MOBSF

ANDROID STATIC ANALYSIS REPORT

Dost (9.5.5)

File Name:	Dost.apk
Package Name:	com.mobilinkbank
Scan Date:	Jan. 5, 2025, 12:06 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	14	3	3	1

FILE INFORMATION

File Name: Dost.apk
Size: 41.35MB
MD5: 482d45c13a1729546802038ed1b6d97f
SHA1: e6d056264ebf39f8e7ae170bc802175818d8c0c6
SHA256: e41748ce7be2046453cef38917c9baf06e5cb612f1bd613ce73edb9854bc4fea

APP INFORMATION

App Name: Dost
Package Name: com.mobilinkbank
Main Activity: com.mobilinkbank.MainActivity
Target SDK: 34
Min SDK: 27
Max SDK:
Android Version Name: 9.5.5

Android Version Code: 53

APP COMPONENTS

Activities: 16
Services: 13
Receivers: 8
Providers: 9
Exported Activities: 0
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: CN=Muhammad Ashraf, OU=ITO, O=Mobilink Microfinance Bank Limited, L=Karachi, S=Sindh, C=PK
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-01-23 06:56:03+00:00
Valid To: 2047-01-16 06:56:03+00:00
Issuer: CN=Muhammad Ashraf, OU=ITO, O=Mobilink Microfinance Bank Limited, L=Karachi, S=Sindh, C=PK
Serial Number: 0x56055b78
Hash Algorithm: sha256
md5: 0d5c4082da685f0a99d867ebeb06b138
sha1: 6cd02896d729b6ad0e57685af54555a47ab1b354
sha256: 172cbf83ce1fb6d901314187d1589b88664fe7f423b250e7bd3f7eb7c49790a8
sha512: 681f5b66e908b9db15b4fbc857828206bc396a09d9a0d84a578e136d27d744550572fed01fd58e10f8140a307f4ed5ae22134e9f48f22be77892339418c05631
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 0ebdc42749803cf98d24aec7a451e35e77fb2a7c5f705c6fdb53a833e7aecd9c
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.mobilinkbank.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 5 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.1, minSdk=27]	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	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
3	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.
4	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.
5	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: 2 | WARNING: 7 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	b7/a.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java io/flutter/plugins/pathprovider/Messages.java io/flutter/plugins/pathprovider/PathProviderPlugin.java p9/a.java
				b1/o.java c0/d.java com/baseflow/geolocator/a.java com/veridiumid/sdk/analytics/AnalyticsLibraryDataDumpInternalUse.java com/veridiumid/sdk/fourf/ui/InstructionalDialog.java com/veridiumid/sdk/log/Timber.java d0/f.java g3/a.java io/flutter/Log.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivity.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterFragment.java io/flutter/embedding/android/FlutterFragmentActivity.java io/flutter/embedding/android/FlutterImageVi

NO	ISSUE	SEVERITY	STANDARDS	FILES
	The App logs information. Sensitive		CWE: CWE-532: Insertion of Sensitive	ew.java io/flutter/embedding/android/FlutterSurfaceView.java io/flutter/embedding/android/FlutterTextureView.java io/flutter/embedding/android/FlutterView.java io/flutter/embedding/android/KeyEmbedderResponder.java io/flutter/embedding/android/KeyboardManager.java io/flutter/embedding/engine/FlutterEngine.java io/flutter/embedding/engine/FlutterEngineConnectionRegistry.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/dart/DartExecutor.java io/flutter/embedding/engine/dart/DartMessenger.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/loader/ResourceExtractor.java io/flutter/embedding/engine/plugins/shim/ShimPluginRegistry.java io/flutter/embedding/engine/plugins/shim/ShimRegistrar.java io/flutter/embedding/engine/plugins/util/GeneratedPluginRegister.java io/flutter/embedding/engine/renderer/FlutterRenderer.java io/flutter/embedding/engine/systemchannels/AccessibilityChannel.java io/flutter/embedding/engine/systemchannels/BackGestureChannel.java io/flutter/embedding/engine/systemchannels

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	Information into Log File OWASP MASVS: MSTG-STORAGE-3	/DeferredComponentChannel.java io/flutter/embedding/engine/systemchannels/KeyEventChannel.java io/flutter/embedding/engine/systemchannels/LifecycleChannel.java io/flutter/embedding/engine/systemchannels/LocalizationChannel.java io/flutter/embedding/engine/systemchannels/MouseCursorChannel.java io/flutter/embedding/engine/systemchannels/NavigationChannel.java io/flutter/embedding/engine/systemchannels/PlatformChannel.java io/flutter/embedding/engine/systemchannels/PlatformViewsChannel.java io/flutter/embedding/engine/systemchannels/RestorationChannel.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/embedding/engine/systemchannels/SpellCheckChannel.java io/flutter/embedding/engine/systemchannels/SystemChannel.java io/flutter/embedding/engine/systemchannels/TextInputChannel.java io/flutter/plugin/common/BasicMessageChannel.java io/flutter/plugin/common/EventChannel.java io/flutter/plugin/common/MethodChannel.java io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/editing/ListenableEditingState.java io/flutter/plugin/editing/TextEditingDelta.java io/flutter/plugin/editing/TextInputPlugin.java io/flutter/plugin/platform/ImageReaderPlatformViewRenderTarget.java io/flutter/plugin/platform/PlatformPlugin.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/plugin/platform/PlatformViewWrapper.java io/flutter/plugin/platform/PlatformViewsController.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/plugin/platform/SingleViewWindowManager.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/plugins/imagepicker/FileUtils.java io/flutter/plugins/urllauncher/UrlLauncherPlugin.java io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/FlutterNativeView.java io/flutter/view/FlutterView.java j0/o0.java j0/q.java n1/a.java o7/f.java q3/a.java w0/u0.java
				com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/URLCredentialContract.java com/pichillilorenzo/flutter_inappwebview_android/types/ClientCertResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/HttpAuthResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/URLCredential.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/defaultdata/securepreferences/SecurePreferences.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/veridiumid/sdk/internal/licensing/domain/model/License.java com/veridiumid/sdk/internal/licensing/domain/model/SdkLicense.java
3	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	io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterActivityLaunchConfigs.java io/flutter/embedding/engine/loader/ApplicationInfoLoader.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/plugin/editing/SpellCheckPlugin.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingUtils.java io/flutter/plugins/googlemaps/Convert.java io/flutter/plugins/imagepicker/ImagePickerCache.java io/flutter/plugins/sharedpreferences/SharedPreferencesPigeonOptions.java v/b.java
4	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	t/w.java y2/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/pichillilorenzo/flutter_inappwebview_android/credential_database/CredentialDatabaseHelper.java h7/i.java u3/m0.java u3/t0.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	io/flutter/plugins/imagepicker/ImagePickerDelegate.java m5/c.java n1/a.java p9/a.java
7	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	n8/a.java n8/b.java o8/a.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	y2/b.java
9	The file or SharedPreference 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/unikrew/faceoff/fingerprint/SecureStorage/c.java com/unikrew/faceoff/liveness/SecureStorage/c.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 m5/b.java w7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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 f7/a.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java f7/b.java
13	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	io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/platform/PlatformPlugin.java
14	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 e9/c.java

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	b7/a.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsChannelDelegate.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/TrustedWebActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java e3/a.java f3/a.java f3/p.java f3/t.java io/flutter/plugins/imagepicker/ImagePickerDelegate.java io/flutter/plugins/urllauncher/UrlLauncher.java v/c.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java e3/a.java f3/a.java f3/p.java f3/t.java io/flutter/plugins/urllauncher/UrlLauncher.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	b7/a.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java e3/a.java f3/a.java f3/p.java p/y0.java
00091	Retrieve data from broadcast	collection	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ActionBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java com/veridiumid/sdk/activities/BiometricsAggregateActivity.java com/veridiumid/sdk/fourf/FourFBiometricsActivity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java
00022	Open a file from given absolute path of the file	file	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/analytics/AnalyticsLibraryDataDumpInternalUse.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java g1/m.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/plugins/imagepicker/ImagePickerDelegate.java io/flutter/plugins/pathprovider/PathProviderPlugin.java n1/a.java
00104	Check if the given path is directory	file	io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00002	Open the camera and take picture	camera	com/veridiumid/sdk/fourf/camera/FourFCamera1.java
00183	Get current camera parameters and change the setting.	camera	com/unikrew/faceoff/liveness/common/d.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java
00013	Read file and put it into a stream	file	com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/Util.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java com/unikrew/faceoff/liveness/SecureStorage/b.java com/veridiumid/sdk/security/AesCbcWithIntegrity.java g1/m.java h8/i.java j/n.java j0/h.java l2/b0.java m0/c0.java m5/c.java n1/a.java o7/e.java
00202	Make a phone call	control	f3/t.java
00203	Put a phone number into an intent	control	f3/t.java
00096	Connect to a URL and set request method	command network	com/pichillilorenzo/flutter_inappwebview_android/Util.java k3/d.java n5/c.java
00089	Connect to a URL and receive input stream from the server	command network	k3/d.java n5/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	k3/d.java n5/c.java
00014	Read file into a stream and put it into a JSON object	file	m5/c.java
00003	Put the compressed bitmap data into JSON object	camera	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java x0/p.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java x0/p.java
00175	Get notification manager and cancel notifications	notification	j0/o0.java
00162	Create InetSocketAddress object and connecting to it	socket	k9/f.java k9/k.java
00163	Create new Socket and connecting to it	socket	k9/f.java k9/k.java
00012	Read data and put it into a buffer stream	file	n1/a.java
00005	Get absolute path of file and put it to JSON object	file	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/FlutterImageView.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/FlutterImageView.java
00147	Get the time of current location	collection location	j/s.java
00075	Get location of the device	collection location	j/s.java
00115	Get last known location of the device	collection location	j/s.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview_android/Util.java
00030	Connect to the remote server through the given URL	network	com/pichillilorenzo/flutter_inappwebview_android/Util.java
00094	Connect to a URL and read data from it	command network	com/pichillilorenzo/flutter_inappwebview_android/Util.java
00024	Write file after Base64 decoding	reflection file	com/veridiumid/sdk/security/AesCbcWithIntegrity.java
00191	Get messages in the SMS inbox	sms	p/y0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00121	Create a directory	file command	k0/a.java
00125	Check if the given file path exist	file	k0/a.java
00192	Get messages in the SMS inbox	sms	p9/a.java
00028	Read file from assets directory	file	com/veridiumid/sdk/model/help/AssetsHelper.java io/flutter/embedding/engine/loader/ResourceExtractor.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/561575225539/namespaces/firebase:fetch?key=AIzaSyD9wvcAY65mc49aGnfH-rrrx29wCl0JdZM. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	4/44	android.permission.FLASHLIGHT, 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 MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 216.58.210.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
licensing.prod.veridium-dev.com	ok	**IP:** 3.64.32.202 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
unikrewutilsbackend.azurewebsites.net	ok	**IP:** 104.45.1.117 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.
firebase.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 93.184.215.14 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
faceoffauthentication.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
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.
faceoffmobilebackend.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

DOMAIN	STATUS	GEOLOCATION
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
facial-spoof-detection2.services-backend.com	ok	**IP:** 104.26.14.87 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
issuetracker.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
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
"FACEOFF_API" : "MjA5LDE4MSw3NCwyMjYsMTcxLDE0LDI0Nyw5MSw5LDIxMywyMTgsNzEsNTYsMTg4LDY4LDIzOSw3OSwyNTMsMiwxMjMsMTg5LDEzNSwxMTcsMTczLDIyMiw5NSwyMTYsMTgxLDE3Myw0LDE3OCwyNDEsMjksMzksNDUsMTI5LDI0Nyw5NiwyNDYsNzUsMTY3LDExOCwxMDYsMjIxLDE0OSwyMjgsOTgsNDMsMTQ2LDMwLDE1NywyMzksOTAsMTY5LDEwOSwyNDUsMTAzLDE1OCw1LDExNywxOCwyNCw5NSw5OSwxODksOTUsNjksMjIzLDQ5LDEzNSwxMTEsNzksMTA4LDMsMjM0LDMsOSwxNDUsMTQwLDIxOCw1MCwxNDIsMzksMjQ0LDEwOCw4MCwyMjksMjIxLDUzLDEzNCwxMzEsMjQwLDg3LDIzNCwxOTUsMTEyLDE3LDIyNCwyMDUsMTI4LDE3MiwyMjYsMjQ0LDI3LDIwOSwxMDYsMTYxLDI0MSw4MywzMSwxNzYsMTYxLDE3NCwyMzEsNjUsMTMsMTc4LDI0OSwyMjksMTA1LDg1LDE4NCwxMDIsMTk1LDIxNCwxNzksNjIsMTQyLDE2NywyNDAsMTMwLDE3LDIxNSw0NSwyNTQsNDcsNTQsNjAsNDYsNzYsNDUsMTMsODYsMzIsNywyMTUsOSwxNzksMSwxODQsMjQ4LDI1MSw4NSwxMTMsMTYxLDIyNSwxNTksMjQsOTIsMjEyLDIyMywxNjAsMTIxLDIwOCwxMTcsMTM2LDExNiwyOSw0MiwxMDgsMTMyLDExOCw5MiwxNTgsMTE1LDg3LDIwMywxMDEsNzAsMTgyLDEsNDQsMTYxLDE5MCwyMTEsOTQsOTUsMTk0LDIyMCwxOTUsMjM3LDIwNyw0LDEwOCwyMjksMjUzLDEyLDQzLDkyLDE4NSwxNDQsMTcsMjcsNDIsMjM4LDY0LDEzNiwxODksMTgsNywyMjIsMjM2LDE4OCwxNzIsMTg5LDI2LDE1MiwxNzMsMjAsMjAxLDIyMiwxMDIsMjI2LDI0NCwxNjEsOTIsMTIwLDE5MywxMzUsNDYsNTksMTQwLDUsMjUwLDU0LDkyLDE0OCwyMjUsNDQsMTk0LDQ2LDE2Myw4Myw2MCwyMDQsMTU1LDE0MCw3OCwzMywxOTIsMjM4LDIzOCwxNDksMjMxLDE0LDIxNywxLDAsMSw="

POSSIBLE SECRETS
"FINGERPRINT_API" : "MjM5LDIzLDI0MiwxOTQsMTE4LDYsNjQsMTY3LDYyLDEyNywyMjQsOSwyMDMsMjExLDc0LDg0LDE3OCwyMzgsNDIsMTgxLDIxNywyMDIsMjYsMjUxLDIxMCw3MSwyMzgsMTAyLDE1NCw3MywyMTIsOTksMSwxODUsMTUwLDEyLDExNCwyNDEsMTc1LDc2LDk0LDIzMCwxMjAsMTMwLDIwMSwyNTAsMTg2LDIyNyw1OSw5NCwyMzIsNTYsMTUwLDIzNCw3NCw1OCwxMzgsODYsMTE3LDEwOSwxMzcsNzMsMTEsMjI4LDEwMiwxMDYsMjIsNDIsMTc4LDExOSwzOCwxNSwzOSwxMjAsMTYxLDIwOCwyOCwyMiwzNywxOCw5NSwxMjMsMTQ1LDE5NSwxMzgsMTM3LDE1LDE4NywyNCwxODIsMjEyLDE5LDIzLDIzMCwyMzYsOTIsMTQ3LDEzOCwxNzksMjE4LDE4NCwxMTYsMCwxMzQsOTIsMTkyLDIyMSwyMjUsMTU5LDI0OSw0MSwxNDMsMjI5LDIxMiwxMjMsMTY2LDIzNCwyMDksMjcsMzYsMTQ5LDIwMywyMjEsMzcsMTQ5LDIzLDQ1LDI0NSwyMzEsMjQ0LDY5LDIzMCwyMTEsNDYsMTg1LDY2LDM2LDc3LDc1LDI2LDM2LDIwMCwxNzgsMTAyLDEwMiwyNDUsMTczLDE0MywxNTAsMTg5LDUxLDM3LDgxLDg3LDE1NCwxNjYsNjIsMiwxNzIsNjIsMjM0LDM1LDQsNDgsMTAxLDQ1LDEwMSwxMjksMTcyLDE4NSw5MSwyMzIsMjQyLDczLDIwOCwzOCwxOTQsMTE0LDE5NSwxODEsMjE2LDc1LDEzMCw1MiwxNTIsMjAwLDExNiwxNjAsMTIyLDE3NCwyNDksOSwyMzUsMjEwLDE5Nyw3MiwxNCwyNDMsMTI1LDExOCwyNDMsMTA1LDEwMywxMDMsMjUxLDE0OCwyMzgsOTAsMTc3LDAsMTY5LDEzMywxNSwxNTYsMTM5LDIzOSwxMTMsMTk5LDIwOSwxNDgsMTkyLDIwOCwxMzgsMzIsMiwyMTUsMTk1LDE4MSw0MCwxMzcsNDQsMjQ0LDAsMTA2LDI1MSwxMjcsMTQzLDE3NywxNTksMTY0LDg0LDE3MCw3MiwxNzcsMTI2LDE3NCw1MSwyMDMsODcsMTA5LDIyOSw1OCwxODIsMjA5LDQyLDYzLDEsMCwxLA=="
"GOOGLE_MAPS_API_KEY" : "AIzaSyAgkU429i4BDN7CSkrOq1uz0NfCB16_LBY"
"google_api_key" : "AIzaSyD9wvcAY65mc49aGnfH-rrrx29wCl0JdZM"
"google_crash_reporting_api_key" : "AIzaSyD9wvcAY65mc49aGnfH-rrrx29wCl0JdZM"
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy

PLAYSTORE INFORMATION

Title: DOST – Powered by MMBL

Score: 4.0833335 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.mobilinkbank

Developer Details: Mobilink Microfinance Bank Limited, Mobilink+Microfinance+Bank+Limited, 3-A/2, Kaghan Road, F-8 Markaz, Islamabad, Pakistan, http://www.mobilinkbank.com, info@mobilinkbank.com,

Release Date: Jul 13, 2021 **Privacy Policy:** Privacy link

Description:

Introducing the Enhanced DOST App – Powered by Mobilink Microfinance Bank Limited (MMBL), Pakistan's largest digital bank, designed to offer convenient, secure, and accessible online banking services to MMBL account holders nationwide. At MMBL, we are committed to staying at the forefront of providing inclusive financial services to our valued customers. Now, effortlessly send up to PKR 1,500,000 per day from anywhere, at any time . Watch your savings grow with yearly profits at the market's best rates . Apply for loans right from the comfort of your home, pay your bills with ease , and top up your mobile phone in seconds . For our female customers, female-centric app layout is available ♀, and Gold Loan customers can quickly renew their loans with ease . Experience hassle-free banking and save valuable time with the New DOST app. MMBL customers can access a wide range of functions offered by the new DOST app 24/7. Access to all of your account information is available in real-time. Key elements include: * New and Improved UI with New Logo (New Feature) * Account title fetched (New Feature) * Guest mode for Non-Account Holders * Account maintenance certificate * Statement downloads with date range selection (New Feature) * Withholding tax certificate & Bank statement download up to 2 years * In App Biometric verification * Face ID * Customized Women Centric theme (New Feature) ♀ * Repay and Repurchase Gold based loans from Dost app, without branch visit. * Open a New Account * Login (with Existing Account) * Signup (with Existing Account) * Account Summary * Customer Profile Management * Branch & ATM Locator *Contact us via email, WhatsApp or phone number * Money Transfer to MMBL * Money Transfer Other Bank Accounts * Loan Application * Fori cash, Fori cash Plus, just click on Loans section * Earn from Investment in Term Deposits (TDR) * Earn Profit UI Changed-TDR (New Feature) * Available in English & Urdu language * View MMBL loan products on login screen under product tab * Utility Bill Payment * Mobile Top-up * Favorites Management * Request for Instrument * Block Cheque * Loan Summary * Debit Card Management * PIN Changing * Temporary Card Blocking * Card Unblocking * Permanent Card Blocking * Complaint Registration * Password Changing/Reset With the enhanced UI design, MMBL customers can access a wide array of digital banking services and perform various transactions with ease using the New DOST App. Manage money transfers, bill payments, mobile top-ups, loan details, e-statements, check and debit card management, and much more, all with just a few clicks. The New DOST App provides access to over a hundred billers, including utility providers, telecom companies, government institutions, the Securities and Exchange Commission of Pakistan (SECP), airlines, internet service providers (ISPs), educational institutions, and more. In addition, the New DOST app provides 24/7 continuous and quick access to the MMBL Customer Support Team via instant WhatsApp Chat, email and Contact number which can be accessed from the homepage of the app. DOST-Aapka Mukammal Digital Bank empowers you with the convenience of digital banking wherever you are, as soon as you download the app. For Internet banking, you can also use the same set of features by going to dost.mobilinkbank.com from your browser. To learn more about our products and services and have an effortless digital banking experience, visit www.mobilinkbank.com or connect with us on Facebook: https://web.facebook.com/MobilinkMicrofinanceBankLimited Twitter: https://twitter.com/mobilinkbank LinkedIn: https://www.linkedin.com/company/mobilink-microfinance-bank-ltd YouTube Channel: https://www.youtube.com/@mobilinkmicrofinancebank2901 Tiktok Channel: https://www.tiktok.com/@mobilinkbank2

SCAN LOGS

Timestamp	Event	Error
2025-01-05 00:06:40	Generating Hashes	OK

2025-01-05 00:06:40	Extracting APK	OK
2025-01-05 00:06:40	Unzipping	OK
2025-01-05 00:06:41	Parsing APK with androguard	OK
2025-01-05 00:06:41	Extracting APK features using aapt/aapt2	OK
2025-01-05 00:06:41	Getting Hardcoded Certificates/Keystores	OK
2025-01-05 00:06:44	Parsing AndroidManifest.xml	OK
2025-01-05 00:06:44	Extracting Manifest Data	OK
2025-01-05 00:06:44	Manifest Analysis Started	OK
2025-01-05 00:06:44	Performing Static Analysis on: Dost (com.mobilinkbank)	OK
2025-01-05 00:06:44	Fetching Details from Play Store: com.mobilinkbank	OK
2025-01-05 00:06:45	Checking for Malware Permissions	OK

2025-01-05 00:06:45	Fetching icon path	OK
2025-01-05 00:06:45	Library Binary Analysis Started	OK
2025-01-05 00:06:45	Reading Code Signing Certificate	OK
2025-01-05 00:06:46	Running APKiD 2.1.5	OK
2025-01-05 00:06:50	Updating Trackers Database....	OK
2025-01-05 00:06:50	Detecting Trackers	OK
2025-01-05 00:06:55	Decompiling APK to Java with JADX	OK
2025-01-05 00:07:34	Converting DEX to Smali	OK
2025-01-05 00:07:34	Code Analysis Started on - java_source	OK
2025-01-05 00:07:36	Android SBOM Analysis Completed	OK
2025-01-05 00:08:15	Android SAST Completed	OK

2025-01-05 00:08:15	Android API Analysis Started	OK
2025-01-05 00:08:51	Android API Analysis Completed	OK
2025-01-05 00:08:52	Android Permission Mapping Started	OK
2025-01-05 00:09:27	Android Permission Mapping Completed	OK
2025-01-05 00:09:28	Android Behaviour Analysis Started	OK
2025-01-05 00:09:32	Android Behaviour Analysis Completed	OK
2025-01-05 00:09:32	Extracting Emails and URLs from Source Code	OK
2025-01-05 00:09:36	Email and URL Extraction Completed	OK
2025-01-05 00:09:36	Extracting String data from APK	OK
2025-01-05 00:09:36	Extracting String data from Code	OK
2025-01-05 00:09:36	Extracting String values and entropies from Code	OK

2025-01-05 00:09:40	Performing Malware check on extracted domains	OK
2025-01-05 00:09:42	Saving to Database	OK

Report Generated by - MobSF v4.2.9

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.