MOBSF

ANDROID STATIC ANALYSIS REPORT

Askari Digital (2.1.18)

File Name:	Askari Digital.apk
Package Name:	com.askari
Scan Date:	Nov. 14, 2024, 7:52 p.m.
App Security Score:	44/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	20	2	1	4

FILE INFORMATION

File Name: Askari Digital.apk
Size: 47.67MB
MD5: aa4150980af83572a286c9ac6552b0d6
SHA1: 2102abb693cefe5a0b79e14215652568680296d0
SHA256: fe1984a9fed4eddcc4cb6ce969e322be53bccf5297730bd6edbb7f2dbefc9e05

APP INFORMATION

App Name: Askari Digital
Package Name: com.askari

Main Activity: .Activities.Login.SplashScreenActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 2.1.18
Android Version Code: 84

APP COMPONENTS

Activities: 222
Services: 12
Receivers: 5
Providers: 7
Exported Activities: 2
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=92, ST=Punjab, L=Islamabad, O=Askari Bank Ltd, OU=Wemsol Pvt Ltd, CN=Askari Bank Ltd
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-06-05 07:08:37+00:00
Valid To: 2040-05-29 07:08:37+00:00
Issuer: C=92, ST=Punjab, L=Islamabad, O=Askari Bank Ltd, OU=Wemsol Pvt Ltd, CN=Askari Bank Ltd
Serial Number: 0x7fbf11ad
Hash Algorithm: sha256
md5: de1f9ea658b7879fc16c422fef29bbcd
sha1: 8cd87bf53caed8bfce948b59694b354cb3aec2b4
sha256: 94ccd978b0b67de3e61412b59f13c3f0ffc925e31fdcc0693ef8bf1b2d8e6a00
sha512: 56a5081061203b37016046cf9a01c61a48df38fd57f6acf0fcdc6fc084fd93111140cd4f884a67a5b3db411375b876740bfc267c7215854952215064adf3a076
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: abc692936e14ba3304720ac9f533ef167c348850f577a64d088aac1631e3f54a
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
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_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.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_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.askari.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check FINDINGS: Compiler — r8
classes2.dex	FINDINGS: Anti-VM Code — Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check FINDINGS: Compiler — r8

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
possible VM 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>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	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	Service (com.avanzasolutions.apps_sdk.service.APPSFirebaseMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (com.avanzasolutions.apps_sdk.view.AppsMainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.avanzasolutions.apps_sdk.view.scan_qr.AppsScanQRActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (com.avanzasolutions.apps_sdk.ApduService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NFC_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.
6	Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	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.
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **3** | WARNING: **9** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/avanzasolutions/apps_sdk/APPSManager.java com/avanzasolutions/apps_sdk/ApduService.java com/avanzasolutions/apps_sdk/extras/HelperMethod.java com/avanzasolutions/apps_sdk/hce/RequestLogger.java com/avanzasolutions/apps_sdk/hce/enroll/presenter/AccountProvisionPresenter.java com/avanzasolutions/apps_sdk/hce/enroll/presenter/AccountVerifyPresenter.java com/avanzasolutions/apps_sdk/hce/enroll/presenter/EnrollFragmentPresenter.java com/avanzasolutions/apps_sdk/presenter/account_list/AccountListPresenterImpl.java

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	va com/avanzasolutions/apps_sdk/presenter/main/AccountsPresenterImpl.java com/avanzasolutions/apps_sdk/presenter/main/CardEnrollPresenterImpl.java com/avanzasolutions/apps_sdk/presenter/main/CardProvisionPresenterImpl.java com/avanzasolutions/apps_sdk/presenter/main/CardVerifyPresenterImpl.java com/avanzasolutions/apps_sdk/presenter/main/GenerateQRPresenterImpl.java com/avanzasolutions/apps_sdk/presenter/main/HCEPayPresenterImpl.java com/avanzasolutions/apps_sdk/presenter/main/QRScannerActivityPresenterImpl.java com/avanzasolutions/apps_sdk/presenter/payment/PaymentComfimationFragmentPresenterImpl.java com/avanzasolutions/apps_sdk/repository/AccountRepository.java com/avanzasolutions/apps_sdk/service/APPSFirebaseMessagingService.java com/avanzasolutions/apps_sdk/view/account/AccountFragment.java com/avanzasolutions/apps_sdk/view/account/AccountListFragment.java com/avanzasolutions/apps_sdk/view/adapter/AccountRVAdapter.java com/avanzasolutions/apps_sdk/view/generate_qr/GenerateQRFragment.java com/avanzasolutions/apps_sdk/view/hce_pay/HCEPayFragment.java com/avanzasolutions/apps_sdk/view/payment/PaymentReceiptFragment.java com/avanzasolutions/apps_sdk/view/styles/FontCache.java com/bumptech/glide/Glide.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/util/pool/FactoryPools.java com/j256/ormlite/android/AndroidLog.java com/j256/ormlite/android/OrmliteTransactionalProcessor.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/j256/ormlite/logger/LocalLog.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/geolocation/GeolocationModule.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativemathematics/MathematicsModule.java com/upi/hcesdk/U_.java com/upi/hcesdk/apdu/CUP_ReadRecord.java com/upi/hcesdk/mpp/Uah.java com/upi/hcesdk/mpp/Ub.java com/upi/hcesdk/mpp/Uh.java com/upi/hcesdk/mpp/Uk.java com/upi/hcesdk/mpp/Um.java io/card/payment/CardIOActivity.java io/card/payment/CardScanner.java io/card/payment/OverlayView.java io/card/payment/Util.java io/card/payment/i18n/I18nManager.java o/ApiExceptionMapper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/ForwardingMultimap.java o/LoggerLevel.java o/IterablesUnmodifiableIterable.java o/LocalCacheValueIterator.java o/Maps10.java o/PostprocessorProducerRepeatedPostprocessorConsumer1.java o/ProgressBarDrawable.java o/QueueFileLogStore.java o/TransformAnimatedNode.java o/checkNotifications.java o/createSignatureStream.java o/deleteView.java o/deprecated_onlyIfCached.java o/findEssentialMat_17.java o/generateDefaultOkHttp.java o/getContentInfos.java o/getHiPriQueue.java o/getImagePipeline.java o/getJWEKeySelector.java o/getKeyProgressIncrement.java o/getSqlArgValue.java o/getStringFlagValue.java o/i_.java o/invokeUniqueEvent.java o/isRecognizing.java o/lowerBoundType.java o/nativeBufferSpecSetDepthStencilFormat.java o/newLatLngBounds.java o/readAsDataURL.java o/replaceExistingNonRootView.java o/setAnimationType.java o/setInitialPage.java retrofit/Platform.java retrofit/android/AndroidLog.java
2	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/airbnb/android/react/maps/AirMapModule.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/reactnativecommunity/webview/RNCWebViewModule.java o/CardboardEmulatorControllerCallbacks.java o/generateDefaultOkHttp.java o/getBitmapPool.java o/getJWEKeySelector.java o/setActiveIndicatorWidth.java
3	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/j256/ormlite/android/AndroidCompiledStatement.java com/j256/ormlite/android/AndroidDatabaseConnection.java com/j256/ormlite/android/compat/ApiCompatibility.java com/j256/ormlite/android/compat/BasicApiCompatibility.java com/j256/ormlite/android/compat/JellyBeanApiCompatibility.java o/ModuleDataCleanerCleanable.java o/mapSelectStarRow.java o/nextString.java o/readAsDataURL.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/avanzasolutions/apps_sdk/presenter/main/GenerateQRPresenterImpl.java com/bangcle/CryptoTool.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/reactnativecommunity/webview/RNCWebViewModule.java io/card/payment/CardScanner.java o/DSTU7624CFB128.java o/DVCSMessage.java o/DevServerHelperBundleType.java o/ProtobufDataEncoderContext1.java o/SessionsSettingsupdateSettings1.java o/getNativeViewHierarchyManager.java o/getQrType.java o/getTotalNativeNodeContributionToParent.java o/glDetachShader.java o/isAtLeastJellyBean.java o/requestBodyStart.java org/opencv/android/StaticHelper.java org/tensorflow/lite/task/core/TaskJniUtils.java
5	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/avanzasolutions/apps_sdk/extras/HCEEnvironment.java com/bumptech/glide/manager/RequestManagerRetriever.java o/CenterCrop.java o/CertPathValidationResult.java o/TailAppendingInputStream.java o/checkName.java o/inet6AddressToAscii.java o/initDigest.java o/isNumber.java o/lambdaprepareNativeSession1.java o/replaceValues.java o/setSingleLine.java
6	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	o/allMatch.java o/findConstructor.java o/setLevels_0.java
7	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	o/decodeToString.java o/findConstructor.java o/handleSetPressed.java
8	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	o/CamelliaKeyGen.java o/RequestInterceptorTapeCommand1.java o/fisheye_solvePnP_0.java o/getCertReqId.java o/getExtendedKeyUsage.java o/onDetachFromView.java o/populateSessionDeviceData.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/avanzasolutions/apps_services/RetrofitInstance.java com/upi/hcesdk/mpp/U_.java com/upi/hcesdk/mpp/Uah.java o/solve_0.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nimbusds/jose/jwk/ECKey.java o/solve_0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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/nimbusds/jose/crypto/RSA_OAEP.java com/nimbusds/jose/jwk/ECKey.java com/nimbusds/jose/jwk/RSAKey.java o/parsePathParameters.java o/set_samplerTrackMaxNegNum_0.java
12	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/nimbusds/jose/crypto/AESCBC.java com/nimbusds/jose/jca/JCASupport.java o/DoubleMath.java o/getTypeMappings.java
13	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/ClipboardModule.java o/RequestBuilderMimeOverridingTypedOutput.java
14	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	o/allMatch.java o/decodeToString.java o/handleSetPressed.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	o/getTc.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bangcle/CryptoTool.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/j256/ormlite/android/apptools/OrmLiteSqliteOpenHelper.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/nimbusds/jose/util/IOUtils.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/upi/hcesdk/Uj.java io/card/payment/CardScanner.java o/AudioAttributesImplApi21.java o/CardboardEmulator.java o/DSTU7624CFB128.java o/LineProcessor.java o/WebSocketReaderFrameCallback.java o/X962Parameters.java o/adjustCounter.java o/checkControllerConfigurationTypeOrThrow.java o/findFundamentalMat_1.java o/flip.java o/generateDefaultOkHttp.java o/getAllowedHandwritingDelegatorPackageName.java o/getBitmapPool.java o/getJWEKeySelector.java o/getPersistenceKey.java o/modDouble.java o/setOnViewTreeOwnersAvailable.java org/opencv/android/StaticHelper.java org/tensorflow/lite/task/core/TaskJniUtils.java retrofit/mime/TypedFile.java
			com/avanzasolutions/apps_sdk/view/AppsMainActivity.java com/avanzasolutions/apps_sdk/view/payment/PaymentActivity.java com/truid/android/TruIDLaunchActivity.java io/card/payment/DataEntryActivity.java o/AddAccountRequest.java o/AirMapCalloutManager.java o/CMSSecureReadable.java o/CancellationToken.java o/CenterCrop.java o/CycleDetectingLockFactoryPolicy.java o/DispatcherPerThreadQueuedDispatcherEvent.java o/EncodedPath.java o/FirebaseAnalyticsEvent.java o/GenericHybridParameters.java o/HashBiMapView1.java o/HceLogPayload.java o/LocalCacheValueReference.java o/MediaStoreFileLoader.java o/MultisetsFilteredMultiset.java o/NameConstraintValidatorException.java o/ProtobufDataEncoderContext1.java o/ReactCookieJarContainer.java o/SignatureSpi.java o/TailAppendingInputStream.java o/TaskApiCallBuilder.java o/TlsNullCipher.java o/VrVREventVrCoreLockScreenEvent.java o/XMSSPublicKeyParameters1.java o/addShiftedByBitsSafe.java o/appendUriIntoKey.java

RULE ID	BEHAVIOUR	LABEL	FILES
			o/createDefault.java o/decodeStringValue.java o/endBatchMode.java
00091	Retrieve data from broadcast	collection	o/enforceCallingUriPermission.java o/engineGetDigestLength.java o/engineLoad.java o/from.java o/generatedIdSequence.java o/getCollapseIcon.java o/getInBitmapCacheSince.java o/getItem.java o/getMessageTime.java o/getNativeViewHierarchyManager.java o/getPermittedSubtrees.java o/getQrType.java o/getTotalNativeNodeContributionToParent.java o/get_0.java o/glDetachShader.java o/isEncodedMemoryCacheProbingEnabled.java o/isSessionRestart.java o/jniCallJSCallback.java o/lambdasetStereoModeEnabled0GvrLayoutImpl.java o/maxStaleSeconds.java o/nGet.java o/nativeGetNeckModelFactor.java o/newCodecokhttp.java o/onEventDispatch.java o/queryCache.java o/reduceInPlace.java o/replaceValues.java o/requestBodyStart.java o/retainAllImpl.java o/sdkVersion.java o/setCookieJar.java o/setCustomerAccounts.java o/setExperimentalThreadHandoffQueueEnabled.java o/setExpiresInSecs.java o/setIndeterminateTintList.java o/setResourceRemovedListener.java o/setSmallByteArrayPoolStatsTracker.java o/shouldPostprocess.java o/showResendOTPButton.java o/startMessagingService.java o/subscribeToAnalyticsEvents.java o/updateFade.java o/updateViewAccessibility.java
00079	Hide the current app's icon	evasion	o/S.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/avanzasolutions/apps_sdk/presenter/main/GenerateQRPresenterImpl.java com/avanzasolutions/apps_sdk/view/payment/PaymentReceiptFragment.java com/karumi/dexter/listener/multi/SnackbarOnAnyDeniedMultiplePermissionsListener.java com/karumi/dexter/listener/single/SnackbarOnDeniedPermissionListener.java o/DVCSMessage.java o/SyncTask.java o/createAssetTypeface.java o/findConstructor.java o/initDigest.java o/onProvideContentCaptureStructure.java o/scheduledefault.java o/setAnimationProgress.java o/setBankName.java o/setReadVersion.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/avanzasolutions/apps_sdk/presenter/main/GenerateQRPresenterImpl.java com/dylanvann/fastimage/FastImageSource.java com/karumi/dexter/listener/multi/SnackbarOnAnyDeniedMultiplePermissionsListener.java com/karumi/dexter/listener/single/SnackbarOnDeniedPermissionListener.java o/CutAboveValue.java o/DVCSMessage.java o/detectMultiScale_4.java o/glDeleteFramebuffers.java o/initDigest.java o/maybeUpdateTypeface.java o/onProvideContentCaptureStructure.java o/setAnimationProgress.java o/setBankName.java
00199	Stop recording and release recording resources	record	com/lwansbrough/RCTCamera/RCTCameraModule.java o/DestructorThreadTerminus.java o/postOrderTraversal.java
00198	Initialize the recorder and start recording	record	com/lwansbrough/RCTCamera/RCTCameraModule.java o/DestructorThreadTerminus.java o/postOrderTraversal.java
00194	Set the audio source (MIC) and recorded file format	record	o/DestructorThreadTerminus.java o/postOrderTraversal.java
00197	Set the audio encoder and initialize the recorder	record	o/DestructorThreadTerminus.java o/postOrderTraversal.java
00196	Set the recorded file format and output path	record file	o/DestructorThreadTerminus.java o/postOrderTraversal.java
00041	Save recorded audio/video to file	record	com/lwansbrough/RCTCamera/RCTCameraModule.java o/DestructorThreadTerminus.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java o/PKCS8Generator.java
00043	Calculate WiFi signal strength	collection wifi	o/PKCS8Generator.java
00130	Get the current WIFI information	wifi collection	com/avanzasolutions/apps_sdk/extras/HelperMethod.java com/learnium/RNDeviceInfo/RNDeviceModule.java o/PKCS8Generator.java o/initDigest.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java o/PKCS8Generator.java
00112	Get the date of the calendar event	collection calendar	o/JceKeyTransAuthenticatedRecipient.java o/cancelNoCallbacks.java o/createAnimation.java o/getNativeViewHierarchyManager.java o/getNoOpListener.java o/setBottomSheetCancelable.java o/startCap.java

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	com/lwansbrough/RCTCamera/RCTCameraModule.java io/card/payment/CardScanner.java o/dispatchCreateViewTranslationRequest.java o/getAfterBoundaryOptions.java o/isAnyPolicyInhibited.java o/javaDigit.java o/littleEndianToInt.java o/postOrderTraversal.java
00012	Read data and put it into a buffer stream	file	com/bangcle/CryptoTool.java io/card/payment/CardScanner.java o/DSTU7624CFB128.java o/LineProcessor.java o/generateDefaultOkHttp.java org/opencv/android/StaticHelper.java org/tensorflow/lite/task/core/TaskJniUtils.java
00094	Connect to a URL and read data from it	command network	com/bangcle/CryptoTool.java io/card/payment/CardScanner.java o/SessionsSettingsupdateSettings1.java o/X962Parameters.java org/opencv/android/StaticHelper.java org/tensorflow/lite/task/core/TaskJniUtils.java
00202	Make a phone call	control	o/onProvideContentCaptureStructure.java o/setAnimationProgress.java
00203	Put a phone number into an intent	control	o/onProvideContentCaptureStructure.java o/setAnimationProgress.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	o/createAssetTypeface.java o/initDigest.java o/onProvideContentCaptureStructure.java o/setAnimationProgress.java o/setBankName.java o/setReadVersion.java
00096	Connect to a URL and set request method	command network	o/SessionsSettingsupdateSettings1.java o/getDirectApkLdPaths.java o/getTitleLocalizationKey.java o/setInitialPage.java retrofit/client/UrlConnectionClient.java
00087	Check the current network type	network	o/setInitialPage.java o/setPointerLeave.java
00103	Check the active network type	network	o/setInitialPage.java o/setReadVersion.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/nimbusds/jose/util/DefaultResourceRetriever.java o/SessionsSettingsupdateSettings1.java o/X962Parameters.java o/getTitleLocalizationKey.java o/setInitialPage.java retrofit/client/UrlConnectionClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/nimbusds/jose/util/DefaultResourceRetriever.java o/SessionsSettingsupdateSettings1.java o/getTitleLocalizationKey.java o/setInitialPage.java retrofit/client/UrlConnectionClient.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncStorageModule.java o/CountingMemoryCacheEntry.java o/handleResponse.java o/setSingleLine.java
00022	Open a file from given absolute path of the file	file	com/avanzasolutions/apps_sdk/presenter/main/GenerateQRPresenterImpl.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/oblador/vectoricons/VectorIconsModule.java com/truid/android/TruID.java com/truid/android/vision/FingerprintDetectionHandler.java o/BasicOCSPRespBuilderResponseObject.java o/CardboardEmulator.java o/CardboardEmulatorControllerCallbacks.java o/DevServerHelperBundleType.java o/LineProcessor.java o/ProtobufDataEncoderContext1.java o/SecT163R2Point.java o/adjustCounter.java o/findConstructor.java o/generateDefaultOkHttp.java o/getBitmapPool.java o/getNativeViewHierarchyManager.java o/getQrType.java o/getTotalNativeNodeContributionToParent.java o/getTrustBlock.java o/glDetachShader.java o/requestBodyStart.java o/shouldPostpone.java retrofit/mime/TypedFile.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java o/SessionsSettingsupdateSettings1.java o/X962Parameters.java o/getDirectApkLdPaths.java
00108	Read the input stream from given URL	network command	o/SessionsSettingsupdateSettings1.java o/X962Parameters.java
00137	Get last known location of the device	location collection	com/avanzasolutions/apps_sdk/extras/HelperMethod.java com/reactnativecommunity/geolocation/GeolocationModule.java o/setContentTransitionManager.java
00115	Get last known location of the device	collection location	com/avanzasolutions/apps_sdk/extras/HelperMethod.java com/avanzasolutions/apps_sdk/view/account/AccountFragment.java com/reactnativecommunity/geolocation/GeolocationModule.java o/appendUriIntoKey.java
00054	Install other APKs from file	reflection	o/getNativeViewHierarchyManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00121	Create a directory	file command	o/ProtobufDataEncoderContext1.java o/getNativeViewHierarchyManager.java o/getQrType.java o/getTotalNativeNodeContributionToParent.java o/glDetachShader.java o/requestBodyStart.java
00092	Send broadcast	command	o/ProtobufDataEncoderContext1.java o/getNativeViewHierarchyManager.java o/getQrType.java o/getTotalNativeNodeContributionToParent.java o/glDetachShader.java o/requestBodyStart.java
00125	Check if the given file path exist	file	o/ProtobufDataEncoderContext1.java o/getNativeViewHierarchyManager.java o/getQrType.java o/getTotalNativeNodeContributionToParent.java o/glDetachShader.java o/requestBodyStart.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	o/hasCompatibleSdkService.java
00195	Set the output path of the recorded file	record file	com/lwansbrough/RCTCamera/RCTCameraModule.java
00007	Use absolute path of directory for the output media file path	file	com/lwansbrough/RCTCamera/RCTCameraModule.java
00162	Create InetSocketAddress object and connecting to it	socket	o/obtainExtrasFromImage.java
00163	Create new Socket and connecting to it	socket	o/obtainExtrasFromImage.java
00098	Check if the network is connected	network	o/setPointerLeave.java
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	o/CountingMemoryCacheEntry.java o/setSingleLine.java
00187	Query a URI and check the result	collection sms calllog calendar	o/CountingMemoryCacheEntry.java o/getIssuingDistributionPoint.java o/setSingleLine.java
00147	Get the time of current location	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java o/appendUriIntoKey.java o/getDrawerViewAbsoluteGravity.java o/toJWSObject.java
00075	Get location of the device	collection location	com/avanzasolutions/apps_sdk/view/account/AccountFragment.java com/reactnativecommunity/geolocation/GeolocationModule.java o/C0210f.java o/appendUriIntoKey.java
00177	Check if permission is granted and request it	permission	o/shouldLayout.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	o/BasicOCSPRespBuilderResponseObject.java o/CustomNamedCurves5.java

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	o/ProtobufDataEncoderContext1.java
00005	Get absolute path of file and put it to JSON object	file	o/ProtobufDataEncoderContext1.java
00004	Get filename and put it to JSON object	file collection	com/reactnativecommunity/asyncstorage/AsyncStorageModule.java o/ProtobufDataEncoderContext1.java o/RemovalCause2.java
00014	Read file into a stream and put it into a JSON object	file	com/reactnativecommunity/asyncstorage/AsyncStorageModule.java
00185	Start capturing camera preview frames to the screen	camera	o/dispatchCreateViewTranslationRequest.java o/postOrderTraversal.java
00184	Set camera preview texture	camera	o/postOrderTraversal.java
00002	Open the camera and take picture	camera	o/postOrderTraversal.java
00182	Open camera.	camera	o/dispatchCreateViewTranslationRequest.java o/postOrderTraversal.java
00186	Control camera to take picture	camera	o/postOrderTraversal.java
00100	Check the network capabilities	collection network	o/initDigest.java
00076	Get the current WiFi information and put it into JSON	collection wifi	o/initDigest.java
00124	Check the current active network type	network	o/initDigest.java
00072	Write HTTP input stream into a file	command network file	o/SessionsSettingsupdateSettings1.java
00024	Write file after Base64 decoding	reflection file	com/upi/hcesdk/mpp/Um.java
00153	Send binary data over HTTP	http	o/getTitleLocalizationKey.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00189	Get the content of a SMS message	sms	o/getIssuingDistributionPoint.java
00188	Get the address of a SMS message	sms	o/getIssuingDistributionPoint.java
00200	Query data from the contact list	collection contact	o/getIssuingDistributionPoint.java
00201	Query data from the call log	collection calllog	o/getIssuingDistributionPoint.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java o/getIssuingDistributionPoint.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	o/glDeleteFramebuffers.java
00016	Get location info of the device and put it to JSON object	location collection	o/BrokenJCEBlockCipherBrokePBEWithSHA1AndDES.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/400040001917/namespaces/firebase:fetch?key=AIzaSyAC-A6fShUrLuyqSvPsToaQ5fkEJXPeAR0 is enabled. Ensure that the configurations are not sensitive. \\nMIIHITCCBgmgAwIBAgIQC8Czut09xdJtnUzi633y5zANBgkqhkiG9w0BAQsFADBZ\\nMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMTMwMQYDVQQDEypE\\naWdpQ2VydCBHbG9iYWwgRzIgVExTIFJTQSBTSEEyNTYgMjAyMCB----END CERTIFICATE-----', 'PLive': '-----BEGIN CERTIFICATE----- \\nMIIHITCCBgmgAwIBAgIQC8Czut09xdJtnUzi633y5zANBgkqhkiG9w0BAQsFADBZ\\nMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMTMwMQYDVQQDEypE\\naWdpQ2VydCBHbG9iYWwgRzIgVExTIFJTQSBTSEEyNTYgMjAyMCB----END CERTIFICATE-----', 'UAT': '-----BEGIN CERTIFICATE----- \\nMIIHITCCBgmgAwIBAgIQC8Czut09xdJtnUzi633y5zANBgkqhkiG9w0BAQsFADBZ\\nMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMTMwMQYDVQQDEypE\\naWdpQ2VydCBHbG9iYWwgRzIgVExTIFJTQSBTSEEyNTYgMjAyMCB----END CERTIFICATE-----'}, 'state': 'UPDATE', 'templateVersion': '23'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.SYSTEM_ALERT_WINDOW, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	2/44	com.google.android.c2dm.permission.RECEIVE, 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
umps.unionpayintl.com	IP: 43.159.74.239 Country: China Region: Beijing City: Beijing

DOMAIN	COUNTRY/REGION
umpstest.unionpayintl.com	IP: 43.159.74.225 Country: China Region: Beijing City: Beijing

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
mbapp.apps.net.pk	ok	**IP:** 125.209.101.219 **Country:** Pakistan **Region:** Sindh **City:** Karachi **Latitude:** 24.905600 **Longitude:** 67.082199 **View:** Google Map
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
release-api.truid.ai	ok	**IP:** 34.195.108.8 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
purl.org	ok	**IP:** 207.241.225.157 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
umps.unionpayintl.com	ok	**IP:** 43.159.74.239 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 172.217.169.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
secure.askaribank.com	ok	**IP:** 104.18.23.41 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
hblbbapp.com	ok	**IP:** 45.60.76.176 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
docs.swmansion.com	ok	**IP:** 172.67.142.188 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
35.238.46.115	ok	**IP:** 35.238.46.115 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
unionpayterms.apps.net.pk	ok	**IP:** 172.67.73.92 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 172.217.169.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
umpstest.unionpayintl.com	ok	**IP:** 43.159.74.225 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.140.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
172.16.9.123	ok	**IP:** 172.16.9.123 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
askaribank.com	ok	**IP:** 104.18.23.41 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
mbappprod.apps.net.pk	ok	**IP:** 125.209.101.222 **Country:** Pakistan **Region:** Sindh **City:** Karachi **Latitude:** 24.905600 **Longitude:** 67.082199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hysabkytabtest.askaribank.com	ok	**IP:** 103.214.40.102 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
ns.useplus.org	ok	**IP:** 54.83.4.77 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
iptc.org	ok	**IP:** 3.64.29.21 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
advance-loan.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
api.whatsapp.com	ok	**IP:** 157.240.9.53 **Country:** Bulgaria **Region:** Sofia (stolitsa) **City:** Sofia **Latitude:** 42.697510 **Longitude:** 23.324150 **View:** Google Map
askaribank.threatcast.guardsquare.com	ok	**IP:** 35.201.110.144 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.npes.org	ok	**IP:** 104.21.43.185 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.hblibank.com.pk	ok	**IP:** 45.60.183.102 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
secure.askaribank.com.pk	ok	**IP:** 104.18.3.57 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
cipa.jp	ok	**IP:** 118.82.81.189 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
google.com	ok	**IP:** 142.250.187.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
xerces.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
webview.golootlo.pk	ok	**IP:** 65.9.66.55 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
www.aiim.org	ok	**IP:** 199.60.103.225 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
support@askaribank.com	o/setAnimationProgress.java
support@askaribank.com	o/onProvideContentCaptureStructure.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"fcmToken" : ""

POSSIBLE SECRETS
"google_api_key" : "AIzaSyAC-A6fShUrLuyqSvPsToaQ5fkEJXPeAR0"
"google_crash_reporting_api_key" : "AIzaSyAC-A6fShUrLuyqSvPsToaQ5fkEJXPeAR0"
"google_maps_key" : "AIzaSyC97dwYnxusXZuXbeA3xXEy8dZrNccwIAs"
"password" : "Password"
"username" : "Username"
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
2809101935305809009699697900030956075912436855801486595765584287239730126759 5
1009979067550553047720818155359252248698410825720534578748235158755771479905292727772441528526992987964833566996828420279728960527471731754805904856071347468521419286809125615028022221856475391909026561163678472701450190667942909301854462163997308722217328898303231940973554032134009725883228768509467406639 62
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
3826F008A8C51D7B95284D9D03FF0E00CE2CD723A
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34
MQVwithSHA512KDFAndSharedInfo
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
127971af8721782ecffa3
020A601907B8C953CA1481EB10512F78744A3205FD
917715298965546059455881490183827502172968583935207241727433257254743749798 01
c49d360886e704936a6678e1139d26b7819f7e90
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883

POSSIBLE SECRETS
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
DB7C2ABF62E35E668076BEAD208B
7988514166341097689762711893575632374730795191650763975830047269233887353395 9
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF
7513f48395fca348b20cc898dfb3c53ae563da38aaf9393345c449f5df1a4636
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
e8b4011604095303ca3b8099982be09fcb9ae616
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
a82bc7f7-c4b5-4ece-8904-d9f4af847a82
9162fbe73984472a0a9d0590
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
6BA06FE51464B2BD26DC57F48819BA9954667022C7D03
BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985
00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
E95E4A5F737059DC60DF5991D45029409E60FC09

POSSIBLE SECRETS
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
1E589A8595423412134FAA2DBDEC95C8D8675E58
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129
D2C0FB15760860DEF1EEF4D696E6768756151754
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
703900853520833051995477180190184378409208826471640810353226014583522983966 01
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72
42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437669456364882730370838934791080835932647976778601915343474400961034231316672578686920 48219493287863336020338479709268434224762105576023501613261478065276102850944540333865234 1
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
31a92ee2029fd10d901b113e990710f0d21ac6b6
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148
1420117415975634811963682860223180897432761383952437387628725734419274593935127189736311660784676003608489466235676257952827747192122419290710461342083806363940845126918288940005715246254452957693493567527289568315417 7 5441763139384457191755096847107846595662547942312293338483924514339614727760681880609734239
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
b8adf1378a6eb73409fa6c9c637ba7f5

POSSIBLE SECRETS
0217C05610884B63B9C6C7291678F9D341
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB
5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE
00E8BEE4D3E2260744188BE0E9C723
287926658148546112969923474583802841350286367782291130057563347309963038881 24
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
74D59FF07F6B413D0EA14B344B20A2DB049B50C3
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA
036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a
B0075E2301321961B3CDEA1F7F3D2626
57896044618658097711785492504343953927102133160255826820068844496087732066703
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE428782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562CE1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83
51DEF1815DB5ED74FCC34C85D709
046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C

POSSIBLE SECRETS
B99B99B099B323E02709A4D696E6768756151751
1053CDE42C14D696E67687561517533BF3F83345
MQVwithSHA384KDFAndSharedInfo
B10B8F96A080E01DDE92DE5EAE5D54EC52C99FBCFB06A3C69A6A9DCA52D23B616073E28675A23D189838EF1E2EE652C013ECB4AEA906112324975C3CD49B83BFACCBDD7D90C4BD7098488E9C219A73724EFFD6FAE5644738FAA31A4FF55BCCC0A151AF5F0DC8B4BD45BF37DF365C1A65E68CFDA76D4DA708DF1FB2BC2E4A4371
5F49EB26781C0EC6B8909156D98ED435E45FD59918
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF
072546B5435234A422E0789675F432C89435DE5242
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
4E13CA542744D696E67687561517552F279A8C84
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297
b3fb3400dec5c4adceb8655d4c94
DB7C2ABF62E35E668076BEAD2088
0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C
AC4032EF4F2D9AE39DF30B5C8FFDAC506CDEBE7B89998CAF74866A08CFE4FFE3A6824A4E10B9A6F0DD921F01A70C4AFAAB739D7700C29F52C57DB17C620A8652BE5E9001A8D66AD7C17669101999024AF4D027275AC1348BB8A762D0521BC98AE247150422EA1ED409939D54DA7460CDB5F6C6B250717CBEF180EB34118E98D119529A45D6F834566E3025E316A330EFBB77A86F0C1AB15B051AE3D428C8F8ACB70A8137150B8EEB10E183EDD19963DDD9E263E4770589EF6AA21E7F5F2FF381B539CCE3409D13CD566AFBB48D6C019181E1BCFE94B30269EDFE72FE9B6AA4BD7B5A0F1C71CFFF4C19C418E1F6EC017981BC087F2A7065B384B890D3191F2BFA
1157920892373161954235709850086879078532698466564056403945758400791312963931 6
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

POSSIBLE SECRETS
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1
34BC51A6046A624881701EFD17115CBA
DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24 117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4 C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0 864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF 92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF 8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A8 4031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F66 3F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
640338811429272026836498814504334739859317602688849412888527458039088786386 12
298188939177312407334712732403147699272405508123836956891464952616045659902 47
96341f1138933bc2f503fd44
2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976123057 5
11fd54f3e6ac57d90d6420e2bee56c3f26565e5de00a3644a065e874276e8da2
5EEEFCA380D02919DC2C6558BB6D8A5D
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23 AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335E08C47 20E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B91 4D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
8834235323891921647916487503603088853144765972529603627924508606096998 39

POSSIBLE SECRETS
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63
26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
FFFFFFFE0000000075A30D1B9038A115
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
127021248288932417465907042777176443525787653508916535812817507265705031260985098497423188333483401180925999995120988934130659205614996724254121049274349357074920312769561451689224110579311248812610229678534638401693520013288995000362260684222750813532307004517341633685004541062586971416883686778842537820383
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3
10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C
985BD3ADBAD4D696E676875615175A21B43A97E3
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3
1243ae1b4d71613bc9f780a03690e

POSSIBLE SECRETS
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3
AD107E1E9123A9D0D660FAA79559C51FA20D64E5683B9FD1B54B1597B61D0A75E6FA141DF95A56DBAF9A3C407BA1DF15EB3D688A309C180E1DE6B85A1274A0A66D3F8152AD6AC2129037C9EDEFDA4DF8D91E8FEF55B7394B7AD5B7D0B6C12207C9F98D11ED34DBF6C6BA0B2C8BBC27BE6A00E0A0B9C49708B3BF8A31709188368128613OBC8985DB1602E714415D9330278273C7DE31EFDC7310F7121FD5A07415987D9ADC0A486DCDF93ACC44328387315D75E198C641A480CD86A1B9E587E8BE60E69CC928B2B9C52172E413042E9B23F10B0E16E79763C9B53DCF4BA80A29E3FB73C16B8E75B97EF363E2FFA31F71CF9DE5384E71B81C0AC4DFFE0C10E64F
A4D1CBD5C3FD34126765A442EFB99905F8104DD258AC507FD6406CFF14266D31266FEA1E5C41564B777E690F5504F213160217B4B01B886A5E91547F9E2749F4D7FBD7D3B9A92EE1909D0D2263F80A76A6A24C087A091F531DBF0A0169B6A28AD662A4D18E73AFA32D779D5918D08BC8858F4DCEF97C2A24855E6EEB22B3B2E5
DF1A98AE24EDBFECD45A7409084A07831F7B420FE4826E8F5BFA89C49C12CA68F0A0B6715C633AC78033FD61D739987ABC6D29AF4C0D80F8C90BB48E74778CB6DEFB5D846D443473452DC56ACA462BDA76422C04036F62D83F27A5CEA0D4AD5659E9C6FDA1439161F7DFEA39127685519907742E33958E03C00AB61EA8846BEB
0095E9A9EC9B297BD4BF36E059184F
023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd
659EF8BA043916EEDE8911702B22
E95E4A5F737059DC60DFC7AD95B3D8139515620C
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
4D41A619BCC6EADF0448FA22FAD567A9181D37389CA
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
03F7061798EB99E238FD6F1BF95B48FEEB4854252B
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB
517cc1b727220a94fe13abe8fa9a6ee0
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6

POSSIBLE SECRETS
7fffffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063
c469684435deb378c4b65ca9591e2a5763059a2e
1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D
10C0FB15760860DEF1EEF4D696E676875615175D
003088250CA6E7C7FE649CE85820F7
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4
0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085
00689918DBEC7E5A0DD6DFC0AA55C7
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F
7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
801C0D34C58D93FE997177101F80535A4738CEBCBF389A99B36371EB
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
2AA058F73A0E33AB486B0F610410C53A7F132310
03E5A88919D7CAFCBF415F07C2176573B2
00F50B028E4D696E6768756151752904727 83FB1
20a013ea157e87d2ea307d6e7313baf6620cb067db79d145

POSSIBLE SECRETS
4D696E676875615175985BD3ADBADA21B43A97E2
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
3086d221a7d46bcde86c90e49284eb153dab
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
e43bb460f0b80cc0c0b075798e948060f8321b7d
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
6b8cf07d4ca75c88957d9d670591
6C010747560991222210569 11C77D77E77A777E7E7E77FCB
6836319614495570078444416561182725289510217088876144205509505128755031408 3023
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315
9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35
470fa2b4ae81cd56ecbcda9735803434cec591fa
57896044618658097711785492504343953926634992332820282019728792003956564823190
0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
D09E8800291CB85396CC6717393284AAA0DA64BA
114ca50f7a8e2f3f657c1108d9d44cfd8
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5 BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
0c14416e6f6e796d6f75732053656e64657220202020
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5

POSSIBLE SECRETS
A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92
1157920892373161954235709850086879078530737629084992432253781558050790688503 23
401028774D7777C7B7666D1366EA432071274F89FF01E718
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
E87579C11079F43DD824993C2CEE5ED3
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9
4099B5A457F9D69F79213D094C4BCD4D4262210B
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96

POSSIBLE SECRETS
C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
C49D360886E704936A6678E1139D26B7819F7E90
7A1F6653786A68192803910A3D30B2A2018B21CD54
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136
115792089210356248762697446949407573530086143415290314195533631308867097853948
002757A1114D696E6768756151755316C05E0BD4
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
6127C24C05F38A0AAAF65C0EF02C
04B8266A46C55657AC734CE38F018F2192
12511cfe811d0f4e6bc688b4d
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD 71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689 DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C 6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54B FF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AE D6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFF
0108B39E77C4B108BED981ED0E890E117C511CF072

POSSIBLE SECRETS
90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614
1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
004D696E67687561517512D8F03431FCE63B88F4
21c8b5470a64adbb25bc84316cbc449361d86839
627710173538668076383578942320766641608390870039032496127 9
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
db92371d2126e9700324977504e8c90e
3086d221a7d46bcde86c90e49284eb15
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B
703900853520833051995477180190184378410795166300451804712843468437056335026 16
91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
54af400d79f7a137df47854f78c1b9bb89745526ec94396dc1845cbf6976cbb6
F518AA8781A8DF278ABA4E7D64B7CB9D49462353
E95E4A5F737059DC60DFC7AD95B3D8139515620F
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618

POSSIBLE SECRETS
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
6db14acc9e21c820ff28b1d5ef5de2b0
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
B4E134D3FB59EB8BAB57274904664D5AF50388BA
EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F
0340340340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91
4105836372515214212932612978004726840911444101599372555483525631403946740129 1
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
71169be7330b3038edb025f1
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD
040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F
BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677
71169be7330b3038edb025f1d0f9
1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
22123dc2395a05caa7423daeccc94760a7d462256bd56916
3FB32C9B73134D0B2E77506660EDBD484CA7B18F21EF205407F4793A1A0BA12510DBC15077BE463FFF4FED4AAC0BB555BE3A6C1B0C6B47B1BC3773BF7E8C6F62901228F8C28CBB18A55AE31341000A650196F931C77A57F2DDF463E5E9EC144B777DE62AAAB8A8628AC376D282D6ED3864E67982428EBC831D14348F6F2F9193B5045AF2767164E1DFC967C1FB3F2E55A4BD1BFFE83B9C80D052B985D182EA0ADB2A3B7313D3FE14C8484B1E052588B9B7D2BBD2DF016199ECD06E1557CD0915B3353BBB64E0EC377FD028370DF92B52C7891428CDC67EB6184B523D1DB246C32F63078490F00EF8D647D148D47954515E2327CFEF98C582664B4C0F6CC41659
B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1
1335318132727206734338595199483190012179423759678474868994823595993696425287347124615904033277318214103280125292538719147885989931033105677441361963648030647213778266568986864684632777101508094011826087702016153249904683329312949209127762411378780302243557466062839716593764268326742697808800616315281634758 87
393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB
010092537397ECA4F6145799D62B0A19CE06FE26AD
57896044618658097711785492504343953926634992332820282019728792003956564823193

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24 117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4 C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0 864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF 92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF 8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A8 4031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F66 3F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A403 7C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA26 8359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFF
04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065
3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3
1451887755777639901511587432083070202422614380984889313550570919659315177065956574359078912654149167643992684236991305777574330831666511589145701059710742276692757882915756220901998212975756543223550490431013061082131040808010565293748926901442915057816663730454818359472391642885328171302299245556663073719855
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
D6031998D1B3BBFEBF59CC9BBFF9AEE1
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
DB7C2ABF62E35E7628DFAC6561C5
4A6E0856526436F2F88DD07A341E32D04184572BEB710
e4437ed6010e88286f547fa90abfe4c42212
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
115792089210356248762697446949407573530086143415290314195533631308867097853951

POSSIBLE SECRETS
07A526C63D3E25A256A007699F5447E32AE456B50E
03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3
24B7B137C8A14D696E6768756151756FD0DA2E5C
7d7374168ffe3471b60a857686a19475d3bfa2ff
e44046539bb5b584279553ca6eacca937c8e16cf
5FF6108462A2DC8210AB403925E638A19C1455D21
10E723AB14D696E6768756151756FEBF8FCB49A9
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24 117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
8CF83642A709A097B447997640129DA299B1A47D1EB3750BA308B0FE64F5FBD3
48439561293906451759052585252797914202762949526041747995844080717082404635286
1157920892373161954235709850086879078532699846656405640394575840079131296393 19
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFF
2866537B676752636A68F56554E12640276B649EF7526267
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F
6e2c7e24b7c7eae9fc94882c9f31befa00594872
00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
36134250956749795798585127919587881956611106672985015071877198253568414405109
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784

POSSIBLE SECRETS
87A8E61DB4B6663CFFBBD19C651959998CEEF608660DD0F25D2CEED4435E3B00E00DF8F1D61957D4FAF7DF4561B2AA3016C3D91134096FAA3BF4296D830E9A7C209E0C6497517ABD5A8A9D306BCF67ED91F9E6725B4758C022E0B1EF4275BF7B6C5BFC11D45F9088B941F54EB1E59BB8BC39A0BF12307F5C4FDB70C581B23F76B63ACAE1CAA6B7902D52526735488A0EF13C6D9A51BFA4AB3AD8347796524D8EF6A167B5A41825D967E144E5140564251CCACB83E6B486F6B3CA3F7971506026C0B857F689962856DED4010ABD0BE621C3A3960A54E710C375F26375D7014103A4B54330C198AF126116D2276E11715F693877FAD7EF09CADB094AE91E1A1597
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73
c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192
0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0
36DF0AAFD8B8D7597CA10520D04B
6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF
00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
962eddcc369cba8ebb260ee6b6a126d9346e38c5
70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9
047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44
6b8cf07d4ca75c88957d9d67059037a4

POSSIBLE SECRETS
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D
MQVwithSHA256KDFAndSharedInfo
3045AE6FC8422f64ED579528D38120EAE12196D5
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513
000E0D4D696E6768756151750CC03A4473D03679
9760508f15230bccb292b982a2eb840bf0581cf5
103FAEC74D696E676875615175777FC5B191EF30
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
8d5155894229d5e689ee01e6018a237e2cae64cd
ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259
25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
70390085352083305199547718019018437841079516630045180471284346843705633502619
10B7B4D696E676875615175137C8A16FD0DA2211
6EE3CEEB230811759F20518A0930F1A4315A827DAC
00BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
3045AE6FC8422F64ED579528D38120EAE12196D5
32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C
A335926AA319A27A1D00896A6773A4827ACDAC73
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFF
0307AF69989546103D79329FCC3D74880F33BBE803CB
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE13098533C8B3FFFFFFFFFFFFFFFF
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
85E25BFE5C86226CDB12016F7553F9D0E693A268
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
139454871199115825601409655107690713107041707059928031797758001454375765357722984094124368522288239833039114681648076688236921220737322672160740747771700911134550432053804647694904686120113087816240740184800477047157336662926249423571248823968542221753660143391485680840520336859458494803187341288580489525163
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 16
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e457779de
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4
07A11B09A76B562144418FF3FF8C2570B8
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B

PLAYSTORE INFORMATION

Title: Askari Mobile App

Score: 4.39 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.askari

Developer Details: ASKARI BANK LIMITED, ASKARI+BANK+LIMITED, None, http://www.askaribank.com.pk, digitalbanking@askaribank.com.pk,

Release Date: Dec 20, 2015 **Privacy Policy:** Privacy link

Description:

Askari bank has redesigned this App keeping in view the ease of use. The new services allow you to save your branch visits, and access your accounts anytime, anywhere. The app has enhanced security features with secure Biometric Authentication and Access Code. Now you can apply online for consumer products, go Cardless on ATM, find deals & discounts, use QR for making payments and much more. Download our new app now and 'Go Digital'! What's New!!! Enhanced Security Login to the app with your ID/Password and get an access code for more security. You can also enable convenient biometric feature that saves you from shoulder surfing. Account Details Check real time available balances of all linked accounts and view last 10 transactions through mini statement option. Payments • Utility bills (K-Electric, LESCO, FESCO, IESCO,PESCO, SSGC, SNGPL, GEPCO, HESCO, MEPCO, SEPCO, Askari Housing, PTCL, DHA, Bahria Town, Nayatel, Daewoo Bus, Nadra Esahulat) • Schools (APS, Beacon House, Bahria School, Fauji Foundation, Cosmopolitan grammar school) • University fees (LUMS) • Mobile top-ups (Telenor, Zong, Jazz, Ufone, Warid) • Government taxes (FBR, SECP, GoP, Sindh Revenue Board) • Insurance payments (Jubliee Life Insurance, EFU) • E-Commerce transactions (KuickPay merchants) • Investments (CDC–IPO) • Other banks' Credit Card payments (1Bill Option) • Business payments via B2B (HABALL) Funds Transfer Conveniently transfer funds up to PKR 1M to any member bank accounts and Mobile Wallets. Go Cardless Use Cardless Cash Withdrawal option to withdraw cash from any Askari Bank ATM. You can also make easy and fast QR payments by scanning QR Codes. Online Tickets Purchase bus and cinema tickets instantly through our mobile app and avoid standing in long ques. Credit Card Management Manage your credit card and make bill payments through multiple options. Debit Card Management Manage your Debit Card easily through our app. You can check status of cards in use or block your card temporarily. This feature provides extra layer of security. Daily Fund Transfer Limits Personalize your transfer limits as per your convenience within the defined range and make your funds more secure. Manage Cheques & Cheque Books Stop any cheque payment and view history of submitted cheques. You can also order your cheque book using this app. Deals & Discounts Stay updated with all the deals and discounts in your city and avail exciting offers just in few clicks. Reward Points Earn reward points by performing any of the following transactions and redeem the points to avail fee waiver on multiple banking product & services. • Utility bill payments • Mobile top-ups • Interbank funds transfer (IBFT) Apply Online for Consumer Products Apply online for Mastercard Credit Cards, Personal Finance, Ask4Car and Mortgage Finance without visiting the branch. Simply fill in the details using our new app and our team will get in touch with you for further process. ATM Locator This new feature lets you find the nearest ATMs without any hassle.

SCAN LOGS

Timestamp	Event	Error
2024-11-14 19:52:05	Generating Hashes	OK
2024-11-14 19:52:05	Extracting APK	OK
2024-11-14 19:52:05	Unzipping	OK
2024-11-14 19:52:06	Getting Hardcoded Certificates/Keystores	OK
2024-11-14 19:52:06	Parsing APK with androguard	OK
2024-11-14 19:52:09	Parsing AndroidManifest.xml	OK
2024-11-14 19:52:09	Extracting Manifest Data	OK
2024-11-14 19:52:09	Performing Static Analysis on: Askari Digital (com.askari)	OK
2024-11-14 19:52:09	Fetching Details from Play Store: com.askari	OK
2024-11-14 19:52:12	Manifest Analysis Started	OK

2024-11-14 19:52:12	Checking for Malware Permissions	OK
2024-11-14 19:52:12	Fetching icon path	OK
2024-11-14 19:52:12	Library Binary Analysis Started	OK
2024-11-14 19:52:12	Reading Code Signing Certificate	OK
2024-11-14 19:52:13	Running APKiD 2.1.5	OK
2024-11-14 19:52:20	Detecting Trackers	OK
2024-11-14 19:52:24	Decompiling APK to Java with JADX	OK
2024-11-14 19:53:28	Converting DEX to Smali	OK
2024-11-14 19:53:28	Code Analysis Started on - java_source	OK
2024-11-14 19:54:01	Android SAST Completed	OK
2024-11-14 19:54:01	Android API Analysis Started	OK
2024-11-14 19:54:25	Android API Analysis Completed	OK
2024-11-14 19:54:25	Android Permission Mapping Started	OK
2024-11-14 19:54:56	Android Permission Mapping Completed	OK
2024-11-14 19:55:13	Email and URL Extraction Completed	OK
2024-11-14 19:55:13	Android Behaviour Analysis Started	OK
2024-11-14 20:03:47	Android Behaviour Analysis Completed	OK

2024-11-14 20:03:47	Extracting String data from APK	OK
2024-11-14 20:03:47	Extracting String data from Code	OK
2024-11-14 20:03:47	Extracting String values and entropies from Code	OK
2024-11-14 20:03:56	Performing Malware check on extracted domains	OK
2024-11-14 20:04:18	Saving to Database	OK
