



ANDROID STATIC ANALYSIS REPORT



 AL Habib Mobile (1.0.56)

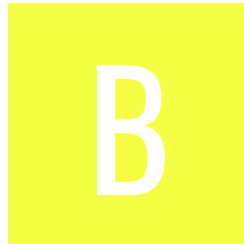
File Name: AL Habib Mobile.apk

Package Name: com.ofss.digx.mobile.obdx.bahl

Scan Date: Nov. 14, 2024, 7:48 p.m.






App Security Score: 50/100 (MEDIUM RISK)

Grade:



Trackers Detection: 8/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	18	2	3	1

FILE INFORMATION

File Name: AL Habib Mobile.apk

Size: 103.87MB

MD5: 50831bb3b973805360b1612848d729a1

SHA1: 9e28c7cf7d3a3bf77465391d062b70413c990c36

SHA256: d887e5007dfd78a476974f96d26cef1e8efcf83a96e855d69118abb1974d3659

APP INFORMATION

App Name: AL Habib Mobile

Package Name: com.ofss.digx.mobile.obdx.bahl

Main Activity: com.ofss.digx.mobile.android.SplashActivity

Target SDK: 34

Min SDK: 23

Max SDK:

Android Version Name: 1.0.56

Android Version Code: 10056

APP COMPONENTS

Activities: 17

Services: 13

Receivers: 7

Providers: 6

Exported Activities: 1

Exported Services: 2

Exported Receivers: 3

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: True

v4 signature: False

X.509 Subject: C=92, ST=Sindh, L=Karachi, O=Techlogix, OU=Financial Services, CN=Sagar Kumar

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2020-08-10 09:24:05+00:00

Valid To: 2120-07-17 09:24:05+00:00

Issuer: C=92, ST=Sindh, L=Karachi, O=Techlogix, OU=Financial Services, CN=Sagar Kumar

Serial Number: 0x65f3c03b

Hash Algorithm: sha256

md5: 7dbf68a652156943bf57bf10954b487

sha1: 874a1313aad2f270a851615a1ba30041a7f17a17

sha256: cfefc1759d4f5dfa71070e731784fb00cdef93de5b05f4424974cff6135cd3dc

sha512: 9c5c05d612337aeecf44ade3e2c3297015a9bb967b3a94327de5d9d4d0f7f524805acf508e2fa1be77b370d3bf4d6b0faff83310258549e0ccc5760a34e35ed8

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 744b340cf1afd96c73137957ac2e2ab6ab5e85330a6943532db96ee04cf85351

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

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

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check
	Compiler	unknown (please file detection issue!)
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	dx

NETWORK SECURITY

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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 7 | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
4	Activity (com.unikrew.faceoff.Fingerprint.FingerPrintScanner) 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	Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) 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.
6	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) 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.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.
9	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/a.java aa/b.java b9/k.java bb/r.java bh/a.java c2/c.java c2/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/agomezmoron/savelImageGallery/SavelImageGallery.java com/agontuk/RNFusedLocation/RNFusedLocationModule.java com/agontuk/RNFusedLocation/d.java com/bumptechnology/glides/b.java com/bumptechnology/glides/load/data/b.java com/bumptechnology/glides/load/data/j.java com/bumptechnology/glides/load/data/l.java com/learnium/RNDeviceInfo/RNDeviceInfoModule.java com/learnium/RNDeviceInfo/c.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/lwansbrough/RCTCamera/a.java com/lwansbrough/RCTCamera/b.java com/lwansbrough/RCTCamera/e.java com/ofss/digx/mobile/android/MainActivity.java com/ofss/digx/mobile/android/PeekabooConnect.java com/ofss/digx/mobile/android/plugins/BarcodeScanner.java com/ofss/digx/mobile/android/plugins/FetchPlugin.java com/ofss/digx/mobile/android/plugins/TwitterPaymentDialog/DialogInit.java com/ofss/digx/mobile/android/plugins/fingerprintauth/FingerprintAuth.java com/otpverification/AppHashGenerator.java com/reactnativecommunity/asyncstorage/c.java com/reactnativemathematics/MathematicsModule.java com/swmansion/gesturehandler/react/g.java com/swmansion/gesturehandler/react/h.java com/th3rdwave/safeareacontext/g.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/veridiumid/sdk/VeridiumSDK.java com/veridiumid/sdk/VeridiumSDKImpl.java com/veridiumid/sdk/activities/BiometricsAg gregateActivity.java com/veridiumid/sdk/analytics/Analytics.java com/veridiumid/sdk/analytics/AnalyticsLibra ryDataDumpInternalUse.java com/veridiumid/sdk/crypto/TransactionSign ingHelper.java com/veridiumid/sdk/defaultdata/securepref erences/LegacySecurePreferences.java com/veridiumid/sdk/defaults/biometricsetti ngsdefaultui/BiometricSettingsFragment.jav a com/veridiumid/sdk/fourf/ExportConfig.java com/veridiumid/sdk/fourf/FourFLoader.java com/veridiumid/sdk/fourf/camera/Camera1 PreviewView.java com/veridiumid/sdk/fourf/camera/FourFCa mera1.java com/veridiumid/sdk/fourf/camera/FourFCa mera2.java com/veridiumid/sdk/fourf/camera/ImageTa ggingQueue.java com/veridiumid/sdk/fourf/ui/FourFUIFragn ent.java com/veridiumid/sdk/fourf/ui/InstructionalDi alog.java com/veridiumid/sdk/internal/licensing/Licen singRepository.java com/veridiumid/sdk/log/Timber.java com/veridiumid/sdk/model/ManifestVeridiu mSDKModel.java com/veridiumid/sdk/model/biometrics/engi ne/impl/DecentralizedBiometricsEngineImpl. java com/veridiumid/sdk/model/biometrics/engi ne/impl/ModularBiometricProcessor.java com/veridiumid/sdk/model/biometrics/pack aging/IBiometricFormats.java com/veridiumid/sdk/model/biometrics/persi

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	stence/impl/BytesTemplatesStorage.java com/veridiumid/sdk/model/biometrics/results/BiometricResultsParser.java com/veridiumid/sdk/model/help/AssetsHelper.java com/veridiumid/sdk/security/AesCbcWithIntegrity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java com/veridiumid/sdk/support/BiometricBaseActivity.java com/veridiumid/sdk/support/help/CustomCountDownTimer.java d0/c.java d2/h.java d2/i.java d2/k.java d2/q.java d2/z.java d6/f.java e2/i.java e2/j.java e9/a.java f2/e.java f2/i.java fc/c0.java fc/e0.java fc/g0.java fc/l.java fc/y.java g2/a.java g7/b.java g7/e.java g7/i.java g7/o.java g7/s.java g7/t.java g7/z.java ga/s.java h1/d.java h2/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				h2/d.java h2/h.java h2/s.java h2/t.java h7/k.java h7/n.java hc/c.java hc/f.java i7/b.java ia/h0.java j/g.java j2/a.java j7/b.java k/c.java k0/a.java k2/b0.java k2/c.java k2/d.java k2/k.java k2/m.java k2/n.java k2/r.java k2/z.java ld/d.java md/a.java md/b.java md/c.java md/d.java n0/a.java n9/h.java nd/c.java nl/lightbase/a.java o2/a.java o2/d.java o2/j.java od/a.java pd/b.java q0/a.java q2/e.java q2/f.java q2/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q2/p.java q2/r.java q2/s.java q3/g.java qd/b.java qd/e.java r0/b.java r2/d.java rd/b.java rd/h.java rd/n.java s8/g.java sa/f.java sc/m.java sd/c.java se/a.java t/d.java t1/c.java t2/h.java td/b.java u/f.java u2/d.java u2/k.java u4/b.java u4/e.java u4/f.java u4/g.java v4/a.java v4/b.java va/g.java va/o.java w1/v.java w2/a.java w4/e.java wb/b.java x0/a.java x4/a.java x4/d.java x4/f.java x8/b.java v8/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x0/e.java xb/c.java y0/k.java y0/q0.java y1/a.java y2/a.java ya/g.java yc/a.java yc/b.java yc/c.java yc/d.java yc/k.java yc/q.java z1/d.java z1/e.java
2	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	b5/a.java com/agomezmoron/saveImageGallery/SaveImageGallery.java com/learnium/RNDeviceInfo/RNDeviceInfoModule.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java g7/y.java m5/a.java nl/xservices/plugins/SocialSharing.java pd/b.java qd/e.java yc/c.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/ofss/digx/mobile/android/plugins/fcm/MyFirebaseMessagingService.java y7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/ClipboardModule.java nl/xservices/plugins/SocialSharing.java od/a.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/veridiumid/sdk/internal/licensing/ws/LicensingServiceApi.java ve/b.java
6	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	b5/a.java com/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/n.java com/lwansbrough/RCTCamera/RCTCameraModule.java k0/a.java wb/c.java
7	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	b2/g.java cb/b.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/defaultdata/securepreferences/SecurePreferences.java com/veridiumid/sdk/internal/licensing/domain/model/License.java com/veridiumid/sdk/internal/licensing/domain/model/SdkLicense.java d2/d.java d2/p.java d2/x.java db/e.java db/w.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	bb/i.java com/veridiumid/sdk/model/help/AndroidHelper.java ga/c.java ia/h.java te/i.java
9	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/f.java i9/m0.java i9/v0.java qd/a.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/veridiumid/sdk/model/help/EncryptionUtils.java p5/c.java wb/b.java yc/k.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java
12	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	g7/y.java sc/n.java xf/a.java xf/b.java yf/a.java
13	The file or SharedPreferences is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ofss/digx/mobile/android/plugins/fingerprintauth/FingerprintAuth.java com/unikrew/faceoff/fingerprint/SecureStorage/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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	u4/c.java

NIAP ANALYSIS v1.3

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

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
---------	-----------	-------	-------

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	b5/f.java cb/f.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/lwansbrough/RCTCamera/a.java com/oblador/vectoricons/VectorIconsModule.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/analytics/AnalyticsLibraryDataDumpInternalUse.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java f0/m.java g5/c.java k0/a.java m5/a.java pd/b.java q1/b.java q1/c.java qd/e.java x1/d.java yg/h.java
00091	Retrieve data from broadcast	collection	com/veridiumid/sdk/activities/BiometricsAggregateActivity.java com/veridiumid/sdk/fourf/FourFBiometricsActivity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java g7/t.java h7/p.java pd/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ofss/digx/mobile/android/plugins/GoogleMaps.java com/ofss/digx/mobile/android/plugins/fcm/MyFirebaseMessagingService.java com/ofss/digx/mobile/android/plugins/fileopener2/FileOpener2.java g7/a0.java g7/b.java g7/t.java g7/z.java h7/a.java nl/xservices/plugins/SocialSharing.java pd/b.java qd/b.java rd/h.java yc/a.java yc/u.java
00096	Connect to a URL and set request method	command network	com/ofss/digx/mobile/android/plugins/fcm/MyFirebaseMessagingService.java ld/d.java q1/c.java x1/h.java xb/c.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/j.java com/ofss/digx/mobile/android/plugins/fcm/MyFirebaseMessagingService.java ld/d.java nl/lightbase/a.java q1/c.java x1/h.java xb/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java com/ofss/digx/mobile/android/plugins/fcm/MyFirebaseMessagingService.java ld/d.java nl/lightbase/a.java q1/c.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/agomezmoron/saveImageGallery/SaveImageGallery.java yg/h.java
00036	Get resource file from res/raw directory	reflection	com/airbnb/android/react/maps/g.java com/airbnb/android/react/maps/q.java com/dylanvann/fastimage/f.java g7/a0.java g7/b.java g7/z.java nl/xservices/plugins/SocialSharing.java p8/a.java y4/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a7/a0.java a7/w.java a7/x.java bb/a0.java cb/f.java com/airbnb/android/react/maps/f.java com/airbnb/android/react/maps/n.java com/bumptech/glide/load/a.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/reactnativecommunity/asyncstorage/c.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java com/veridiumid/sdk/security/AesCbcWithIntegrity.java f0/m.java g7/s.java gb/e.java h2/f.java ha/f.java ib/a.java k0/a.java nl/lightbase/a.java okio/p.java q1/b.java q1/c.java w6/d.java wb/c.java x1/d.java y1/a.java yc/c.java z4/b.java
00189	Get the content of a SMS message	sms	a7/w.java a7/x.java g7/t.java p5/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	a7/w.java a7/x.java g7/t.java p5/f.java
00200	Query data from the contact list	collection contact	a7/w.java a7/x.java g7/t.java p5/f.java
00201	Query data from the call log	collection callog	a7/w.java a7/x.java g7/t.java p5/f.java
00014	Read file into a stream and put it into a JSON object	file	cb/f.java ib/a.java wb/c.java
00028	Read file from assets directory	file	com/veridiumid/sdk/model/help/AssetsHelper.java
00109	Connect to a URL and get the response code	network command	com/bumptechnology/load/data/j.java ld/d.java q1/c.java x1/h.java xb/c.java
00054	Install other APKs from file	reflection	com/ofss/digx/mobile/android/plugins/fileopener2/FileOpener2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ofss/digx/mobile/android/plugins/fileopener2/FileOpener2.java g7/z.java nl/xservices/plugins/SocialSharing.java yc/a.java
00002	Open the camera and take picture	camera	com/veridiumid/sdk/fourf/camera/FourFCamera1.java x8/b.java
00183	Get current camera parameters and change the setting.	camera	com/lwansbrough/RCTCamera/RCTCameraModule.java com/lwansbrough/RCTCamera/b.java com/lwansbrough/RCTCamera/e.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java md/b.java md/d.java x8/b.java
00199	Stop recording and release recording resources	record	com/lwansbrough/RCTCamera/RCTCameraModule.java x8/b.java x8/c.java
00198	Initialize the recorder and start recording	record	com/lwansbrough/RCTCamera/RCTCameraModule.java x8/b.java x8/c.java
00194	Set the audio source (MIC) and recorded file format	record	x8/b.java x8/c.java
00197	Set the audio encoder and initialize the recorder	record	x8/b.java x8/c.java
00196	Set the recorded file format and output path	record file	x8/b.java x8/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms callog calendar	c2/c.java g7/t.java
00005	Get absolute path of file and put it to JSON object	file	cb/f.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java
00004	Get filename and put it to JSON object	file collection	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java
00147	Get the time of current location	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java
00075	Get location of the device	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java
00137	Get last known location of the device	location collection	com/reactnativecommunity/geolocation/GeolocationModule.java
00115	Get last known location of the device	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java
00058	Connect to the specific WIFI network	wifi control	td/b.java
00012	Read data and put it into a buffer stream	file	k0/a.java x1/d.java yc/c.java
00003	Put the compressed bitmap data into JSON object	camera	i7/b.java
00094	Connect to a URL and read data from it	command network	fb/a.java ld/d.java nl/lightbase/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	ld/d.java nl/lightbase/a.java
00195	Set the output path of the recorded file	record file	com/lwansbrough/RCTCamera/RCTCameraModule.java
00007	Use absolute path of directory for the output media file path	file	com/lwansbrough/RCTCamera/RCTCameraModule.java
00041	Save recorded audio/video to file	record	com/lwansbrough/RCTCamera/RCTCameraModule.java
00191	Get messages in the SMS inbox	sms	g7/b.java g7/t.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java g7/y.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java g7/y.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	com/veridiumid/sdk/security/AesCbcWithIntegrity.java
00015	Put buffer stream (data) to JSON object	file	g7/y.java
00125	Check if the given file path exist	file	g7/y.java
00104	Check if the given path is directory	file	g7/y.java
00153	Send binary data over HTTP	http	x1/h.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/c.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	g7/t.java
00187	Query a URI and check the result	collection sms calllog calendar	g7/t.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/137588857223/namespaces/firebase:fetch?key=AlzaSyA7DhAHk9aLpmHN5A7ZLEnAPRRdMC-Dvts . This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.READ_CONTACTS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_WIFI_STATE, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.VIBRATE
Other Common Permissions	5/44	android.permission.FLASHLIGHT, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, 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 MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
unikrew-faceoff-telemetry.azurewebsites.net	ok	IP: 65.52.250.96 Country: United Arab Emirates Region: Dubayy City: Dubai Latitude: 25.258169 Longitude: 55.304722 View: Google Map
meezan-faceoff-ids.covalent.pk	ok	No Geolocation information available.
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.
xml.org	ok	IP: 104.239.240.11 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: Google Map
login.bankalhabib.com	ok	IP: 103.93.208.49 Country: Pakistan Region: Sindh City: Karachi Latitude: 24.905600 Longitude: 67.082199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
purl.org	ok	IP: 207.241.225.157 Country: United States of America Region: California City: San Francisco Latitude: 37.781734 Longitude: -122.459435 View: Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
faceoffauthentication.azurewebsites.net	ok	IP: 13.77.82.141 Country: United States of America Region: Virginia City: Boydton Latitude: 36.667641 Longitude: -78.387497 View: Google Map
maps.google.com	ok	IP: 172.217.169.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
faceoffmobilebackend.azurewebsites.net	ok	IP: 13.77.82.141 Country: United States of America Region: Virginia City: Boydton Latitude: 36.667641 Longitude: -78.387497 View: Google Map

DOMAIN	STATUS	GEOLOCATION
unikrew-faceoff-licensing.azurewebsites.net	ok	IP: 65.52.250.96 Country: United Arab Emirates Region: Dubayy City: Dubai Latitude: 25.258169 Longitude: 55.304722 View: Google Map
mobile.bankalhabib.com	ok	IP: 103.93.208.51 Country: Pakistan Region: Sindh City: Karachi Latitude: 24.905600 Longitude: 67.082199 View: Google Map
firebase.google.com	ok	IP: 216.58.212.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
facebook.com	ok	IP: 157.240.9.35 Country: Bulgaria Region: Sofia (stolitsa) City: Sofia Latitude: 42.697510 Longitude: 23.324150 View: Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	IP: 142.250.184.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
developer.android.com	ok	IP: 142.251.140.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
graph-video.s	ok	No Geolocation information available.
www.googleapis.com	ok	IP: 142.251.140.10 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
graph.s	ok	No Geolocation information available.
ns.useplus.org	ok	IP: 54.83.4.77 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
firebase-settings.crashlytics.com	ok	IP: 172.217.17.227 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
iptc.org	ok	IP: 3.64.29.21 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
api.whatsapp.com	ok	IP: 157.240.9.53 Country: Bulgaria Region: Sofia (stolitsa) City: Sofia Latitude: 42.697510 Longitude: 23.324150 View: Google Map

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
www.npes.org	ok	IP: 172.67.183.61 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
.facebook.com	ok	No Geolocation information available.
developers.facebook.com	ok	IP: 157.240.9.18 Country: Bulgaria Region: Sofia (stolitsa) City: Sofia Latitude: 42.697510 Longitude: 23.324150 View: Google Map
cipa.jp	ok	IP: 118.82.81.189 Country: Japan Region: Tokyo City: Tokyo Latitude: 35.689507 Longitude: 139.691696 View: Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	IP: 142.250.187.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
xerces.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
licensing.prod.veridium-dev.com	ok	IP: 35.158.19.174 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
www.w3.org	ok	IP: 104.18.22.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.aiim.org	ok	IP: 199.60.103.225 Country: United States of America Region: Massachusetts City: Cambridge Latitude: 42.370129 Longitude: -71.086304 View: Google Map
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"KEY_OAM_URL" : "https://login.bankalhabib.com/oauth2/rest/token"
"KEY_OAUTH_PROVIDER_URL" : "https://login.bankalhabib.com/oauth2/rest/token"
"KEY_SERVER_URL" : "https://mobile.bankalhabib.com"
"X_TOKEN_TYPE" : ""

POSSIBLE SECRETS

```
"com.google.firebase.crashlytics.mapping_file_id" : "46c88422b4f24a6ea77233494392b54d"
```

```
"google_api_key": "AlzaSyA7DhAHk9aLpmHN5A7ZLEnAPRRdMC-Dvts"
```

```
"google_crash_reporting_api_key" : "AlzaSyA7DhAHk9aLpmHN5A7ZLEnAPRRdMC-Dvts"
```

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

e44046539bb5b584279553ca6eacca937c8e16cf

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

5e8f16062ea3cd2c4a0d547876baa6f38cabf625

9b8f518b086098de3d77736f9458a3d2f6f95a37

470fa2b4ae81cd56ecbda9735803434cec591fa

ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmlRyb2lkLmFwcHMubWVzc2FnZW5n

3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f

cc2751449a350f668590264ed76692694a80308a

21c8b5470a64adbb25bc84316cbc449361d86839

2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

POSSIBLE SECRETS
258EAF5-E914-47DA-95CA-C5AB0DC85B11
6e2c7e24b7c7eae9fc94882c9f31befa00594872

PLAYSTORE INFORMATION

Title: AL Habib Mobile

Score: 2.92 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** [com.ofss.digx.mobile.obdx.bahl](https://play.google.com/store/apps/details?id=com.ofss.digx.mobile.obdx.bahl)

Developer Details: Bank AL Habib, Bank+AL+Habib, None, <https://www.bankalhabib.com/>, info@bankalhabib.com,

Release Date: Aug 17, 2020 **Privacy Policy:** [Privacy link](#)

Description:

Experience hassle-free banking with the new AL Habib Mobile app designed to make your digital banking experience more convenient. Manage your finances quickly and securely with a host of new features that provide you with an enhanced user experience. Here's What's New: · Multiple Funds Transfers · Multiple Bill Payments · Instant Stop Cheque Facility · Credit Card bill payment of other banks through the 1BILL feature · Withholding tax and Balance Certificate · Forex Calculators · Transaction Based OTP · Retrieve User ID by using "Forgot User ID" option without calling the Helpline · Set frequent payments as Favourites on the main dashboard

SCAN LOGS

Timestamp	Event	Error
2024-11-14 19:48:16	Generating Hashes	OK
2024-11-14 19:48:16	Extracting APK	OK

2024-11-14 19:48:16	Unzipping	OK
2024-11-14 19:48:19	Getting Hardcoded Certificates/Keystores	OK
2024-11-14 19:48:19	Parsing APK with androguard	OK
2024-11-14 19:48:29	Parsing AndroidManifest.xml	OK
2024-11-14 19:48:29	Extracting Manifest Data	OK
2024-11-14 19:48:29	Performing Static Analysis on: AL Habib Mobile (com.ofss.digx.mobile.obdx.bahl)	OK
2024-11-14 19:48:29	Fetching Details from Play Store: com.ofss.digx.mobile.obdx.bahl	OK
2024-11-14 19:48:31	Manifest Analysis Started	OK
2024-11-14 19:48:31	Checking for Malware Permissions	OK
2024-11-14 19:48:31	Fetching icon path	OK
2024-11-14 19:48:31	Library Binary Analysis Started	OK

2024-11-14 19:48:32	Reading Code Signing Certificate	OK
2024-11-14 19:48:34	Running APKiD 2.1.5	OK
2024-11-14 19:48:42	Detecting Trackers	OK
2024-11-14 19:48:44	Decompiling APK to Java with JADX	OK
2024-11-14 19:49:05	Converting DEX to Smali	OK
2024-11-14 19:49:05	Code Analysis Started on - java_source	OK
2024-11-14 19:49:16	Android SAST Completed	OK
2024-11-14 19:49:16	Android API Analysis Started	OK
2024-11-14 19:49:20	Android API Analysis Completed	OK
2024-11-14 19:49:20	Android Permission Mapping Started	OK
2024-11-14 19:49:31	Android Permission Mapping Completed	OK

2024-11-14 19:49:32	Email and URL Extraction Completed	OK
2024-11-14 19:49:32	Android Behaviour Analysis Started	OK
2024-11-14 19:49:38	Android Behaviour Analysis Completed	OK
2024-11-14 19:49:38	Extracting String data from APK	OK
2024-11-14 19:49:38	Extracting String data from Code	OK
2024-11-14 19:49:38	Extracting String values and entropies from Code	OK
2024-11-14 19:49:41	Performing Malware check on extracted domains	OK
2024-11-14 19:49:59	Saving to Database	OK

Report Generated by - MobSF v4.1.9

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](#).