




ANDROID STATIC ANALYSIS REPORT



 Alfa (2.8.2)

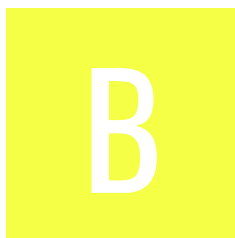
File Name: Alfalah.apk

Package Name: com.base.bankalfalah

Scan Date: Oct. 19, 2024, 11:17 a.m.






App Security Score: 47/100 (MEDIUM RISK)

Grade:



Trackers Detection: 7/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	17	2	2	2

FILE INFORMATION

File Name: Alfalah.apk

Size: 92.12MB

MD5: 870bb8759aabd706a899881d728f25ec

SHA1: 8a6c710115ca168ebc40555cb03f13310ec31029

SHA256: 73f9f0db6f21d6b1db212e5f7bbee5c4993edad4fc41ee8aacc88b1b2d27bbe4

APP INFORMATION

App Name: Alfa

Package Name: com.base.bankalfalah

Main Activity: .openalfa.home.views.SplashActivity

Target SDK: 33

Min SDK: 23

Max SDK:

Android Version Name: 2.8.2

Android Version Code: 310

APP COMPONENTS

Activities: 671

Services: 17

Receivers: 11

Providers: 6

Exported Activities: 3

Exported Services: 2

Exported Receivers: 4

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: C=92, ST=Sindh, L=Karachi, O=Monet, OU=development, CN=azeem yaseen

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2015-10-21 15:09:17+00:00

Valid To: 2114-09-27 15:09:17+00:00

Issuer: C=92, ST=Sindh, L=Karachi, O=Monet, OU=development, CN=azeem yaseen

Serial Number: 0x49201c31

Hash Algorithm: sha256

md5: e6f4abebd416b3036028c325d91b1823

sha1: 01fbd53a97fd563af09e3a680d04cb690d7e5c9a

sha256: a0c36ae6d83676e8e75e15ac9e594ddae924142ad5b286ba4b46c6ade8cae5f4

sha512: 9a119b2aecbc07ed38a542f9659746837139f4a492f0e33d935a6657dcceb18324533344207da2bf13caa57254a97d897540c17a627283152c24bf4fbf4f73b8

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: c958e26d6c699806e749d36278f217a237925ace08bdfcfc08eae3a162a4b87a

Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.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.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.hmkcode.android.gcm.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.base.bankalfalah.BaseApplication.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.base.bankalfalah.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.hardware.camera.autofocus	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECORD_VIDEO	unknown	Unknown permission	Unknown permission from android reference
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.HIGH_SAMPLING_RATE_SENSORS	normal	Access higher sampling rate sensor data	Allows an app to access sensor data with a sampling rate greater than 200 Hz.



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

FILE	DETAILS	
lib/arm64-v8a/libbf0a.so	FINDINGS	DETAILS
	Obfuscator	DexGuard 9.x
lib/arm64-v8a/libd49d.so	FINDINGS	DETAILS
	Obfuscator	DexGuard 9.x
lib/arm64-v8a/libe920.so	FINDINGS	DETAILS
	Obfuscator	DexGuard 9.x
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check
	Obfuscator	unreadable field names unreadable method names
	Compiler	r8

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Obfuscator	unreadable field names unreadable method names
	Compiler	r8
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.HARDWARE check emulator file check
	Compiler	r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
.openalfa.home.views.SplashActivity	Schemes: http://, Hosts: alfapayqr.pk, Paths: /AlfaLoad,

NETWORK SECURITY

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

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: 1 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/APKTOOL_DUMMYVAL_0x7f170006]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (.openalfa.nfc.CardManagementNfcActivity) 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	Activity (.openalfa.nfc.NfcActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (.openalfa.nfc.NfcPaymentActivity) 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.
6	Broadcast Receiver (.utils.AlfaChatBroadCastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Service (.openalfa.nfc.sdk.payment.THceService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NFC_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.
9	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.
10	Service (com.ceesolutions.alfalah.utils.SignalRService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

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

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<p>butterknife/ButterKnife.java com/adjust/sdk/Logger.java com/adjust/sdk/sig/NativeLibHelper.java com/adjust/sdk/sig/SignerInstance.java com/airbnb/lottie/parser/moshi/JsonReader.java com/base/bankalfalah/dashboard/ui/activities/FinancialAdvisoryActivity.java com/base/bankalfalah/openalfa/account_opening_vdc/ui/activities/CreateVDCActivity.java com/base/bankalfalah/openalfa/goalBaseSaving/SaveAndInvestMainMenuActivity.java com/base/bankalfalah/openalfa/home/views/CoolOffActivity.java com/base/bankalfalah/openalfa/k_trade/activities/KTradeActivity.java com/base/bankalfalah/openalfa/overviewnew/view/activity/CCStatementDownloadActivity.java com/base/bankalfalah/openalfa/payments/donations/views/OnlinePaymentMainActivity.java com/base/bankalfalah/openalfa/recent-payment/acti</p>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/base/bankalfalah/openalfa/raas/payment/acti vity/PeastAccountSelectionActivity.java com/base/bankalfalah/openalfa/td/NewTDRActivity. java com/base/bankalfalah/openalfa/term_deposit_reva mped/activity/ScheduleTDRBookingActivityRevamp ed.java com/base/bankalfalah/openalfa/virtual_debit_card/ activity/VDCCreationActivity.java com/bumptechnology/glide/GeneratedAppGlideModuleIm pl.java com/bumptechnology/glide/Glide.java com/bumptechnology/glide/load/engine/DecodeJob.java com/bumptechnology/glide/load/engine/GlideException.ja va com/bumptechnology/glide/load/resource/bitmap/Default ImageHeaderParser.java com/bumptechnology/glide/load/resource/bitmap/VideoD ecoder.java com/bumptechnology/glide/request/SingleRequest.java com/ceesolutions/alfalah/Activities/FormScreen.jav a com/ceesolutions/alfalah/Activities/ForwardConvers ationScreen.java com/ceesolutions/alfalah/Activities/HomeScreen\$M ediaSessionCompat\$Token.java com/ceesolutions/alfalah/Activities/HomeScreen\$R \$Interpolator.java com/ceesolutions/alfalah/Activities/HomeScreen.jav a com/ceesolutions/alfalah/Activities/ImportFromAdd ressBook.java com/ceesolutions/alfalah/Activities/NewGroupScree n.java com/ceesolutions/alfalah/Activities/ProfileSettingsSc reen.java com/ceesolutions/alfalah/Activities/QuestionScreen. java com/ceesolutions/alfalah/chatMessenger/ChatMess engerScreen.java com/ceesolutions/alfalah/chatMessenger/views/Cha tMessageView.java com/ceesolutions/alfalah/chatMessenger/views/Cha

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tMessageViewLeft.java com/ice/resolutions/alfalah/utills/SignalRService.java com/github/dhaval2404/imagepicker/ImagePickerActivity.java com/identity/Capture4FActivity.java com/identity/CaptureFingersActivity.java com/identity/CaptureThumbActivity.java com/identity/DeduplicationIdentyResponse.java com/identity/Enroll2TActivity.java com/identity/Enroll4FActivity.java com/identity/EnrollFingersActivity.java com/identity/EnrollThumbActivity.java com/identity/FingerActivity.java com/identity/FingerOutput.java com/identity/FingersProcessor.java com/identity/HandOutput.java com/identity/IdentyLog.java com/identity/IdentyResponse.java com/identity/IdentySdk.java com/identity/IntroActivity.java com/identity/PngjBadSignature.java com/identity/PngjException.java com/identity/PngjInputException.java com/identity/PngjPrematureEnding.java com/identity/SlapOutput.java com/identity/Verify2TActivity.java com/identity/Verify4FActivity.java com/identity/VerifyFingersActivity.java com/identity/VerifyIdentyResponse.java com/identity/VerifyThumbActivity.java com/identity/app/s3/Captures3Meta.java com/identity/d/PngjBadSignature.java com/identity/d/PngjException.java com/identity/e/valueOf.java com/identity/enums/Template.java com/identity/ex/PostCaptureOutPut.java com/identity/getFingerPrintQualityScore.java com/identity/getMatchingTime.java com/identity/getQualityScore.java com/identity/getScore.java com/identity/getSpoofScore.java com/identity/isQualityFailed.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/identity/ui/c/PngjPrematureEnding.java com/identity/ui/c/getQualityScore.java com/identity/valueOf.java com/mastercard/mpqr/pushpayment/model/PushPaymentData.java com/rygelouv/audiosensei/player/AudioSenseiListObserver.java com/theartofdev/edmodo/cropper/CropImageActivity.java com/wang/avi/AVLoadingIndicatorView.java com/yalantis/ucrop/UCropActivity.java me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java org/camera/preview/PngjBadSignature.java org/cameracontroller/PngjException.java org/tensorflow/lite/NativeInterpreterWrapper.java x/AccountMaintenanceCertificateActivity.java x/AccountMaintenanceCertificateTCsActivity.java x/AccountStatementActivity.java x/AlfaWebViewActivity.java x/AndroidPopup_androidKt\$Popup\$4.java x/AndroidPopup_androidKt\$Popup\$5.java x/AndroidPopup_androidKt\$Popup\$8\$measure\$1.java x/AndroidPopup_androidKt\$Popup\$9.java x/AndroidPopup_androidKt\$Popup\$popupId\$1.java x/AndroidPopup_androidKt\$Popup\$popupLayout\$1\$1\$1.java x/AndroidViewHolder\$onNestedFling\$1.java x/AppEventsLoggerUtility\$GraphAPIActivityType.java x/ApplyQRCardActivity.java x/AvailableFundAndInvestedPlansActivity.java x/BaseGmsClient.java x/BaseImplementation.java x/BasePendingResult.java x/CCStatementDownloadActivity.java x/CHVerificationMethod.java x/CRMAActivity.java x/CallbackManagerImpl\$RequestCodeOffset.java x/CardWrapper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x/CardsMenuActivity.java x/CheckboxKt\$Checkbox\$2\$1.java x/CnicExpiryUpdateActivity.java x/ColorsKt\$LocalColors\$1.java x/Constants.java x/ConstraintAnchor\$Type.java x/ConstraintReference\$IncorrectConstraintException.java x/CreateBeneficiarySuccessfulActivity.java x/CreditCardCreatePasswordActivity_ViewBinding.java x/CreditDetails.java x/DialogAction.java x/DragAndDropPermissionsCompat.java x/EMI.java x/EncashmentTermsActivity.java x/FragmentContainerView.java x/FragmentManager\$6.java x/FundInvestmentSuccessActivity_ViewBinding.java x/GoogleApiManager.java x/GraphicsLayerModifierKt\$graphicsLayer\$\$inlined\$debugInspectorInfo\$1.java x/IGmsCallbacks.java x/Keep.java x/Legend\$LegendForm.java x/Legend\$LegendHorizontalAlignment.java x/LifecycleCallback.java x/ListenerHolders.java x/MFServerResponse.java x/MediaBrowserCompat\$SearchResultReceiver.java x/MethodInvocation.java x/MutableCreationExtras.java x/MutualFundIVRCallSuccessActivity.java x/MutualFundOtacActivity_ViewBinding.java x/NfcCardEnrollmentSuccessActivity.java x/NfcHoldNearReaderActivity.java x/OneBillPaymentMainActivity_ViewBinding.java x/OperationCanceledException.java x/OrbitsActivity.java x/OtherBankActivity.java x/OtherBillPaymentCheckoutActivity.java x/OtherBillPaymentActivity.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	x/PackageDetailsActivity.java x/PartialItemCollection\$1.java x/PartialItemCollectionWithListener\$1.java x/PayITTitleFetchDetailsModel.java x/PayeeTransferActivityNew.java x/PersistedEvents\$SerializationProxyV1\$a.java x/PopupLayout\$Content\$4.java x/PromoHistoryActivity.java x/PromoMainActivity.java x/PurposeListObject.java x/PurposeTypeListObject.java x/R.java x/RDANomineeActivity.java x/RaastTitleFetchDetailsActivity.java x/RegistrationMainActivity.java x/RootTelemetryConfigManager.java x/RootTelemetryConfiguration.java x/SLICFetchTitle.java x/SLICPayment.java x/ScheduledPassCodeActivity.java x/SchoolPaymentPasscodeActivity2.java x/ServicesDonationActivity.java x/ServicesMainActivity.java x/ServicesMenuActivity.java x/ShapeStroke\$LineJoinType.java x/Share.java x/SharedElementCallback.java x/SubcomposeLayoutKt\$SubcomposeLayout\$5\$1.java x/SuccessEncashmentActivity_ViewBinding.java x/SupplyChainActivity.java x/SupplyChainMoneySend_ViewBinding.java x/TDIslamicRatesActivity_ViewBinding.java x/TDRatesActivityRevamped.java x/TaxRebateActivity.java x/TelemetryLogging.java x/TopUpYourAccountActivity.java x/TshInitState.java x/TshPaymentErrorData.java x/TshPushSender.java x/TypeCategory.java x/VDCOtacOtpActivity.java x/VectorComposeKt\$Path\$1.java

NO	ISSUE	SEVERITY	STANDARDS	<div>FILES</div> <div> x/ViewModelProvider.java x/WFAvailFinanceActivity.java x/WageFinancingActivity.java x/WalletPinGenerationActivity_ViewBinding.java x/WidgetRun\$RunType.java x/WindowInsetsCompat\$Impl21.java x/WindowInsetsCompat\$Impl28.java x/WindowInsetsCompat\$Impl29.java x/WrappedComposition.java x/access\$getACCEPTABLE_CLASSES\$cp.java x/callStartTransitionListener.java x/completeWakefullIntent.java x/consumeSystemWindowInsets.java x/createFailedResult.java x/createFragmentContainer.java x/forceFailureUnlessReady.java x/getAccessibilityClassName.java x/getAllowEnterTransitionOverlap.java x/getAnimatedVisibility.java x/getAnimator.java x/getBarHeight.java x/getBatchPeriodMillis.java x/getChartView.java x/getCodeCacheDir.java x/getColor.java x/getComposition.java x/getConfig.java x/getContent.java x/getContentHeight.java x/getContext.java x/getDataModel.java x/getDistToClosestEdge.java x/getDrawerElevation.java x/getEmojiTextViewHelper.java x/getEnterTransitionCallback.java x/getExitAnim.java x/getHost.java x/getImageMatrix.java x/getInflater.java x/getInfo.java x/getJobs.java x/getLastScanTimeMs.java </div>

NO	ISSUE	SEVERITY	STANDARDS	Files x/getLastWindowInsets.java x/getMethodTimingTelemetryEnabled.java x/getMinimumMaxLifecycleState.java x/getOnRequestDisallowInterceptTouchEvent\$ui_release.java x/getPadding.java x/getParams.java x/getParentFragmentManager.java x/getParentLayoutDirection.java x/getQuery.java x/getRetainInstance.java x/getReturnTransition.java x/getSearchViewTextMinWidthDp.java x/getSelectedView.java x/getSharedElementEnterTransition.java x/getSharedElementReturnTransition.java x/getSpeed.java x/getSuggestionCommitIconResId.java x/getSupportBackgroundTintList.java x/getSystemWindowInsets.java x/getTargetFragment.java x/getThumbOffset.java x/getTokenResult.java x/getTypeFromString.java x/getVerticalScrollFactorCompat.java x/getView.java x/getVisibleInsets\$e\$a.java x/goToWHTCertificate.java x/initLifecycle.java x/instantiate.java x/isDsrpSupported.java x/isErrorState.java x/isTypeVisible.java x/lambda\$bindViews\$0\$combasebankalfalahopenalfaservicesviewsSearchActivity.java x/lambda\$initView\$1\$combasebankalfalahopenalfaqrcardsApplyQRCardSuccessActivity.java x/lambda\$initilizeControls\$0\$combasebankalfalahopenalfamutualFundsrevampviewrdaRDANomineeActivity.java x/log.java x/notifyListener.java x/onActivityPostResumed.java

NO	ISSUE	SEVERITY	STANDARDS	<div> <div>FILES</div> <div> x/onActivityResult.java x/onCancelEntryClick.java x/onCreateAnimation.java x/onCreateView.java x/onIssuanceDateEdittextClick.java x/onPaymentTypeClick.java x/onRequestPermissionsResult.java x/performActivityCreated.java x/performViewCreated.java x/prepareCallInternal.java x/readCurrentStateIfPossible.java x/registerIn.java x/registerOnPreAttachListener.java x/requireContext.java x/savedStateProvider.java x/setAnimationFromJson.java x/setAskingAttribution.java x/setAttachListener.java x/setBackgroundDrawable.java x/setCenterTextSizePixels.java x/setChecked.java x/setDefaultActionButtonContentDescription.java x/setDpMargin.java x/setDrawEntryLabels.java x/setEmojiCompatEnabled.java x/setExpandActivityOverflowButtonDrawable.java x/setExpandedFormat.java x/setExtraBottomOffset.java x/setFillColorResource.java x/setFirstHorizontalBias.java x/setFirstHorizontalStyle.java x/setGravity.java x/setGroupDividerEnabled.java x/setHorizontalAlign.java x/setHorizontalGravity.java x/setIconified.java x/setId.java x/setImageURI.java x/setImeVisibility.java x/setIsFocusable.java x/setItemInvoker.java x/setKeyListener.java </div> </div>

NO	ISSUE	SEVERITY	STANDARDS	x/setListSelectionHidden.java x/setMarkdownText.java x/setMinAndMaxProgress.java x/setMinValue\$a.java x/setNoDataTextColor.java x/setOnChartValueSelectedListener.java x/setOnCloseListener.java x/setOnConstraintsChanged.java x/setOnDoubleTapListener.java x/setOnFitSystemWindowsListener.java x/setOnMarkerClickListener.java x/setOrientation.java x/setPaddingLeft.java x/setPan.java x/setParentLayoutDirection.java x/setPopupBackgroundDrawable.java x/setProgress.java x/setQuery.java x/setQueryRefinementEnabled.java x/setScrimColor.java x/setSearchView.java x/setSlideToCancelText.java x/setStableInsets.java x/setSupportButtonTintMode.java x/setSupportCompoundDrawablesTintMode.java x/setSwipeListener.java x/setTabSelected.java x/setTextClassifier.java x/setTextOnInternal.java x/setUpdate.java x/setVerticalBias.java x/setVerticalGap.java x/setWrapMode.java x/setupLayoutResource.java x/tryToAddRecreator.java x/zak.java x/zan.java x/zzqd.java x/zzqh.java x/zzqk.java x/zzql.java x/zzrf.java x/zzri.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	x/zzrj.java x/zzrk.java x/zztc.java com/adjust/sdk/Constants.java com/adjust/sdk/sig/KeystoreHelper.java x/AndroidCompositionLocals_androidKt\$ProvideAn droidCompositionLocals\$4\$e\$a.java x/AvailableFundDetailsActivity.java x/BringIntoViewKt\$ModifierLocalBringIntoViewPare nt\$1.java x/CoreTextFieldKt\$CoreTextField\$focusModifier\$1.j ava x/DisposableSaveableStateRegistry_androidKt\$Disp osableSaveableStateRegistry\$saveableStateRegistry \$1.java x/HoverInteractionKt\$collectIsHoveredAsState\$1.jav a x/InvestNowFormActivity_ViewBinding.java x/ProductItemFragment.java x/RedeemInvestmentActivity.java x/ViewTreeViewModelStoreOwner.java x/WalletOpeningRejectionOldActivity_ViewBinding.j ava x/WithLifecycleStateKt\$suspendWithStateAtLeastUn checked\$2\$2.java x/onCreateGoalClick.java x/withResumed\$\$forInline.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	x/SearchBar\$ScrollingViewBehavior.java x/getCenterView.java x/getCornerSize.java x/getSearchPrefixText.java x/getTextView.java x/getToolBar.java x/getUserSetVisibility.java x/setCloseIconContentDescription.java x/setCloseIconEnabledResource.java x/setIconTintList.java x/setupHeaderLayout.java x/setVisible.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/aditya/filebrowser/Constants.java com/base/bankalfalah/openalfa/term_deposit/activity/TDReceiptActivity.java com/base/bankalfalah/openalfa/term_deposit_revamped/activity/TDReceiptActivityRevamped.java com/ceesolutions/alfalah/chatMessenger/ChatMessengerScreen.java com/identity/app/PngjBadSignature.java x/FeesDetailsActivity.java x/Keep.java x/PartialUtilityBillPaymentActivity.java x/PopupLayout\$Content\$4.java x/PopupLayout\$canCalculatePosition\$2.java x/R.java x/TDIslamicRatesActivity_ViewBinding.java x/drainQueue.java x/getInflater.java x/getProgressStartPosition.java x/markDelivered.java x/trackNewSessionI.java
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/base/bankalfalah/openalfa/account_opening_vdc/ui/activities/VDCTopUpActivity.java com/base/bankalfalah/openalfa/td/TopUpYourAccountActivity.java x/Keep.java x/VectorComposeKt\$Group\$2\$6.java x/VehicleDiscrepancyFragment\$onClick\$2.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	org/java_websocket/drafts/Draft_10.java x/TDIslamicRatesActivity_ViewBinding.java x/getDataModel.java x/getIntrinsicHeight.java x/getOpacity.java x/scheduleDrawable.java x/switchMap.java x/zzrr.java x/zzry.java
7	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/sun/jna/Native.java com/theartofdev/edmodo/cropper/CropImageActivity.java x/IGmsCallbacks.java x/readCurrentStatelfPossible.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	x/getCheckedIconSize.java x/setButtonTintList.java x/setChipIconVisible.java x/setTargetElevation.java x/zzkx.java
9	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	x/ViewModelKt.java x/setCounterOverflowTextAppearance.java
10	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	x/ProfileSettingsScreen.java x/getAnimatedVisibility.java x/getCloseIconContentDescription.java x/hasAlpha.java x/setChipIconEnabled.java x/setChipIconSizeResource.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	x/setOnPhotoTapListener.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	x/setCheckedState.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----------------	-------	-------	---------	---------	---------------------

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libbarhopper_v3.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libe920.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/librsjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	armeabi-v7a/libjnidispatch.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libbf0a.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libGHDSDFIUPOIFDLS8DSFN23LK.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strcat_chk', '__memcpy_chk', '__memmove_chk', '__vsnprintf_chk', '__vsprintf_chk', '__memset_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libfinger-native-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi-v7a/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/librsjni_androidx.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libRSSupport.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi-v7a/libonnxruntime.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>\$ORIGIN high</p> <p>The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	True NX info The binary	STACK CANARY info This binary	Partial RELRO warning This binary	None RPATH info The	None RUNPATH info The binary	False FORTIFY warning The binary does not	SYMBOLS STRIPPED warning Symbols are
12	armeabi-v7a/libtensorflowlite_jni.so	has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	binary does not have run-time search path or RPATH set.	does not have RUNPATH set.	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.	available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libsupport-native-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libd49d.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__memset_chk', '__read_chk', '__vsprintf_chk', '__memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/libpl_droidsonroids_gif.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strncat_chk', '__memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	armeabi-v7a/libc++_shared.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libbarhopper_v3.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strlen_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	arm64-v8a/libe920.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	arm64-v8a/librsjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libjnidispatch.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	arm64-v8a/libbf0a.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	arm64-v8a/libGHDSDFIUPOIFDLS8DSFN23LK.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__memcpy_chk', '__memmove_chk', '__vsprintf_chk', '__memset_chk', '__strcat_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	arm64-v8a/libfinger-native-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	arm64-v8a/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	arm64-v8a/librsjni_androidx.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	arm64-v8a/libRSSupport.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk', '__vsprintf_chk', '__strncat_chk', '__strchr_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	arm64-v8a/libonnxruntime.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>\$ORIGIN high</p> <p>The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	True NX info The binary	STACK CANARY info This binary	Partial RELRO warning This binary	None RPATH info The	None RUNPATH info The binary	False FORTIFY warning The binary does not	SYMBOLS STRIPPED warning Symbols are
28	arm64-v8a/libtensorflowlite_jni.so	has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	binary does not have run-time search path or RPATH set.	does not have RUNPATH set.	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.	available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	arm64-v8a/libsupport-native-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsprintf_chk', '__memmove_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	arm64-v8a/libd49d.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions:</p> <pre>['__vsprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__read_chk', '__memset_chk']</pre>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	arm64-v8a/libpl_droidsonroids_gif.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strncat_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	arm64-v8a/libc++_shared.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
33	armeabi-v7a/libbarhopper_v3.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	armeabi-v7a/libe920.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	armeabi-v7a/librsjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	armeabi-v7a/libjnidispatch.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	armeabi-v7a/libbf0a.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	armeabi-v7a/libGHDSDFIUPOIFDLS8DSFN23LK.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strcat_chk', '__memcpy_chk', '__memmove_chk', '__vsnprintf_chk', '__vsprintf_chk', '__memset_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	armeabi-v7a/libfinger-native-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	armeabi-v7a/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	armeabi-v7a/librsjni_androidx.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
42	armeabi-v7a/libRSSupport.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	armeabi-v7a/libonnxruntime.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>\$ORIGIN high</p> <p>The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	True NX info The binary	STACK CANARY info This binary	Partial RELRO warning This binary	None RPATH info The	None RUNPATH info The binary	False FORTIFY warning The binary does not	SYMBOLS STRIPPED warning Symbols are
44	armeabi-v7a/libtensorflowlite_jni.so	has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	binary does not have run-time search path or RPATH set.	does not have RUNPATH set.	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.	available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
45	armeabi-v7a/libsupport-native-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	armeabi-v7a/libd49d.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__memset_chk', '__read_chk', '__vsprintf_chk', '__memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	armeabi-v7a/libpl_droidsonroids_gif.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strncat_chk', '__memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
48	armeabi-v7a/libc++_shared.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	arm64-v8a/libbarhopper_v3.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strlen_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
50	arm64-v8a/libe920.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
51	arm64-v8a/librsjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
52	arm64-v8a/libjnidispatch.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
53	arm64-v8a/libbf0a.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
54	arm64-v8a/libGHDSDFIUPOIFDLS8DSFN23LK.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__memcpy_chk', '__memmove_chk', '__vsprintf_chk', '__memset_chk', '__strcat_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	arm64-v8a/libfinger-native-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
56	arm64-v8a/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_memcpy_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
57	arm64-v8a/librsjni_androidx.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
58	arm64-v8a/libRSSupport.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk', '__vsprintf_chk', '__strncat_chk', '__strchr_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
59	arm64-v8a/libonnxruntime.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>\$ORIGIN high</p> <p>The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	True NX info The binary	STACK CANARY info This binary	Partial RELRO warning This binary	None RPATH info The	None RUNPATH info The binary	False FORTIFY warning The binary does not	SYMBOLS STRIPPED warning Symbols are
60	arm64-v8a/libtensorflowlite_jni.so	has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	binary does not have run-time search path or RPATH set.	does not have RUNPATH set.	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.	available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
61	arm64-v8a/libsupport-native-lib.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsprintf_chk', '_memmove_chk', '_memcpy_chk', '_vsnprintf_chk', '_read_chk', '_strlen_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
62	arm64-v8a/libd49d.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '_strlen_chk', '_memcpy_chk', '_memmove_chk', '_read_chk', '_memset_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
63	arm64-v8a/libpl_droidsonroids_gif.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strncat_chk']</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
64	arm64-v8a/libc++_shared.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>False warning</p> <p>Symbols are available.</p>

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/24	android.permission.RECORD_AUDIO, android.permission.GET_ACCOUNTS, android.permission.WAKE_LOCK, android.permission.READ_PHONE_STATE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_CONTACTS, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION
Other Common Permissions	9/45	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, android.permission.CALL_PHONE, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, android.permission.WRITE_CONTACTS, com.google.android.gms.permission.ACTIVITY_RECOGNITION, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.BATTERY_STATS

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
www.tensorflow.org	ok	IP: 142.250.181.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
goo.gle	ok	IP: 67.199.248.12 Country: United States of America Region: New York City: New York City Latitude: 40.739288 Longitude: -73.984955 View: Google Map
subscription.adjust.com	ok	IP: 185.151.204.52 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
developer.android.com	ok	IP: 142.250.181.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	IP: 157.240.227.1 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
gdpr.adjust.com	ok	IP: 185.151.204.50 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
www.bankalfalah.com	ok	IP: 20.101.192.56 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
app.adjust.com	ok	IP: 185.151.204.7 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
alfa-4fe5f.firebaseio.com	ok	IP: 35.201.97.85 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
www.google.com	ok	IP: 142.250.199.164 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
licensemgr.identity.io	ok	IP: 100.25.84.110 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
github.com	ok	IP: 20.207.73.82 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

FIREBASE URL	DETAILS
https://alfa-4fe5f.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
instant.loan@bankalfalah.com claims@efulife.com info@tpllife.com zakat@bankalfalah.com	Android String Resource
android-sdk-releaser@liw11.prod	apktool_out/lib/armeabi-v7a/libbarhopper_v3.so
h@h.ixd	apktool_out/lib/armeabi-v7a/libGHDSDFIUPOIFDLS8DSFN23LK.so
android-sdk-releaser@liw11.prod	apktool_out/lib/arm64-v8a/libbarhopper_v3.so
i@matchers_size	apktool_out/lib/arm64-v8a/libfinger-native-lib.so
k@9.jn8	apktool_out/lib/arm64-v8a/libsupport-native-lib.so
android-sdk-releaser@liw11.prod	lib/armeabi-v7a/libbarhopper_v3.so
h@h.ixd	lib/armeabi-v7a/libGHDSDFIUPOIFDLS8DSFN23LK.so
android-sdk-releaser@liw11.prod	lib/arm64-v8a/libbarhopper_v3.so
i@matchers_size	lib/arm64-v8a/libfinger-native-lib.so

EMAIL	FILE
k@9.jn8	lib/arm64-v8a/libsupport-native-lib.so

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
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
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AlzaSyDH2cb367vKtYjHOkhMBHYBHfT17HPm8p0"

POSSIBLE SECRETS
"firebase_database_url" : "https://alfa-4fe5f.firebaseio.com"
"google_api_key" : "AlzaSyDH2cb367vKtYjHOkhMBHYBHft17HPm8p0"
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
4b2d8ee6a4fbaaf2785ce5abd971486d
470fa2b4ae81cd56ecbcd9735803434cec591fa
9b8f518b086098de3d77736f9458a3d2f6f95a37
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
sha256/WRZpbTFXnD5+4xfigGBYquLxOHxQkzPzotyt1n8d47g=
cc2751449a350f668590264ed76692694a80308a
sha256/RQeZkB42znUfsDIIFWIRiYEckI7nHwNFwWCrnMMJbVc=
sha256/Wec45nQiFwKvHtuHxSAMGkt19k+uPSw9JlEkxhvYPHk=
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
sha256/6dKrwNBf2r9MfijlpgqPJtbnFvc6yJglPvm2+FgXRg=
QWERTYUIOPASDFGHJKLZXCVBNMqwertyuiopasdfghjklzxcvbnm1234567890

POSSIBLE SECRETS
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303932353231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d0101040500038181005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2
12345678912345678912345678912345
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
e2b606b641a43e3109ad37a6a1230d18
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
c7207a39f4cef35dc61916124acb61ad225ad46a

PLAYSTORE INFORMATION

Title: Alfa by Bank Alfalah

Score: 4.326087 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** [com.base.bankalfalah](https://play.google.com/store/apps/details?id=com.base.bankalfalah)

Developer Details: Bank Alfalah Limited, Bank+Alfalah+Limited, None, <https://www.bankalfalah.com/>, adcbafl@gmail.com,

Release Date: Feb 25, 2016 **Privacy Policy:** [Privacy link](#)

Description:

Alfa your life and check banking off your daily to do list. Manage your savings. Track your expenses. Pay your bills. Make appointments with your branch. Request new cheque

book. Or just go shopping. Alfa will keep you ahead. 1. Simple steps to install, account opening and start using Alfa on your Android device a. Download Alfa to your android device from Google Play Store. b. Open your Alfa Account in 3 easy steps. c. Login using your existing Bank Alfalah Internet Banking credentials or; d. Register using your Bank Alfalah Active Debit Card credentials Alfa requires both SMS and Call permission to provide our valued customer better experience within Alfa Mobile App. SMS Permission: SMS permission is required for auto sense functionality of One Time Pincode on various transactions. This option helps our customer to avoid navigation between Alfa App & SMS Inbox. Call Permission: In order to provide customers an option to initiate call to Bank's Helpline within Alfa App. 2. View account balance, last 30 days statement and transaction details for all your accounts linked with Debit Card. 3. View your credit cards' details, available limit, due date, outstanding, minimum payment and reward points. Pay your Credit Card bill instantly. 4. Easily access your loans & bancassurance details 5. Have complete control over account; request for Cheque book, address change, subscription of SMS alerts & e-Statement. 6. Make instant fund transfers to Bank Alfalah and Other IBFT enabled Bank customers. 7. Safely add payees right from the app. No need to log in to internet banking to add a payee or you can even add payee while performing a transaction. 8. Recharge your Prepaid Mobile or pay your postpaid bill instantly. 9. Pay your utility bills including ISP (Internet Service Provider) charges instantly. 10. One click view of Special Offers credit & debit card customers. 11. Locate Bank Alfalah Branches, ATMs and Cash Deposit Machines near you (through GPS). 12. Apply for Bank Alfalah products instantly. You are now ready to bank with Bank Alfalah right from your Android device! For any other details please visit www.bankalfalah.com

SCAN LOGS

Timestamp	Event	Error
2024-10-19 11:42:34	Generating Hashes	OK
2024-10-19 11:42:34	Extracting APK	OK
2024-10-19 11:42:34	Unzipping	OK
2024-10-19 11:42:36	Getting Hardcoded Certificates/Keystores	OK
2024-10-19 11:42:36	Parsing AndroidManifest.xml	OK
2024-10-19 11:42:36	Parsing APK with androguard	OK

2024-10-19 11:42:37	Extracting Manifest Data	OK
2024-10-19 11:42:37	Performing Static Analysis on: Alfa (com.base.bankalfalah)	OK
2024-10-19 11:42:37	Fetching Details from Play Store: com.base.bankalfalah	OK
2024-10-19 11:42:41	Manifest Analysis Started	OK
2024-10-19 11:42:41	Reading Network Security config from APKTOOL_DUMMYVAL_0x7f170006.xml	OK
2024-10-19 11:42:41	Parsing Network Security config	OK
2024-10-19 11:42:41	Checking for Malware Permissions	OK
2024-10-19 11:42:41	Fetching icon path	OK
2024-10-19 11:42:41	Library Binary Analysis Started	OK
2024-10-19 11:42:41	Analyzing apktool_out/lib/armeabi-v7a/libbarhopper_v3.so	OK
2024-10-19 11:42:41	Analyzing apktool_out/lib/armeabi-v7a/libe920.so	OK

2024-10-19 11:42:42	Analyzing apktool_out/lib/armeabi-v7a/librsjni.so	OK
2024-10-19 11:42:42	Analyzing apktool_out/lib/armeabi-v7a/libjnidispatch.so	OK
2024-10-19 11:42:42	Analyzing apktool_out/lib/armeabi-v7a/libbf0a.so	OK
2024-10-19 11:42:42	Analyzing apktool_out/lib/armeabi-v7a/libGHDSDFIUPOIFDLS8DSFN23LK.so	OK
2024-10-19 11:42:42	Analyzing apktool_out/lib/armeabi-v7a/libfinger-native-lib.so	OK
2024-10-19 11:42:44	Analyzing apktool_out/lib/armeabi-v7a/libsigner.so	OK
2024-10-19 11:42:44	Analyzing apktool_out/lib/armeabi-v7a/librsjni_androidx.so	OK
2024-10-19 11:42:44	Analyzing apktool_out/lib/armeabi-v7a/libRSSupport.so	OK
2024-10-19 11:42:45	Analyzing apktool_out/lib/armeabi-v7a/libonnxruntime.so	OK
2024-10-19 11:42:45	Analyzing apktool_out/lib/armeabi-v7a/libtensorflowlite_jni.so	OK
2024-10-19 11:42:46	Analyzing apktool_out/lib/armeabi-v7a/libsupport-native-lib.so	OK

2024-10-19 11:42:47	Analyzing apktool_out/lib/armeabi-v7a/libd49d.so	OK
2024-10-19 11:42:47	Analyzing apktool_out/lib/armeabi-v7a/libpl_droidsonroids_gif.so	OK
2024-10-19 11:42:47	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK
2024-10-19 11:42:48	Analyzing apktool_out/lib/arm64-v8a/libbarhopper_v3.so	OK
2024-10-19 11:42:48	Analyzing apktool_out/lib/arm64-v8a/libe920.so	OK
2024-10-19 11:42:48	Analyzing apktool_out/lib/arm64-v8a/librsjni.so	OK
2024-10-19 11:42:48	Analyzing apktool_out/lib/arm64-v8a/libjnidispatch.so	OK
2024-10-19 11:42:49	Analyzing apktool_out/lib/arm64-v8a/libbf0a.so	OK
2024-10-19 11:42:49	Analyzing apktool_out/lib/arm64-v8a/libGHDSDFIUPOIFDLS8DSFN23LK.so	OK
2024-10-19 11:42:49	Analyzing apktool_out/lib/arm64-v8a/libfinger-native-lib.so	OK
2024-10-19 11:42:51	Analyzing apktool_out/lib/arm64-v8a/libsigner.so	OK

2024-10-19 11:42:51	Analyzing apktool_out/lib/arm64-v8a/librsjni_androidx.so	OK
2024-10-19 11:42:51	Analyzing apktool_out/lib/arm64-v8a/libRSSupport.so	OK
2024-10-19 11:42:52	Analyzing apktool_out/lib/arm64-v8a/libonnxruntime.so	OK
2024-10-19 11:42:52	Analyzing apktool_out/lib/arm64-v8a/libtensorflowlite_jni.so	OK
2024-10-19 11:42:52	Analyzing apktool_out/lib/arm64-v8a/libsupport-native-lib.so	OK
2024-10-19 11:42:54	Analyzing apktool_out/lib/arm64-v8a/libd49d.so	OK
2024-10-19 11:42:54	Analyzing apktool_out/lib/arm64-v8a/libpl_droidsonroids_gif.so	OK
2024-10-19 11:42:54	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2024-10-19 11:42:55	Analyzing lib/armeabi-v7a/libbarhopper_v3.so	OK
2024-10-19 11:42:55	Analyzing lib/armeabi-v7a/libe920.so	OK
2024-10-19 11:42:55	Analyzing lib/armeabi-v7a/librsjni.so	OK

2024-10-19 11:42:55	Analyzing lib/armeabi-v7a/libjnidispatch.so	OK
2024-10-19 11:42:55	Analyzing lib/armeabi-v7a/libbf0a.so	OK
2024-10-19 11:42:55	Analyzing lib/armeabi-v7a/libGHDSDFIUPOIFDLS8DSFN23LK.so	OK
2024-10-19 11:42:55	Analyzing lib/armeabi-v7a/libfinger-native-lib.so	OK
2024-10-19 11:42:57	Analyzing lib/armeabi-v7a/libsigner.so	OK
2024-10-19 11:42:57	Analyzing lib/armeabi-v7a/librsjni_androidx.so	OK
2024-10-19 11:42:57	Analyzing lib/armeabi-v7a/libRSSupport.so	OK
2024-10-19 11:42:58	Analyzing lib/armeabi-v7a/libonnxruntime.so	OK
2024-10-19 11:42:59	Analyzing lib/armeabi-v7a/libtensorflowlite_jni.so	OK
2024-10-19 11:42:59	Analyzing lib/armeabi-v7a/libsupport-native-lib.so	OK
2024-10-19 11:43:00	Analyzing lib/armeabi-v7a/libd49d.so	OK

2024-10-19 11:43:00	Analyzing lib/armeabi-v7a/libpl_droidsonroids_gif.so	OK
2024-10-19 11:43:00	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2024-10-19 11:43:01	Analyzing lib/arm64-v8a/libbarhopper_v3.so	OK
2024-10-19 11:43:01	Analyzing lib/arm64-v8a/libe920.so	OK
2024-10-19 11:43:01	Analyzing lib/arm64-v8a/librsjni.so	OK
2024-10-19 11:43:01	Analyzing lib/arm64-v8a/libjnidispatch.so	OK
2024-10-19 11:43:01	Analyzing lib/arm64-v8a/libbf0a.so	OK
2024-10-19 11:43:02	Analyzing lib/arm64-v8a/libGHDSDFIUPOIFDLS8DSFN23LK.so	OK
2024-10-19 11:43:02	Analyzing lib/arm64-v8a/libfinger-native-lib.so	OK
2024-10-19 11:43:04	Analyzing lib/arm64-v8a/libsigner.so	OK
2024-10-19 11:43:04	Analyzing lib/arm64-v8a/librsjni_androidx.so	OK

2024-10-19 11:43:04	Analyzing lib/arm64-v8a/libRSSupport.so	OK
2024-10-19 11:43:05	Analyzing lib/arm64-v8a/libonnxruntime.so	OK
2024-10-19 11:43:05	Analyzing lib/arm64-v8a/libtensorflowlite_jni.so	OK
2024-10-19 11:43:05	Analyzing lib/arm64-v8a/libsupport-native-lib.so	OK
2024-10-19 11:43:06	Analyzing lib/arm64-v8a/libd49d.so	OK
2024-10-19 11:43:06	Analyzing lib/arm64-v8a/libpl_droidsonroids_gif.so	OK
2024-10-19 11:43:06	Analyzing lib/arm64-v8a/libc++_shared.so	OK
2024-10-19 11:43:07	Reading Code Signing Certificate	OK
2024-10-19 11:43:09	Running APKiD 2.1.5	OK
2024-10-19 11:43:18	Detecting Trackers	OK
2024-10-19 11:43:21	Decompiling APK to Java with jadx	OK

2024-10-19 11:44:27	Converting DEX to Smali	OK
2024-10-19 11:44:27	Code Analysis Started on - java_source	OK
2024-10-19 11:52:57	Android SAST Completed	OK
2024-10-19 11:52:57	Android API Analysis Started	OK
2024-10-19 12:08:37	Android SAST Completed	OK
2024-10-19 12:08:37	Android API Analysis Started	OK
2024-10-19 12:15:20	Android Permission Mapping Started	OK
2024-10-19 12:23:59	Android Permission Mapping Completed	OK
2024-10-19 12:24:08	Finished Code Analysis, Email and URL Extraction	OK
2024-10-19 12:24:08	Extracting String data from APK	OK
2024-10-19 12:24:08	Extracting String data from SO	OK

2024-10-19 12:24:09	Extracting String data from Code	OK
2024-10-19 12:24:09	Extracting String values and entropies from Code	OK
2024-10-19 12:24:14	Performing Malware check on extracted domains	OK
2024-10-19 12:24:20	Saving to Database	OK
2024-10-19 12:28:28	Android Permission Mapping Started	OK
2024-10-19 12:36:11	Android Permission Mapping Completed	OK
2024-10-19 12:36:18	Finished Code Analysis, Email and URL Extraction	OK
2024-10-19 12:36:18	Extracting String data from APK	OK
2024-10-19 12:36:18	Extracting String data from SO	OK
2024-10-19 12:36:19	Extracting String data from Code	OK
2024-10-19 12:36:19	Extracting String values and entropies from Code	OK

2024-10-19 12:36:23	Performing Malware check on extracted domains	OK
2024-10-19 12:36:28	Saving to Database	OK

Report Generated by - MobSF v4.0.7

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.