

ANDROID STATIC ANALYSIS REPORT

app_icon

Sober Sidekick (2.4.4)

Package Name:	com.sidekick.app.sobersidekick
Scan Date:	Nov. 26, 2024, 4:20 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	6/432

\$\Circ\$ FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	Q HOTSPOT
3	18	3	2	2

FILE INFORMATION

File Name: Sober Sidekick_ Quit Drinking_2.4.4_APKPure.apk

Size: 48.63MB

MD5: 0119c2c48bd13807979e34cfc46404ef

SHA1: 8cbdb90537748aa6ce5ed383caae6d3f1990b9c3

SHA256: 53d4c9dbe69690b8a5ed36c006092a0e78e8784c14912e28d609a7fc512765d0

i APP INFORMATION

App Name: Sober Sidekick

Package Name: com.sidekick.app.sobersidekick

Main Activity: com.hadiyarajesh.composetemplate.MainActivity

Target SDK: 34 Min SDK: 26 Max SDK:

Android Version Name: 2.4.4 Android Version Code: 124

APP COMPONENTS

Activities: 25 Services: 15 Receivers: 9 Providers: 4
Exported Activities: 1
Exported Services: 3
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed v1 signature: False v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2021-06-22 09:47:49+00:00 Valid To: 2051-06-22 09:47:49+00:00

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

Serial Number: 0xb5d332740da891ffad888f030e422a59450f7bd5

Hash Algorithm: sha256

md5: b5fcdd7f7bb12987033aafa389de4fcb

sha1: 87a47b9f556a2187d2ba57bb853ea09b6a3f2516

sha256: a39cf58457b1213ccda52b3e9e715fab950194f092e654b0b380ab35ea2a2e8e

sha512; 66f05627dfa92c8c10bb263001190bda1a43662d9b139bcc430c5729356eb219ca2081db5bb3f56f19ccb8e612fcaabb1a584b94087f36b9170412c29df3afba

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 98be4117a8c67c5c745766ce26773c1872705b2ec98375377f1a29c52b052ba8

Found 1 unique certificates

: APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.sidekick.app.sobersidekick.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.sidekick.app.sobersidekick.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.

PERMISSION	STATUS	INFO	DESCRIPTION
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

ক্ল APKID ANALYSIS

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

FILE	DETAILS		
	FINDINGS	DETAILS	
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check	
classes2.dex	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes3.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check SIM operator check network operator name check device ID check ro.kernel.qemu check	
	Compiler	r8 without marker (suspicious)	

FILE	DETAILS	
	FINDINGS	DETAILS
	Anti Debug Code	Debug.isDebuggerConnected() check
classes4.dex	Anti-VM Code	Build.MODEL check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
	Compiler	r8 without marker (suspicious)
	FINDINGS	DETAILS
classes5.dex	FINDINGS	
	Compiler	r8 without marker (suspicious)
	FINDINGS	DETAILS
classes6.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check
	Compiler	r8 without marker (suspicious)



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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (com.hadiyarajesh.composetemplate.Services.PushNotifications.SidekickMessagingService) 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.
5	Service (com.clevertap.android.sdk.FcmTokenListenerService) 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.
6	Service (com.clevertap.android.sdk.FcmMessageListenerService) 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.
7	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) 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.
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	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

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

</> CODE ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				co/touchlab/kermit/CommonWriter.java co/touchlab/kermit/LogcatWriter.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/Utils/LogcatLogger.java com/airbnb/lottie/utils/LogcatLogger.java com/amplitude/api/AmplitudeLog.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/internal/AFg1jSDK.java com/clevertap/android/sdk/Logger.java com/clevertap/android/sdk/displayunits/CTDisplayUnitType.java com/clevertap/android/sdk/product_config/DefaultXmlParser.java com/clevertap/android/sdk/response/CleverTapResponse.java com/clevertap/android/sdk/response/CleverTapResponse.java com/hadiyarajesh/composetemplate/AppConfig/UserCredentialsPr ovider.java com/hadiyarajesh/composetemplate/Services/Analytics/Appsflyer/ AppsflyerHelperKt.java com/hadiyarajesh/composetemplate/Services/Analytics/Clevertap/ ClevertapHelperKt.iava

NO	ISSUE	SEVERITY	STANDARDS	com/hadiyarajesh/composetemplate/Services/Analytics/Intercom/l
				com/hadiyarajesh/composetemplate/Services/Analytics/SidekickAnalyticsKt\$logEvent\$1.java com/hadiyarajesh/composetemplate/Services/Analytics/SidekickAnalyticsKt\$setAttributesToAnalytics\$1.java com/hadiyarajesh/composetemplate/Services/PushNotifications/CustomParsePushReceiver\$loadImage\$1.java com/hadiyarajesh/composetemplate/Services/PushNotifications/CustomParsePushReceiver.java com/hadiyarajesh/composetemplate/Services/PushNotifications/CustomParsePushReceiverKt.java com/hadiyarajesh/composetemplate/Services/PushNotifications/SidekickMessagingService.java com/hadiyarajesh/composetemplate/model/Channel/Channel.java com/hadiyarajesh/composetemplate/model/Channel/ChannelLijava com/hadiyarajesh/composetemplate/model/Channel/ViewModel/ChannelViewModel\$protectedCheckifRead\$2.java com/hadiyarajesh/composetemplate/model/Channel/ViewModel/ChannelViewModel\$protectedCheckifRead\$2.java com/hadiyarajesh/composetemplate/model/Channel/ViewModel/ChannelViewModel.java com/hadiyarajesh/composetemplate/model/Channel/ViewModel/ChannelViewModel.java com/hadiyarajesh/composetemplate/model/FollowObject/FollowObject.java com/hadiyarajesh/composetemplate/model/Flag/Flag/Kt.java com/hadiyarajesh/composetemplate/model/JourneyCompletion/JourneyCompletionKt.java com/hadiyarajesh/composetemplate/model/JourneyCompletion/JourneyCompletionKt.java com/hadiyarajesh/composetemplate/model/Notion/Database/ViewModel.java com/hadiyarajesh/composetemplate/model/Notion/Database/ViewModel/DatabaseViewModel\$psetPagesForQuery\$1.java com/hadiyarajesh/composetemplate/model/Notion/Database/ViewModel/DatabaseViewModel\$getPagesForQuery\$1.java com/hadiyarajesh/composetemplate/model/Notion/Database/ViewModel/DatabaseViewModel\$getPagesForQuery\$1.java com/hadiyarajesh/composetemplate/model/Notion/Database/ViewModel/DatabaseViewModel\$getPagesForQuery\$1.java com/hadiyarajesh/composetemplate/model/Notion/Database/ViewModel/DatabaseViewModel\$getPagesForQuery\$1.java com/hadiyarajesh/composetemplate/model/Notion/Database/ViewModel/DatabaseViewModel\$getPagesForQuery\$1.j

				community and jestife on posete in plate in toda on the acabase in terms
NO	ISSUE	SEVERITY	STANDARDS	Model/InsurerListViewModel\$searchForMoreInsurers\$1.java com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/MasterjourneyViewmodel\$setSubjourney\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/MasterJourneyViewmodel.java
				com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/MasterJourneyViewmodelKt\$rememberSuperJourneyState\$
				1\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/MasterJourneyViewmodelKt\$rememberSuperJourneyState\$
				2\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/QualifierDatabase\$checkQualifiersForUser\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/QualifierDatabase.java
				com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/SubJourneyDatabase\$rememberFilterAndSortSubJourneys\$
				1\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/SubJourneyDatabase\$safeFetchListInBackground\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Database/View
				Model/SubJourneyDatabase.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/Insurer/I
				nsurer.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/Insurer/
				NotionInsurer.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/Journey/
				NotionJourneyModel.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/Journey/
				ViewModel/JourneyViewModel.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/NotionPa
				ge.java com/hadiyarajesh/composetemplate/model/Notion/Page/NotionPa
				geKt\$convertToParseObject\$4\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/NotionPa
				geKt\$convertToParseObject\$5\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/NotionPa
				geKt\$saveImageUrlAsParseFile\$2.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/NotionPa
				geKt.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/ParseNot
				ionPage.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/PostImag
				eGallery/DeprecatedPostImageGallery.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/PostImag

NO	ISSUE	SEVERITY	CTANDADDC	eGallery/viewiviodei/DeprecatedPostilviageListviewiviodei\$sateFetc ជ្រុំទ្រដូច្នុBackground\$1.java
NO	1550E	SEVERIT	STANDARDS	com/hadiyarajesh/composetemplate/model/Notion/Page/Qualifier
				/QualifierModel.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/Skeleton/
				SkeletonModelKt.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/Skeleton/
				ViewModel/DefaultSkeletonProvider\$fetchSkeleton\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/Skeleton/
				ViewModel/SkeletonViewModel.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/SubJourn
				ey/SubJourneyModel\$getMostRecentJourneyCompletions\$2.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/SubJourn
				ey/ViewModel/SubJourneyViewModel.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/SubJourn
				ey/ViewModel/SubJourneyViewModelKt\$rememberlsCompleted\$1 \$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/SubJourn
				ey/ViewModel/SubJourneyViewModelKt\$rememberTotalUserComp
				letionState\$1\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/SubJourn
				ey/ViewModel/SubJourneyViewModelKt.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/Unlocks/
				UnlockModel.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/ValueCon
				verter\$convert\$6\$1.java
				com/hadiyarajesh/composetemplate/model/Notion/Page/ValueCon
				verter.java
				com/hadiyarajesh/composetemplate/model/Notion/UnitTestsKt\$Jo
	The App logs information. Sensitive		CWE: CWE-532: Insertion of Sensitive	urneyDatabaseList\$2\$1.java com/hadiyarajesh/composetemplate/model/Notion/UnitTestsKt\$Re
1	information should never be logged.	info	Information into Log File	sourcesList\$3\$1.java
	intormation should never be logged.		OWASP MASVS: MSTG-STORAGE-3	com/hadiyarajesh/composetemplate/model/Post/ExtensionsKt.java
				com/hadiyarajesh/composetemplate/model/Post/QueriesKt.java
				com/hadiyarajesh/composetemplate/model/Post/ViewModel/Creat
				ePostViewModel.java
				com/hadiyarajesh/composetemplate/model/Provider/ProviderAda
				pter.java
				com/hadiyarajesh/composetemplate/model/Provider/ProviderAda
				pterKt\$willInit\$1\$2\$1.java
				com/hadiyarajesh/composetemplate/model/Provider/ProviderAda
				pterKt.java
				com/hadiyarajesh/composetemplate/model/Provider/deprecated/ DeprecatedProviderModelKt.java
				com/hadiyarajesh/composetemplate/model/Provider/viewModel/P
				roviderViewModelKt\$rememberFilteredProviders\$2\$1.java
1 1		I		. 5.1.55. Herrinodelikeri eliteriberi ikeredi Tovidel 5424 fijava

				com/hadiyarajesh/composetemplate/model/User/ExtensionsKt\$set
NO	ISSUE	SEVERITY	STANDARDS	FobES ate\$1\$1\$1.java
				com/hadiyarajesh/composetemplate/model/User/ExtensionsKt.jav
				a de la constant de l
				com/hadiyarajesh/composetemplate/model/User/UserKt\$increme
				ntPostViewCount\$1.java
				com/hadiyarajesh/composetemplate/model/User/UserKt.java
				com/hadiyarajesh/composetemplate/model/User/ViewModel/Curr entUserViewModel.java
				com/hadiyarajesh/composetemplate/model/User/ViewModel/Curr entUserViewModelKt.java
				com/hadiyarajesh/composetemplate/utility/LocationKt.java
				com/hadiyarajesh/composetemplate/utility/Print\$Companion\$safe Print\$2.java
				com/hadiyarajesh/composetemplate/view/ui/AppKt.java
				com/hadiyarajesh/composetemplate/view/ui/Notion/Cells/Unlocks
				/UnlockCellDetailsKt\$UnlockCellContents\$1.java
				com/hadiyarajesh/composetemplate/view/ui/Notion/Components/
				EmojiOrFileKt\$RenderEmojiOrFile\$1\$1.java
				com/hadiyarajesh/composetemplate/view/ui/Notion/Journey/SubJ
				ourneyCardKt.java
				com/hadiyarajesh/composetemplate/view/ui/Notion/Provider/Prov
				iderListKt\$deprecatedFilteredProvideders\$1\$1.java
				com/hadiyarajesh/composetemplate/view/ui/Notion/Provider/ProviderListKt\$deprecatedFilteredProvideders\$2\$1.java
				com/hadiyarajesh/composetemplate/view/ui/Notion/Resources/Vi deoResourceListKt.java
				com/hadiyarajesh/composetemplate/view/ui/components/Feeling/
				FeelingChartKt\$FeelingChart\$1\$1.java
				com/hadiyarajesh/composetemplate/view/ui/components/Feeling/ FeelingChartKt.java
				com/hadiyarajesh/composetemplate/view/ui/components/Forms/f
				ormsViewModel/CommentFormViewModel\$sendComment\$4\$1.ja
				va
				com/hadiyarajesh/composetemplate/view/ui/components/Forms/formsViewModel/EditProfileFormViewModel.java
				com/hadiyarajesh/composetemplate/view/ui/components/Journey /Components/MultiSelectKt.java
				,
				com/hadiyarajesh/composetemplate/view/ui/components/Journey /JourneyModalViewModel/OnboardingJourneyViewModel.java
				com/hadiyarajesh/composetemplate/view/ui/components/Journey
				/JourneySheet/Components/JourneyOwnerMessageKt\$JourneyOwn
				erMessage\$2\$1.java
				com/hadiyarajesh/composetemplate/view/ui/components/Journey
				/JourneySheet/Components/MinorComponentsKt\$creatorProfilePic ture\$2\$1.java

NO	ISSUE	SEVERITY	STANDARDS	com/hadiyarajesh/composetemplate/view/ui/components/Journey JuffeySeySheet/JourneyScheetKt\$JourneySheet\$2\$1.java com/hadiyarajesh/composetemplate/view/ui/components/Journey
				/Welcomejourney/ComposableSingletons\$WelcomejourneyPreview Kt\$lambda1\$1.java com/hadiyarajesh/composetemplate/view/ui/components/Modal/ ModalViewModel/ModalViewModel.java com/hadiyarajesh/composetemplate/view/ui/components/PopUp/ WriteReviewPopUpKt\$ShowSoberSidekickPopUp\$\$\$1.java com/hadiyarajesh/composetemplate/view/ui/components/PopUp/ WriteReviewPopUpKt.java com/hadiyarajesh/composetemplate/view/ui/components/TimeTra cker/TimeBarKt\$SoberTimeBar\$1\$1.java com/hadiyarajesh/composetemplate/view/ui/components/User/Se arch/SearchUsersViewModel\$onSearchTextChanged\$1.java com/hadiyarajesh/composetemplate/view/ui/components/keyboar ds/TextFieldKt.java com/hadiyarajesh/composetemplate/view/ui/components/keyboar ds/ReyboardViewModels/PhoneKeyboardViewModel.java com/hadiyarajesh/composetemplate/view/ui/navigation/AppNavig ationKt\$addChannelDeepLink\$2.java com/hadiyarajesh/composetemplate/view/ui/navigation/AppNavig ationKt\$popBackOnMainThread\$1.java com/hadiyarajesh/composetemplate/view/ui/navigation/RootNavig ationKt\$navigateOnMainThread\$1.java com/hadiyarajesh/composetemplate/view/ui/navigation/screens/Jo urney/JourneyScreenkt\$JourneyScreen\$2\$1.java com/hadiyarajesh/composetemplate/view/ui/navigation/screens/Jo urney/JourneyScreenkt.java com/hadiyarajesh/composetemplate/view/ui/navigation/screens/Jo urney/JourneyScreenkt.java com/hadiyarajesh/composetemplate/view/ui/navigation/screens/Jo urneyJourneyScreenkt.java com/hadiyarajesh/composetemplate/view/ui/screens/navigation/P ostDetail/PostDetailScreenKt\$PostDetailScreen\$4\$1.java com/hadiyarajesh/composetemplate/viewmodel/ListViewModel\$1o adList\$2.java com/hadiyarajesh/composetemplate/viewmodel/ListViewModel\$1o adList\$2.java com/hadiyarajesh/composetemplate/viewmodel/ListViewModel\$1o adList\$2.java com/hadiyarajesh/composetemplate/viewmodel/ListViewModel\$1o adList\$2.java com/habiyarajesh/composetemplate/viewmodel/ListViewModel\$1o nUpdate\$1.java com/habiyarajesh/composetemplate/viewmodel/ListViewModel\$1o nUpdate\$1.java com/habiyarajesh/composetemplate/viewmodel/ListViewMo

NO	ISSUE	SEVERITY	STANDARDS	com/parse/CachedCurrentInstallationController.java FILES com/parse/ConnectivityNotifier.java
				com/parse/ManifestInfo.java com/parse/NetworkQueryController.java com/parse/NetworkQueryController.java com/parse/Parse.java com/parse/ParseAnalytics.java com/parse/ParseCacheDirMigrationUtils.java com/parse/ParseDateFormat.java com/parse/ParseImpreciseDateFormat.java com/parse/ParseImpreciseDateFormat.java com/parse/ParseInstallation.java com/parse/ParseReyValueCache.java com/parse/ParsePinningEventuallyQueue.java com/parse/ParsePushBroadcastReceiver.java com/parse/ParsePushBroadcastReceiver.java com/parse/ParseRequest.java com/parse/ParseRequest.java com/parse/PushRouter.java com/parse/fcm/ParseFCM.java com/parse/fin/ParseFCM.java com/parse/livequery/OkHttp3SocketClientFactory.java com/parse/livequery/ParseLiveQueryClientImpl.java io/github/alakira/napier/DebugAntilog.java io/github/alakira/napier/DebugAntilog.java io/grpc/android/AndroidChannelBuilder.java io/grpc/android/AndroidChannelBuilder.java io/grpc/okhttp/internal/Platform.java io/ktor/tclient/features/logging/SimpleLogger.java io/ktor/ttil/CoroutinesUtilsKt.java io/ktor/util/CoroutinesUtilsKt.java io/noties/markwon/LinkResolverDef.java io/noties/markwon/PrecomputedTextSetterCompat.java junit/runner/BaseTestRunner.java junit/runner/Version.java junit/textui/TestRunner.java me/leolin/shortcutbadger/ShortcutBadger.java org/slf4j/helpers/Util.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	coil/decode/GifDecoder.java coil/decode/VideoFrameDecoder.java coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/airbnb/lottie/compose/RememberLottieCompositionKt.java com/airbnb/lottie/compose/RememberLottieCompositionKt.java com/airbnb/lottie/compose/RememberLottieCompositionKt.java com/clevertap/android/sdk/Constants.java com/clevertap/android/sdk/Constants.java com/clevertap/android/sdk/product_config/CTProductConfigConsta nts.java com/clevertap/android/sdk/product_config/DefaultXmlParser.java com/ladiyarajesh/composetemplate/AppConfig/UserCredentialsPr ovider.java com/hadiyarajesh/composetemplate/model/Dser/ExtensionsKt.java com/hadiyarajesh/composetemplate/model/User/User.java com/hadiyarajesh/composetemplate/wiew/ui/ParseUtil.java com/hadiyarajesh/composetemplate/view/ui/ParseUtil.java com/hadiyarajesh/composetemplate/view/ui/Components/User/To pUserKt.java com/hadiyarajesh/composetemplate/view/ui/components/User/UserCell/UserCellKt.java com/hadiyarajesh/composetemplate/view/ui/components/User/UserCell/UserCellKt.java com/hadiyarajesh/composetemplate/view/ui/components/User/UserCell/UserCellKt.java com/hadiyarajesh/composetemplate/view/ui/components/User/UserCell/UserCellKt.java com/hadiyarajesh/composetemplate/view/ui/components/User/UserCell/UserCellKt.java com/parse/ParseRESTCommand.java com/parse/ParseRESTCommand.java com/parse/ParseRESTCommand.java com/parse/ParseRESTCommand.java com/parse/ParseUser.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/TransportFrameUtil.java io/ktor/util/PlatformUtilsKt.java io/notes/markwon/html/GssPr

NO	ISSUE	SEVERITY	STANDARDS ncorrect Default	FILES
3	The file or SharedPreference is World Readable. Any App can read from the file	high	OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/internal/AFa1zSDK.java com/appsflyer/internal/AFb1hSDK.java com/appsflyer/internal/AFc1fSDK.java com/appsflyer/internal/AFc1fSDK.java com/hadiyarajesh/composetemplate/Services/PushNotifications/Cu stomParsePushReceiverKt.java com/parse/LocalIdManager.java com/parse/ParsePushBroadcastReceiver.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/PickFirstLoadBalancer.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/OutlierDetectionLoadBalancer.java io/grpc/util/RoundRobinLoadBalancer.java org/junit/runner/manipulation/Ordering.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/amplitude/eventexplorer/EventExplorerInfoActivity.java com/clevertap/android/sdk/inbox/CTInboxButtonClickListener.java
6	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/parse/ParseDigestUtils.java com/parse/ParseRESTCommand.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/amplitude/api/DatabaseHelper.java com/parse/OfflineSQLiteOpenHelper.java com/parse/ParseSQLiteDatabase.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amplitude/api/PinnedAmplitudeClient.java com/clevertap/android/sdk/network/SSLContextBuilder.java com/hadiyarajesh/composetemplate/templateFiles/repository/di/N etworkModule.java io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.java
9	App creates temp file. Sensitive information should never be written into a temp file.	formation should never be written into a warning OWASF		coil/decode/SourceImageSource.java com/parse/ParseCommandCache.java io/ktor/http/cio/CIOMultipartDataBase.java org/junit/rules/TemporaryFolder.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/clevertap/android/sdk/BuildConfig.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.java io/ktor/network/sockets/TcpSocketBuilder.java
11	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/clevertap/android/sdk/inapp/CTInAppBaseFullHtmlFragment.j ava

> SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libcronet.119.0.6045.31.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['read_chk', 'vsnprintf_chk', 'memcpy_chk', 'FD_SET_chk', 'FD_CLR_chk', 'FD_ISSET_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi- v7a/libcronet.119.0.6045.31.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['vsnprintf_chk', 'read_chk', 'memcpy_chk', 'FD_SET_chk', 'FD_CLR_chk', 'FD_CLR_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64- v8a/libcronet.119.0.6045.31.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['read_chk', 'vsnprintf_chk', 'memcpy_chk', 'FD_SET_chk', 'FD_CLR_chk', 'FD_CLR_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86/libcronet.119.0.6045.31.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['read_chk', 'vsnprintf_chk', 'memcpy_chk', 'FD_SET_chk', 'FD_CLR_chk', 'FD_CLSSET_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64/libcronet.119.0.6045.31.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['read_chk', 'vsnprintf_chk', 'memcpy_chk', 'FD_SET_chk', 'FD_CLR_chk', 'FD_CLR_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi- v7a/libcronet.119.0.6045.31.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk', '_read_chk', '_memcpy_chk', '_FD_SET_chk', '_FD_CLR_chk', '_FD_CLR_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64- v8a/libcronet.119.0.6045.31.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['read_chk', 'vsnprintf_chk', 'memcpy_chk', 'FD_SET_chk', 'FD_CLR_chk', 'FD_CLSET_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86/libcronet.119.0.6045.31.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with - fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['read_chk', 'vsnprintf_chk', 'memcpy_chk', 'FD_SET_chk', 'FD_CLR_chk', 'FD_CLR_chk']	True info Symbols are stripped.

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

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1cSDK.java com/appsflyer/internal/AFc1jSDK.java com/appsflyer/internal/AFf1sSDK.java com/appsflyer/internal/AFf1sSDK.java com/clevertap/android/sdk/CleverTapAPl.java com/clevertap/android/sdk/InAppNotificationActivity.java com/clevertap/android/sdk/inapp/CTInAppBaseFragment.java com/clevertap/android/sdk/inbox/CTInboxListViewFragment.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/CTPushNotificationReceiver.java com/clevertap/android/sdk/pushnotification/INotificationRenderer.java com/clevertap/android/sdk/pushnotification/LaunchPendingIntentFactory.java com/clevertap/android/sdk/pushnotification/LaunchPendingIntentFactory.java com/clevertap/android/sdk/pushnotification/LaunchPendingIntentFactory.java com/hadiyarajesh/composetemplate/Services/PushNotifications/CustomParsePushReceiverKt.j ava com/hadiyarajesh/composetemplate/Services/PushNotifications/PushNotificationHandler.java com/parse/ParsePushBroadcastReceiver.java io/noties/markwon/LinkResolverDef.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1sSDK.java com/clevertap/android/sdk/CleverTapAPI.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/CTPushNotificationReceiver.java com/clevertap/android/sdk/pushnotification/CoreNotificationRenderer.java com/clevertap/android/sdk/pushnotification/INotificationRenderer.java com/clevertap/android/sdk/pushnotification/LaunchPendingIntentFactory.java com/clevertap/android/sdk/pushnotification/LaunchPendingIntentFactory.java com/levertap/android/sdk/pushnotification/LaunchPendingIntentFactory.java com/parse/ParsePushBroadcastReceiver.javaNnotifications/CustomParsePushReceiverKt.j ava com/parse/ParsePushBroadcastReceiver.java io/noties/markwon/LinkResolverDef.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00091	Retrieve data from broadcast collection		com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1jSDK.java com/clevertap/android/sdk/CleverTapAPI.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java
00089	Connect to a URL and receive input stream from the server	command network	com/amplitude/api/ConfigManager.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/clevertap/android/sdk/Utils.java com/hadiyarajesh/composetemplate/model/Notion/Page/NotionPageKt\$saveImageUrlAsParse File\$2.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/appsflyer/internal/AFb1uSDK.java com/clevertap/android/sdk/Utils.java com/hadiyarajesh/composetemplate/model/Notion/Page/NotionPageKt\$saveImageUrlAsParse File\$2.java

RULE ID	BEHAVIOUR LABEL		FILES
00013	Read file and put it into a stream	file	coil/fetch/ContentUriFetcher.java com/airbnb/lottie/compose/RememberLottieCompositionKt.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1nSDK.java com/clevertap/android/sdk/utils/FileUtils.java com/parse/ParseCountingFileHttpBody.java com/parse/ParseFile.java com/parse/ParseFile.titls.java com/parse/ParseFileUtils.java io/grpc/TlsChannelCredentials.java io/grpc/TlsServerCredentials.java io/grpc/ttil/AdvancedTlsX509KeyManager.java io/grpc/util/AdvancedTlsX509TrustManager.java io/ktor/http/cio/ClOMultipartDataBase.java junit/runner/BaseTestRunner.java okio/Okio_JvmOkioKt.java org/junit/experimental/max/MaxHistory.java
00022	Open a file from given absolute path of the file		coil/disk/DiskCache.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/appsflyer/internal/AFg1nSDK.java com/clevertap/android/sdk/utils/ImageCache.java com/parse/ParseCacheDirMigrationUtils.java com/parse/ParseFileUtils.java
00034	Query the current data network type collection network		com/clevertap/android/sdk/Utils.java
00123	Save the response to JSON after connecting to the remote server		com/clevertap/android/sdk/Utils.java

RULE ID	BEHAVIOUR LABEL		FILES
00109	Connect to a URL and get the response code network command		com/amplitude/api/ConfigManager.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/appsflyer/internal/AFf1oSDK.java com/clevertap/android/sdk/Utils.java
00094	Connect to a URL and read data from it	command network	com/clevertap/android/sdk/Utils.java
00108	Read the input stream from given URL network command		com/clevertap/android/sdk/Utils.java
00163	Create new Socket and connecting to it	socket	io/grpc/android/UdsSocket.java io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java io/ktor/network/sockets/SocketImpl.java io/ktor/network/sockets/TCPSocketBuilderJvmKt.java io/ktor/network/sockets/TcpSocketBuilder.java io/ktor/network/sockets/UDPSocketBuilder.java io/ktor/network/sockets/UDPSocketBuilderJvmKt.java
00162	Create InetSocketAddress object and connecting to it	socket	io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java io/ktor/network/sockets/SocketImpl.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java com/hadiyarajesh/composetemplate/AppConfig/UserCredentialsProvider.java
00078	Get the network operator name	collection telephony	com/amplitude/api/DeviceInfo.java com/appsflyer/internal/AFh1cSDK.java com/clevertap/android/sdk/DeviceInfo.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1nSDK.java com/parse/ParseFile.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java com/clevertap/android/sdk/db/DBAdapter.java com/parse/ParseFile.java
00137	Get last known location of the device	location collection	com/amplitude/api/DeviceInfo.java
00115	Get last known location of the device	collection location	com/amplitude/api/DeviceInfo.java com/clevertap/android/sdk/LocationManager.java
00132	Query The ISO country code	telephony collection	com/amplitude/api/DeviceInfo.java com/hbb20/CountryCodePicker.java
00016	Get location info of the device and put it to JSON object	location collection	com/amplitude/api/AmplitudeClient.java com/clevertap/android/sdk/utils/CTJsonConverter.java
00065	Get the country code of the SIM card provider	collection	com/clevertap/android/sdk/DeviceInfo.java com/hbb20/CountryCodePicker.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java com/appsflyer/internal/AFg1nSDK.java
00191	Get messages in the SMS inbox sms		com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1qSDK.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00009	Put data in cursor to JSON object	file	com/amplitude/api/DatabaseHelper.java com/clevertap/android/sdk/db/DBAdapter.java com/parse/OfflineStore.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message sms		me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS) sms calllog collection		com/hadiyarajesh/composetemplate/AppConfig/UserCredentialsProvider.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	com/hadiyarajesh/composetemplate/AppConfig/UserCredentialsProvider.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/hadiyarajesh/composetemplate/AppConfig/UserCredentialsProvider.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/LottieCompositionFactory.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://sober-sidekick.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/97140448785/namespaces/firebase:fetch? key=AlzaSyDSyA1KjmtjHKWe5WIUhi3lf6jKKLErNMU. This is indicated by the response: {'state': 'NO_TEMPLATE'}

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.GET_ACCOUNTS, android.permission.VIBRATE
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

• OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
DOMAIN	COUNTRY/REGION

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
doh.dns.sb	ok	IP: 216.128.181.13 Country: United States of America Region: Florida City: West Palm Beach Latitude: 26.708525 Longitude: -80.065750 View: Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.112.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
smonitorsdk.s	ok	No Geolocation information available.
dnsnl.alekberg.net	ok	IP: 89.38.131.38 Country: Romania Region: Arges City: Curtea de Arges Latitude: 45.133331 Longitude: 24.683331 View: Google Map
api.notion.com	ok	IP: 172.64.146.254 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map
alekberg.net	ok	No Geolocation information available.
www.google.com	ok	IP: 142.250.69.100 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
doh.familyshield.opendns.com	ok	IP: 146.112.41.3 Country: United Kingdom of Great Britain and Northern Ireland Region: England City: London Latitude: 51.508530 Longitude: -0.125740 View: Google Map
sdlsdk.s	ok	No Geolocation information available.
nextdns.io	ok	IP: 172.67.68.89 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.youtube.com	ok	IP: 172.217.1.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
doh.quickline.ch	ok	IP: 212.60.61.246 Country: Switzerland Region: Bern City: Biel Latitude: 47.132401 Longitude: 7.244110 View: Google Map

DOMAIN	STATUS	GEOLOCATION
chromium.dns.nextdns.io	ok	IP: 155.138.130.135 Country: United States of America Region: Colorado City: Broomfield Latitude: 39.920540 Longitude: -105.086647 View: Google Map
sconversions.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
dns.levonet.sk	ok	IP: 109.236.119.2 Country: Slovakia Region: Presovsky kraj City: Levoca Latitude: 49.021729 Longitude: 20.592119 View: Google Map
odvr.nic.cz	ok	IP: 185.43.135.1 Country: Czechia Region: Praha, Hlavni mesto City: Prague Latitude: 50.088039 Longitude: 14.420760 View: Google Map
sapp.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
dns.quad9.net	ok	IP: 149.112.112 Country: United States of America Region: California City: San Francisco Latitude: 37.796986 Longitude: -122.462738 View: Google Map
dns11.quad9.net	ok	IP: 9.9.9.11 Country: United States of America Region: California City: Berkeley Latitude: 37.879318 Longitude: -122.265205 View: Google Map
dns.sb	ok	IP: 185.222.222.222 Country: Belgium Region: Brussels Hoofdstedelijk Gewest City: Brussels Latitude: 50.850449 Longitude: 4.348780 View: Google Map
developers.cloudflare.com	ok	IP: 104.16.6.189 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
svalidate.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
public.dns.iij.jp	ok	IP: 103.2.57.6 Country: Japan Region: Tokyo City: Tokyo Latitude: 35.689507 Longitude: 139.691696 View: Google Map
www.nic.cz	ok	IP: 217.31.205.50 Country: Czechia Region: Praha, Hlavni mesto City: Prague Latitude: 50.088039 Longitude: 14.420760 View: Google Map
www.gstatic.com	ok	IP: 172.217.1.3 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
app.termly.io	ok	IP: 104.18.31.234 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
android.asset	ok	No Geolocation information available.
dns64.dns.google	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sobersidekick.back4app.io	ok	IP: 3.164.92.70 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
parsefiles.back4app.com	ok	IP: 18.245.96.7 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.example.com	ok	No Geolocation information available.
doh-01.spectrum.com	ok	IP: 24.240.146.7 Country: United States of America Region: Louisiana City: Monroe Latitude: 32.509312 Longitude: -92.119301 View: Google Map
api2.amplitude.com	ok	IP: 52.39.157.96 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map

DOMAIN	STATUS	GEOLOCATION
cleanbrowsing.org	ok	IP: 51.161.115.44 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839 Longitude: -73.587807 View: Google Map
sadrevenue.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
doh.cox.net	ok	IP: 68.105.28.11 Country: United States of America Region: Florida City: Pensacola Latitude: 30.421310 Longitude: -87.216911 View: Google Map
doh.xfinity.com	ok	IP: 75.75.77.197 Country: United States of America Region: New Jersey City: Mount Laurel Latitude: 39.947819 Longitude: -74.911682 View: Google Map
scdn-ssettings.s	ok	No Geolocation information available.
parseapi.back4app.com	ok	IP: 13.33.165.124 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
regionconfig.amplitude.com	ok	IP: 13.33.165.67 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map
doh.cleanbrowsing.org	ok	IP: 185.228.168.168 Country: United States of America Region: California City: Temecula Latitude: 33.530987 Longitude: -117.103394 View: Google Map
sregister.s	ok	No Geolocation information available.
doh-02.spectrum.com	ok	IP: 24.240.146.8 Country: United States of America Region: Louisiana City: Monroe Latitude: 32.509312 Longitude: -92.119301 View: Google Map
static.wizrocket.com	ok	IP: 3.164.92.21 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
dns.google	ok	IP: 8.8.8.8 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
simpression.s	ok	No Geolocation information available.
www.quad9.net	ok	IP: 216.21.3.77 Country: United States of America Region: California City: Berkeley Latitude: 37.879318 Longitude: -122.265205 View: Google Map
sober-sidekick.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.slf4j.org	ok	IP: 159.100.250.151 Country: Switzerland Region: Vaud City: Lausanne Latitude: 46.515999 Longitude: 6.632820 View: Google Map

DOMAIN	STATUS	GEOLOCATION
developers.google.com	ok	IP: 172.217.165.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.cisco.com	ok	IP: 184.26.152.97 Country: United States of America Region: Illinois City: Chicago Latitude: 41.850029 Longitude: -87.650047 View: Google Map
dns10.quad9.net	ok	IP: 9.9.9.10 Country: United States of America Region: California City: Berkeley Latitude: 37.879318 Longitude: -122.265205 View: Google Map
doh.opendns.com	ok	IP: 146.112.41.2 Country: United Kingdom of Great Britain and Northern Ireland Region: England City: London Latitude: 51.508530 Longitude: -0.125740 View: Google Map

DOMAIN	STATUS	GEOLOCATION
ktor.io	ok	IP: 3.164.92.39 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
sars.s	ok	No Geolocation information available.
chrome.cloudflare-dns.com	ok	IP: 162.159.61.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
ip-api.com	ok	IP: 208.95.112.1 Country: United States of America Region: North Carolina City: Skyland Latitude: 35.483757 Longitude: -82.521996 View: Google Map
sviap.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ui-avatars.com	ok	IP: 104.26.8.185 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
john.doe@example.com	com/hadiyarajesh/composetemplate/model/DummyDataKt.java
testuser@example.com	com/hadiyarajesh/composetemplate/model/User/ExtensionsKt.java
this@tocommonresponse.message	com/hadiyarajesh/flower_retrofit/common/ExtendRetrofitKt.java
this@copy.slice	io/ktor/util/NIOKt.java
appro@openssl.org	lib/x86_64/libcronet.119.0.6045.31.so
appro@openssl.org	lib/arm64-v8a/libcronet.119.0.6045.31.so
appro@openssl.org	apktool_out/lib/x86_64/libcronet.119.0.6045.31.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libcronet.119.0.6045.31.so



TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Bolts	Analytics	https://reports.exodus-privacy.eu.org/trackers/403
CleverTap	Location, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/174
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
"firebase_database_url" : "https://sober-sidekick.firebaseio.com"
"google_api_key" : "AlzaSyDSyA1KjmtjHKWe5WlUhi3lf6jKKLErNMU"
"intercom_article_double_author" : "□□□□{author_first_name1}□{author_first_name2}"
"intercom_article_multiple_authors" : "DDDD{author_first_name1}DD{number_of_other_authors}D"
"intercom_article_single_author" : "□□□{author_first_name}"
"intercom_article_double_author" : "□□□{author_first_name1}□{author_first_name2}"
"sidekick_password" : "SIDEKICK_PASSWORD"
"parse_client_key" : "LXUbHdMcVHnPh2OKO6CNeEmbQPLx2HQcbfehAaNq"

POSSIBLE SECRETS
"sidekick_username" : "SIDEKICK_USERNAME"
"com.google.firebase.crashlytics.mapping_file_id" : "0000000000000000000000000000000000
"intercom_article_single_author" : "DDDD{author_first_name}"
"google_crash_reporting_api_key" : "AlzaSyDSyA1KjmtjHKWe5WlUhi3lf6jKKLErNMU"
"parse_api_key" : "Wuo5quzr8f2vZDeSSskftVcDKPUpm16VHdDLm3by"
"preference_file_key" : "com.sidekick.app.sobersidekick.sharePref"
f260dff31e4e43bdac60abc376f496bd
XWZ6tfSk4HBrFmWIVDjKccJK1O3d0Z4Uu0FCH5f2
70a98c9dd14a4cec9693c2ca99003213
9a04f079-9840-4286-ab92-e65be0885f95
568ffdd85ae142d189cf43be1a3a15a0
Np40v3BXEDjAnLqriQNI7OW3QuIVUnp0acJUfypLo77
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
0d6d78422cad08ec40cebe89d2f86130
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
1638408ac36d4e15a585bf73b48b79f6
8c473ef632ff42e4a428fa08238d2c6e

POSSIBLE SECRETS
ddaa8dd2-6d4b-41c8-a47b-8463048b375b
e2719d58-a985-b3c9-781a-b030af78d30e
c76b9b6a188d43a09957c13e835bc6a2fe7ac772-
e60440e5dc28cef6ced0de47f22ca9fab1bb23e6
a21cc48796004980a5e7bba820e0e5fe
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
LXUbHdMcVHnPh2OKO6CNeEmbQPLx2HQcbfehAaNq
a3f1ffdab3bb4368af299f1dcd07f9f7
ocrt7WW8qLcKRqiwhOfzIqbSEkxo4Vk9O9u3XMVY
796b23b4bd7c4effb2c86cbc88a4e573
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
151772b62f91af014b6f681e7ede7191
Nuo5quzr8f2vZDeSSskftVcDKPUpm16VHdDLm3by
p0c4cd1e-be09-469e-be5e-ba8291b4f224
eccb7dbe17a6499ba5ed34cd69c2226e
3731f8f3abfb422d5b0582b10be9e793

POSSIBLE SECRETS 470fa2b4ae81cd56ecbcda9735803434cec591fa 3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F 23456789abcdefghjkmnpqrstvwxyz ff1aa84dc3204c4eb15d6d7ae66a73de 7414fdebb67b4a0bb4c9b439130b85c6 3a8261022f8c69d371cfc7b7970c4624 FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901 a47afc668fab43f8872abeb60c73b7cf



Title: Sober Sidekick: Quit Drinking

Score: 4.809264 Installs: 100,000+ Price: 0 Android Version Support: Category: Health & Fitness Play Store URL: com.sidekick.app.sobersidekick

Developer Details: Empathy Health Tech, Empathy+Health+Tech, None, https://sobersidekick.com, chris@sobersidekick.com,

Release Date: Jun 26, 2021 Privacy Policy: Privacy link

Description:

The World's Largest Virtual Recovery Community Sober Sidekick - the sober community with addiction recovery support. Quit drinking alcohol today with your sober buddy app, with sobriety counter and tracker that helps you track daily your sober time. You are never alone with Sober Sidekick. Stop drinking, stay sober and get the right support. Your Sober Buddy App Quit drinking with Sober Sidekick, a sobriety and addiction recovery app for those struggling with alcohol or drugs. Our sober community members are here to support you. Receive guidance on how to stay sober and start your recovery journey today Join a judgment-free social network Alcohol addiction is fed in isolation. Immerse yourself in an understanding community of users who are on the path to recovery too. Stop drinking alcohol, take the first step and remember, you are not alone in this. Quit drinking or using drugs - start your addiction recovery journey with Sober Sidekick, your sobriety app. Track your addiction recovery daily Stay sober, day after day, from alcohol and drugs. Track your daily progress with our sobriety tracker feature. Get sober - our sobriety counter helps you count the days clean and accomplish goals and keep the motivation up: one day, 30 days, 60 days, and more. Sober Sidekick - More than a Social Network, a Valuable Sober Community Sober social networks features within the app will help you create your support system. Sober time, addiction recovery struggles, and wins can be shared in anonymous posts. Receive and lend recovery support through comments or empathy badges (likes). You can also message users directly. Alcohol or drugs recovery relies heavily on community; connect with a supportive, ego-free social network. All the addiction recovery help in one app Addiction recovery support & resources are offered in the app. Have a direct line to

24/7 AA and NA meetings. You will find motivational content and blogs to support your journey to an addiction-free life. Our sober community is here to support and has the same goal - Quit drinking or using drug and start your addiction recovery journey today. Stop drinking alcohol, seek addiction recovery and join our Sober Sidekick community today, where users have access to addiction recovery resources and daily support. Sober Sidekick - Your sobriety counter and tracker to start your addiction recovery today. Here are our app features to make your recovery journey easier: Sober Community: - Addiction recovery isn't easy; connect with accountability partners (AA meetings) to stay on track with sobriety goals - Quit drinking and receive help: AA support is available every time you reach out, guaranteed! - Our Sobriety tracker & counter app gives you everything you need to keep moving forward Sober Tracker: - Days sober can be tracked (days, weeks, months & years) - Stay clean with our sobriety counter that helps you track days clean - Sober time: track and hit milestones, then celebrate! Sober Social Network: - Sober stories: share social media posts, comments, and empathy badges (likes) - Declare "I am sober" to the world, even if it's anonymously - Sober posts are anonymous, so you can keep your identity private - Sober social network available through direct messaging feature Addiction Recovery Resources: - Addiction Recovery Counselors are available when you need help - AA meetings and NA meetings via Zoom 24/7 - Sober perspectives and support available through motivational content and blogs - Alcohol Treatment options, IOP treatments, Outpatient Programs, Substance Abuse Programs, Alcoholics Anonymous, Narcotics Anonymous, Dharma Recovery and more - unlock motivations and find what works for you! Join our sober community to receive the support you need to get sober and stay that way.

∷ SCAN LOGS

Timestamp	Event	Error
2024-11-26 16:20:05	Generating Hashes	OK
2024-11-26 16:20:05	Extracting APK	OK
2024-11-26 16:20:05	Unzipping	OK
2024-11-26 16:20:06	Getting Hardcoded Certificates/Keystores	OK
2024-11-26 16:20:06	Parsing APK with androguard	OK
2024-11-26 16:20:09	Parsing AndroidManifest.xml	OK
2024-11-26 16:20:09	Extracting Manifest Data	ОК

2024-11-26 16:20:09	Manifest Analysis Started	ОК
2024-11-26 16:20:10	Performing Static Analysis on: Sober Sidekick (com.sidekick.app.sobersidekick)	ОК
2024-11-26 16:20:10	Fetching Details from Play Store: com.sidekick.app.sobersidekick	ОК
2024-11-26 16:20:11	Checking for Malware Permissions	ОК
2024-11-26 16:20:11	Fetching icon path	ОК
2024-11-26 16:20:11	Library Binary Analysis Started	ОК
2024-11-26 16:20:11	Analyzing lib/x86_64/libcronet.119.0.6045.31.so	ОК
2024-11-26 16:20:11	Analyzing lib/x86_64/libandroidx.graphics.path.so	OK
2024-11-26 16:20:11	Analyzing lib/armeabi-v7a/libcronet.119.0.6045.31.so	ОК
2024-11-26 16:20:11	Analyzing lib/armeabi-v7a/libandroidx.graphics.path.so	ОК
2024-11-26 16:20:11	Analyzing lib/arm64-v8a/libcronet.119.0.6045.31.so	OK
2024-11-26 16:20:11	Analyzing lib/arm64-v8a/libandroidx.graphics.path.so	ОК

2024-11-26 16:20:11	Analyzing lib/x86/libcronet.119.0.6045.31.so	OK
2024-11-26 16:20:11	Analyzing lib/x86/libandroidx.graphics.path.so	ОК
2024-11-26 16:20:11	Analyzing apktool_out/lib/x86_64/libcronet.119.0.6045.31.so	OK
2024-11-26 16:20:12	Analyzing apktool_out/lib/x86_64/libandroidx.graphics.path.so	ОК
2024-11-26 16:20:12	Analyzing apktool_out/lib/armeabi-v7a/libcronet.119.0.6045.31.so	ОК
2024-11-26 16:20:12	Analyzing apktool_out/lib/armeabi-v7a/libandroidx.graphics.path.so	ОК
2024-11-26 16:20:12	Analyzing apktool_out/lib/arm64-v8a/libcronet.119.0.6045.31.so	ОК
2024-11-26 16:20:12	Analyzing apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so	ОК
2024-11-26 16:20:12	Analyzing apktool_out/lib/x86/libcronet.119.0.6045.31.so	OK
2024-11-26 16:20:12	Analyzing apktool_out/lib/x86/libandroidx.graphics.path.so	OK
2024-11-26 16:20:12	Reading Code Signing Certificate	ОК
2024-11-26 16:20:12	Running APKiD 2.1.5	ОК

2024-11-26 16:20:20	Updating Trackers Database	ОК
2024-11-26 16:20:20	Detecting Trackers	OK
2024-11-26 16:20:27	Decompiling APK to Java with JADX	ОК
2024-11-26 16:21:29	Converting DEX to Smali	ОК
2024-11-26 16:21:29	Code Analysis Started on - java_source	ОК
2024-11-26 16:21:47	Android SBOM Analysis Completed	ОК
2024-11-26 16:21:49	Android SAST Completed	ОК
2024-11-26 16:21:49	Android API Analysis Started	ОК
2024-11-26 16:21:53	Android API Analysis Completed	ОК
2024-11-26 16:21:54	Android Permission Mapping Started	ОК
2024-11-26 16:21:57	Android Permission Mapping Completed	ОК
2024-11-26 16:21:57	Android Behaviour Analysis Started	ОК

2024-11-26 16:22:02	Android Behaviour Analysis Completed	OK
2024-11-26 16:22:02	Extracting Emails and URLs from Source Code	ОК
2024-11-26 16:22:06	Email and URL Extraction Completed	ОК
2024-11-26 16:22:06	Extracting String data from APK	OK
2024-11-26 16:22:06	Extracting String data from SO	OK
2024-11-26 16:22:07	Extracting String data from Code	ОК
2024-11-26 16:22:07	Extracting String values and entropies from Code	ОК
2024-11-26 16:22:17	Performing Malware check on extracted domains	ОК
2024-11-26 16:22:34	Saving to Database	ОК

Report Generated by - MobSF v4.2.6

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.