	STATUS	INFO	DESCRIPTION
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.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
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.
com.baritastic.view.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

🔍 APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
Compiler	r8 without marker (suspicious)

FILE	DETAILS
classes2.dex	

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE 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)

FILE	DETAILS		
classes3.dex	**FINDINGS**	**DETAILS**	
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible VM check	
	Compiler	r8 without marker (suspicious)	

🗔 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.baritastic.view.activity.AppIntroActivity	Schemes: http://, https://, baritastic://, Hosts: bariapps.page.link, openapp, Mime Types: vnd.google.fitness.data_type/com.google.step_count.cumulative, vnd.google.fitness.data_type/com.google.step_count.delta, Path Prefixes: /baritastic, /bari, Path Patterns: .*,

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

📇 CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

🔍 MANIFEST ANALYSIS

HIGH: **3** | WARNING: **12** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (com.baritastic.view.activity.auth.LoginActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	App Link assetlinks.json file not found [android:name=com.baritastic.view.activity.AppIntroActivity] [android:host=https://bariapps.page.link]	high	App Link asset verification URL (https://bariapps.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
5	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (com.baritastic.view.receivers.AlarmReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.baritastic.view.receivers.BootReminderReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	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.
11	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Broadcast Receiver (com.facebook.CampaignTrackingReceiver) 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.
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.
14	High Intent Priority (900) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
15	High Intent Priority (500) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **6** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				bolts/MeasurementEvent.java com/aigestudio/wheelpicker/WheelPicker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/cognito/clientcontext/data/UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/ApplicationDataCollector.java com/amazonaws/cognito/clientcontext/util/SignatureGenerator.java com/baritastic/view/activity/AppIntroActivity.java com/baritastic/view/activity/EnterPassCodeActivity.java com/baritastic/view/activity/FoodBarCodeScannerActivity.java com/baritastic/view/activity/FoodSettingsActivity.java com/baritastic/view/activity/JournalFullImageView.java com/baritastic/view/activity/LandingScreen.java com/baritastic/view/activity/MileStoneSplitActivity.java com/baritastic/view/activity/MyAlertDialog.java com/baritastic/view/activity/PDFLoadActivity.java com/baritastic/view/activity/ScannedBarcodeActivity.java com/baritastic/view/activity/SignUpBaseActivity.java com/baritastic/view/activity/SplashActivity.java com/baritastic/view/activity/auth/LicenseAgreementActivity.java com/baritastic/view/adapter/ExerciseAdapter.java com/baritastic/view/adapter/StrengthAdapter.java com/baritastic/view/adapter/ToDoListNewAdapter.java com/baritastic/view/adapter/ToDoListPostOpAdapter.java com/baritastic/view/adapter/ToDoListPreOpAdapter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				adapter.java com/baritastic/view/adapter/ToDoListWeightManageOpAdapter.java com/baritastic/view/barcodeNative/CameraSource.java com/baritastic/view/database/DatabaseHandler.java com/baritastic/view/database/Table_Search.java com/baritastic/view/database/Table_UserInfo.java com/baritastic/view/database/Table_Water.java com/baritastic/view/database/Table_Water_New.java com/baritastic/view/database/VitaminRemindersTable.java com/baritastic/view/database/VitaminTable.java com/baritastic/view/database/WeightNewTable.java com/baritastic/view/database/chatdatabase/MyGroupTable.java com/baritastic/view/fragments/AboutSurgeryFragment.java com/baritastic/view/fragments/AboutSurgeryMainFragment.java com/baritastic/view/fragments/AboutSurgeryNestedFragment.java com/baritastic/view/fragments/AddChecklistFragment.java com/baritastic/view/fragments/AddCustomizeMealTypeFragment.java com/baritastic/view/fragments/AddFoodDetailFragment.java com/baritastic/view/fragments/AddNewMeasurementFragment.java com/baritastic/view/fragments/AddNewTodoFragment.java com/baritastic/view/fragments/AddWeightFragment.java com/baritastic/view/fragments/AreaScaleLoginFragment.java com/baritastic/view/fragments/BMIDetailFra

NO	ISSUE	SEVERITY	STANDARDS	FILES
				gment.java com/baritastic/view/fragments/BeforeAfterDetailFragment.java com/baritastic/view/fragments/BeforeAfterListFragment.java com/baritastic/view/fragments/BeforeFullimageFragment.java com/baritastic/view/fragments/CalendarFragment.java com/baritastic/view/fragments/CalenderFilterFragment.java com/baritastic/view/fragments/ChartFragment.java com/baritastic/view/fragments/ChecklistsTabFragment.java com/baritastic/view/fragments/ContactCatFragment.java com/baritastic/view/fragments/ContactSurgenActivity.java com/baritastic/view/fragments/ContactUsDetailFragment.java com/baritastic/view/fragments/ContactUsListFragment.java com/baritastic/view/fragments/ContactUsNestedFragment.java com/baritastic/view/fragments/ContactUsSubCat1Fragment.java com/baritastic/view/fragments/ContactUsSubCat2Fragment.java com/baritastic/view/fragments/ContactUsSubCat3Fragment.java com/baritastic/view/fragments/CreateMealMainFragment.java com/baritastic/view/fragments/CreateTimeLineFragment.java com/baritastic/view/fragments/CustomizeListFragment.java com/baritastic/view/fragments/CustomizeMealTypeFragment.java com/baritastic/view/fragments/CustomizeNutritionListFragment.java com/baritastic/view/fragments/CustomizeNutritionTopFragment.java com/baritastic/view/fragments/DailyNotesAd

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/baritastic/view/fragments/DailyNotesAddEditFragment.java
				com/baritastic/view/fragments/DailyNotesCalendarFragment.java
				com/baritastic/view/fragments/DailyNotesFragment.java
				com/baritastic/view/fragments/DefaultSearchFragment.java
				com/baritastic/view/fragments/DetailNewbieFragment.java
				com/baritastic/view/fragments/DeviceFragment.java
				com/baritastic/view/fragments/DietGuidelineDetailFragment.java
				com/baritastic/view/fragments/DietGuidelineFragment.java
				com/baritastic/view/fragments/DietGuidelineNestedFragment.java
				com/baritastic/view/fragments/DietMainCatFragment.java
				com/baritastic/view/fragments/DynamicSectionCatFragment.java
				com/baritastic/view/fragments/EditFoodDetailFragment.java
				com/baritastic/view/fragments/EditInfoFragment.java
				com/baritastic/view/fragments/EditJourneyFragment.java
				com/baritastic/view/fragments/EditJourneyNewFragment.java
				com/baritastic/view/fragments/EditSurgeryFragment.java
				com/baritastic/view/fragments/ExerciseMainDetailFragment.java
				com/baritastic/view/fragments/ExerciseMainFragment.java
				com/baritastic/view/fragments/FAQDetailFragment.java
				com/baritastic/view/fragments/FAQFragment.java
				com/baritastic/view/fragments/FeedBackFragment.java
				com/baritastic/view/fragments/FitBitUserBoard.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/baritastic/view/fragments/FitbitJawbone Fragment.java
				com/baritastic/view/fragments/FoodDiaryFra gment.java
				com/baritastic/view/fragments/FoodDiaryPie ChartFragment.java
				com/baritastic/view/fragments/FoodDiaryTo pFragment.java
				com/baritastic/view/fragments/FoodListTab1. java
				com/baritastic/view/fragments/FoodListTab2. java
				com/baritastic/view/fragments/FoodListTab3. java
				com/baritastic/view/fragments/FoodListTab4. java
				com/baritastic/view/fragments/FoodMicroph oneFragment.java
				com/baritastic/view/fragments/FoodMultiple TabFragment.java
				com/baritastic/view/fragments/FoodNewTab ViewFragment.java
				com/baritastic/view/fragments/FoodSearchM ultiNewFragment.java
				com/baritastic/view/fragments/FoodSearchN ewFragment.java
				com/baritastic/view/fragments/FoodShareFra gment.java
				com/baritastic/view/fragments/ForgotPasswo rdFragment.java
				com/baritastic/view/fragments/FrequentNew ListFragment.java
				com/baritastic/view/fragments/FullGallerySh owFragment.java
				com/baritastic/view/fragments/GoalModuleF ragment.java
				com/baritastic/view/fragments/GoogleFitFrag ment.java
				com/baritastic/view/fragments/HowToUseAp pFragment.java
				com/baritastic/view/fragments/HowToUseAp pNestedFragment.java
				com/baritastic/view/fragments/HowToUseThi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sAppFragment.java com/baritastic/view/fragments/InstructionCatNewFragment.java com/baritastic/view/fragments/InstructionDetailFragment.java com/baritastic/view/fragments/InstructionFragment.java com/baritastic/view/fragments/InstructionNestedFragment.java com/baritastic/view/fragments/InvitationFragment.java com/baritastic/view/fragments/LanguageListFragment.java com/baritastic/view/fragments/LoginFragment.java com/baritastic/view/fragments/MainMenuFragment.java com/baritastic/view/fragments/MeasurementDetailFragment.java com/baritastic/view/fragments/MeasurementFragment.java com/baritastic/view/fragments/MemberPortalListFragment.java com/baritastic/view/fragments/MyAccountFragment.java com/baritastic/view/fragments/MyCreateFoodModule.java com/baritastic/view/fragments/MyCreateFoodModule2.java com/baritastic/view/fragments/NewCWaterModuleFragment.java com/baritastic/view/fragments/NewbieAppointmentFragment.java com/baritastic/view/fragments/NewbieFragment.java com/baritastic/view/fragments/NonSurgicalCatMainFragment.java com/baritastic/view/fragments/NonSurgicalDetailFragment.java com/baritastic/view/fragments/NonSurgicalNestedFragment.java com/baritastic/view/fragments/NonSurgicalWeightLossFragment.java com/baritastic/view/fragments/NutContentD

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/baritastic/view/fragments/NutContentDetailFragment.java
				com/baritastic/view/fragments/NutritionPicSubmitFragment.java
				com/baritastic/view/fragments/OnlineSeminarFragment.java
				com/baritastic/view/fragments/OurVideosFragment.java
				com/baritastic/view/fragments/OurWebsiteFragment.java
				com/baritastic/view/fragments/PDFReportFragment.java
				com/baritastic/view/fragments/PasscodeFragment.java
				com/baritastic/view/fragments/PasswordSettingFragment.java
				com/baritastic/view/fragments/PersonalInformationFragment.java
				com/baritastic/view/fragments/PhotosFragment.java
				com/baritastic/view/fragments/PreviousMeasurementFragment.java
				com/baritastic/view/fragments/PushMessageListFragment.java
				com/baritastic/view/fragments/PushNotificationFragment.java
				com/baritastic/view/fragments/QuickAddFragment.java
				com/baritastic/view/fragments/QuickAddVitaminFragment.java
				com/baritastic/view/fragments/RecipeCreatorNewFragment.java
				com/baritastic/view/fragments/RecipeDetailFragment.java
				com/baritastic/view/fragments/RecipeFavouriteListFragment.java
				com/baritastic/view/fragments/RecipeFragment.java
				com/baritastic/view/fragments/RecipeIngredientEditFragment.java
				com/baritastic/view/fragments/RecipeIngredientEditNewFragment.java
				com/baritastic/view/fragments/RecipeListFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	[The App logs information. Sensitive information should never be logged.](#)	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/baritastic/view/fragments/ResetPasswordFragment.java com/baritastic/view/fragments/ResourceFragment.java com/baritastic/view/fragments/SamsungConnectFragment.java com/baritastic/view/fragments/SaveLogRecipeEditFragement.java com/baritastic/view/fragments/SaveLogRecipeFragment.java com/baritastic/view/fragments/SelectMeasurementDateFragment.java com/baritastic/view/fragments/SettingFragment.java com/baritastic/view/fragments/SocialFragment.java com/baritastic/view/fragments/StepChallangeFragment.java com/baritastic/view/fragments/StrengthMainDetailFrament.java com/baritastic/view/fragments/StrengthMainFrament.java com/baritastic/view/fragments/SummaryModuleFragment.java com/baritastic/view/fragments/SupportCatFragment.java com/baritastic/view/fragments/SupportServicesFragment.java com/baritastic/view/fragments/SupportServicesNestedFragment.java com/baritastic/view/fragments/SurgeonConnectFragment.java com/baritastic/view/fragments/SurgeonViewProfile.java com/baritastic/view/fragments/TespoConnectLoginFragment.java com/baritastic/view/fragments/TespoDispenserFragment.java com/baritastic/view/fragments/TimerFragment.java com/baritastic/view/fragments/TimerSettingFragment.java com/baritastic/view/fragments/TrendsModuleFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eFragment.java com/baritastic/view/fragments/TrophiesFragment.java com/baritastic/view/fragments/VideoResourceFragment.java com/baritastic/view/fragments/VideoSubCategoryFragment.java com/baritastic/view/fragments/VitaminCatMainFragment.java com/baritastic/view/fragments/VitaminNestedFragment.java com/baritastic/view/fragments/VitaminSupplementFragment.java com/baritastic/view/fragments/WebViewFragment.java com/baritastic/view/fragments/WeightEditFragment.java com/baritastic/view/fragments/WeightEditNewFragment.java com/baritastic/view/fragments/WeightLogBookFragment.java com/baritastic/view/fragments/WeightMainFragment.java com/baritastic/view/fragments/WeightSettingsFragment.java com/baritastic/view/fragments/WhereYouLostFragment.java com/baritastic/view/fragments/WiFiScaleFragment.java com/baritastic/view/fragments/signUp/CheckSurgeryDateAvailableFragment.java com/baritastic/view/fragments/signUp/ConnectProgramFragment.java com/baritastic/view/fragments/signUp/HeightFragment.java com/baritastic/view/fragments/signUp/NameAndAgeFragment.java com/baritastic/view/fragments/signUp/SurgeryDateSelection.java com/baritastic/view/fragments/signUp/SurgeryFragment.java com/baritastic/view/fragments/signUp/SurgeryTypeFragment.java com/baritastic/view/fragments/signUp/Weigh

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tFragment.java com/baritastic/view/groupWorkFragments/CreateGroupFragment.java
				com/baritastic/view/groupWorkFragments/GroupAdminSettingFragment.java
				com/baritastic/view/groupWorkFragments/GroupInvitesFragment.java
				com/baritastic/view/groupWorkFragments/GroupMainFragment.java
				com/baritastic/view/groupWorkFragments/GroupMemberChatFragment.java
				com/baritastic/view/groupWorkFragments/GroupMemberSettingsFragment.java
				com/baritastic/view/groupWorkFragments/MyGroupsFragment.java
				com/baritastic/view/receivers/AlarmReceiver.java
				com/baritastic/view/services/AutomaticNotificationService.java
				com/baritastic/view/services/DrinkToEatCountDown.java
				com/baritastic/view/services/EatToEatCountDown.java
				com/baritastic/view/utils/AppUtility.java
				com/baritastic/view/utils/ApplicationController.java
				com/baritastic/view/utils/ApplicationLifecycleHandler.java
				com/baritastic/view/utils/CalUtil.java
				com/baritastic/view/utils/Helper.java
				com/baritastic/view/utils/PhotoUtility.java
				com/baritastic/view/vitaminfragment/AddReminderFragment.java
				com/baritastic/view/vitaminfragment/AddWaterReminderFragment.java
				com/baritastic/view/vitaminfragment/EditReminderFragment.java
				com/baritastic/view/vitaminfragment/EditWaterReminderFragment.java
				com/baritastic/view/vitaminfragment/VitaminMainFragment.java
				com/baritastic/view/vitaminfragment/VitaminNameFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/baritastic/view/vitaminfragment/VitaminReminderFragment.java
				com/baritastic/view/webservice/WebRequest.java
				com/baritastic/view/widget/UpdateWidgetService.java
				com/baritastic/view/widget/WidgetActivity.java
				com/bruce/pickerview/LoopView.java
				com/bumptech/glide/Glide.java
				com/bumptech/glide/disklrucache/DiskLruCache.java
				com/bumptech/glide/gifdecoder/GifHeaderParser.java
				com/bumptech/glide/gifdecoder/StandardGifDecoder.java
				com/bumptech/glide/load/data/AssetPathFetcher.java
				com/bumptech/glide/load/data/HttpUrlFetcher.java
				com/bumptech/glide/load/data/LocalUriFetcher.java
				com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
				com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java
				com/bumptech/glide/load/engine/DecodeJob.java
				com/bumptech/glide/load/engine/DecodePath.java
				com/bumptech/glide/load/engine/Engine.java
				com/bumptech/glide/load/engine/GlideException.java
				com/bumptech/glide/load/engine/SourceGenerator.java
				com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java
				com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java
				com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java
				com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				~~ com/bumptech/glide/load/engine/executor/G lideExecutor.java

com/bumptech/glide/load/engine/executor/R untimeCompat.java
com/bumptech/glide/load/engine/prefill/Bit mapPreFillRunner.java
com/bumptech/glide/load/model/ByteBuffer Encoder.java
com/bumptech/glide/load/model/ByteBuffer FileLoader.java
com/bumptech/glide/load/model/FileLoader. java
com/bumptech/glide/load/model/ResourceL oader.java
com/bumptech/glide/load/model/ResourceU riLoader.java
com/bumptech/glide/load/model/StreamEnc oder.java
com/bumptech/glide/load/resource/DefaultO nHeaderDecodedListener.java
com/bumptech/glide/load/resource/bitmap/ BitmapEncoder.java
com/bumptech/glide/load/resource/bitmap/ BitmapImageDecoderResourceDecoder.java
com/bumptech/glide/load/resource/bitmap/ DefaultImageHeaderParser.java
com/bumptech/glide/load/resource/bitmap/ Downsampler.java
com/bumptech/glide/load/resource/bitmap/ DrawableToBitmapConverter.java
com/bumptech/glide/load/resource/bitmap/ HardwareConfigState.java
com/bumptech/glide/load/resource/bitmap/T ransformationUtils.java
com/bumptech/glide/load/resource/bitmap/ VideoDecoder.java
com/bumptech/glide/load/resource/gif/Byte BufferGifDecoder.java
com/bumptech/glide/load/resource/gif/GifDr awableEncoder.java
com/bumptech/glide/load/resource/gif/Strea mGifDecoder.java
com/bumptech/glide/manager/DefaultConne

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ctivityMonitorFactory.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/github/barteksc/pdfviewer/PDFView.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/joooonho/SelectableRoundedImageView.java com/mikhaellopez/circularimageview/CircularImageView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				rImageView.java com/mine/github/mikephil/charting/charts/BarChart.java
				com/mine/github/mikephil/charting/charts/BarLineChartBase.java
				com/mine/github/mikephil/charting/charts/Chart.java
				com/mine/github/mikephil/charting/charts/CombinedChart.java
				com/mine/github/mikephil/charting/charts/HorizontalBarChart.java
				com/mine/github/mikephil/charting/charts/PieRadarChartBase.java
				com/mine/github/mikephil/charting/components/AxisBase.java
				com/mine/github/mikephil/charting/data/ChartData.java
				com/mine/github/mikephil/charting/data/CombinedData.java
				com/mine/github/mikephil/charting/data/LineDataSet.java
				com/mine/github/mikephil/charting/data/PieEntry.java
				com/mine/github/mikephil/charting/listener/BarLineChartTouchListener.java
				com/mine/github/mikephil/charting/renderer/ScatterChartRenderer.java
				com/mine/github/mikephil/charting/utils/FileUtils.java
				com/mine/github/mikephil/charting/utils/Utils.java
				com/nostra13/universalimageloader/cache/disc/impl/ext/DiskLruCache.java
				com/samsung/android/sdk/healthdata/HealthDataObserver.java
				com/samsung/android/sdk/healthdata/HealthDataStore.java
				com/samsung/android/sdk/healthdata/HealthPermissionManager.java
				com/samsung/android/sdk/internal/database/BulkCursorToCursorAdaptor.java
				com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
				com/samsung/android/sdk/internal/healthda

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ta/HealthResultHolderImpl.java com/samsung/android/sdk/internal/healthda ta/StreamUtil.java com/shockwave/pdfium/PdfiumCore.java io/realm/BaseRealm.java io/realm/DynamicRealm.java io/realm/Realm.java io/realm/RealmCache.java io/realm/RealmObject.java io/realm/RealmResults.java io/realm/internal/FinalizerRunnable.java io/realm/internal/OsRealmConfig.java io/realm/internal/RealmCore.java io/realm/internal/Util.java me/crosswall/lib/coverflow/core/CoverTransf ormer.java me/crosswall/lib/coverflow/core/LinkagePag erContainer.java me/crosswall/lib/coverflow/core/PagerContai ner.java me/dm7/barcodescanner/core/CameraPrevie w.java me/dm7/barcodescanner/zxing/ZXingScanne rView.java org/greenrobot/eventbus/Logger.java org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java
				com/amazonaws/mobileconnectors/s3/transf erutility/TransferTable.java com/baritastic/view/database/All_ExercisesTa ble.java com/baritastic/view/database/All_StrengthTa ble.java com/baritastic/view/database/CancelAlarmTa ble.java com/baritastic/view/database/CreateMealTab le.java com/baritastic/view/database/CustomizeNutT able.java com/baritastic/view/database/CustomizeTabl e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	[App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.](#)	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/baritastic/view/database/DatabaseHandler.java com/baritastic/view/database/ExerciseLogTable.java com/baritastic/view/database/FavRecipesTable.java com/baritastic/view/database/FavoriteMealTable.java com/baritastic/view/database/FoodStreakTable.java com/baritastic/view/database/JournalTable.java com/baritastic/view/database/LocalEventTable.java com/baritastic/view/database/MealSectionTable.java com/baritastic/view/database/MeasurementTable.java com/baritastic/view/database/MileStoneWeightsTable.java com/baritastic/view/database/MyRecipeTable.java com/baritastic/view/database/My_Table_Meal2.java com/baritastic/view/database/NewAdsTable.java com/baritastic/view/database/NewBieTable.java com/baritastic/view/database/NewWaterTable.java com/baritastic/view/database/NutDetailTable.java com/baritastic/view/database/Recipe_Ingredients_Table.java com/baritastic/view/database/ReminderOnFoodTable.java com/baritastic/view/database/ReminderTable.java com/baritastic/view/database/Step_CaloriesBurnTable.java com/baritastic/view/database/StrengthLogTable.java com/baritastic/view/database/Table_Goal.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/baritastic/view/database/Table_Meal2.java
				com/baritastic/view/database/Table_Search.java
				com/baritastic/view/database/Table_UserInfo.java
				com/baritastic/view/database/Table_Water.java
				com/baritastic/view/database/Table_Water_New.java
				com/baritastic/view/database/VitaminReminderDataTable.java
				com/baritastic/view/database/VitaminRemindersTable.java
				com/baritastic/view/database/VitaminScheduleTable.java
				com/baritastic/view/database/VitaminTable.java
				com/baritastic/view/database/WeightNewTable.java
				com/baritastic/view/database/WeightSettingTable.java
				com/baritastic/view/database/chatdatabase/GroupMemberTable.java
				com/baritastic/view/database/chatdatabase/GroupMessageTable.java
				com/baritastic/view/database/chatdatabase/InviteMemberTable.java
				com/baritastic/view/database/chatdatabase/MyGroupTable.java
				com/baritastic/view/database/chatdatabase/NotificationTable.java
				com/downloader/database/AppDbHelper.java
				com/downloader/database/DatabaseOpenHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/baritastic/view/activity/PDFLoadActivity.java com/baritastic/view/fragments/CreateTimeLineFragment.java com/baritastic/view/fragments/DailyNotesAddEditFragment.java com/baritastic/view/fragments/FoodShareFragment.java com/baritastic/view/fragments/NutritionPicSubmitFragment.java com/baritastic/view/fragments/PDFReportFragment.java com/baritastic/view/fragments/PhotosFragment.java com/baritastic/view/groupWorkFragments/GroupAdminSettingFragment.java com/baritastic/view/groupWorkFragments/GroupMemberSettingsFragment.java com/baritastic/view/utils/AppMediaUtils.java com/baritastic/view/utils/FileUtils.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java com/mine/github/mikephil/charting/charts/Chart.java com/mine/github/mikephil/charting/utils/FileUtils.java com/nostra13/universalimageloader/utils/StorageUtils.java
				bolts/MeasurementEvent.java com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/auth/policy/conditions/ConditionFactory.java com/amazonaws/auth/policy/conditions/S3ConditionFactory.java com/amazonaws/cognito/clientcontext/data/

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	[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	UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/DeviceDataCollector.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/amazonaws/services/s3/Headers.java com/amazonaws/services/s3/model/S3ObjectSummary.java com/baritastic/view/database/CreateMealTable.java com/baritastic/view/database/FavoriteMealTable.java com/baritastic/view/database/MyRecipeTable.java com/baritastic/view/database/My_Table_Meal2.java com/baritastic/view/database/NutDetailTable.java com/baritastic/view/database/Recipe_Ingredients_Table.java com/baritastic/view/database/Table_Goal.java com/baritastic/view/database/Table_Meal2.java com/baritastic/view/database/VitaminReminderDataTable.java com/baritastic/view/fragments/LoginFragment.java com/baritastic/view/modals/NT_Constants.java com/baritastic/view/preferences/PreferenceUtils.java com/baritastic/view/utils/AppConstant.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/baritastic/view/activity/PDFLoadActivity.java com/baritastic/view/webservice/EasyX509TrustManager.java com/baritastic/view/webservice/WebRequest.java
6	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	bolts/WebViewAppLinkResolver.java com/baritastic/view/fragments/AreaScaleLoginFragment.java com/baritastic/view/fragments/FitbitJawboneFragment.java
7	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/amazonaws/services/s3/AmazonS3Client.java com/amazonaws/services/s3/internal/MD5DigestCalculatingInputStream.java com/amazonaws/util/Md5Utils.java com/downloader/utils/Utils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/amazonaws/retry/PredefinedRetryPolicies.java com/baritastic/view/activity/LandingScreen.java com/baritastic/view/activity/SplashActivity.java com/baritastic/view/fragments/CreateTimeLineFragment.java com/baritastic/view/fragments/FoodDiaryFragment.java com/baritastic/view/fragments/NewbieAppointmentFragment.java com/baritastic/view/fragments/PhotosFragment.java com/baritastic/view/receivers/AlarmReceiver.java com/baritastic/view/receivers/TimerAlarmReceiver.java com/baritastic/view/vitaminfragment/AddWaterReminderFragment.java com/baritastic/view/vitaminfragment/EditWaterReminderFragment.java com/baritastic/view/vitaminfragment/VitaminMainFragment.java com/baritastic/view/widget/UpdateWidgetService.java
9	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/amazonaws/services/s3/internal/crypto/EncryptionUtils.java com/baritastic/view/utils/AppUtility.java
10	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/joooonho/BuildConfig.java

🏳 SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__strcat_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__strcat_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi-v7a/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	armeabi-v7a/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	armeabi/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	armeabi/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	armeabi/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	armeabi/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	x86/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	mips/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	mips/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	mips/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	mips/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	arm64-v8a/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	arm64-v8a/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	arm64-v8a/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	arm64-v8a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__strcat_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
33	arm64-v8a/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	x86_64/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	x86_64/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	x86_64/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	x86_64/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__strcat_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	x86_64/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	armeabi-v7a/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	armeabi-v7a/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANANY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	armeabi-v7a/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
42	armeabi-v7a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	armeabi-v7a/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
44	armeabi/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
45	armeabi/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	armeabi/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	armeabi/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
48	x86/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	x86/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
50	x86/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
51	x86/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
52	x86/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
53	mips/libmodpng.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
54	mips/libjniPdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	mips/libmodpdfium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
56	mips/libmodft2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

🪪 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

⛓ BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	bolts/AppLinkNavigation.java bolts/AppLinks.java bolts/MeasurementEvent.java com/baritastic/view/activity/LandingScreen.java com/baritastic/view/activity/MyAlertDialog.java com/baritastic/view/activity/auth/LoginActivity.java com/baritastic/view/activity/auth/SignUpActivity.java com/baritastic/view/fragments/AboutSurgeryFragment.java com/baritastic/view/fragments/AboutSurgeryMainFragment.java com/baritastic/view/fragments/ContactUsDetailFragment.java com/baritastic/view/fragments/FAQFragment.java com/baritastic/view/fragments/HowToUseAppFragment.java com/baritastic/view/fragments/HowToUseAppNestedFragment.java com/baritastic/view/fragments/HowToUseThisAppFragment.java com/baritastic/view/fragments/OnlineSeminarFragment.java com/baritastic/view/fragments/OurVideosFragment.java com/baritastic/view/fragments/OurWebsiteFragment.java com/baritastic/view/fragments/ResourceFragment.java com/baritastic/view/fragments/SocialFragment.java com/baritastic/view/fragments/SurgeonConnectFragment.java com/baritastic/view/fragments/SurgeonViewProfile.java com/baritastic/view/fragments/VideoCategoryFragment.java com/baritastic/view/fragments/VideoMainCategoryFragment.java com/baritastic/view/fragments/VideoResourceFragment.java com/baritastic/view/fragments/VideoSubCategoryFragment.java com/baritastic/view/fragments/VitaminCatMainFragment.java com/baritastic/view/fragments/VitaminSupplementFragment.java com/baritastic/view/fragments/signUp/ConnectProgramFragment.java com/baritastic/view/receivers/AlarmReceiver.java com/baritastic/view/receivers/TimerAlarmReceiver.java com/baritastic/view/utils/AppUtility.java com/samsung/android/sdk/healthdata/HealthConnectionErrorResult.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	bolts/AppLinkNavigation.java com/baritastic/view/activity/LandingScreen.java com/baritastic/view/activity/auth/LoginActivity.java com/baritastic/view/activity/auth/SignUpActivity.java com/baritastic/view/fragments/AboutSurgeryFragment.java com/baritastic/view/fragments/AboutSurgeryMainFragment.java com/baritastic/view/fragments/ContactUsDetailFragment.java com/baritastic/view/fragments/FAQFragment.java com/baritastic/view/fragments/HowToUseAppNestedFragment.java com/baritastic/view/fragments/HowToUseThisAppFragment.java com/baritastic/view/fragments/OurVideosFragment.java com/baritastic/view/fragments/OurWebsiteFragment.java com/baritastic/view/fragments/ResourceFragment.java com/baritastic/view/fragments/SurgeonConnectFragment.java com/baritastic/view/fragments/SurgeonViewProfile.java com/baritastic/view/fragments/VideoSubCategoryFragment.java com/baritastic/view/fragments/VitaminCatMainFragment.java com/baritastic/view/fragments/VitaminSupplementFragment.java com/baritastic/view/fragments/signUp/ConnectProgramFragment.java com/baritastic/view/utils/AppUtility.java
00036	Get resource file from res/raw directory	reflection	bolts/AppLinkNavigation.java bolts/MeasurementEvent.java com/amazonaws/mobileconnectors/s3/transferutility/TransferDBBase.java com/baritastic/view/receivers/AlarmReceiver.java com/baritastic/view/utils/AppUtility.java
00091	Retrieve data from broadcast	collection	com/baritastic/view/activity/AppIntroActivity.java com/baritastic/view/activity/LandingScreen.java com/baritastic/view/activity/SplashActivity.java
00096	Connect to a URL and set request method	command network	com/amazonaws/http/UrlHttpClient.java com/baritastic/view/utils/ApiUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	bolts/WebViewAppLinkResolver.java com/amazonaws/http/UrlHttpClient.java com/amazonaws/util/HttpUtils.java com/baritastic/view/customview/SecureImageDownloader.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/downloader/httpclient/DefaultHttpClient.java com/nostra13/universalimageloader/core/download/BaseImageDownloader.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00109	Connect to a URL and get the response code	network command	bolts/WebViewAppLinkResolver.java com/amazonaws/http/UrlHttpClient.java com/amazonaws/util/HttpUtils.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/downloader/httpclient/DefaultHttpClient.java com/nostra13/universalimageloader/core/download/BaseImageDownloader.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00094	Connect to a URL and read data from it	command network	bolts/WebViewAppLinkResolver.java com/amazonaws/http/UrlHttpClient.java com/baritastic/view/customview/FileDownloader.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00108	Read the input stream from given URL	network command	bolts/WebViewAppLinkResolver.java com/amazonaws/http/UrlHttpClient.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	android/print/PdfDocumentAdapter.java com/amazonaws/auth/PropertiesCredentials.java com/amazonaws/internal/ReleasableInputStream.java com/amazonaws/internal/ResettableInputStream.java com/amazonaws/regions/RegionUtils.java com/amazonaws/services/s3/internal/RepeatableFileInputStream.java com/amazonaws/services/s3/internal/ServiceUtils.java com/amazonaws/util/Md5Utils.java com/baritastic/view/fragments/CreateTimeLineFragment.java com/baritastic/view/fragments/PhotosFragment.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/getkeepsafe/relinker/elf/ElfParser.java com/nostra13/universalimageloader/cache/disc/impl/ext/DiskLruCache.java com/nostra13/universalimageloader/core/download/BaseImageDownloader.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java okio/Okio.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java
00030	Connect to the remote server through the given URL	network	bolts/WebViewAppLinkResolver.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/downloader/httpclient/DefaultHttpClient.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/amazonaws/auth/PropertiesCredentials.java com/amazonaws/mobileconnectors/s3/transfermanager/TransferManager.java com/amazonaws/mobileconnectors/s3/transfermanager/internal/DownloadImpl.java com/amazonaws/mobileconnectors/s3/transferutility/TransferDBUtil.java com/amazonaws/mobileconnectors/s3/transferutility/TransferObserver.java com/amazonaws/services/s3/internal/ServiceUtils.java com/baritastic/view/activity/PDFLoadActivity.java com/baritastic/view/fragments/CreateTimeLineFragment.java com/baritastic/view/fragments/NutritionPicSubmitFragment.java com/baritastic/view/fragments/PhotosFragment.java com/baritastic/view/groupWorkFragments/GroupAdminSettingFragment.java com/baritastic/view/groupWorkFragments/GroupMemberSettingsFragment.java com/baritastic/view/utils/AppUtility.java com/baritastic/view/utils/FileUtils.java com/getkeepsafe/relinker/ReLinkerInstance.java com/github/mikephil/charting/charts/Chart.java com/mine/github/mikephil/charting/charts/Chart.java com/nostra13/universalimageloader/cache/disc/impl/BaseDiskCache.java com/nostra13/universalimageloader/core/LoadAndDisplayImageTask.java io/realm/RealmConfiguration.java io/realm/internal/OsRealmConfig.java io/realm/internal/OsSharedRealm.java io/realm/internal/Util.java
00012	Read data and put it into a buffer stream	file	com/amazonaws/util/Md5Utils.java com/nostra13/universalimageloader/core/download/BaseImageDownloader.java
00121	Create a directory	file command	com/baritastic/view/fragments/CreateTimeLineFragment.java com/baritastic/view/fragments/DailyNotesAddEditFragment.java com/baritastic/view/fragments/NutritionPicSubmitFragment.java com/baritastic/view/fragments/PhotosFragment.java com/baritastic/view/groupWorkFragments/GroupAdminSettingFragment.java com/baritastic/view/groupWorkFragments/GroupMemberSettingsFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/baritastic/view/fragments/CreateTimeLineFragment.java com/baritastic/view/fragments/DailyNotesAddEditFragment.java com/baritastic/view/fragments/NutritionPicSubmitFragment.java com/baritastic/view/fragments/PDFReportFragment.java com/baritastic/view/fragments/PhotosFragment.java com/baritastic/view/groupWorkFragments/GroupAdminSettingFragment.java com/baritastic/view/groupWorkFragments/GroupMemberSettingsFragment.java
00112	Get the date of the calendar event	collection calendar	com/baritastic/view/activity/LandingScreen.java com/baritastic/view/fragments/FoodDiaryFragment.java com/baritastic/view/fragments/GoogleFitFragment.java com/baritastic/view/fragments/MainMenuFragment.java com/baritastic/view/fragments/NewbieAppointmentFragment.java com/baritastic/view/fragments/PDFReportFragment.java com/baritastic/view/fragments/SamsungConnectFragment.java com/baritastic/view/utils/AppUtility.java com/baritastic/view/vitaminfragment/AddWaterReminderFragment.java com/baritastic/view/vitaminfragment/EditWaterReminderFragment.java
00009	Put data in cursor to JSON object	file	com/amazonaws/mobileconnectors/s3/transferutility/TransferUtility.java com/baritastic/view/database/FavoriteMealTable.java com/baritastic/view/fragments/DailyNotesAddEditFragment.java com/baritastic/view/fragments/MainMenuFragment.java com/baritastic/view/fragments/PhotosFragment.java com/baritastic/view/fragments/SamsungConnectFragment.java com/baritastic/view/groupWorkFragments/GroupAdminSettingFragment.java com/baritastic/view/groupWorkFragments/GroupMemberSettingsFragment.java
00031	Check the list of currently running applications	reflection collection	com/baritastic/view/utils/AppUtility.java
00191	Get messages in the SMS inbox	sms	com/baritastic/view/utils/AppUtility.java
00123	Save the response to JSON after connecting to the remote server	network command	bolts/WebViewAppLinkResolver.java

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	com/baritastic/view/groupWorkFragments/GroupAdminSettingFragment.java com/baritastic/view/groupWorkFragments/GroupMemberSettingsFragment.java
00005	Get absolute path of file and put it to JSON object	file	com/baritastic/view/fragments/PhotosFragment.java com/baritastic/view/groupWorkFragments/GroupAdminSettingFragment.java com/baritastic/view/groupWorkFragments/GroupMemberSettingsFragment.java
00078	Get the network operator name	collection telephony	com/amazonaws/cognito/clientcontext/datacollection/TelephonyDataCollector.java
00034	Query the current data network type	collection network	com/amazonaws/cognito/clientcontext/datacollection/TelephonyDataCollector.java
00065	Get the country code of the SIM card provider	collection	com/amazonaws/cognito/clientcontext/datacollection/TelephonyDataCollector.java
00202	Make a phone call	control	com/baritastic/view/fragments/ContactUsDetailFragment.java com/baritastic/view/fragments/SurgeonViewProfile.java
00203	Put a phone number into an intent	control	com/baritastic/view/fragments/ContactUsDetailFragment.java com/baritastic/view/fragments/SurgeonViewProfile.java
00014	Read file into a stream and put it into a JSON object	file	com/baritastic/view/fragments/PhotosFragment.java
00004	Get filename and put it to JSON object	file collection	com/baritastic/view/webservice/WebRequest.java
00002	Open the camera and take picture	camera	com/baritastic/view/barcodeNative/CameraSource.java
00183	Get current camera parameters and change the setting.	camera	com/baritastic/view/barcodeNative/CameraSource.java me/dm7/barcodescanner/core/BarcodeScannerView.java me/dm7/barcodescanner/core/CameraPreview.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/amazonaws/mobileconnectors/s3/transferutility/TransferDBUtil.java

🗄 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://vaulted-aleph-652.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/453840267901/namespaces/firebase:fetch?key=AIzaSyCDJmbClTBicoUvbYQnUPSUuH9k3UGQO8o is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'android_update_info': '{"production":{"enabled":true,"live_version":"375","force_update":true,"message":"We have a new required update. Please update your app to continue."},"staging":{"enabled":false,"live_version":"345","force_update":false,"message":"We have a new required update. Please update your app to continue. (Staging)"}}', 'ios_update_info': '{"production":{"enabled":true,"live_version":"3.70","force_update":true,"message":"We have a new required update. Please update your app to continue."},"staging":{"enabled":false,"live_version":"3.47","force_update":false,"message":"We have a new required update. Please update your app to continue."}}'}, 'state': 'UPDATE', 'templateVersion': '283'}

⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.CAMERA, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WAKE_LOCK, android.permission.GET_TASKS, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	8/44	android.permission.FLASHLIGHT, android.permission.READ_CALENDAR, android.permission.CALL_PHONE, android.permission.ACTIVITY_RECOGNITION, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

❗ OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
s3-us-west-1.amazonaws.com	ok	**IP:** 52.219.192.24 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.baritastic.com	ok	**IP:** 172.64.149.150 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
obesitycoverage.com	ok	**IP:** 141.193.213.11 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
prod-v2.bariapps.com	ok	**IP:** 18.189.75.186 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map
docs.google.com	ok	**IP:** 173.194.219.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.nutritionix.com	ok	No Geolocation information available.
smilebariatric.com	ok	**IP:** 162.159.134.42 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.ngs.ac.uk	ok	**IP:** 130.246.140.235 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Appleton **Latitude:** 51.709511 **Longitude:** -1.361360 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bariapps.com	ok	**IP:** 18.189.75.186 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** [Google Map](#)
baritastic-smile-production.s3.us-east-2.amazonaws.com	ok	**IP:** 3.5.131.229 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** [Google Map](#)
hub.samsungapps.com	ok	**IP:** 54.77.39.19 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** [Google Map](#)
vaulted-aleph-652.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)
stage.bariapps.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
s3.amazonaws.com	ok	**IP:** 54.231.192.232 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
trackapi.nutritionix.com	ok	**IP:** 23.21.36.233 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
docs.mongodb.com	ok	**IP:** 15.197.167.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.bariapps.com	ok	**IP:** 18.189.75.186 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stage-v2.bariapps.com	ok	**IP:** 18.188.149.17 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map
acs.amazonaws.com	ok	No Geolocation information available.
realm.io	ok	**IP:** 13.224.53.90 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.amazon.com	ok	**IP:** 23.204.249.185 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
baritastic-smile-staging.s3.us-east-2.amazonaws.com	ok	**IP:** 52.219.99.82 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map

✉ EMAILS

EMAIL	FILE
info@bariapps.com	com/baritastic/view/utils/AppConstant.java
email@mailinator.com	com/baritastic/view/fragments/EditInfoFragment.java
grams0@mailinator.com	com/baritastic/view/fragments/LoginFragment.java
app@baritastic.com	com/baritastic/view/fragments/SurgeonConnectFragment.java
app@baritastic.com	com/baritastic/view/activity/auth/SignUpActivity.java
app@baritastic.com	com/baritastic/view/activity/auth/LoginActivity.java

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Clave"
"com_facebook_device_auth_instructions" : "□□□facebook.com/device□□□□□□□□"
"google_api_key" : "AIzaSyCDJmbClTBicoUvbYQnUPSUuH9k3UGQO8o"
"user_name" : "Username"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_crash_reporting_api_key" : "AIzaSyCDJmbClTBicoUvbYQnUPSUuH9k3UGQO8o"
"password" : "Password"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□□"
"firebase_database_url" : "https://vaulted-aleph-652.firebaseio.com"

POSSIBLE SECRETS

308204a830820390a003020102020900936eacbe07f201df300d06092a864886f70d0101050500308194310b3009060355040613025553311330110603550408130a43616c69666f7
26e69613116301406035504070713d0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f6964110300e060355040b1307416e64726f6964110300e060355040
31307416e64726f69643122302006092a864886f70d0109011613616e64726f6964616e64726f69642e636f6d301e170d30383032323930313333334365a170d33353037373137303
1333334365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504070713d0d4d6f756e7461696e20566965773110300e0603
55040a1307416e64726f6964110300e060355040b1307416e64726f6964110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f69644
0616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d003082010802820101008206931904dec60b24b1edc762e0d9d8253e3ecd6ceb1de2ff068ca8e8
bca8cd6bd3786ea70aa76ce60ebb0f993559ffd93e77a943e7e83d4b64b8e4fea2d3e656f1e267a81bbfb230b578c20443be4c7218b846f5211586f038a14e89c2be387f8ebecf8fcac3
da1ee330c9ea93d0a7c3dc4af350220d50080732e0809717ee6a053359e6a694ec2cb3f284a0a466c87a94d83b31093a67372e2f6412c06e6d42f15818dffe0381cc0cd444da6cddc3b
82458194801b32564134fbfde98c9287748dbf5676a540d8154c8bbca07b9e247553311c46b9af76fdeeccc8e69e7c8a2d08e782620943f99727d3c04fe72991d99df9bae38a0b2177f
a31d5b6afee91f020103a381fc3081f9301d0603551d0e04160414485900563d272c46ae118605a47419ac09ca8c113081c90603551d230481c13081be8014485900563d272c46ae1
18605a47419ac09ca8c11a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504070713d0d4d6f756e7461696
e20566965773110300e060355040a1307416e64726f6964110300e060355040b1307416e64726f6964110300e06035504031307416e64726f69643122302006092a864886f70d0
109011613616e64726f6964616e64726f69642e636f6d820900936eacbe07f201df300c0603551d13040530030101ff300d06092a864886f70d0101050500038201010007aaf968ceb
50c441055118d0daabaf015b8a765a27a715a2c2b44f221415ffdace03095abfa42df70708726c2069e5c36eddae0400be29452c084bc27eb6a17eac9dbe182c204eb15311f455d824
b656dbe4dc2240912d7586fe88951d01a8feb5ae5a4260535df83431052422468c36e22c2a5ef994d61dd7306ae4c9f6951ba3c12f1d1914ddc61f1a62da2df827f603fea5603b2c540
dbd7c019c36bab29a4271c117df523cdbc5f3817a49e0efa60cbd7f74177e7a4f193d43f4220772666e4c4d83e1bd5a86087cf34f2dec21e245ca6c2bb016e683638050d2c430eea7c2
6a1c49d3760a58ab7f1a82cc938b4831384324bd0401fa12163a50570e684d

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

470fa2b4ae81cd56ecbcda9735803434cec591fa

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

ce8295cb41d41e79c0df0af860136332

ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

5e8f16062ea3cd2c4a0d547876baa6f38cabf625

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

9b8f518b086098de3d77736f9458a3d2f6f95a37

7a5b85d3ee2e0991ca3502602e9389a98f55c0576b887125894a7ec03823f8d3

POSSIBLE SECRETS

7724d616fb03de975c6b837c4cf8592d

2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

308204a830820390a003020102020900b3998086d056cffa300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f
726e69613116301406035504071307134d4f756e7461696e2056696577311130030e060355040a1307416e64726f6964311030 0e060355040b1307416e64726f6964311030 0e06035504
031307416e64726f696431122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303034313532323430353035305a170d333530393031323
2343035305a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 0d4d6f756e7461696e2056566965773110300e060
355040a1307416e64726f69643110300e060355040b1307416e64726f6964311030 0e06035504031307416e64726f696431122302006092a864886f70d0109011613616e64726f6964
40616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d003082010802820101009c780592ac0d5d381cdeaa65ecc8a6006e36480c6d7207b12011be
50863aabe2b55d009adf7146d6f2202280c7cd4d7bdb26243b8a806c26b34b137523a49268224904dc01493e7c0acf1a05c874f69b037b60309d9074d24280e16bad2a8734361951
eaf72a482d09b204b1875e12ac98c1aa773d6800b9eafde56d58bed8e8da16f9a360099c37a834a6dfedb7b6b44a049e07a269fccf2c5496f2cf36d64df90a3b8d8f34a3baab4cf53371
ab27719b3ba58754ad0c53fc14e1db45d51e234fbbe93c9ba4edf9ce54261350ec535607bf69a2ff4aa07db5f7ea200d09a6c1b49e21402f89ed1190893aab5a9180f152e82f85a4575
3cf5fc19071c5eec827020103a381fc3081f9301d0603551d0e041604144fe4a0b3dd9cba29f71d7287c4e7c38f2086c2993081c90603551d230481c13081be80144fe4a0b3dd9cba29f
71d7287c4e7c38f2086c299a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 0d4d6f756e74616
96e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f6964311030 0e06035504031307416e64726f696431122302006092a864886f70
d0109011613616e64726f696440616e64726f69642e636f6d820900b3998086d056cffa300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010057255 1b
8d93a1f73de0f6d469f86dad6701400293c88a0cd7cd778b73dafcc197fab76e6212e56c1c761cfc42fd733de52c50ae08814cefc0a3b5a1a4346054d829f1d82b42b2048bf88b5d1492
9ef85f60edd12d72d55657e22e3e85d04c831d613d19938bb8982247fa321256ba12d1d6a8f92ea1db1c373317ba0c037f0d1aff645aef224979fba6e7a14bc025c71b98138cef3ddfc
059617cf24845cf7b40d6382f7275ed738495ab6e5931b9421765c491b72fb68e080dbdb58c2029d347c8b328ce43ef6a8b15533edfbe989bd6a48dd4b202eda94c6ab8dd5b839920
3daae2ed446232e4fe9bd961394c6300e5138e3cfd285e6e4e483538cb8b1b357

3071c8717539de5d5353f4c8cd59a032

cc2751449a350f668590264ed76692694a80308a

7d73d21f1bd82c9e5268b6dcf9fde2cb

POSSIBLE SECRETS

308204d4308203bca003020102020900d20995a79c0daad6300d06092a864886f70d01010505003081a2310b3009060355040613024b523114301206035504081305036f7574682
04b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115
301306035504031300c53616d73756e67204365727443125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d3131303632323132
323531325a170d3338313130373132323531325a3081a2310b3009060355040613024b5231143012060355040813050536f757468204b6f726561311330110603550407130a53757
76f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d4331153013060355040313000c53616d73756e6720436
572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d0030820108028201
0100c986384a3e1f2fb206670e78ef232215c0d26f45a22728db99a44da11c35ac33a71fe071c4a2d6825a9b4c88b333ed96f3c5e6c666d60f3ee94c490885abcf8dc660f707aabc77ea
d3e2d0d8aee8108c15cd260f2e85042c28d2f292daa3c6da0c7bf2391db7841aade8fdf0c9d0defcf77124e6d2de0a9e0d2da746c3670e4ffcdc85b701bb4744861b96ff7311da3603c5
a10336e55ffa34b4353eedc85f51015e1518c67e309e39f87639ff178107f109cd18411a6077f26964b6e63f8a70b9619db04306a323c1a1d23af867e19f14f570ffe573d0e3a0c2b3063
2aaec3173380994be1e341e3a90bd2e4b615481f46db39ea83816448ec35feb1735c1f3020103a382010b30820107301d0603551d0e04160414932c3af70b627a0c7610b5a0e7427d
6cfaea3f1e3081d70603551d230481cf3081cc8014932c3af70b627a0c7610b5a0e7427d6cfaea3f1ea181a8a481a53081a2310b3009060355040613024b523114301206035504081305
0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1
303444d4331153013060355040313000c53616d73756e67204365727443125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900d2099
5a79c0daad6300c0603551d13040530030101ff300d06092a864886f70d01010505000382010100329601fe40e036a4a86cc5d49dd8c1b5415998e72637538b0d430369ac51530f63
aace8c019a1a66616a2f1bb2c5fabd6f313261f380e3471623f053d9e3c53f5fd6d1965d7b000e4dc244c1b27e2fe9a323ff077f52c4675e86247aa801187137e30c9bbf01c567a4299d
b4bf0b25b7d7107a7b81ee102f72ff47950164e26752e114c42f8b9d2a42e7308897ec640ea1924ed13abbe9d120912b62f4926493a86db94c0b46f44c6161d58c2f648164890c512d
fb28d42c855bf470dbee2dab6960cad04e81f71525ded46cdd0f359f99c460db9f007d96ce83b4b218ac2d82c48f12608d469733f05a3375594669ccbf8a495544d6c5701e9369c08c8
10158

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

POSSIBLE SECRETS

308204d4308203bca003020102020900e5eff0a8f66d92b3300d06092a864886f70d01010505003081a2310b3009060355040613024b5231143012060355040813b536f75746820 4b6f7265561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d4331153 0130603550403130c53616d73756e67204365727427431253023060920086092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d31313036323231323 23531335a170d3338313130373132323531335a3081a2310b3009060355040613024b5231143012060355040813b536f757468204b6f7265561311330110603550407130a53757577 6f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d4331153013060355040313c53616d73756e6672043657 27431253023060920086092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010 100e9f1edb42423201dce62e68f2159ed8ea766b43a43d348754841b72e9678ce6b03d06d31532d88f2ef2d5ba39a028de0857983cd321f5b7786c2d3699df4c0b40c8d856f147c5dc 54b9d1d671d1a51b5c5364da36fc5b0fe825afb513ec7a2db862c48a6046c43c3b71a1e275155f6c30aed2a68326ac327f60160d427cf55b617230907a84edbff21cc256c628a16f15d5 5d49138cdf2606504e1591196ed0bdc25b7cc4f67b33fb29ec4dbb13dbe6f3467a0871a49e620067755e6f095c3bd84f8b7d1e66a8c6d1e5150f7fa9d95475dc7061a321aaf9c686b09 be23ccc59b35011c6823ffd5874d8fa2a1e5d276ee5aa381187e26112c7d5562703b36210b020103a382010b30820107301d0603551d0e041604145b115b23db35655f9f77f787569 61006eebe3a9e3081d70603551d230481cf3081cc80145b115b23db35655f9f77f78756961006eebe3a9ea181a8a481a53081a2310b3009060355040613024b52311430120603550 408130b536f757468204b6f7265561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355 040b1303444d4331153013060355040313c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e6672636f6d820900 e5eff0a8f66d92b3300c0603551d13040530030101ff300d06092a864886f70d0101050500038201010039c91877eb09c2c84445443673c77a1219c5c02e6552fa2fbad0d736bc5ab6e baf0375e520fe9799403ecb71659b23afda1475a34ef4b2e1ffcba8d7ff385c21cb6482540bce3837e6234fd4f7dd576d7fcfe9cfa925509f772c494e1569fe44e6fcd4122e483c2caa2c63 9566dbcfe85ed7818d5431e73154ad453289fb56b607643919cf534fbeefbdc2009c7fcb5f9b1fa97490462363fa4bedc5e0b9d157e448e6d0e7cfa31f1a2faa9378d03c8d1163d3803b c69bf24ec77ce7d559abcaf8d345494abf0e3276f0ebd2aa08e4f4f6f5aaea4bc523d8cc8e2c9200ba551dd3d4e15d5921303ca9333f42f992ddb70c2958e776c12d7e3b7bd74222eb5 c7a

308201e53082014ea00302010202044f54468b300d06092a864886f70d01010505003037310b3009060355040613025553311030e060355040a1307416e64726f696443116301406 03550403130d416e64726f696420446562756730301e170d31323033330353034353232375a170d3432303232363034353232375a3037310b30090603550406130255533110300e060 355040a1307416e64726f69643116301406035504031300d416e64726f69642044656275673019f300d06092a864886f70d010101050003818d00308189028181008a53be36d02be fe1d152724281630bd1c42eff0edf5fdca8eb944f536ab3f54dca9b22cfb421b37706a4ad259101815723202b359250cf6c59905032798273462bfa3f9f1881f7475ee5b25849edefac81 085815f42383a44cb2be1bfd5c1f049ef42f5818f35fe0b1131c769cee347d558395a5fa87c3d425b2b9c819cf91870203010001300d06092a864886f70d0101050500038181000051299 92268a01e0941481931f3f9b6647fbe25ee0bc9648f35d56c55f8cfa6c935fb3d435125fd60ef566769ac7e64fe2823409461ca7a04570c43baaab3fb877bf3a6a8dd9ef7e69944f65b0e 5e36f2ac2bf085fdeda063898855ea2ce84c60655d824844fe1659a77c12604c3fb84d41df6f1a7705a1b9962ac2fdc9933122

g72o7uAglSVKXfM0gZlmeyIUuBrmOHfP

▶ PLAYSTORE INFORMATION

Title: Baritastic - Bariatric Tracker

Score: 4.741274 **Installs:** 500,000+ **Price:** 0 **Android Version Support: Category:** Medical **Play Store URL:** com.baritastic.view

Developer Details: BariApps, BariApps, None, http://www.baritastic.com, info@bariapps.com,

Release Date: Sep 4, 2014 **Privacy Policy:** Privacy link

Description:

Baritastic is the # 1 app for bariatric surgery! Baritatric surgery patients have specific goals, requirements and guidelines before and after surgery. And now there is a free app specifically built for bariatric surgery. * Nutrition and Water Tracking * Reminders - Vitamins, Water, Protein Shakes, Meals, Other * Bariatric Food, Water, and Bite Timer * Patient Journal - Log thoughts, take pics, rate your hunger an happiness. * Newbie Checklist - Stay on task and get to surgery. * Bariatric Specific Recipes * Bariatric Specific Resources * Baritastic Social Support Group * Connect to YOUR Bariatric Program Through the Baritastic App * and more! Whether you are considering weight loss surgery or are already losing weight, this app is for you. Lap Band, gastric bypass, gastric sleeve, gastric balloon, duodenal switch - it's all here. Notes: We are always improving the app and appreciate your feedback. You can now connect to your bariatric program via the app. Once connected, you'll have access to your discharge instructions, support group calendar, diet guidelines, key contacts, and much more. If your bariatric program hasn't given you a code, ask them for one or tell them about Baritastic and we'll get them set-up.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:05:55	Generating Hashes	OK
2025-08-29 20:05:55	Extracting APK	OK
2025-08-29 20:05:55	Unzipping	OK
2025-08-29 20:05:56	Parsing APK with androguard	OK
2025-08-29 20:05:56	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:05:56	Getting Hardcoded Certificates/Keystores	OK

2025-08-29 20:06:00	Parsing AndroidManifest.xml	OK
2025-08-29 20:06:00	Extracting Manifest Data	OK
2025-08-29 20:06:00	Manifest Analysis Started	OK
2025-08-29 20:06:00	Performing Static Analysis on: Baritastic (com.baritastic.view)	OK
2025-08-29 20:06:01	Fetching Details from Play Store: com.baritastic.view	OK
2025-08-29 20:06:02	Checking for Malware Permissions	OK
2025-08-29 20:06:02	Fetching icon path	OK
2025-08-29 20:06:02	Library Binary Analysis Started	OK
2025-08-29 20:06:02	Analyzing lib/arm64-v8a/libmodpng.so	OK
2025-08-29 20:06:02	Analyzing lib/arm64-v8a/libjniPdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/arm64-v8a/libmodpdfium.so	OK

2025-08-29 20:06:02	Analyzing lib/arm64-v8a/librealm-jni.so	OK
2025-08-29 20:06:02	Analyzing lib/arm64-v8a/libmodft2.so	OK
2025-08-29 20:06:02	Analyzing lib/x86_64/libmodpng.so	OK
2025-08-29 20:06:02	Analyzing lib/x86_64/libjniPdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/x86_64/libmodpdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/x86_64/librealm-jni.so	OK
2025-08-29 20:06:02	Analyzing lib/x86_64/libmodft2.so	OK
2025-08-29 20:06:02	Analyzing lib/armeabi-v7a/libmodpng.so	OK
2025-08-29 20:06:02	Analyzing lib/armeabi-v7a/libjniPdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/armeabi-v7a/libmodpdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/armeabi-v7a/librealm-jni.so	OK

2025-08-29 20:06:02	Analyzing lib/armeabi-v7a/libmodft2.so	OK
2025-08-29 20:06:02	Analyzing lib/armeabi/libmodpng.so	OK
2025-08-29 20:06:02	Analyzing lib/armeabi/libjniPdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/armeabi/libmodpdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/armeabi/libmodft2.so	OK
2025-08-29 20:06:02	Analyzing lib/x86/libmodpng.so	OK
2025-08-29 20:06:02	Analyzing lib/x86/libjniPdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/x86/libmodpdfium.so	OK
2025-08-29 20:06:02	Analyzing lib/x86/librealm-jni.so	OK
2025-08-29 20:06:03	Analyzing lib/x86/libmodft2.so	OK
2025-08-29 20:06:03	Analyzing lib/mips/libmodpng.so	OK

2025-08-29 20:06:03	Analyzing lib/mips/libjniPdfium.so	OK
2025-08-29 20:06:03	Analyzing lib/mips/libmodpdfium.so	OK
2025-08-29 20:06:03	Analyzing lib/mips/libmodft2.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/arm64-v8a/libmodpng.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/arm64-v8a/libjniPdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/arm64-v8a/libmodpdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/arm64-v8a/librealm-jni.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/arm64-v8a/libmodft2.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/x86_64/libmodpng.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/x86_64/libjniPdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/x86_64/libmodpdfium.so	OK

2025-08-29 20:06:03	Analyzing apktool_out/lib/x86_64/librealm-jni.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/x86_64/libmodft2.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi-v7a/libmodpng.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi-v7a/libjniPdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi-v7a/libmodpdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi-v7a/librealm-jni.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi-v7a/libmodft2.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi/libmodpng.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi/libjniPdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi/libmodpdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/armeabi/libmodft2.so	OK

2025-08-29 20:06:03	Analyzing apktool_out/lib/x86/libmodpng.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/x86/libjniPdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/x86/libmodpdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/x86/librealm-jni.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/x86/libmodft2.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/mips/libmodpng.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/mips/libjniPdfium.so	OK
2025-08-29 20:06:03	Analyzing apktool_out/lib/mips/libmodpdfium.so	OK
2025-08-29 20:06:04	Analyzing apktool_out/lib/mips/libmodft2.so	OK
2025-08-29 20:06:04	Reading Code Signing Certificate	OK
2025-08-29 20:06:05	Running APKiD 2.1.5	OK

2025-08-29 20:06:11	Detecting Trackers	OK
2025-08-29 20:06:14	Decompiling APK to Java with JADX	OK
2025-08-29 20:06:41	Converting DEX to Smali	OK
2025-08-29 20:06:41	Code Analysis Started on - java_source	OK
2025-08-29 20:06:44	Android SBOM Analysis Completed	OK
2025-08-29 20:06:52	Android SAST Completed	OK
2025-08-29 20:06:52	Android API Analysis Started	OK
2025-08-29 20:06:59	Android API Analysis Completed	OK
2025-08-29 20:06:59	Android Permission Mapping Started	OK
2025-08-29 20:07:06	Android Permission Mapping Completed	OK
2025-08-29 20:07:07	Android Behaviour Analysis Started	OK

2025-08-29 20:07:16	Android Behaviour Analysis Completed	OK
2025-08-29 20:07:16	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:07:20	Email and URL Extraction Completed	OK
2025-08-29 20:07:20	Extracting String data from APK	OK
2025-08-29 20:07:21	Extracting String data from SO	OK
2025-08-29 20:07:21	Extracting String data from Code	OK
2025-08-29 20:07:21	Extracting String values and entropies from Code	OK
2025-08-29 20:07:26	Performing Malware check on extracted domains	OK
2025-08-29 20:07:39	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.