ANDROID STATIC ANALYSIS REPORT

MCB Live (2.20.800215)

File Name:	MCB Live.apk
Package Name:	com.mcb.mcblive
Scan Date:	Nov. 14, 2024, 8:26 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
3	14	2	2	2

FILE INFORMATION

File Name: MCB Live.apk
Size: 113.86MB
MD5: 9dd0aa902af6b3a82856797e865000c7
SHA1: 14bf24e784233e7926b895d1a6232a54ddb6d890
SHA256: b9d2697a68ce1d57129a22f33b0bdcfd625e848bd2a27d241d5c2138c529b949

APP INFORMATION

App Name: MCB Live
Package Name: com.mcb.mcblive
Main Activity: com.ofss.digx.mobile.android.SplashActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 2.20.800215

Android Version Code: 800215

APP COMPONENTS

Activities: 18
Services: 18
Receivers: 10
Providers: 10
Exported Activities: 4
Exported Services: 1
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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-09-07 10:16:09+00:00
Valid To: 2051-09-07 10:16:09+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe3f7b86fe8f2492a22b1c4e79bba1284b03d51c6
Hash Algorithm: sha256
md5: dda91af4aba21de20d978707c3410933
sha1: 0c6989861c6309f7895b085734f783f0b83c13ef
sha256: 5b9027ebb2354e7dcf3a71808c07eeeaba29374de896fcbd159f59297d62be81
sha512: d191b06b0e7429a357041e398942c9937a8b0ee580161bbedd340340e177b4dbdb61b79048f18a9d39a0703027f0f5924407ae76536687b67e68a4b47b0bdc6e
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: d029d0f48046f356da20c7e708dba5a0a7596c115a95dd3fa6551e094a00732b
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
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.
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.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.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
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.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.
com.google.android.providers.gsf.permission.READ_GSERVICES	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.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.

PERMISSION	STATUS	INFO	DESCRIPTION
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
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.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>9dd0aa902af6b3a82856797e865000c7.apk</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table></td></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.MANUFACTURER check
possible Build.SERIAL check
possible VM check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table></td></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.ofss.digx.mobile.android.SplashActivity	Schemes: http://, https://, Hosts: \@@HTTP_HOST, \@@HTTPS_HOST,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.mcb.mcblive,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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

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

🔍 MANIFEST ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Broadcast Receiver (com.ofss.digx.mobile.android.MainActivity$SMSListener) 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.
3	Activity (com.tlx.custom.plugins.covalent.FaceoffDemoBaseActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
7	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
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: **4** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				bom/F.java com/adobe/xmp/XMPMetaFactory.java com/agomezmoron/saveImageGallery/SaveImageGallery.java com/agontuk/RNFusedLocation/FusedLocationProvider.java com/agontuk/RNFusedLocation/LocationManagerProvider.java com/agontuk/RNFusedLocation/RNFusedLocationModule.java com/airbnb/android/react/maps/AirMapGradientPolyline.java com/airbnb/android/react/maps/AirMapHeatmap.java com/airbnb/android/react/maps/FileUtil.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Do

NO	ISSUE	SEVERITY	STANDARDS	FILES
				wnsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.jav

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	a com/drew/imaging/ImageMetadataReader.java com/drew/lang/CompoundException.java com/drew/tools/ExtractJpegSegmentTool.java com/drew/tools/ProcessAllImagesInFolderUtility.java com/drew/tools/ProcessUrlUtility.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/MaskView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lwansbrough/RCTCamera/MutableImage.java com/lwansbrough/RCTCamera/RCTCamera.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/lwansbrough/RCTCamera/RCTCameraViewFinder.java com/ofss/digx/mobile/android/AppController.java com/ofss/digx/mobile/android/MainActivity.java com/ofss/digx/mobile/android/MainApplicationOBDX.java com/ofss/digx/mobile/android/PlayIntegrityHelper.java com/ofss/digx/mobile/android/SplashActivity.java com/ofss/digx/mobile/android/SpyUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ofss/digx/mobile/android/infra/HttpWorker.java com/ofss/digx/mobile/android/plugins/AndroidWearPlugin.java com/ofss/digx/mobile/android/plugins/AppPreferences.java com/ofss/digx/mobile/android/plugins/BarcodeScanner.java com/ofss/digx/mobile/android/plugins/FetchPlugin.java com/ofss/digx/mobile/android/plugins/LiveExperiencePlugin.java com/ofss/digx/mobile/android/plugins/Permissions.java com/ofss/digx/mobile/android/plugins/TwitterPaymentDialog/DialogInit.java com/ofss/digx/mobile/android/plugins/UniversalLinks/UniversalLinksPlugin.java com/ofss/digx/mobile/android/plugins/UniversalLinks/model/JSMessage.java com/ofss/digx/mobile/android/plugins/fcm/FirebasePlugin.java com/ofss/digx/mobile/android/plugins/fcm/FirebasePluginInstanceIDService.java com/ofss/digx/mobile/android/plugins/fcm/FirebasePluginMessagingService.java com/ofss/digx/mobile/android/plugins/fcm/NotificationsDatabase.java com/ofss/digx/mobile/android/plugins/fcm/OnActionableNotificationReceiver.java com/ofss/digx/mobile/android/plugins/fcm/OnNotificationOpenReceiver.java com/ofss/digx/mobile/android/plugins/fingerprintauth/BiometricFragment.java com/ofss/digx/mobile/android/plugins/fingerprintauth/FingerprintAuth.java com/ofss/digx/mobile/android/util/Helper.java com/ofss/digx/mobile/obdxcore/infra/OBDXTokenLoginController.java com/reactnativecommunity/asyncstorage/Asyn

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/geolocation/GeolocationModule.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativemathematics/MathematicsModule.java com/scottyab/rootbeer/RootBeer.java com/scottyab/rootbeer/RootBeerNative.java com/scottyab/rootbeer/util/QLog.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/nodes/DebugNode.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaView.java com/tlx/custom/plugins/covalent/Covalent.java com/tlx/custom/plugins/covalent/FaceoffDemoBaseActivity.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java com/veridiumid/sdk/VeridiumSDK.java com/veridiumid/sdk/VeridiumSDKImpl.java com/veridiumid/sdk/activities/BiometricsAggregateActivity.java com/veridiumid/sdk/analytics/Analytics.java com/veridiumid/sdk/analytics/LoggingVeridium.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/veridiumid/sdk/crypto/TransactionSigningHelper.java com/veridiumid/sdk/defaultdata/DataStorage.java com/veridiumid/sdk/defaults/biometricsettingsdefaultui/BiometricSettingsFragment.java com/veridiumid/sdk/fourf/ExportConfig.java com/veridiumid/sdk/fourf/FourFLoader.java com/veridiumid/sdk/fourf/VeridiumSDKFourFInitializer.java com/veridiumid/sdk/fourf/camera/Camera1PreviewView.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java com/veridiumid/sdk/fourf/camera/ImageTaggingQueue.java com/veridiumid/sdk/fourf/ui/FourFUIFragment.java com/veridiumid/sdk/fourf/ui/InstructionalDialog.java com/veridiumid/sdk/internal/licensing/LicensingRepository.java com/veridiumid/sdk/licensing/LicensingManager.java com/veridiumid/sdk/log/Timber.java com/veridiumid/sdk/model/ManifestVeridiumSDKModel.java com/veridiumid/sdk/model/biometrics/engine/impl/DecentralizedBiometricsEngineImpl.java com/veridiumid/sdk/model/biometrics/engine/impl/ModularBiometricProcessor.java com/veridiumid/sdk/model/biometrics/engine/processing/handling/impl/AdaptiveEnrollmentHandler.java com/veridiumid/sdk/model/biometrics/engine/processing/handling/impl/AuthenticationHandler.java com/veridiumid/sdk/model/biometrics/packagi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ng/IBiometricFormats.java com/veridiumid/sdk/model/biometrics/persistence/impl/BytesTemplatesStorage.java com/veridiumid/sdk/model/biometrics/results/BiometricResultsParser.java com/veridiumid/sdk/model/help/AssetsHelper.java com/veridiumid/sdk/model/help/Devices.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java com/veridiumid/sdk/support/BiometricBaseActivity.java com/veridiumid/sdk/support/help/CustomCountDownTimer.java com/veridiumid/sdk/support/ui/AspectRatioSafeFrameLayout.java com/wenkesj/voice/VoiceModule.java com/zoontek/rnpermissions/RNPermissionsModule.java me/leolin/shortcutbadger/ShortcutBadger.java nl/lightbase/PanoramaView.java org/altbeacon/beacon/BeaconParser.java org/altbeacon/beacon/logging/InfoAndroidLogger.java org/altbeacon/beacon/logging/VerboseAndroidLogger.java org/altbeacon/beacon/logging/WarningAndroidLogger.java org/altbeacon/beacon/service/ScanState.java org/altbeacon/beacon/utils/EddystoneTelemetryAccessor.java
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/ofss/digx/mobile/android/plugins/fcm/NotificationsDatabase.java org/json/Test.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java org/reactnative/facedetector/tasks/FileFaceDetectionAsyncTask.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/ofss/digx/mobile/android/infra/HttpWorker.java com/ofss/digx/mobile/obdxcore/infra/AbstractVolleyLoginController.java com/veridiumid/sdk/internal/licensing/ws/LicensingServiceApi.java io/socket/engineio/client/transports/PollingXHR.java
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/FileUtil.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/reactnativecommunity/webview/RNCWebViewModule.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/agomezmoron/saveImageGallery/SaveImageGallery.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/reactnativecommunity/webview/RNCWebViewModule.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java nl/xservices/plugins/SocialSharing.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/learnium/RNDeviceInfo/RNDeviceModule.java com/ofss/digx/mobile/android/plugins/fingerprintauth/FingerprintAuth.java com/unikrew/faceoff/fingerprint/SecureStorage/c.java com/unikrew/faceoff/fingerprint/Telemetry/SharedPreferenceHelper.java com/veridiumid/sdk/VeridiumSDK.java
7	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
8	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/agontuk/RNFusedLocation/FusedLocationProvider.java com/ofss/digx/mobile/android/plugins/fcm/FirebasePluginMessagingService.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

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/lwansbrough/RCTCamera/RCTCamera.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/lwansbrough/RCTCamera/RCTCameraViewFinder.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java
00022	Open a file from given absolute path of the file	file	com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/lwansbrough/RCTCamera/MutableImage.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/oblador/vectoricons/VectorIconsModule.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/analytics/LoggingVeridium.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java org/altbeacon/beacon/service/ScanState.java org/reactnative/camera/tasks/ResolveTakenPictureAsyncTask.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/airbnb/android/react/maps/AirMapLocalTile.java com/airbnb/android/react/maps/FileUtil.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/drew/imaging/ImageMetadataReader.java com/drew/imaging/avi/AviMetadataReader.java com/drew/imaging/bmp/BmpMetadataReader.java com/drew/imaging/eps/EpsMetadataReader.java com/drew/imaging/gif/GifMetadataReader.java com/drew/imaging/ico/IcoMetadataReader.java com/drew/imaging/jpeg/JpegMetadataReader.java com/drew/imaging/jpeg/JpegSegmentReader.java com/drew/imaging/mp4/Mp4MetadataReader.java com/drew/imaging/pcx/PcxMetadataReader.java com/drew/imaging/png/PngMetadataReader.java com/drew/imaging/psd/PsdMetadataReader.java com/drew/imaging/quicktime/QuickTimeMetadataReader.java com/drew/imaging/raf/RafMetadataReader.java com/drew/imaging/wav/WavMetadataReader.java com/drew/imaging/webp/WebpMetadataReader.java com/drew/tools/FileUtil.java com/drew/tools/ProcessAllImagesInFolderUtility.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java nl/lightbase/PanoramaView.java okio/Okio__JvmOkioKt.java org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java org/altbeacon/beacon/service/MonitoringStatus.java org/altbeacon/beacon/service/ScanState.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/airbnb/android/react/maps/AirMapMarker.java com/airbnb/android/react/maps/ImageReader.java com/dylanvann/fastimage/FastImageSource.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.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
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/NetworkFetcher.java io/socket/engineio/client/transports/PollingXHR.java
00089	Connect to a URL and receive input stream from the server	command network	com/airbnb/lottie/network/NetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/ofss/digx/mobile/android/AppController.java io/socket/engineio/client/transports/PollingXHR.java nl/lightbase/PanoramaView.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java
00109	Connect to a URL and get the response code	network command	com/airbnb/lottie/network/NetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java io/socket/engineio/client/transports/PollingXHR.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java
00094	Connect to a URL and read data from it	command network	io/socket/engineio/client/transports/PollingXHR.java nl/lightbase/PanoramaView.java nl/xservices/plugins/SocialSharing.java
00108	Read the input stream from given URL	network command	io/socket/engineio/client/transports/PollingXHR.java nl/lightbase/PanoramaView.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/ofss/digx/mobile/android/MainActivity.java com/ofss/digx/mobile/android/plugins/fcm/FirebasePlugin.java com/ofss/digx/mobile/android/plugins/fcm/OnActionableNotificationReceiver.java com/veridiumid/sdk/activities/BiometricsAggregateActivity.java com/veridiumid/sdk/fourf/FourFBiometricsActivity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java
00195	Set the output path of the recorded file	record file	com/lwansbrough/RCTCamera/RCTCameraModule.java
00199	Stop recording and release recording resources	record	com/lwansbrough/RCTCamera/RCTCameraModule.java
00198	Initialize the recorder and start recording	record	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
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/NetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/ofss/digx/mobile/android/AppController.java nl/lightbase/PanoramaView.java
00054	Install other APKs from file	reflection	com/ofss/digx/mobile/android/plugins/fileopener2/FileOpener2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ofss/digx/mobile/android/AppController.java com/ofss/digx/mobile/android/plugins/GoogleMaps.java com/ofss/digx/mobile/android/plugins/Permissions.java com/ofss/digx/mobile/android/plugins/UniversalLinks/UniversalLinksPlugin.java com/ofss/digx/mobile/android/plugins/fcm/FirebasePluginMessagingService.java com/ofss/digx/mobile/android/plugins/fileopener2/FileOpener2.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java nl/xservices/plugins/SocialSharing.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ofss/digx/mobile/android/plugins/fileopener2/FileOpener2.java nl/xservices/plugins/SocialSharing.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00028	Read file from assets directory	file	com/veridiumid/sdk/model/help/AssetsHelper.java
00175	Get notification manager and cancel notifications	notification	com/ofss/digx/mobile/android/plugins/fcm/FirebasePlugin.java
00014	Read file into a stream and put it into a JSON object	file	org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java
00024	Write file after Base64 decoding	reflection file	nl/xservices/plugins/SocialSharing.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/agomezmoron/saveImageGallery/SaveImageGallery.java com/airbnb/android/react/maps/ImageUtil.java org/reactnative/camera/tasks/ResolveTakenPictureAsyncTask.java
00147	Get the time of current location	collection location	com/agontuk/RNFusedLocation/LocationUtils.java com/reactnativecommunity/geolocation/GeolocationModule.java
00075	Get location of the device	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java
00115	Get last known location of the device	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java
00005	Get absolute path of file and put it to JSON object	file	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java
00004	Get filename and put it to JSON object	file collection	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java
00123	Save the response to JSON after connecting to the remote server	network command	com/ofss/digx/mobile/android/AppController.java
00012	Read data and put it into a buffer stream	file	com/drew/imaging/ImageMetadataReader.java com/drew/tools/ProcessAllImagesInFolderUtility.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 com/ofss/digx/mobile/android/util/Helper.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
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
00035	Query the list of the installed packages	reflection	com/ofss/digx/mobile/android/SpyUtils.java
00125	Check if the given file path exist	file	com/ofss/digx/mobile/android/SpyUtils.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
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	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	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	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/192070169474/namespaces/firebase:fetch?key=AIzaSyBy4lT-7SjAbln0xo-U7k8VX0QNhfK6X1c. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	16/25	android.permission.INTERNET, 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.GET_ACCOUNTS, android.permission.READ_EXTERNAL_STORAGE, 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, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	7/44	android.permission.FLASHLIGHT, android.permission.WRITE_CONTACTS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
meezan-faceoff-ids.covalent.pk	ok	No Geolocation information available.
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.
ns.adobe.com	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
mcblive.com	ok	**IP:** 104.18.2.174 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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

TRACKERS

TRACKER	CATEGORIES	URL
AltBeacon		https://reports.exodus-privacy.eu.org/trackers/219
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
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" : "@@KEY_OAM_URL"
"KEY_OAUTH_PROVIDER_URL" : "@@KEY_OAUTH_PROVIDER_URL"
"KEY_SERVER_URL" : "https://mcblive.com"
"X_TOKEN_TYPE" : "@@X_TOKEN_TYPE"
"google_api_key" : "AIzaSyBy4lT-7SjAbln0xo-U7k8VX0QNhfK6X1c"
"google_crash_reporting_api_key" : "AIzaSyBy4lT-7SjAbln0xo-U7k8VX0QNhfK6X1c"
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
6e2c7e24b7c7eae9fc94882c9f31befa00594872
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573530086143415290314195533631308867097853951
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

POSSIBLE SECRETS
21c8b5470a64adbb25bc84316cbc449361d86839
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
7a5b85d3ee2e0991ca3502602e9389a98f55c0576b887125894a7ec03823f8d3
e44046539bb5b584279553ca6eacca937c8e16cf
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
115792089210356248762697446949407573529996955224135760342422259061068512044369
470fa2b4ae81cd56ecbcda9735803434cec591fa
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

PLAYSTORE INFORMATION

Title: MCB Live

Score: 2.27 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.mcb.mcblive

Developer Details: MCB Bank Ltd., 7701131036861724674, None, https://www.mcb.com.pk/customer_services/contact-us, info@mcb.com.pk,

Release Date: Sep 9, 2021 **Privacy Policy:** Privacy link

Description:

MCB Live is the new flagship digital banking solution of MCB Bank that has been designed from the ground up to offer new and improved services to our customers, with a view to securely and conveniently conduct financial and non-financial transactions. MCB Live has a completely new user interface and an intuitive layout that will enable you to conduct digital banking transactions conveniently on the go or from wherever you may be. MCB Live is Fresh, its Fast, its Futuristic! MCB Live comes with a new set of features, just a few of which are mentioned below: • Bill Payment to 1,000+ Billers • Swiftly Transfer Funds to any Bank via Quick Transfer • Secure financial transactions through OTP • Multiple Accounts Management • Cheque Book Request, Status inquiry and Stop Cheque Request • Account Statement with details of up to 10 transactions • e-Statement Subscription & Un-subscription • Efficiently manage your MCB Debit and Credit Cards • Request for new/replacement Cards online • Activate your Cards for eCommerce, online & International use online • Lodge a detailed Complaint quickly from within the app • Conveniently Donate to leading NGOs and social causes • Download Withholding Tax Certificate • Locate your nearest MCB ATM through the in-app ATM Locator & much, much more! In order to take advantage of the new MCB Live experience, please manually uninstall your existing app and then download the new app from this App Store. For any queries or concerns regarding MCB Live, please call 111-000-622 or send us an email at info@mcb.com.pk from your registered mobile number. Please note that MCB Bank will continue to provide technical support for MCB Mobile till the foreseen future. Thank you for your patronage and support.

SCAN LOGS

Timestamp	Event	Error
2024-11-14 20:26:31	Generating Hashes	OK
2024-11-14 20:26:31	Extracting APK	OK
2024-11-14 20:26:31	Unzipping	OK

2024-11-14 20:26:34	Getting Hardcoded Certificates/Keystores	OK
2024-11-14 20:26:34	Parsing APK with androguard	OK
2024-11-14 20:26:48	Parsing AndroidManifest.xml	OK
2024-11-14 20:26:48	Extracting Manifest Data	OK
2024-11-14 20:26:48	Performing Static Analysis on: MCB Live (com.mcb.mcblive)	OK
2024-11-14 20:26:48	Fetching Details from Play Store: com.mcb.mcblive	OK
2024-11-14 20:26:51	Manifest Analysis Started	OK
2024-11-14 20:26:51	Checking for Malware Permissions	OK
2024-11-14 20:26:51	Fetching icon path	OK
2024-11-14 20:26:51	Library Binary Analysis Started	OK
2024-11-14 20:26:51	Reading Code Signing Certificate	OK

2024-11-14 20:26:56	Running APKiD 2.1.5	OK
2024-11-14 20:27:12	Detecting Trackers	OK
2024-11-14 20:27:29	Decompiling APK to Java with JADX	OK
2024-11-14 20:28:08	Converting DEX to Smali	OK
2024-11-14 20:28:08	Code Analysis Started on - java_source	OK
2024-11-14 20:28:28	Android SAST Completed	OK
2024-11-14 20:28:28	Android API Analysis Started	OK
2024-11-14 20:28:39	Android API Analysis Completed	OK
2024-11-14 20:28:39	Android Permission Mapping Started	OK
2024-11-14 20:30:07	Android Permission Mapping Completed	OK
2024-11-14 20:30:10	Email and URL Extraction Completed	OK

2024-11-14 20:30:10	Android Behaviour Analysis Started	OK
2024-11-14 20:30:14	Android Behaviour Analysis Completed	OK
2024-11-14 20:30:14	Extracting String data from APK	OK
2024-11-14 20:30:14	Extracting String data from Code	OK
2024-11-14 20:30:14	Extracting String values and entropies from Code	OK
2024-11-14 20:30:18	Performing Malware check on extracted domains	OK
2024-11-14 20:30:28	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.