

ANDROID STATIC ANALYSIS REPORT



digiBOP (1.3.9)

File Name:	digiBOP.apk
Package Name:	com.digibop.mobile
Scan Date:	Nov. 14, 2024, 8:22 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

飛 HIGH	▲ MEDIUM	i INFO	✓ SECURE	® HOTSPOT
5	18	3	4	1

FILE INFORMATION

File Name: digiBOP.apk

Size: 35.95MB

MD5: 0b4d631ead301fdb2bdebb1d353c6076

SHA1: 036fe0b5bb3b929eb9d10cd8bf6b615817cacb67

SHA256: 5f348d04576079dd8ad91015eb4e6ae905db258cbba3e4aca7369b4e54f2bc19

1 APP INFORMATION

App Name: digiBOP

Package Name: com.digibop.mobile

Main Activity: com.digibop.mobile.KonyMobileBankin

Target SDK: 33 Min SDK: 21 Max SDK:

Android Version Name: 1.3.9

APP COMPONENTS

Activities: 11 Services: 15 Receivers: 6 Providers: 4

Exported Activities: 2 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: 2023-02-23 11:54:41+00:00 Valid To: 2053-02-23 11:54:41+00:00

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

Serial Number: 0xfe30378d9324b6f831da7bab2ec8231802ab213c

Hash Algorithm: sha256

md5: 012e8f871cc59a269cbf1353f3e97b94

sha1: 487d081c919a4c49cb9fdbe3434afd2cb381f849

sha256: 2f425b187f9930cc64cc21a09cb967716d7e8d5b5dcee33e95b993c0a3de55ff

sha512: 434fc6e7b35c06d404535cda9dc486d5b7c5c83d72d4cf2fcf4d8604bfb75dd185e517b319f5d2e1c416de055adddf7e6563c57b4838a30e5b93489846241c7d

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 1682b2971cf962e0e117cf29a85312af4e7c307db9c13792a7fac4daa9b959e7

Found 1 unique certificates

E APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.digibop.mobile.permission.MAPS_RECEIVE	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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_COARSE_LOCATION	dangerous	coarse (network- based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.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.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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BROADCAST_SMS	signature	send SMS-received broadcast	Allows an application to broadcast a notification that an SMS message has been received. Malicious applications may use this to forge incoming SMS messages.
android.permission.CONTROL_LOCATION_UPDATES	SignatureOrSystem	control location update notifications	Allows enabling/disabling location update notifications from the radio. Not for use by common applications.
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_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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_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.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.

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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.



FILE	DETAILS			
	FINDINGS	DETAILS		
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check possible VM check		
	Anti Debug Code	Debug.isDebuggerConnected() check		
	Compiler	unknown (please file detection issue!)		
	FINDINGS	DETAILS		
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check Build.TAGS check		
	Obfuscator	unreadable field names unreadable method names		
	Compiler	unknown (please file detection issue!)		

FILE	DETAILS		
	FINDINGS	DETAILS	
classes3.dex	Compiler	unknown (please file detection issue!)	

△ NETWORK SECURITY

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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 6 | 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	Broadcast Receiver (com.konylabs.api.sms.SMSBroadcastReceiver) 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	Broadcast Receiver (com.konylabs.api.location.KonyGeofenceBroadcastReceiver) 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.
4	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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	Activity (com.unikrew.faceoff.HomeActivity) 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.wifi.sdk.bop.MainActivity) 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.

</> CODE ANALYSIS

HIGH: 4 | WARNING: 9 | INFO: 3 | SECURE: 3 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/hidglobal/ia/activcastle/crypto/tls/Export erLabel.java com/hidglobal/ia/activcastle/jcajce/spec/TLSK eyMaterialSpec.java com/kony/binarydatamanager/BinaryFileAdap terWithMetadata/constants/Constants.java com/kony/binarydatamanager/constant/Binar

NO	ISSUE	SEVERITY	STANDARDS	yDataManagerConstants.java For For Sony/logger/Constants/LoggerConstants. java
1	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/kony/sdkcommons/CommonUtility/KNY CommonConstants.java com/kony/sdkcommons/Database/KNYDatab aseErrorMessages.java com/kony/sdkcommons/Network/NetworkCo re/KNYHttpJobIntentService.java com/kony/sdkcommons/Network/NetworkCo re/KNYHttpService.java com/konylabs/api/box2flex/WidgetDataExtrac tor.java com/konylabs/api/crypto/CryptoAPI.java com/konylabs/api/gms/GMSConstants.java com/konylabs/api/ui/LuaListBox.java com/konylabs/api/ui/LuaApi.java com/konylabs/api/ui/LuaTextField2.java com/konylabs/api/ui/LuaTextField2.java com/konylabs/api/ui/flex/LuaFlexLayout.java com/konylabs/api/ui/flex/LuaFlexLayout.java com/konylabs/api/ui/flex/LuaFlexLayout.java com/konylabs/api/ui/flex/LuaFlexLayout.java com/konylabs/api/uil/KonyLogger.java com/konylabs/api/uil/KonyLogger.java com/konylabs/api/uil/KonyLogger.java com/veridiumid/sdk/defaultdata/secureprefer ences/SecurePreferences.java com/veridiumid/sdk/internal/licensing/domai n/model/SdkLicense.java com/veridiumid/sdk/internal/licensing/domai

NO	ISSUE	SEVERITY	STANDARDS	nts/SyncErrorMessages.java FILES
				
				com/hidgiobai/la/activcastle/asn1/anssi/ANSS
				ObjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/bsi/BSIObje
				ctldentifiers.java
				com/hidglobal/ia/activcastle/asn1/cmp/CMPO
				bjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/cms/CMSO
				bjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/crmf/CRMF
				ObjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/cryptopro/
				CryptoProObjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/dvcs/DVCS
				ObjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/eac/Certific
				ateHolderAuthorization.java
				com/hidglobal/ia/activcastle/asn1/eac/EACOb
				ectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/gnu/GNUO
				bjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/iana/IANAC
				bjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/isismtt/ISIS
				MTTObjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/kisa/KISAO bjectIdentifiers.java
				1 2
				com/hidglobal/ia/activcastle/asn1/microsoft/ MicrosoftObjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/misc/MiscC
				bjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/nist/NISTO
				bjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/ntt/NTTObj
				ectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/ocsp/OCSP
				ObjectIdentifiers.java
				com/hidglobal/ia/activcastle/asn1/oiw/OIWOb
				jectIdentifiers.java

NO	ISSUE	SEVERITY	STANDARDS	com/hidglobal/ia/activcastle/asn1/pkcs/PKCS ElliptS identifiers.java com/hidglobal/ia/activcastle/asn1/rosstandart
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	/RosstandartObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/sec/SECObj ectIdentifiers.java com/hidglobal/ia/activcastle/asn1/smime/SMI MECapabilities.java com/hidglobal/ia/activcastle/asn1/smime/SMI MECapability.java com/hidglobal/ia/activcastle/asn1/teletrust/Te leTrusTObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/ua/UAObje ctIdentifiers.java com/hidglobal/ia/activcastle/asn1/x500/style/ BCStyle.java com/hidglobal/ia/activcastle/asn1/x500/style/ RFC4519Style.java com/hidglobal/ia/activcastle/asn1/x509/Acces sDescription.java com/hidglobal/ia/activcastle/asn1/x509/Exten sion.java com/hidglobal/ia/activcastle/asn1/x509/FeyP urposeld.java com/hidglobal/ia/activcastle/asn1/x509/Policy QualifierId.java com/hidglobal/ia/activcastle/asn1/x509/X509 AttributeIdentifiers.java com/hidglobal/ia/activcastle/asn1/x509/X509E xtension.java com/hidglobal/ia/activcastle/asn1/x509/X509E xtensions.java com/hidglobal/ia/activcastle/asn1/x509/X509 Name.java com/hidglobal/ia/activcastle/asn1/x509/X509 ObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/x509/X509 ObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/x509/yso9 ObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/x509/yso9 ObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/x509/yso9 ObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/x509/yso9 ObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/x509/yso9 ObjectIdentifiers.java com/hidglobal/ia/activcastle/asn1/x509/ysigi/si glObjectIdentifiers.java

cm/hidglobal/ia/activcastle/jcajce/provider/a symmetric/x509/waliusa_jaya com/hidglobal/ia/activcastle/jcajce/provider/d igest/SM-3_jaya com/hidglobal/ia/activcastle/jcajce/provider/k eystore/pkcs12/PKC512KeyStoreSpi.jaya com/hidglobal/ia/activcastle/jcajce/provider/s ymmetric/AE5_jaya com/hidglobal/ia/activcastle/jcajce/provider/s ymmetric/AE5_jaya com/hidglobal/ia/activcastle/jcajce/provider/s ymmetric/DE5dea_jaya com/hidglobal/ia/activcastle/jcajce/provider/s ymmetric/DE5dea_jaya com/hidglobal/ia/activcastle/jcajce/provider/s ymmetric/DE5dea_jaya com/hidglobal/ia/activcastle/jcajce/provider/s ymmetric/RE5_jaya com/hidglobal/ia/activcastle/jcajce/provider/s ymmetric/RE5_jaya com/hidglobal/ia/activcastle/jce/PKC510Certifi cationRequest_jaya com/hidglobal/ia/activcastle/jce/provider/PKI XCertPatrivaliddatorSpi.jaya com/hidglobal/ia/activcastle/jce/provider/S50 9CertificareObject_jaya com/hidglobal/ia/activcastle/jce/provider/yetA pplicationTag_jaya com/hidglobal/ia/activcastle/jce/provider/yalu eOf_jaya com/hidglobal/ia/activcastle/pcyc/asn1/PQCO bjectIdentifiers_jaya com/hidglobal/ia/activcastle/pcyc/crypto/mceli ece/McElieceColayer-playa/com/hidglobal/ia/activcastle/pcyc/crypto/mceli ece/McElieceColayer-player-player-player-player-player-player-player-player-player-player-player-player-player-
ece/McElieceFujisakiCipher.java com/hidglobal/ia/activcastle/pqc/crypto/mceli

NO	ISSUE	SEVERITY	STANDARDS	com/hidglobal/ia/activcastle/pqc/crypto/mceli Fde/fc6cEliecePointchevalCipher.java com/hidglobal/ia/activcastle/pqc/jcajce/provid
				er/mceliece/McElieceCCA2KeyFactorySpi.java com/hidglobal/ia/activcastle/pqc/jcajce/provid er/mceliece/McElieceKeyFactorySpi.java com/hidglobal/ia/activcastle/x509/PKIXCertPa thReviewer.java com/hidglobal/ia/activcastle/x509/main.java com/hidglobal/ia/internal/ASN1BitString.java com/hidglobal/ia/internal/getLengthOfHeader .java com/hidglobal/ia/internal/getObject.java com/hidglobal/ia/internal/readLength.java
				Cz/msebera/androld/httpcilent/conn/params/ ʃama/exataβæs/MagalesquareExample.java Jama/test/TestMatrix.java com/example/mvisamodule/MainActivity.java com/example/mvisamodule/QRScanParser.ja va com/hidglobal/ia/activcastle/LICENSE.java com/hidglobal/ia/activcastle/asn1/util/Dump.j ava com/hidglobal/ia/activcastle/crypto/engines/N accacheSternEngine.java com/hidglobal/ia/activcastle/crypto/generator s/NaccacheSternKeyPairGenerator.java com/hidglobal/ia/activcastle/jcajce/provider/k eystore/pkcs12/PKCS12KeyStoreSpi.java com/hidglobal/ia/activcastle/jcajce/provider/s ymmetric/util/BaseWrapCipher.java com/hidglobal/ia/activcastle/jce/provider/Bro kenJCEBlockCipher.java com/hidglobal/ia/activcastle/math/ec/tools/Di scoverEndomorphisms.java com/hidglobal/ia/activcastle/math/ec/tools/F2 mSqrtOptimizer.java com/hidglobal/ia/activcastle/math/ec/tools/Tr aceOptimizer.java com/hidglobal/ia/activcastle/pqc/crypto/gmss

NO	ISSUE	SEVERITY	STANDARDS	/GMSSKeyPairGenerator.java Folim 6 idglobal/ia/activcastle/pqc/crypto/gmss /GMSSPrivateKeyParameters.java
NO	ISSUE	SEVERITY	STANDARDS	
				com/konylabs/api/sms/AppSignatureHashHel per.java com/konylabs/api/util/EventRecurrence.java com/konylabs/api/util/KonyLogger.java

NO	ISSUE	SEVERITY	STANDARDS	com/konylabs/api/util/RecurrenceProcessor.ja FaLES com/konylabs/api/util/RecurrenceSet.java
3	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	com/konylabs/automation/vm/KonyAutomati onVM.java com/konylabs/js/api/JSAutomation/JSAutomat ionLib.java com/konylabs/jsbindings/ClassLoaderInjector. java com/loopj/android/http/LogHandler.java com/neovisionaries/ws/client/SNIHelper.java com/tbruyelle/rxpermissions2/RxPermissions Fragment.java com/tbruyelle/rxpermissions2/RxPermissions Fragment.java com/temenos/hidapprove/AsyncOTPGenerati onThread.java com/temenos/hidapprove/ProvisionEventList ener.java com/temenos/hidapprove/ProvisionIngThread.java com/temenos/hidapprove/ProvisioningThread.java com/temenos/hidapprove/service/BiometricS ervice.java com/temenos/hidapprove/service/Fingerprint Handler.java com/temenos/hidapprove/service/Fingerprint Handler.java com/temenos/hidapprove/utils/PasswordUtil.java com/temenos/hidapprove/utils/PinDialogUtil.java com/temenos/hidapprove/utils/SDKContainer Util.java com/temenos/hidapprove/utils/SDKContainer Util.java com/veridiumid/sdk/VeridiumSDK.java com/veridiumid/sdk/VeridiumSDK.java com/veridiumid/sdk/VeridiumSDKImpl.java com/veridiumid/sdk/VeridiumSDKImpl.java com/veridiumid/sdk/Acativities/BiometricsAggregateActivity.java com/veridiumid/sdk/Analytics/Analytics.java

NO	ISSUE	SEVERITY	STANDARDS	com/veridiumid/sdk/analytics/AnalyticsLibrar
				com/veridiumid/sdk/crypto/TransactionSignin gHelper.java
	1			com/veridiumid/sdk/defaultdata/DataStorage.
	1			java
	1	'		com/veridiumid/sdk/defaultdata/secureprefer
	1	'		ences/LegacySecurePreferences.java
	1	'		com/veridiumid/sdk/defaults/biometricsetting
	1	'		sdefaultui/BiometricSettingsFragment.java
	1	'		com/veridiumid/sdk/fourf/ExportConfig.java
	1	'		com/veridiumid/sdk/fourf/FourFLoader.java
	1			com/veridiumid/sdk/fourf/PlatformLoggerCon
	1	'		nector.java
	1	'		com/veridiumid/sdk/fourf/VeridiumSDKFourFl
	1	'		nitializer.java
	1			com/veridiumid/sdk/fourf/camera/Camera1Pr
	1	'		eviewView.java
	1	'		com/veridiumid/sdk/fourf/camera/FourFCam
	1			era1.java
	1	'		com/veridiumid/sdk/fourf/camera/FourFCam
	1	'		era2.java
	1	'		com/veridiumid/sdk/fourf/camera/lmageTagg
	1	'		ingQueue.java
	1	'		com/veridiumid/sdk/fourf/ui/FourFUIFragmen
	1	'		t.java
	1	'		com/veridiumid/sdk/fourf/ui/InstructionalDial
	1	'		og.java
	1	'		com/veridiumid/sdk/internal/licensing/Licensi
	1	'		ngRepository.java
	1	'		com/veridiumid/sdk/licensing/LicensingMana
	1	'		ger.java
	1	'		com/veridiumid/sdk/log/Timber.java
	1	'		com/veridiumid/sdk/model/ManifestVeridium
	1	'		SDKModel.java
	1	'		com/veridiumid/sdk/model/biometrics/engin
	1	'		e/impl/DecentralizedBiometricsEngineImpl.jav
	1			a
	1	'		com/veridiumid/sdk/model/biometrics/engin
	1	'		e/impl/ModularBiometricProcessor.java

NO	ISSUE	SEVERITY	STANDARDS	com/veridiumid/sdk/model/biometrics/engin FloribSessing/handling/impl/AdaptiveEnrollme ntHandler.java
				com/veridiumid/sdk/model/biometrics/engin e/processing/handling/impl/AuthenticationHandler.java com/veridiumid/sdk/model/biometrics/packaging/lBiometricFormats.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/security/AesCbcWithIntegrity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java com/veridiumid/sdk/support/BiometricBaseActivity.java com/veridiumid/sdk/support/BiometricBaseActivity.java com/veridiumid/sdk/support/help/CustomCountDownTimer.java com/veridiumid/sdk/support/ui/AspectRatioSafeFrameLayout.java com/wifi/sdk/bop/GpsUtils.java com/wifi/sdk/bop/MainActivity.java cz/msebera/android/httpclient/conn/util/PublicSuffixMatcherLoader.java cz/msebera/android/httpclient/extras/PRNGFixes.java cz/msebera/android/httpclient/extras/PRNGFixes.java cz/msebera/android/httpclient/impl/conn/DefaultClientConnection.java cz/msebera/android/httpclient/impl/conn/DefaultClientConnection.java cz/msebera/android/httpclient/impl/execchain/MainClientExec.java
				ebtbuvojaiggibc/C0288.java

ebtbuvojaiggibc/C0288.java sync/kony/com/syncv2library/Android/Logger /SyncLogger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/hidglobal/ia/internal/ASN1BitString.java com/hidglobal/ia/internal/getIntegrityCheck.ja va com/hidglobal/ia/internal/getLengthOfHeader .java com/hidglobal/ia/internal/getNames.java com/hidglobal/ia/internal/getOID.java com/hidglobal/ia/internal/getOID.java com/konylabs/api/crypto/CryptoAPI.java com/neovisionaries/ws/client/HandshakeRead er.java com/unikrew/faceoff/fingerprint/SecureStorag e/b.java com/veridiumid/sdk/model/help/EncryptionU tils.java com/veridiumid/sdk/security/AesCbcWithInte grity.java cz/msebera/android/httpclient/extras/PRNGFi xes.java cz/msebera/android/httpclient/impl/auth/NTL MEngineImpl.java cz/msebera/android/httpclient/impl/client/cac he/BasicldGenerator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/hidglobal/ia/activcastle/asn1/ua/DSTU41 45PointEncoder.java com/hidglobal/ia/activcastle/crypto/prng/Fixe dSecureRandom.java com/hidglobal/ia/activcastle/crypto/prng/SP8 00SecureRandom.java com/hidglobal/ia/activcastle/crypto/prng/X93 1SecureRandom.java com/hidglobal/ia/activcastle/math/ec/ECCurve .java com/hidglobal/ia/activcastle/math/ec/ECField Element.java com/hidglobal/ia/activcastle/math/raw/Mod.j ava com/hidglobal/ia/activcastle/pqc/math/lineara lgebra/GF2Polynomial.java com/hidglobal/ia/activcastle/pqc/math/lineara lgebra/GF2nONBField.java com/hidglobal/ia/activcastle/pqc/math/lineara lgebra/GF2nPolynomialElement.java com/loopj/android/http/SimpleMultipartEntity .java cz/msebera/android/httpclient/entity/mime/ MultipartEntityBuilder.java ebtbuvojaiggibc/C0345.java ebtbuvojaiggibc/C0340.java ebtbuvojaiggibc/C0340.java
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/konylabs/api/util/Preferences.java com/unikrew/faceoff/fingerprint/SecureStorag e/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/kony/CaptureSignature.java com/kony/logger/b/i.java com/konylabs/api/box2flex/WidgetDataExtrac tor.java com/konylabs/api/imageprocessing/Image.jav a com/konylabs/api/io/KonyFile.java com/konylabs/api/io/KonyFileSystem.java com/konylabs/api/ui/KonyWeb.java com/konylabs/api/ui/LuaCamera.java com/konylabs/api/uil/MediaUtil.java com/konylabs/automation/vm/KonyAutomati onVM.java com/konylabs/js/api/JSAutomation/JSAutomat ionLib.java com/konylabs/js/api/JSFileSystemLib.java com/konymp/konympsocialshare/SocialShare .java com/unikrew/faceoff/FaceoffDemoBaseActivit y.java com/unikrew/faceoff/fingerprint/FingerprintSc annerActivity.java com/veridiumid/sdk/fourf/camera/FourFCam era2.java net/ndctech/pdfutils/PDFUtils.java
8	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/konylabs/jsbindings/ProxyBuilder.java com/loopj/android/http/FileAsyncHttpRespon seHandler.java
9	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	com/kony/sdkcommons/Database/SQLiteCiph erDatabaseHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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/AndroidHelp er.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelp er.java
12	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/hidglobal/ia/internal/getCertificateChain.j ava com/hidglobal/ia/internal/getData.java com/hidglobal/ia/internal/getEncryptedKeyDa ta.java com/kony/sdkcommons/Database/SQLiteAnd roidDatabaseHelper.java com/konylabs/api/db/KonySQLDatabase.java com/konylabs/api/db/KonySQLStatement.java com/konylabs/api/html5/LocalStorageLib.java com/konylabs/api/i18n/KonyI18n.java com/konylabs/notification/KonyLocalNotificati onDB.java com/konylabs/notification/KonyNotificationSe ttingsDB.java
13	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/konylabs/api/util/MediaUtil.java
14	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/loopj/android/http/MySSLSocketFactory.j ava cz/msebera/android/httpclient/conn/ssl/SSLC onnectionSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLS ocketFactory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	This App uses SafetyNet API.	secure	OWASP MASVS: MSTG-RESILIENCE-7	com/konylabs/api/gms/safetynet/KonySafety NetApiManager.java
16	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/hidglobal/ia/internal/hasEncodedTagValu e.java com/kony/sdkcommons/Network/NetworkCo re/KNYPublicKeyPinningManager.java com/kony/sdkcommons/Network/NetworkCo re/KNYSSLSocketFactory.java com/konylabs/api/net/KonyPublicKeyPinning Manager.java com/konylabs/api/net/KonySSLSocketFactory URLConnection.java com/loopj/android/http/MySSLSocketFactory.j ava com/veridiumid/sdk/internal/licensing/ws/Lic ensingServiceApi.java cz/msebera/android/httpclient/conn/ssl/SSLC ontextBuilder.java cz/msebera/android/httpclient/ssl/SSLContext Builder.java
17	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	cz/msebera/android/httpclient/impl/auth/NTL MEnginelmpl.java
18	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	cz/msebera/android/httpclient/impl/auth/NTL MEnginelmpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
19	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/hidglobal/ia/internal/EncryptedObjectSto reData.java com/hidglobal/ia/internal/getAdjustedDate.jav a com/hidglobal/ia/internal/getEncryptionAlgori thm.java

■ NIAP ANALYSIS v1.3

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

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/hidglobal/ia/internal/isNumericString.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java com/konylabs/api/map/KonyMapUtils.java com/konylabs/api/net/KonyHttpRequestURLConnection.java com/konylabs/api/net/ServiceInvokerURLConnection.java com/konylabs/automation/util/KonyAutomationUtil.java
00123	Save the response to JSON after connecting to the remote server	network command	com/konylabs/api/map/KonyMapUtils.java com/konylabs/api/net/KonyHttpRequestURLConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/hidglobal/ia/activcastle/x509/PKIXCertPathReviewer.java com/hidglobal/ia/internal/isNumericString.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java com/konylabs/api/map/KonyMapUtils.java com/konylabs/api/net/KonyHttpRequestURLConnection.java com/konylabs/api/net/ServiceInvokerURLConnection.java com/konylabs/automation/util/KonyAutomationUtil.java
00163	Create new Socket and connecting to it	socket	com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java com/konylabs/api/map/KonyMapUtils.java com/konylabs/api/net/KonyHttpRequestURLConnection.java com/konylabs/api/net/ServiceInvokerURLConnection.java com/neovisionaries/ws/client/SocketInitiator.java com/neovisionaries/ws/client/WebSocket.java cz/msebera/android/httpclient/conn/MultihomePlainSocketFactory.java cz/msebera/android/httpclient/conn/scheme/PlainSocketFactory.java cz/msebera/android/httpclient/conn/socket/PlainConnectionSocketFactory.ja va cz/msebera/android/httpclient/conn/ssl/SSLConnectionSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLSocketFactory.java cz/msebera/android/httpclient/impl/pool/BasicConnFactory.java
00030	Connect to the remote server through the given URL	network	com/hidglobal/ia/activcastle/x509/PKIXCertPathReviewer.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java com/konylabs/api/map/KonyMapUtils.java com/konylabs/api/net/KonyHttpRequestURLConnection.java com/konylabs/api/net/ServiceInvokerURLConnection.java com/konylabs/automation/util/KonyAutomationUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/hidglobal/ia/activcastle/x509/PKIXCertPathReviewer.java com/hidglobal/ia/internal/isNumericString.java com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java com/konylabs/api/map/KonyMapUtils.java com/konylabs/api/net/KonyHttpRequestURLConnection.java com/konylabs/api/net/ServiceInvokerURLConnection.java com/konylabs/automation/util/KonyAutomationUtil.java
00183	Get current camera parameters and change the setting.	camera	com/konylabs/api/ui/KonyCamera.java com/konylabs/api/ui/KonyVideoCamera.java com/konylabs/api/ui/MLCamera/KonyMLCamera.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java
00199	Stop recording and release recording resources	record	com/konylabs/api/Media/Recorder.java com/konylabs/api/ui/KonyVideoCamera.java
00198	Initialize the recorder and start recording	record	com/konylabs/api/Media/Recorder.java com/konylabs/api/ui/KonyVideoCamera.java
00006	Scheduling recording task	record	com/konylabs/api/ui/KonyVideoCamera.java
00041	Save recorded audio/video to file	record	com/konylabs/api/Media/Recorder.java com/konylabs/api/ui/KonyVideoCamera.java
			Jama/test/TestMatrix.java com/hidglobal/ia/activcastle/asn1/getInstance.java com/hidglobal/ia/activcastle/asn1/util/Dump.java com/hidglobal/ia/internal/ASN1ApplicationSpecific.java com/hidglobal/ia/internal/DERTaggedObject.java com/hidglobal/ia/internal/DERTags.java com/hidglobal/ia/internal/valueOf.java com/kony/binary/utility/BlobFileUtils.java com/kony/binarydatamanager/uploadHandlers/BytesUploadHandlerTask.jav

RULE ID	BEHAVIOUR	LABEL	a com/kony/binarydatamanager/uploadHandlers/MultipartUploadHandlerTask FILES .java com/kony/cms/client/e.java
00013	Read file and put it into a stream	file	com/konylabs/android/FunctionalPreview.java com/konylabs/api/ML/ImageClassifier/KonyImageClassifier.java com/konylabs/api/Media/MediaServer.java com/konylabs/api/StandardLib.java com/konylabs/api/ds/KonyDataSource.java com/konylabs/api/funcmodules/KonyFunctionalModules.java com/konylabs/api/i18n/KonyI18n.java com/konylabs/api/io/KonyFile.java com/konylabs/api/io/KonyFileSystem.java com/konylabs/api/io/RawBytes.java com/konylabs/api/io/RawBytes.java com/konylabs/api/io/RawBytes.java com/konylabs/ymintf/KonyJavaScriptVM.java com/konylabs/vmintf/KonyJavaScriptVM.java com/loopj/android/http/JsonStreamerEntity.java com/loopj/android/http/SimpleMultipartEntity.java com/loopj/android/http/SimpleMultipartEntity.java com/unikrew/faceoff/fingerprint/SecureStorage/b.java com/veridiumid/sdk/security/AesCbcWithIntegrity.java cz/msebera/android/httpclient/conn/util/PublicSuffixMatcherLoader.java cz/msebera/android/httpclient/entity/FileEntity.java cz/msebera/android/httpclient/entity/FileEntity.java cz/msebera/android/httpclient/extras/PRNGFixes.java cz/msebera/android/httpclient/impl/client/cache/FileResource.java cz/msebera/android/httpclient/ssl/SSLContextBuilder.java ebtbuvojaiggibc/C0273.java ebtbuvojaiggibc/C0291.java ebtbuvojaiggibc/C0363.java okio/Okio.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/hidglobal/ia/internal/valueOf.java com/kony/cms/client/e.java com/kony/logger/b/i.java com/konylabs/api/io/KonyFile.java com/konylabs/api/io/KonyFileSystem.java com/konylabs/api/io/RawBytes.java com/konylabs/apm/KonyAPMCrashReporter.java com/konymp/konympsocialshare/SocialShare.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/analytics/AnalyticsLibraryDataDumpInternalUse.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java ebtbuvojaiggibc/C0313.java ebtbuvojaiggibc/C0334.java ebtbuvojaiggibc/C0368.java
00012	Read data and put it into a buffer stream	file	com/hidglobal/ia/internal/valueOf.java com/konylabs/android/FunctionalPreview.java com/konylabs/api/StandardLib.java com/konylabs/api/io/KonyFile.java com/konylabs/vmintf/KonyJavaScriptVM.java
00189	Get the content of a SMS message	sms	com/konylabs/api/contacts/ContactAPISdk3.java com/konylabs/api/contacts/ContactAPISdk5.java com/konylabs/api/util/MediaUtil.java com/konylabs/js/api/JSCameraLib.java
00188	Get the address of a SMS message	sms	com/konylabs/api/contacts/ContactAPISdk3.java com/konylabs/api/contacts/ContactAPISdk5.java com/konylabs/api/util/MediaUtil.java com/konylabs/js/api/JSCameraLib.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	com/konylabs/api/contacts/ContactAPISdk3.java com/konylabs/api/contacts/ContactAPISdk5.java com/konylabs/api/util/MediaUtil.java com/konylabs/js/api/JSCameraLib.java
00187	Query a URI and check the result	collection sms calllog calendar	com/konylabs/api/contacts/ContactAPISdk3.java com/konylabs/api/contacts/ContactAPISdk5.java
00201	Query data from the call log	collection calllog	com/konylabs/api/contacts/ContactAPISdk3.java com/konylabs/api/contacts/ContactAPISdk5.java com/konylabs/api/util/MediaUtil.java com/konylabs/js/api/JSCameraLib.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/konylabs/android/KonyAppInitializer.java com/konylabs/android/KonyMain.java com/konylabs/api/StandardLib.java com/konylabs/api/permissions/RuntimePermissionsLib.java com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java com/konylabs/api/util/MediaUtil.java com/konylabs/api/wearable/KonyWearable.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/konylabs/android/KonyMain.java com/konylabs/api/StandardLib.java com/konylabs/api/permissions/RuntimePermissionsLib.java com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java com/konylabs/api/wearable/KonyWearable.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/konylabs/api/StandardLib.java com/konylabs/api/imageprocessing/Image.java com/konylabs/api/ui/KonyButton.java com/konylabs/api/ui/KonyCamera.java com/konylabs/api/util/MediaUtil.java
00036	Get resource file from res/raw directory	reflection	com/konylabs/android/KonyMain.java com/konylabs/api/StandardLib.java com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java com/konylabs/api/util/MediaUtil.java
00024	Write file after Base64 decoding	reflection file	com/kony/binary/utility/BinaryDataUtils.java com/veridiumid/sdk/security/AesCbcWithIntegrity.java net/ndctech/pdfutils/PDFUtils.java
00202	Make a phone call	control	com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java
00203	Put a phone number into an intent	control	com/konylabs/api/ui/KonyCordovaWeb.java com/konylabs/api/ui/KonyWeb.java
00091	Retrieve data from broadcast	collection	com/kony/Sign.java com/kony/push/custom/CustomPushNotificationReceiver.java com/konylabs/android/KonyAppInitializer.java com/konylabs/android/KonyMain.java com/konylabs/gcm/KonyGCMBroadcastReceiver.java com/konylabs/notification/KonyLocalNotificationBroadcastReceiver.java com/konylabs/pushNotification/KonyPushManager.java com/veridiumid/sdk/activities/BiometricsAggregateActivity.java com/veridiumid/sdk/fourf/FourFBiometricsActivity.java com/veridiumid/sdk/support/AbstractBiometricsActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	com/kony/binarydatamanager/uploadHandlers/BytesUploadHandlerTask.jav a com/kony/binarydatamanager/uploadHandlers/MultipartUploadHandlerTask .java com/loopj/android/http/JsonStreamerEntity.java
00004	Get filename and put it to JSON object	file collection	com/kony/binarydatamanager/manager/OnlineBinaryUploadManager.java com/kony/binarydatamanager/uploadHandlers/BytesUploadHandlerTask.jav a com/kony/binarydatamanager/uploadHandlers/MultipartUploadHandlerTask .java com/loopj/android/http/JsonStreamerEntity.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java
00192	Get messages in the SMS inbox	sms	com/konylabs/api/net/ServiceInvokerURLConnection.java com/konylabs/api/util/MediaUtil.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/konylabs/api/util/MediaUtil.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/konylabs/api/util/MediaUtil.java
00191	Get messages in the SMS inbox	sms	com/konylabs/api/util/CalendarAPI.java com/konylabs/api/util/MediaUtil.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/konylabs/api/util/MediaUtil.java
00005	Get absolute path of file and put it to JSON object	file	com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	com/neovisionaries/ws/client/SocketInitiator.java cz/msebera/android/httpclient/conn/MultihomePlainSocketFactory.java cz/msebera/android/httpclient/conn/scheme/PlainSocketFactory.java cz/msebera/android/httpclient/conn/socket/PlainConnectionSocketFactory.ja va cz/msebera/android/httpclient/conn/ssl/SSLConnectionSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLSocketFactory.java cz/msebera/android/httpclient/impl/pool/BasicConnFactory.java
00002	Open the camera and take picture	camera	com/konylabs/api/ui/KonyCamera.java com/veridiumid/sdk/fourf/camera/FourFCamera1.java
00033	Query the IMEI number	collection	com/konylabs/api/OSLib.java
00083	Query the IMEI number	collection telephony	com/konylabs/api/OSLib.java
00028	Read file from assets directory	file	com/konylabs/android/FunctionalPreview.java com/konylabs/api/crypto/CryptoAPI.java com/konylabs/api/net/KonyPublicKeyPinningManager.java com/veridiumid/sdk/model/help/AssetsHelper.java
00015	Put buffer stream (data) to JSON object	file	com/konylabs/api/ui/KonySkin.java
00047	Query the local IP address	network collection	cz/msebera/android/httpclient/impl/SocketHttpClientConnection.java cz/msebera/android/httpclient/impl/SocketHttpServerConnection.java
00009	Put data in cursor to JSON object	file	com/konyffi/contacts/ContactPicker.java
00194	Set the audio source (MIC) and recorded file format	record	com/konylabs/api/Media/Recorder.java

RULE ID	BEHAVIOUR	LABEL	FILES
00197	Set the audio encoder and initialize the recorder	record	com/konylabs/api/Media/Recorder.java
00196	Set the recorded file format and output path	record file	com/konylabs/api/Media/Recorder.java
00034	Query the current data network type	collection network	com/konylabs/js/api/JSNetworkLib.java
00147	Get the time of current location	collection location	com/konylabs/api/location/KonyAndroidLocationManager.java
00075	Get location of the device	collection location	com/konylabs/api/location/KonyAndroidLocationManager.java
00137	Get last known location of the device	location collection	com/konylabs/api/location/KonyAndroidLocationManager.java
00112	Get the date of the calendar event	collection calendar	com/hidglobal/ia/internal/addAll.java com/konylabs/api/util/CalendarAPI.java
00023	Start another application from current application	reflection control	com/konylabs/android/KonyMain.java
00094	Connect to a URL and read data from it	command network	com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java com/konylabs/automation/util/KonyAutomationUtil.java
00108	Read the input stream from given URL	network command	com/kony/sdkcommons/Network/NetworkCore/KNYHttpConnectionUtil.java com/konylabs/automation/util/KonyAutomationUtil.java
00128	Query user account information	collection account	com/konylabs/api/contacts/ContactAPISdk5.java



TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/927418688349/namespaces/firebase:fetch?key=AlzaSyC-b9PWT8qdvSrFpUMyMec-WTNJ4YBNef4. This is indicated by the response: {'state': 'NO_TEMPLATE'}

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/25	android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.READ_PHONE_STATE, android.permission.READ_CONTACTS, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_SMS, android.permission.VIBRATE, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_SETTINGS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	5/44	android.permission.BROADCAST_SMS, android.permission.CHANGE_WIFI_STATE, com.google.android.c2dm.permission.RECEIVE, android.permission.FLASHLIGHT, 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

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.bouncycastle.org	ok	IP: 203.32.61.103 Country: Australia Region: Victoria City: Fitzroy Latitude: -37.798389 Longitude: 144.978333 View: Google Map
unikrew-faceoff-telemetry.azurewebsites.net	ok	IP: 65.52.250.96 Country: United Arab Emirates Region: Dubayy City: Dubai Latitude: 25.258169 Longitude: 55.304722 View: Google Map
meezan-faceoff-ids.covalent.pk	ok	No Geolocation information available.
example.com	ok	IP: 93.184.215.14 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.
xml.org	ok	IP: 104.239.240.11 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
faceoffauthentication.azurewebsites.net	ok	IP: 13.77.82.141 Country: United States of America Region: Virginia City: Boydton Latitude: 36.667641 Longitude: -78.387497 View: Google Map
xmlpull.org	ok	IP: 185.199.110.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map

DOMAIN	STATUS	GEOLOCATION
licensing.prod.veridium-dev.com	ok	IP: 35.158.19.174 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
www.w3.org	ok	IP: 104.18.23.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
faceoffmobilebackend.azurewebsites.net	ok	IP: 13.77.82.141 Country: United States of America Region: Virginia City: Boydton Latitude: 36.667641 Longitude: -78.387497 View: Google Map
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



EMAIL	FILE
xvpm@rfki.aj	com/konylabs/js/api/JSAutomation/JSAutomationWidgetLib.java
xvpm@rfki.aj	com/konylabs/automation/vm/KonyAutomationVM.java

A TRACKERS

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

POSSIBLE SECRETS
"google_api_key" : "AlzaSyC-b9PWT8qdvSrFpUMyMec-WTNJ4YBNef4"
"google_crash_reporting_api_key" : "AlzaSyC-b9PWT8qdvSrFpUMyMec-WTNJ4YBNef4"
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
28091019353058090096996979000309560759124368558014865957655842872397301267595
10099790675505530477208181553592522486984108257205345787482351587557714799052927277724415285269929879648335669968284202797289605274717 31754805904856071347468521419286809125615028022221856475391909026561163678472701450190667942909301854462163997308722217328898303231940 97355403213400972588322876850946740663962
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD33 6747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C8 13F0DF45BE8112F4
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
7B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
3826F008A8C51D7B95284D9D03FF0E00CE2CD723A
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34

POSSIBLE SECRETS
MQVwithSHA512KDFAndSharedInfo
127971af8721782ecffa3
020A601907B8C953CA1481EB10512F78744A3205FD
91771529896554605945588149018382750217296858393520724172743325725474374979801
c49d360886e704936a6678e1139d26b7819f7e90
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15 DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
DB7C2ABF62E35E668076BEAD208B
79885141663410976897627118935756323747307951916507639758300472692338873533959
324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
e8b4011604095303ca3b8099982be09fcb9ae616

POSSIBLE SECRETS
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
9162fbe73984472a0a9d0590
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
6BA06FE51464B2BD26DC57F48819BA9954667022C7D03
00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
E95E4A5F737059DC60DF5991D45029409E60FC09
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
1E589A8595423412134FAA2DBDEC95C8D8675E58
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129

POSSIBLE SECRETS
D2C0FB15760860DEF1EEF4D696E6768756151754
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
70390085352083305199547718019018437840920882647164081035322601458352298396601
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72
42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437 66945636488273037083893479108083593264797677860191534347440096103423131667257868692048219493287863336020338479709268434224762105576023 5016132614780652761028509445403338652341
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
31a92ee2029fd10d901b113e990710f0d21ac6b6
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
14201174159756348119636828602231808974327613839524373876287257344192745939351271897363116607846760036084894662356762579528277471921224 19290710461342083806363940845126918288940005715246254452957693493567527289568315417754417631393844571917550968471078465956625479423122

POSSIBLE SECRETS
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
b8adf1378a6eb73409fa6c9c637ba7f5
0217C05610884B63B9C6C7291678F9D341
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCD F028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665 772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB
5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE
00E8BEE4D3E2260744188BE0E9C723
28792665814854611296992347458380284135028636778229113005756334730996303888124
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
74D59FF07F6B413D0EA14B344B20A2DB049B50C3

023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10

216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA

036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a

57896044618658097711785492504343953927102133160255826820068844496087732066703

C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE4 28782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562C E1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930 E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83

51DEF1815DB5ED74FCC34C85D709

046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C

B99B99B099B323E02709A4D696E6768756151751

1053CDE42C14D696E67687561517533BF3F83345

MQVwithSHA384KDFAndSharedInfo

B10B8F96A080E01DDE92DE5EAE5D54EC52C99FBCFB06A3C69A6A9DCA52D23B616073E28675A23D189838EF1E2EE652C013ECB4AEA906112324975C3CD49B83BFAC CBDD7D90C4BD7098488E9C219A73724EFFD6FAE5644738FAA31A4FF55BCCC0A151AF5F0DC8B4BD45BF37DF365C1A65E68CFDA76D4DA708DF1FB2BC2E4A4371

5F49EB26781C0EC6B8909156D98ED435E45FD59918

072546B5435234A422E0789675F432C89435DE5242

033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097

0667ACEB38AF4E488C407433FFAE4F1C811638DF20

29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA

cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953

4E13CA542744D696E67687561517552F279A8C84

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297

b3fb3400dec5c4adceb8655d4c94

DB7C2ABF62E35E668076BEAD2088

0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C

AC4032EF4F2D9AE39DF30B5C8FFDAC506CDEBE7B89998CAF74866A08CFE4FFE3A6824A4E10B9A6F0DD921F01A70C4AFAAB739D7700C29F52C57DB17C620A8652BE 5E9001A8D66AD7C17669101999024AF4D027275AC1348BB8A762D0521BC98AE247150422EA1ED409939D54DA7460CDB5F6C6B250717CBEF180EB34118E98D11952 9A45D6F834566E3025E316A330EFBB77A86F0C1AB15B051AE3D428C8F8ACB70A8137150B8EEB10E183EDD19963DDD9E263E4770589EF6AA21E7F5F2FF381B539CCE 3409D13CD566AFBB48D6C019181E1BCFE94B30269EDFE72FE9B6AA4BD7B5A0F1C71CFFF4C19C418E1F6EC017981BC087F2A7065B384B890D3191F2BFA

03375D4CE24FDE434489DE8746E71786015009E66E38A926DD

115792089237316195423570985008687907853269984665640564039457584007913129639316

D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA 9C77877AAAC6AC7D35245D1692E8EE1

02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7

0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB

043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE

790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16

64033881142927202683649881450433473985931760268884941288852745803908878638612

29818893917731240733471273240314769927240550812383695689146495261604565990247

96341f1138933bc2f503fd44

5EEEFCA380D02919DC2C6558BB6D8A5D

3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723

038D16C2866798B600F9F08BB4A8E860F3298CE04A5798

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB8 05276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F 0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D606 3D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F 784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7 ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B

0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05

883423532389192164791648750360308885314476597252960362792450860609699839

1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63

26DC5C6CF94A4B44F330B5D9BBD77CBF958416295CF7F1CF6BCCDC18FF8C07B6

FFFFFFF0000000075A30D1B9038A115

04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD

A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377

CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D

2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988

7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826

 $12702124828893241746590704277717644352578765350891653581281750726570503126098509849742318833348340118092599999512098893413065920561499\\67242541210492743493570749203127695614516892241105793112488126102296785346384016935200132889950003622606842227508135323070045173416336\\85004541062586971416883686778842537820383$

0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9

010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967

04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3

10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1

0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D

06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C

985BD3ADBAD4D696F676875615175A21B43A97F3

7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE

027d29778100c65a1da1783716588dce2b8b4aee8e228f1896

04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD4 2A5A0989D1EE71B1B9BC0455FB0D2C3

1243ae1b4d71613bc9f780a03690e

04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7 E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B32 0430C8591984F601CD4C143EF1C7A3

AD107E1E9123A9D0D660FAA79559C51FA20D64E5683B9FD1B54B1597B61D0A75E6FA141DF95A56DBAF9A3C407BA1DF15EB3D688A309C180E1DE6B85A1274A0A66 D3F8152AD6AC2129037C9EDEFDA4DF8D91E8FEF55B7394B7AD5B7D0B6C12207C9F98D11ED34DBF6C6BA0B2C8BBC27BE6A00E0A0B9C49708B3BF8A317091883681 286130BC8985DB1602E714415D9330278273C7DE31EFDC7310F7121FD5A07415987D9ADC0A486DCDF93ACC44328387315D75E198C641A480CD86A1B9E587E8BE60 E69CC928B2B9C52172E413042E9B23F10B0E16E79763C9B53DCF4BA80A29E3FB73C16B8E75B97EF363E2FFA31F71CF9DE5384E71B81C0AC4DFFE0C10E64F

A4D1CBD5C3FD34126765A442EFB99905F8104DD258AC507FD6406CFF14266D31266FEA1E5C41564B777E690F5504F213160217B4B01B886A5E91547F9E2749F4D7FBD7D3B9A92EE1909D0D2263F80A76A6A24C087A091F531DBF0A0169B6A28AD662A4D18E73AFA32D779D5918D08BC8858F4DCEF97C2A24855E6EEB22B3B2E5

0095E9A9EC9B297BD4BF36E059184F

023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd

659EF8BA043916EEDE8911702B22

E95E4A5F737059DC60DFC7AD95B3D8139515620C

04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321

0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294

4D41A619BCC6EADF0448FA22FAD567A9181D37389CA

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

03F7061798EB99E238FD6F1BF95B48FEEB4854252B

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F 8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
7fffffffffffffffffffffffffffffffffffff
c469684435deb378c4b65ca9591e2a5763059a2e
1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D
10C0FB15760860DEF1EEF4D696E676875615175D
003088250CA6E7C7FE649CE85820F7
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA783 24ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012

03E5A88919D7CAFCBF415F07C2176573B2

3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4 0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D 044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97 A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048 B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD 68FC7DC1F5745FA55C706C4A1C5C88964F34D09DFB753AD418C1AD0F4FDFD049A955F5D78491C0B7A2F1575A008CCD727AB376DB6F695515B05BD412F5B8C2F4C 77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085 00689918DBEC7E5A0DD6DFC0AA55C7 02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7F FEFF7F2955727A 7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03 04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D 0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EE80289070FB05D38FF58321F2E800536D538CCDAA3D9 801C0D34C58D93FE997177101F80535A4738CEBCBF389A99B36371EB 0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7 2AA058F73A0E33AB486B0F610410C53A7F132310

POSSIBLE SECRETS
00F50B028E4D696E676875615175290472783FB1
4D696E676875615175985BD3ADBADA21B43A97E2
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F0 0
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B 8
3086d221a7d46bcde86c90e49284eb153dab
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
e43bb460f0b80cc0c0b075798e948060f8321b7d
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
6b8cf07d4ca75c88957d9d670591
6C01074756099122221056911C77D77E77A777E7E7E7F7FCB
68363196144955700784444165611827252895102170888761442055095051287550314083023
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F04699
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5

041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD5526 2B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315

9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35

470fa2b4ae81cd56ecbcda9735803434cec591fa

57896044618658097711785492504343953926634992332820282019728792003956564823190

0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

D09E8800291CB85396CC6717393284AAA0DA64BA

114ca50f7a8e2f3f657c1108d9d44cfd8

0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F82 27DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892

027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5

A9FB57DBA1FFA9BC3F660A909D838D718C397AA3B561A6F7901F0F82974856A7

0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5B D66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD1 6650

0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92

115792089237316195423570985008687907853073762908499243225378155805079068850323

401028774D7777C7B7666D1366EA432071274F89FF01E718

POSSIBLE SECRETS
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
E87579C11079F43DD824993C2CEE5ED3
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9
4099B5A457F9D69F79213D094C4BCD4D4262210B
01AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8

POSSIBLE SECRETS
C49D360886E704936A6678E1139D26B7819F7E90
7A1F6653786A68192803910A3D30B2A2018B21CD54
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136
002757A1114D696E6768756151755316C05E0BD4
6127C24C05F38A0AAAF65C0EF02C
622407086718302403086718302463048A4E
04B8266A46C55657AC734CE38F018F2192
12511cfe811d0f4e6bc688b4d
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035D A5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
0002010102110213408087388879004155326061017160745204739953039525802
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1

0108B39E77C4B108BED981ED0E890E117C511CF072

90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009
D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A
1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB
2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C
1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D
73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73

02197B07845F9BF2D96ADB0F5F3C7F2CFFBD7A3FB8B6FFC35C7FD67F26DDF6285A644F740A2614

1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F

004D696F67687561517512D8F03431FCF63B88F4

6277101735386680763835789423207666416083908700390324961279

B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4

3086d221a7d46bcde86c90e49284eb15

POSSIBLE SECRETS
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D9 27E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B 16E2F1516E23DD3C1A4827AF1B8AC15B
70390085352083305199547718019018437841079516630045180471284346843705633502616
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
F518AA8781A8DF278ABA4E7D64B7CB9D49462353
E95E4A5F737059DC60DFC7AD95B3D8139515620F
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
B4E134D3FB59EB8BAB57274904664D5AF50388BA

EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

71169be7330b3038edb025f1

040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F

71169be7330b3038edb025f1d0f9

22123dc2395a05caa7423daeccc94760a7d462256bd56916

3FB32C9B73134D0B2E77506660EDBD484CA7B18F21EF205407F4793A1A0BA12510DBC15077BE463FFF4FED4AAC0BB555BE3A6C1B0C6B47B1BC3773BF7E8C6F6290 1228F8C28CBB18A55AE31341000A650196F931C77A57F2DDF463E5E9EC144B777DE62AAAB8A8628AC376D282D6ED3864E67982428EBC831D14348F6F2F9193B5045 AF2767164E1DFC967C1FB3F2E55A4BD1BFFE83B9C80D052B985D182EA0ADB2A3B7313D3FE14C8484B1E052588B9B7D2BBD2DF016199ECD06E1557CD0915B3353B BB64E0EC377FD028370DF92B52C7891428CDC67EB6184B523D1DB246C32F63078490F00EF8D647D148D47954515E2327CFEF98C582664B4C0F6CC41659

13353181327272067343385951994831900121794237596784748689948235959936964252873471246159040332773182141032801252925387191478859899310331 05677441361963648030647213778266568986864684632777101508094011826087702016153249904683329312949209127762411378780302243557466062839716 59376426832674269780880061631528163475887

393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB

010092537397ECA4F6145799D62B0A19CE06FE26AD

57896044618658097711785492504343953926634992332820282019728792003956564823193

FFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1 356D6D51C245F485B576625F7FC6F44C42F9A637FD6B0BFF5CB6F406B7FDFF386BFB5A899FA5AF9F24117C4B1FF649286651FCF45B3DC2007CB8A163BF0598DA483 61C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C18 0E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1C BA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86 A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2 699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED 1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DE C9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B3 32051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A9 7A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CC B1A313D55CDA56C9FC2FF29632387FF8D76F3C0468043F8F663F4860FF12BF2D5B0B7474D6F694F91F6DBF115974A3926F12FFF5F438777CB6A932DF8CD8BFC4D07 3B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A40 37C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6 A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382 BC9190DA6FC026F479558F4475677F9AA9F3050F2765694DFC81F56F880B96F7160C980DD98FDD3DFFFFFFFFFFFFFFFFFFF

04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D

8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065

3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1

043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3

14518877557776399015115874320830702024226143809848893135505709196593151770659565743590789126541491676439926842369913057775743308316665 11589145701059710742276692757882915756220901998212975756543223550490431013061082131040808010565293748926901442915057819663730454818359 472391642885328171302299245556663073719855

POSSIBLE SECRETS
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
D6031998D1B3BBFEBF59CC9BBFF9AEE1
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
DB7C2ABF62E35E7628DFAC6561C5
4A6E0856526436F2F88DD07A341E32D04184572BEB710
e4437ed6010e88286f547fa90abfe4c42212
115792089210356248762697446949407573530086143415290314195533631308867097853951
07A526C63D3E25A256A007699F5447E32AE456B50E
03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3
24B7B137C8A14D696E6768756151756FD0DA2E5C
7d7374168ffe3471b60a857686a19475d3bfa2ff

POSSIBLE SECRETS
10E723AB14D696E6768756151756FEBF8FCB49A9
5FF6108462A2DC8210AB403925E638A19C1455D21
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA
FFFFFFF00000000FFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
8CF83642A709A097B447997640129DA299B1A47D1EB3750BA308B0FE64F5FBD3
115792089237316195423570985008687907853269984665640564039457584007913129639319
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
2866537B676752636A68F56554E12640276B649EF7526267
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E

C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1

03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a

87A8E61DB4B6663CFFBBD19C651959998CEEF608660DD0F25D2CEED4435E3B00E00DF8F1D61957D4FAF7DF4561B2AA3016C3D91134096FAA3BF4296D830E9A7C20
9E0C6497517ABD5A8A9D306BCF67ED91F9E6725B4758C022E0B1EF4275BF7B6C5BFC11D45F9088B941F54EB1E59BB8BC39A0BF12307F5C4FDB70C581B23F76B63A
CAE1CAA6B7902D52526735488A0EF13C6D9A51BFA4AB3AD8347796524D8EF6A167B5A41825D967E144E5140564251CCACB83E6B486F6B3CA3F7971506026C0B857
F689962856DED4010ABD0BE621C3A3960A54E710C375F26375D7014103A4B54330C198AF126116D2276E11715F693877FAD7EF09CADB094AE91E1A1597

fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768

000201010211021341318344332435204739953035665802

AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E 8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA9 7B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E 7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73

c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192

36DF0AAFD8B8D7597CA10520D04B

6A91174076B1F0F19C39C031FF8685C1CAF040F5C69A28FF

00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069

04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83

FFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1 82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C F98583FF8F4F1232FFF28183C3FF3B1B4C6FAD733BB5FCBC2FC22005C58FF1837D1683B2C6F34A26C1B2FFFA886B4238611FCFDCDF355B3B6519035BBC34F4DFF99 C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6 9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B 6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1 A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23 BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855 322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C 1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C 6272B045B3B71F9DC6B80D63FDD4A8F9ADB1F6962A69526D43161C1A41D570D7938DAD4A40F329CCFF46AAA36AD004CF600C8381F425A31D951AF64FDB23FCFC 9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C 35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95 F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA 6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFFF

fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f 9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9

047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44

POSSIBLE SECRETS
6b8cf07d4ca75c88957d9d67059037a4
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D
MQVwithSHA256KDFAndSharedInfo
3045AE6FC8422f64ED579528D38120EAE12196D5
000E0D4D696E6768756151750CC03A4473D03679
9760508f15230bccb292b982a2eb840bf0581cf5
103FAEC74D696E676875615175777FC5B191EF30
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
fffffff00000000ffffffffffffbce6faada7179e84f3b9cac2fc632551
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E 34116177DD2259
25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
70390085352083305199547718019018437841079516630045180471284346843705633502619

10B7B4D696E676875615175137C8A16FD0DA2211

6EE3CEEB230811759F20518A0930F1A4315A827DAC

00BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE

3045AE6FC8422F64ED579528D38120EAE12196D5

A335926AA319A27A1D00896A6773A4827ACDAC73

469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9

0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E

0307AF69989546103D79329FCC3D74880F33BBE803CB

D7C134AA264366862A18302575D1D787B09F075797DA89F57FC8C0FF

85E25BFE5C86226CDB12016F7553F9D0E693A268

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

 $13945487119911582560140965510769071310704170705992803179775800145437576535772298409412436852228823983303911468164807668823692122073732\\26721607407477717009111345504320538046476949046861201130878162407401848004770471573366629262494235712488239685422217536601433914856808\\40520336859458494803187341288580489525163$

32010857077C5431123A46B808906756F543423E8D27877578125778AC76

D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC

02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7

f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b5 47c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a

1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e4577779de

00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814

c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4

07A11B09A76B562144418FF3FF8C2570B8

0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500

040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B

> PLAYSTORE INFORMATION

Title: digiBOP- Simple | Speedy | Secure

Score: None Installs: 500,000+ Price: 0 Android Version Support: Category: Finance Play Store URL: com.digibop.mobile

Developer Details: BOP Admin, BOP+Admin, None, None, ibanking@bop.com.pk,

Release Date: None Privacy Policy: Privacy link

Description:

Experience convenient and seamless digital banking with the latest DigiBOP Mobile App. Offering unique features and improved interface, BOP customers can now attend their everyday banking needs anywhere, anytime with the redefined mobile banking app DigiBOP. Funds Transfer: *Transfer within own Accounts *Transfer Funds to BOP Accounts, *Transfer Funds to other bank accounts via RAAST/1-Link *Transfer Funds to wallets/microfinance bank accounts/wallets Bill Payments: *Utility bill payments * Credit Card & Loan Accounts payments * Online Shopping Companies bill payment * Pay Government challans and fees (FBR payments) Mobile Recharge/ Top up * Recharge/ top up your prepaid/ postpaid mobile (Jazz, Telenor, Zong, Ufone) * Purchase prepaid super-card/bundles with BOP mobile banking Account Information * View your account(s) balance(s) and other account details (Branch, IBAN) * Manage multiple accounts with ease * View your transaction history and account statement Card Management: * Activate your debit card * Lock/unlock debit card * Manage permissions on your debit/credit cards Discount & Offers: * Search & Navigate to the nearby deals and discounts offered on BOP cards (Debit/Credit) with BOP mobile banking Locate Us: * Find the nearby BOP ATMs and Branches Basic Banking features: * Login through secure touch ID * Beneficiary Management * Payee Management * Contact Us for complaint and queries * Update your mobile number/password Feedback: * Leave a message and one of our customer care representatives will get back to you Let us know your feedback regarding the BOP mobile banking app Follow us * facebook.com/thebankofpunjab * twitter.com/thebankofpunjab * Visit us: bop.com.pk Our App Privacy Policy: https://digibop.com.pk/privacypolicy.html



Timestamp	Event	Error
2024-11-14 20:22:27	Generating Hashes	ОК
2024-11-14 20:22:27	Extracting APK	ОК
2024-11-14 20:22:27	Unzipping	ОК
2024-11-14 20:22:28	Getting Hardcoded Certificates/Keystores	ОК
2024-11-14 20:22:28	Parsing APK with androguard	ОК
2024-11-14 20:22:31	Parsing AndroidManifest.xml	ОК
2024-11-14 20:22:31	Extracting Manifest Data	ОК
2024-11-14 20:22:31	Performing Static Analysis on: digiBOP (com.digibop.mobile)	ОК
2024-11-14 20:22:31	Fetching Details from Play Store: com.digibop.mobile	ОК
2024-11-14 20:22:34	Manifest Analysis Started	ОК

2024-11-14 20:22:34	Checking for Malware Permissions	ОК
2024-11-14 20:22:34	Fetching icon path	OK
2024-11-14 20:22:34	Library Binary Analysis Started	ОК
2024-11-14 20:22:34	Reading Code Signing Certificate	ОК
2024-11-14 20:22:35	Running APKiD 2.1.5	ОК
2024-11-14 20:22:40	Detecting Trackers	ОК
2024-11-14 20:22:43	Decompiling APK to Java with JADX	ОК
2024-11-14 20:23:13	Converting DEX to Smali	ОК
2024-11-14 20:23:13	Code Analysis Started on - java_source	ОК
2024-11-14 20:23:27	Android SAST Completed	ОК
2024-11-14 20:23:27	Android API Analysis Started	ОК

2024-11-14 20:23:33	Android API Analysis Completed	ОК
2024-11-14 20:23:33	Android Permission Mapping Started	OK
2024-11-14 20:23:48	Android Permission Mapping Completed	ОК
2024-11-14 20:23:52	Email and URL Extraction Completed	ОК
2024-11-14 20:23:52	Android Behaviour Analysis Started	ОК
2024-11-14 20:24:00	Android Behaviour Analysis Completed	ОК
2024-11-14 20:24:00	Extracting String data from APK	ОК
2024-11-14 20:24:00	Extracting String data from Code	ОК
2024-11-14 20:24:00	Extracting String values and entropies from Code	ОК
2024-11-14 20:24:05	Performing Malware check on extracted domains	ОК
2024-11-14 20:24:15	Saving to Database	ОК

Report Generated by - MobSF v4.1.9

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

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