MOBSF

ANDROID STATIC ANALYSIS REPORT

FINCA Pay (8.2)

File Name: FINCA.apk

Package Name:	com.finja.simsim
Scan Date:	Jan. 4, 2025, 11:16 p.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	C
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
12	26	2	2	3

FILE INFORMATION

File Name: FINCA.apk
Size: 18.51MB
MD5: e28574c725e71b483fabd3819b15995f
SHA1: a399282e190d92e7d226ee9d998f52784a24cceb
SHA256: 3a6ae226aef416a78a085699642f3ea927e6caa3b05f041d25fec750e006c04c

APP INFORMATION

App Name: FINCA Pay
Package Name: com.finja.simsim
Main Activity: com.finca.bank.userapp.development.onBoarding.splash.SplashActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 8.2
Android Version Code: 109

APP COMPONENTS

Activities: 56
Services: 17
Receivers: 19
Providers: 7
Exported Activities: 1
Exported Services: 2
Exported Receivers: 6

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=PK, ST=Punjab, L=Lahore, O=FINJA pvt Ltd., OU=FINJA, CN=FINJA
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-10-13 13:09:55+00:00
Valid To: 2041-10-07 13:09:55+00:00
Issuer: C=PK, ST=Punjab, L=Lahore, O=FINJA pvt Ltd., OU=FINJA, CN=FINJA
Serial Number: 0x60daa2e5
Hash Algorithm: sha256
md5: 5556a0f2dc477b83f1565892d88f7004
sha1: 69e7b6d2839de03407b2c7ec2162cc8d24a3842e
sha256: 241ea0d5ac99b9b6e202534bdc9ff4771aa83837184aadc4cb40517d671b5da2
sha512: 0b2a715840d3b536430d89a17def285f54ed8ca365964df7731463d9006108887c267a47b748cd8ca94ffcb952a8f235584fe013440b27179dda9436cedd2c22
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6ded338a832aa51c39345b2983cfdf903f6954c2f5ac36b698727e1fe0e8380c
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.finja.simsim.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.

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.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_INTERNAL_STORAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.CAMERA2	unknown	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.webkit.PermissionRequest	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.finja.simsim.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.TAGS check
SIM operator check
network operator name check
ro.hardware check
ro.kernel.qemu check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE 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>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.finca.bank.userapp.development.onBoarding.splash.SplashActivity	Schemes: https://, http://, Hosts: simsim.page.link, finca.pk, www.finca.pk, Path Patterns: /marketplace-cart, /cash-in, /marketplace-home, /foodify-home, /topup, /marketplace-items, /marketplace-wishlist, /marketplace-category-list, /foodify-meals, /foodify-cart, /marketplace-category-details, /donations, /manage-cards, /my-orders, /send-money, /add-money, /billpayments, /loans,
com.facebook.CustomTabActivity	Schemes: fb317458364280611://, fbconnect://, Hosts: cct.com.finja.simsim,

NETWORK SECURITY

HIGH: **3** | WARNING: **3** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.

NO	SCOPE	SEVERITY	DESCRIPTION
4	https://finca.pk https://finca.org.pk http://10.40.230.181:9091/API http://10.40.230.181:9091 http://10.40.242.47:8080/API http://10.40.242.47:8080 172.30.0.146 172.30.0.146:8080 http://172.30.0.146:8080/API/ 10.40.242.47 10.40.242.47:8080 10.40.230.181 10.40.230.181:9091 api.finca.org.pk newdemoapi.finca.web.pk newdemoapi.finca.pk demoapi4.finca.web.pk finca.pk www.finja.pk finca.org.pk widgets.finca.pk widgets.finca.web.pk widgets2.finca.web.pk biometricmiddleware.finca.pk	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

NO	SCOPE	SEVERITY	DESCRIPTION
5	https://finca.pk https://finca.org.pk http://10.40.230.181:9091/API http://10.40.230.181:9091 http://10.40.242.47:8080/API http://10.40.242.47:8080 172.30.0.146 172.30.0.146:8080 http://172.30.0.146:8080/API/ 10.40.242.47 10.40.242.47:8080 10.40.230.181 10.40.230.181:9091 api.finca.org.pk newdemoapi.finca.web.pk newdemoapi.finca.pk demoapi4.finca.web.pk finca.pk www.finja.pk finca.org.pk widgets.finca.pk widgets.finca.web.pk widgets2.finca.web.pk biometricmiddleware.finca.pk	warning	Domain config is configured to trust system certificates.

NO	SCOPE	SEVERITY	DESCRIPTION
6	https://finca.pk https://finca.org.pk http://10.40.230.181:9091/API http://10.40.230.181:9091 http://10.40.242.47:8080/API http://10.40.242.47:8080 172.30.0.146 172.30.0.146:8080 http://172.30.0.146:8080/API/ 10.40.242.47 10.40.242.47:8080 10.40.230.181 10.40.230.181:9091 api.finca.org.pk newdemoapi.finca.web.pk newdemoapi.finca.pk demoapi4.finca.web.pk finca.pk www.finja.pk finca.org.pk widgets.finca.pk widgets.finca.web.pk widgets2.finca.web.pk biometricmiddleware.finca.pk	high	Domain config is configured to trust user installed certificates.

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: 5 | WARNING: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	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	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
4	App Link assetlinks.json file not found [android:name=com.finca.bank.userapp.development.onBoarding.splash.SplashActivity] [android:host=https://simsim.page.link]	high	App Link asset verification URL (https://simsim.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
5	App Link assetlinks.json file not found [android:name=com.finca.bank.userapp.development.onBoarding.splash.SplashActivity] [android:host=http://simsim.page.link]	high	App Link asset verification URL (http://simsim.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
6	App Link assetlinks.json file not found [android:name=com.finca.bank.userapp.development.onBoarding.splash.SplashActivity] [android:host=http://finca.pk]	high	App Link asset verification URL (http://finca.pk/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
7	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.
8	Broadcast Receiver (com.finca.bank.userapp.development.Attendance.util.TimeChangeBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.finca.bank.userapp.development.Attendance.util.OnBootReceiver) 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.
10	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Broadcast Receiver (com.finca.bank.userapp.development.utilities.smsValidator.MySMSBroadcastReceiver) 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.
12	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.
13	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.
14	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.
16	High Intent Priority (1000) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **3** | WARNING: **10** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				android/view/result/ActivityResultRegistry.java b0/a.java b2/c.java b4/a.java b6/a.java b6/c.java b6/g.java b6/q.java b6/r.java b6/t.java b6/w.java b6/x.java b7/f.java butterknife/ButterKnife.java c2/t.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/utils/c.java com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFa1bSDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1eSDK.java com/appsflyer/internal/AFc1hSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1nSDK.java com/appsflyer/internal/AFc1xSDK.java com/appsflyer/internal/AFd1eSDK.java com/appsflyer/internal/AFd1gSDK.java com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFd1tSDK.java com/appsflyer/internal/AFd1uSDK.java com/appsflyer/internal/AFd1vSDK.java com/appsflyer/internal/AFd1wSDK.java com/appsflyer/internal/AFd1zSDK.java com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.java com/bumptech/glide/b.java com/bumptech/glide/gifdecoder/c.java com/bumptech/glide/gifdecoder/d.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/bitmap_recycle/i.java com/bumptech/glide/load/engine/bitmap_recycle/j.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/n.java com/bumptech/glide/load/engine/w.java com/bumptech/glide/load/model/c.java com/bumptech/glide/load/model/d.java com/bumptech/glide/load/model/g.java com/bumptech/glide/load/model/s.java com/bumptech/glide/load/model/t.java com/bumptech/glide/load/model/u.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/i.java com/bumptech/glide/load/resource/bitmap/k.java com/bumptech/glide/load/resource/bitmap/l.java com/bumptech/glide/load/resource/bitmap/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/resource/bitmap/t.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/c.java com/bumptech/glide/load/resource/gif/h.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/manager/f.java com/bumptech/glide/manager/n.java com/bumptech/glide/manager/o.java com/bumptech/glide/manager/q.java com/bumptech/glide/manager/r.java com/bumptech/glide/request/j.java com/bumptech/glide/request/target/CustomViewTarget$SizeDeterminer.java com/bumptech/glide/request/target/ViewTarget.java com/finca/bank/userapp/development/app/SimSimApp.java com/finca/bank/userapp/development/fcm/MyFirebaseMessagingService.java com/finca/bank/userapp/development/financial/QRPayment/QRAmountFragment.java com/finca/bank/userapp/development/financial/QRPayment/QRConfirmationFragment.java com/finca/bank/userapp/development/financial/localFundsTransfer/SuccessDialogFragment.java com/finca/bank/userapp/development/financial/localFundsTransfer/k.java com/finca/bank/userapp/development/financial/localFundsTransfer/p.java com/finca/bank/userapp/development/financial/miniStatement/ViewWalletFragment.java com/finca/bank/userapp/development/financial/telenor/PostPaidConfirmationFragment.java com/finca/bank/userapp/development/financial/telenor/PrePaidConfirmationFragment.java com/finca/bank/userapp/development/financial/telenor/bundles/BundlesConfirmationFragment.java com/finca/bank/userapp/development/financial/telenor/bundles/MobileBundlesFragment.java com/finca/bank/userapp/development/marketPlace/view/home/BookmeWebViewActivity.java com/finca/bank/userapp/development/onBoarding/getStarted/GetStartedActivity.java com/finca/bank/userapp/development/onBoarding/mobileVerification/EnterMobileNobActivity.java com/finca/bank/userapp/development/onBoarding/mobil

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	eVerification/VerifyMobileOTPNobActivity.java com/finca/bank/userapp/development/onBoarding/splash/SplashActivity.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/ParentActivity.java com/finca/bank/userapp/development/parent/t.java com/finca/bank/userapp/development/upgradeWallet/upgadeWithPaySys/UpgradeWalletWithInstaScanActivity.java com/finca/bank/userapp/development/utilities/fargmentManager/activity/a.java com/finca/bank/userapp/development/utilities/smsValidator/AppSignatureHelper.java com/finca/bank/userapp/development/utilities/smsValidator/MySMSBroadcastReceiver.java com/journeyapps/barcodescanner/a.java com/journeyapps/barcodescanner/e.java com/otaliastudios/cameraview/CameraLogger.java com/otaliastudios/cameraview/c.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 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/LicensingRepositor

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/veridiumid/sdk/internal/licensing/LicensingRequestor.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/packaging/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 d1/d.java d2/b0.java d2/j.java d3/e.java e0/c.java e9/b.java ee/g.java f0/a.java f9/c.java g1/b.java g3/f.java g3/l.java g6/b.java g6/d.java g6/f.java g6/h.java h0/a.java h0/c.java i1/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f1/a.java j1/e.java j3/i.java j8/f.java k4/d.java k4/f.java k4/h.java l1/a.java l1/d.java l1/h.java l3/a.java l5/l.java m0/c.java n/d.java n2/o.java n6/s.java o/f.java o5/a.java o7/o.java o7/v.java p6/f.java pub/devrel/easypermissions/b.java pub/devrel/easypermissions/helper/a.java pub/devrel/easypermissions/helper/c.java sa/i.java t2/m.java t6/x.java ta/a.java ta/c.java ta/g.java ta/h.java ta/l.java ta/n.java ta/q.java u0/a.java u3/d.java u3/h.java u9/e.java u9/g.java v/c.java v9/a.java w0/c.java w0/e.java w2/g.java w4/e.java w4/h.java wa/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x0/e.java x0/j.java y0/a.java y0/b.java y1/a.java z3/j0.java
2	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	android/view/result/ActivityResultRegistry.java com/appsflyer/internal/AFa1ySDK.java com/finca/bank/userapp/development/financial/localFundsTransfer/SuccessDialogFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java ed/a.java ed/b.java fd/a.java he/c.java
3	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/appsflyer/internal/AFb1rSDK.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java com/veridiumid/sdk/model/help/EncryptionUtils.java e9/b.java h5/a.java r1/a.java
4	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/finca/bank/userapp/development/easyTickets/EasyTicketsHomeActivity.java com/finca/bank/userapp/development/marketPlace/view/home/BookmeWebViewActivity.java v2/a.java y2/i.java
5	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
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java w4/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/m.java com/bumptech/glide/load/engine/u.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.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 v0/g.java
8	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 vd/c.java
9	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/journeyapps/barcodescanner/e.java d2/b0.java e9/c.java h0/c.java
10	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	com/finca/bank/userapp/development/onBoarding/login/fingerLogin/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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/finca/bank/userapp/development/financial/localFundsTransfer/SuccessDialogFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java d2/b0.java jb/e.java l3/a.java w4/h.java
12	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	b2/a.java com/airbnb/lottie/network/NetworkCache.java com/appsflyer/internal/AFb1rSDK.java l1/g.java xa/c.java
13	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/finca/bank/userapp/development/onBoarding/getStarted/GetStartedActivity.java k4/h.java
14	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	d2/b0.java
15	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFa1aSDK.java
16	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

NO	ISSUE	SEVERITY	STANDARDS	FILES
17	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	n0/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	a3/c.java a3/g.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFa1uSDK.java com/finca/bank/userapp/development/Attendance/DoorQRActivity.java com/finca/bank/userapp/development/easyTickets/EasyTicketsHomeActivity.java com/finca/bank/userapp/development/financial/QRPayment/ActivityQRPayment.java com/finca/bank/userapp/development/financial/billPayment/BillCategoryListActivity.java com/finca/bank/userapp/development/financial/billPayment/BillSubCategoryListActivity.java com/finca/bank/userapp/development/financial/cardwalla/CardCompaniesListActivity.java com/finca/bank/userapp/development/financial/localFundsTransfer/k.java com/finca/bank/userapp/development/financial/localFundsTransfer/p.java com/finca/bank/userapp/development/financial/quickpay/QuickPayListActivity.java com/finca/bank/userapp/development/financial/quickpay/QuickPayListRevampActivity.java com/finca/bank/userapp/development/financial/telenor/MobileTopUpFragment.java com/finca/bank/userapp/development/financial/telenor/NumberSelectionFragment.java com/finca/bank/userapp/development/financial/telenor/bundles/BundlesNumberSelectionFragment.java com/finca/bank/userapp/development/marketPlace/view/home/BookmeWebViewActivity.java com/finca/bank/userapp/development/onBoarding/guestUserVerification/BlockedCustomerQuestionOptionNob.java com/finca/bank/userapp/development/parent/ParentActivity.java com/finca/bank/userapp/development/parent/t.java com/finca/bank/userapp/development/utilities/receivers/ReferrerReceiver.java com/veridiumid/sdk/activities/BiometricsAggregateActivity.java com/veridiumid/sdk/fourf/FourFBiometricsActivity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java d3/k.java e4/b.java j3/e.java j3/i.java lolodev/permissionswrapper/RequestPermissionsActv.java m3/d0.java m4/a.java t2/b.java t2/v.java v2/a.java x2/g.java x2/m.java z2/a.java z3/j0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00137	Get last known location of the device	location collection	c2/t.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java k4/f.java
00115	Get last known location of the device	collection location	c2/t.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java k4/f.java
00113	Get location and put it into JSON	collection location	c2/t.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java k4/f.java
00016	Get location info of the device and put it to JSON object	location collection	c2/t.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java k4/f.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/appsflyer/internal/AFa1mSDK.java com/appsflyer/internal/AFc1vSDK.java f9/c.java he/d.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/appsflyer/internal/AFa1mSDK.java com/bumptech/glide/load/data/j.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java he/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFa1mSDK.java com/appsflyer/internal/AFc1aSDK.java com/appsflyer/internal/AFc1vSDK.java com/bumptech/glide/load/data/j.java f9/c.java fb/a.java he/d.java
00013	Read file and put it into a stream	file	com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/bumptech/glide/load/a.java com/bumptech/glide/load/model/g.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java e9/c.java fb/a.java l1/g.java m8/d.java p8/e.java r8/a.java u0/a.java wa/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFc1fSDK.java com/finca/bank/userapp/development/easyTickets/EasyTicketsHomeActivity.java com/finca/bank/userapp/development/fcm/MyFirebaseMessagingService.java com/finca/bank/userapp/development/financial/QRPayment/ActivityQRPayment.java com/finca/bank/userapp/development/financial/miniStatement/c.java com/finca/bank/userapp/development/onBoarding/login/fingerLogin/FingerPrintrLoginToEnableActivity.java com/finca/bank/userapp/development/onBoarding/splash/SplashActivity.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/ParentActivity.java com/finca/bank/userapp/development/parent/t.java d2/b0.java e5/b.java k4/h.java o7/w.java t1/a.java u3/f.java u3/i.java v4/y.java w4/e.java
00202	Make a phone call	control	com/finca/bank/userapp/development/onBoarding/login/fingerLogin/FingerPrintrLoginToEnableActivity.java com/finca/bank/userapp/development/parent/t.java k4/h.java
00203	Put a phone number into an intent	control	com/finca/bank/userapp/development/onBoarding/login/fingerLogin/FingerPrintrLoginToEnableActivity.java com/finca/bank/userapp/development/parent/t.java k4/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/finca/bank/userapp/development/fcm/MyFirebaseMessagingService.java com/finca/bank/userapp/development/onBoarding/login/fingerLogin/FingerPrintrLoginToEnableActivity.java com/finca/bank/userapp/development/onBoarding/splash/SplashActivity.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/ParentActivity.java com/finca/bank/userapp/development/parent/t.java e5/b.java k4/h.java o7/w.java v4/y.java
00002	Open the camera and take picture	camera	com/otaliastudios/cameraview/c.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java
00022	Open a file from given absolute path of the file	file	ab/h.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/appsflyer/internal/AFa1aSDK.java com/finca/bank/userapp/development/financial/localFundsTransfer/SuccessDialogFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java com/journeyapps/barcodescanner/e.java com/otaliastudios/cameraview/c.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/analytics/LoggingVeridium.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java h0/a.java h0/c.java kb/b.java m8/d.java n0/b.java s0/p.java va/a.java
00183	Get current camera parameters and change the setting.	camera	com/otaliastudios/cameraview/c.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java ta/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00195	Set the output path of the recorded file	record file	com/otaliastudios/cameraview/c.java
00199	Stop recording and release recording resources	record	com/otaliastudios/cameraview/c.java
00198	Initialize the recorder and start recording	record	com/otaliastudios/cameraview/c.java
00194	Set the audio source (MIC) and recorded file format	record	com/otaliastudios/cameraview/c.java
00197	Set the audio encoder and initialize the recorder	record	com/otaliastudios/cameraview/c.java
00007	Use absolute path of directory for the output media file path	file	com/otaliastudios/cameraview/c.java
00196	Set the recorded file format and output path	record file	com/otaliastudios/cameraview/c.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	b5/a.java k3/g.java
00108	Read the input stream from given URL	network command	w7/d.java
00192	Get messages in the SMS inbox	sms	w4/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java w4/e.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/finca/bank/userapp/development/utilities/contactSyncing/ReadContactsService.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/finca/bank/userapp/development/utilities/contactSyncing/ReadContactsService.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1mSDK.java p6/f.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/finca/bank/userapp/development/utilities/contactSyncing/ReadContactsService.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/finca/bank/userapp/development/utilities/contactSyncing/ReadContactsService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1mSDK.java w0/c.java
00033	Query the IMEI number	collection	k4/f.java u4/c.java
00094	Connect to a URL and read data from it	command network	o8/a.java
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFb1oSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1mSDK.java com/finca/bank/userapp/development/onBoarding/splash/SplashActivity.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java m1/a.java o7/w.java
00014	Read file into a stream and put it into a JSON object	file	e9/c.java m8/d.java r8/a.java
00003	Put the compressed bitmap data into JSON object	camera	com/finca/bank/userapp/development/financial/localFundsTransfer/SuccessDialogFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java l3/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFa1aSDK.java com/finca/bank/userapp/development/financial/localFundsTransfer/SuccessDialogFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java m8/d.java
00121	Create a directory	file command	com/finca/bank/userapp/development/financial/localFundsTransfer/SuccessDialogFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java l3/a.java
00125	Check if the given file path exist	file	com/appsflyer/internal/AFa1aSDK.java com/finca/bank/userapp/development/financial/localFundsTransfer/SuccessDialogFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java l3/a.java
00147	Get the time of current location	collection location	com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java
00075	Get location of the device	collection location	com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java
00009	Put data in cursor to JSON object	file	com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java
00072	Write HTTP input stream into a file	command network file	com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java

RULE ID	BEHAVIOUR	LABEL	FILES
00123	Save the response to JSON after connecting to the remote server	network command	com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFc1vSDK.java com/bumptech/glide/load/data/j.java com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java com/finca/bank/userapp/development/parent/t.java f9/c.java fb/a.java he/d.java
00112	Get the date of the calendar event	collection calendar	com/finca/bank/userapp/development/parent/AuthenticateParentBottomFragment.java com/finca/bank/userapp/development/parent/AuthenticateParentFragment.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFa1iSDK.java
00004	Get filename and put it to JSON object	file collection	com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFa1lSDK.java com/finca/bank/userapp/development/parent/t.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java
00175	Get notification manager and cancel notifications	notification	a5/a.java
00012	Read data and put it into a buffer stream	file	fb/a.java l1/g.java
00162	Create InetSocketAddress object and connecting to it	socket	be/a.java be/f.java
00163	Create new Socket and connecting to it	socket	be/a.java be/f.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	p6/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00187	Query a URI and check the result	collection sms calllog calendar	com/finca/bank/userapp/development/utilities/contactSyncing/ReadContactsService.java p6/f.java
00024	Write file after Base64 decoding	reflection file	s0/p.java
00028	Read file from assets directory	file	com/veridiumid/sdk/model/help/AssetsHelper.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/626021904661/namespaces/firebase:fetch?key=AIzaSyDMjlbAB9V6gmWU2jeJoeFH3kI9DIvl_bc is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'app_update_info_android': '{"latest_app_version_code": 107, "is_force_update_needed": false}', 'app_update_info_ios': '{"latest_app_version_code": "5.3.5", "is_force_update_needed": true }', 'encryption_secret_key': '31a9971aa81342c0', 'encryption_secret_key_dev_uat': 'a9f5c7d2e8b4a3f9d1c6e3f8b7d2c4a53f2d6a4b9c0e19a5b3c7f9e129473f2b3c5f6e1d9a5f4e0c7b8d3f6e9a2b1c4fe2d4b1c8a5f7d9e3b6c5f4d7a8c9e1b2', 'encryption_secret_key_prod': 'J3fG9nX7bO6WpQs1Lt4Kz2Va8DyR5TcHW8AYW0TuvPWT49jqt3ex2xZoycA84wFZK7WlCqx1rZLpnJK2XAnY2KMS1xbIbq8UM9pVx0Wq2Nz5BkRl7Jt1Su4FyGa8KoDd', 'ios_ssl_pinning_hashes': '{"ssl_pinning":{"domains":[{"url":"*.finca.pk","hash":"sha256/i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY=","backup_hash":"5wpiI4ku3EgURtCxCw0izongvHZQp/lr/kQAwRkK3yA="}]}}', 'ssl_pinning_hashes': '{"ssl_pinning":{"domains":[{"url":"*.finca.pk","hash":"sha256/i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY="}]}}'}, 'state': 'UPDATE', 'templateVersion': '15'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/25	android.permission.READ_PHONE_STATE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.VIBRATE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO
Other Common Permissions	9/44	android.permission.CALL_PHONE, android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.FLASHLIGHT, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_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
karachi.icbc.com.cn	IP: 43.152.42.72 Country: China Region: Beijing City: Beijing

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
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
www.samba.com.pk	ok	**IP:** 103.210.4.139 **Country:** Pakistan **Region:** Sindh **City:** Karachi **Latitude:** 24.905600 **Longitude:** 67.082199 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
online.mcb.com.pk	ok	**IP:** 104.16.92.206 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
z7s22.app.goo.gl	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
sregister.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sonelink.s	ok	No Geolocation information available.
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.
mobit.faysalbank.com	ok	**IP:** 172.67.68.231 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
bankislami.com.pk	ok	**IP:** 104.18.28.162 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
cdn-testsettings.s	ok	No Geolocation information available.
ib.jsbl.com	ok	**IP:** 104.19.251.92 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

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
sapp.s	ok	No Geolocation information available.
api.finca.pk	ok	**IP:** 103.215.112.201 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
karachi.icbc.com.cn	ok	**IP:** 43.152.42.72 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
widgets.finca.pk	ok	**IP:** 103.215.112.206 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.ubldigital.com	ok	**IP:** 103.8.14.50 **Country:** Pakistan **Region:** Sindh **City:** Karachi **Latitude:** 24.905600 **Longitude:** 67.082199 **View:** Google Map
www.mobilinkbank.com	ok	**IP:** 119.160.107.141 **Country:** Pakistan **Region:** Islamabad **City:** Islamabad **Latitude:** 33.721481 **Longitude:** 73.043289 **View:** Google Map
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
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
biometricmiddleware.finca.pk	ok	**IP:** 103.215.112.207 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
online.standardchartered.com	ok	No Geolocation information available.
vision.googleapis.com	ok	**IP:** 216.58.211.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.abl.com	ok	**IP:** 104.19.223.192 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
goo.gl	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
summitbank.com.pk	ok	**IP:** 192.124.249.152 **Country:** United States of America **Region:** California **City:** Menifee **Latitude:** 33.679798 **Longitude:** -117.189484 **View:** Google Map
sstats.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.dibpak.com	ok	**IP:** 104.18.8.28 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
widgetsuat.finca.pk	ok	**IP:** 58.27.201.56 **Country:** Pakistan **Region:** Punjab **City:** Rawalpindi **Latitude:** 33.600700 **Longitude:** 73.067902 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
maps.google.com	ok	**IP:** 216.58.209.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.finca.pk	ok	**IP:** 18.165.122.18 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.65 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
us-central1-directory-simsim.cloudfunctions.net	ok	**IP:** 216.239.36.54 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
askaribank.com	ok	**IP:** 104.18.22.41 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.bankalhabib.com	ok	**IP:** 52.163.78.136 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
meezan-faceoff-ids.covalent.pk	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
netbanking.bankalfalah.com	ok	**IP:** 103.55.136.40 **Country:** Pakistan **Region:** Sindh **City:** Karachi **Latitude:** 24.905600 **Longitude:** 67.082199 **View:** Google Map
cdn-settings.s	ok	No Geolocation information available.
www.silkbankdirect.com.pk	ok	**IP:** 61.5.134.73 **Country:** Pakistan **Region:** Sindh **City:** Karachi **Latitude:** 24.905600 **Longitude:** 67.082199 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 216.58.210.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
covalentmiddleware.finca.pk	ok	**IP:** 103.215.112.207 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
journeyapps.com	ok	**IP:** 108.156.22.6 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
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
sattr.s	ok	No Geolocation information available.
www.soneribank.com	ok	**IP:** 104.18.11.111 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
finca.pk	ok	**IP:** 18.165.122.18 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.hblibank.com.pk	ok	**IP:** 192.230.77.102 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
www.facebook.com	ok	**IP:** 157.240.205.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
sars.s	ok	No Geolocation information available.
play.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
ib.habibmetro.com	ok	**IP:** 202.163.115.222 **Country:** Pakistan **Region:** Sindh **City:** Karachi **Latitude:** 24.905600 **Longitude:** 67.082199 **View:** Google Map
svalidate.s	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
fincapay.activation@finca.pk	w4/a.java
fincapay.passwords@finca.pk	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
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

TRACKER	CATEGORIES	URL
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
"APIKeyGetProfilePicUser" : "KlmqZNgCiCKOKccU"
"API_ID_GET_SERVER_TIME" : "393"
"API_KEY_GET_SERVER_TIME" : "gFo1GiHQJwsX1lSn"
"ApiIdGetProfilePicUser" : "410"
"CCAlfaLinkCardKey" : "Uh61v9riN541Rp7Y"
"CCDetailKey" : "ATdXll6kGg4jHCZ6"
"CCLinkForMobileNumberKey" : "EUzSVBNsxGiV3KRy"
"CCPaymentKey" : "8ej2B4a4wl7j2pl0"
"CCRemoveCardKey" : "rhEnfZBsL3lBCIdW"
"CLIENT_TOKEN" : "client_token"

POSSIBLE SECRETS
"FN_TOKEN" : "FN-Token"
"GetAtmCardsKey" : "BEgDa5eakaYX0c68"
"KEY_FCM_TOKEN" : "FCM_TOKEN"
"KeySessionId" : "sessionId"
"KeyToken" : "KeyToken"
"LoanRequestFormKey" : "GCZU3bBJp2Dggjev"
"apiIdFcmToken" : "473"
"apiIdUpgradeProvisionalUser" : "341"
"apiKeyFcmToken" : "EY9Xbj5eQXi8"
"apiKeyUpgradeProvisionalUser" : "yh9HYtr48sEEUv1O"
"apps_flyer_app_key" : "jv8HT5h6ucARBQSdDyoEAY"
"attendence_app_key" : "adF78Kli35N"
"biometric_api" : "MTc1LDIwMSwzNCw1NSwyMDksMjAwLDE3MCwxNjcsODgsMTUyLDIwMSw5MSw5NCwyMzEsMTgsMjIxLDEwOSwyMDIsMjMzLDI0OSw0MywxNTUsMTQ5LDI0NSw0MSwyLDQ5LDE1OSwzOSw4MCw0NywxMjEsMTQ2LDcyLDE1MywxMjEsMjQ5LDE4Myw5MywxNzMsOTIsMTM1LDE3OCwxNzYsOTMsMTY1LDE5NSw2MSwxNjUsMjQwLDEyNCw1MCwxMTMsMTU3LDEwLDUzLDE0Niw1NiwxMTEsMjUsMTcwLDE0MCw2MCwxNTEsMjQsMTExLDE0LDE4LDIwMCwyNTUsNTcsNDgsMTQzLDE0NCw4Myw2NCwyMTYsMTY1LDM1LDYsMTE2LDE0NywxNjQsMTQxLDE3NCwyMiwyMCwyMTIsMTM1LDg4LDAsNjMsMTcwLDIyNCw5Miw0NSw3NSwxNzIsNDIsMjQzLDE1NSwzNSw3OSwyNyw4LDE4MywxODUsMCwxMjYsMzYsMjQ3LDk1LDE1MSwxMjcsMTczLDM1LDEwNCwxNyw0LDIzMCwyMTMsMTg5LDk5LDIxNSwyNDEsNjUsMjM4LDEzOSw3OSwxNzksMjEwLDEwLDEyMiwxOTIsMTY4LDIxMywxOTQsODIsMTM2LDE2MCwxODgsMTU1LDIxOCw0NSwxNzQsODgsMjM1LDEyMiwyMzEsMjMsMTI1LDExNywxMDgsMjAyLDM3LDExNyw1NywwLDY0LDE1MSwyMjMsNTUsMjAzLDUxLDk2LDksMTI1LDI3LDM2LDIxLDQ2LDI0LDE5LDE0LDIzLDIyNiwxNTQsMzcsMTUzLDc1LDQxLDE0MSw1Myw5LDc5LDU1LDIzMywyMjcsMjQsNDgsMiwxNjQsNzgsNTksMTAzLDI1NSwyMjQsNDAsMjM4LDQwLDYsMjMyLDE0MSwzLDIzOCw2OCwxNzgsMTQzLDE2NSw5LDMxLDMwLDk1LDU1LDEyNywxNzgsMjAsOTksMTE5LDc1LDEzNSw4NywyNiwyMjcsMTc5LDEyNiwxNDUsMjA2LDEyMSwyMjIsMTYsODIsMTU0LDE5NywxODgsMjE4LDIwMCwxNzgsOSwxNTksMTc3LDUxLDUzLDY2LDE0MCw4MCwxNywyNCwzNCwyMTksMTI2LDE0MiwyMjMsNjYsMjExLDU1LDEsMCwxLA=="
"com.google.firebase.crashlytics.mapping_file_id" : "888a628f8b6f4310aca90f62fd29a246"

POSSIBLE SECRETS
"demo_youtube_api_key" : "AIzaSyD6TEpFbX4Zm96Zj5WbBmAWtt6wWAgjQFo"
"encryption_secret_key" : "31a9971aa81342c0"
"google_api_key" : "AIzaSyDMjlbAB9V6gmWU2jeJoeFH3kI9DIvl_bc"
"google_crash_reporting_api_key" : "AIzaSyDMjlbAB9V6gmWU2jeJoeFH3kI9DIvl_bc"
"google_maps_key" : "AIzaSyA1yLjdOTNgUskUwsixgyIgVwPCjwFu4Mw"
"keyApplicationKey" : "appKey"
"keyCardToken" : "cardToken"
"keyFingerPrintKey" : "F_SimSim_I_Finger_N_Print_J_Key_A"
"keyIsMicroLoanUser" : "IsMicroLoaneUser"
"keyIsPayRoleUser" : "IsPayRoleUser"
"keyLogedInUserName" : "loginUserName"
"keyScLoanUser" : "IsScLoanUser"
"keySecToken" : "SecToken"
"keySecureToken" : "sec_token"
"keySessionOutMsgDisplayed" : "SessionOutMsgDisplayes"
"key_fb_login_protocol_scheme" : "fb396298997427510"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

POSSIBLE SECRETS
"license_key_value_demo" : "40bbe4a899b84b38a29228a0f7b27133"
"license_key_value_live" : "5ad20af07f5045f7a783347593bcbd98"
"live_youtube_api_key" : "AIzaSyA1yLjdOTNgUskUwsixgyIgVwPCjwFu4Mw"
"mark_attendance_api_endpoint" : "mark_attendance"
"masterpass" : "Masterpass"
"notSimSimUser" : "No"
"otpKey" : "otpKey"
"password" : "Password"
"sec_token_for_merchant" : "SecTokenForMerchant"
"simSimUser" : "Yes"
"stringGetCardInfoKey" : "9IuXPJadpwepZBdz"
"stringUpgradeProvisionalUser" : "UpgradeProvisionalUser/"
"upload_attendance_pic_api_endpoint" : "updateAttendanceImages"
c103703e120ae8cc73c9248622f3cd1e
9b8f518b086098de3d77736f9458a3d2f6f95a37
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
ZmluamFsb2dnZXI6WU5ZTTBkS2p3ZGpFak9IQVpGVUkyNUlnWkR3b0JF
58750a89a1913425aff5955f3da23f23

POSSIBLE SECRETS
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
470fa2b4ae81cd56ecbcda9735803434cec591fa
49f946663a8deb7054212b8adda248c6
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
01360240043788015936020505
cc2751449a350f668590264ed76692694a80308a
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
CC1FEDD56FE38F327F6D672A7A694595
AIzaSyA1yLjdOTNgUskUwsixgyIgVwPCjwFu4Mw
2f9be5a17f4eb9cba710ad86c7b468a3
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

PLAYSTORE INFORMATION

Title: FINCA Pay

Score: 3.6 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.finja.simsim

Developer Details: FINCA Microfinance Bank, FINCA+Microfinance+Bank, None, https://www.finca.pk/, developers@finca.pk,

Release Date: Jan 5, 2017 **Privacy Policy:** Privacy link

Description:

About the App: SimSim has been renamed as FINCA Pay! Here's what we have in store for you: FEATURES • Sign-up in a few clicks to experience banking on the go! • No minimum balance requirement, No paperwork! • Safe & Secure Banking with FINCA Microfinance Bank, a fully regulated bank, trusted by millions of Pakistanis • View your balance & apply for e-statements • Login with Face ID, Touch ID or Passcode • Send and Receive money instantly, anytime, anywhere, 24/7 • Manage bills for 500+ billers from the comfort of your home • Instant Mobile Top-ups HOW TO OPEN A FINCA PAY ACCOUNT • After downloading the application, enter your mobile number & OTP to sign up. • Verify your identity by entering a few personal details • Set up your 4-digit login PIN • Viola! Your FINCA Pay account has been created. ABOUT FINCA FINCA Pay is the digital mobile wallet by FINCA Microfinance Bank Ltd (FMBL) – a fully regulated bank, trusted by millions of Pakistanis. FMBL became a part of FINCA Impact Finance (FIF) network in 2013. FIF is an international network of 16 micro finance institutions and banks offering innovative, responsible and impactful financial services. Since 1985, we have helped 40 million people build their financial health globally.

SCAN LOGS

Timestamp	Event	Error
2025-01-04 23:16:40	Generating Hashes	OK
2025-01-04 23:16:40	Extracting APK	OK
2025-01-04 23:16:40	Unzipping	OK
2025-01-04 23:16:41	Parsing APK with androguard	OK
2025-01-04 23:16:42	Extracting APK features using aapt/aapt2	OK
2025-01-04 23:16:42	Getting Hardcoded Certificates/Keystores	OK

2025-01-04 23:16:48	Parsing AndroidManifest.xml	OK
2025-01-04 23:16:48	Extracting Manifest Data	OK
2025-01-04 23:16:48	Manifest Analysis Started	OK
2025-01-04 23:16:50	Reading Network Security config from network_security_config.xml	OK
2025-01-04 23:16:50	Parsing Network Security config	OK
2025-01-04 23:16:50	Performing Static Analysis on: FINCA Pay (com.finja.simsim)	OK
2025-01-04 23:16:50	Fetching Details from Play Store: com.finja.simsim	OK
2025-01-04 23:16:50	Checking for Malware Permissions	OK
2025-01-04 23:16:50	Fetching icon path	OK
2025-01-04 23:16:50	Library Binary Analysis Started	OK
2025-01-04 23:16:50	Reading Code Signing Certificate	OK
2025-01-04 23:16:51	Running APKiD 2.1.5	OK

2025-01-04 23:16:57	Detecting Trackers	OK
2025-01-04 23:17:03	Decompiling APK to Java with JADX	OK
2025-01-04 23:17:59	Converting DEX to Smali	OK
2025-01-04 23:17:59	Code Analysis Started on - java_source	OK
2025-01-04 23:18:05	Android SBOM Analysis Completed	OK
2025-01-04 23:18:18	Android SAST Completed	OK
2025-01-04 23:18:18	Android API Analysis Started	OK
2025-01-04 23:18:24	Android API Analysis Completed	OK
2025-01-04 23:18:25	Android Permission Mapping Started	OK
2025-01-04 23:18:39	Android Permission Mapping Completed	OK
2025-01-04 23:18:41	Android Behaviour Analysis Started	OK
2025-01-04 23:18:50	Android Behaviour Analysis Completed	OK

2025-01-04 23:18:50	Extracting Emails and URLs from Source Code	OK
2025-01-04 23:18:58	Email and URL Extraction Completed	OK
2025-01-04 23:18:58	Extracting String data from APK	OK
2025-01-04 23:18:58	Extracting String data from Code	OK
2025-01-04 23:18:58	Extracting String values and entropies from Code	OK
2025-01-04 23:19:08	Performing Malware check on extracted domains	OK
2025-01-04 23:19:14	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.