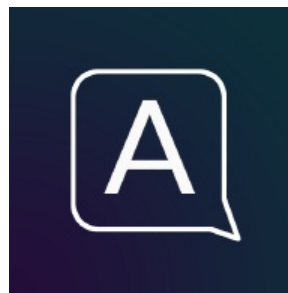




## ANDROID STATIC ANALYSIS REPORT



 Audyn AI Mental Health (1.5.2)

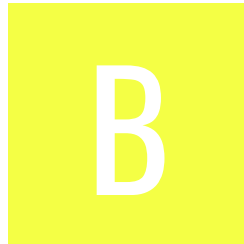
File Name: Audyn AI Mental Health\_1.5.2\_Apkpure.apk

Package Name: com.cognital.audyn

Scan Date: Nov. 28, 2023, 6:49 p.m.






App Security Score: 43/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/428

## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
6	18	3	2	3

## FILE INFORMATION

**File Name:** Audyn AI Mental Health\_1.5.2\_Apkpure.apk

**Size:** 92.39MB

**MD5:** 685aadffa570fb6b33b42e7e2c563f99

**SHA1:** f2185a9b935ed4446717f4f78026edd335111f73

**SHA256:** eb82678f2780746176f25911b9265494665f412645d8cfcbecaf6050e6b48d72

## APP INFORMATION

**App Name:** Audyn AI Mental Health

**Package Name:** com.cognital.audyn

**Main Activity:** com.cognital.audyn.MainActivity

**Target SDK:** 33

**Min SDK:** 23

**Max SDK:**

**Android Version Name:** 1.5.2

Android Version Code: 59

## APP COMPONENTS

Activities: 35

Services: 8

Receivers: 16

Providers: 5

Exported Activities: 5

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

Signature Algorithm: rsassa\_pkcs1v15

Valid From: 2022-12-27 08:26:13+00:00

Valid To: 2052-12-27 08:26:13+00:00

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

Serial Number: 0xa7286b66247488ea90f8f1db31aba8d49bb7fc5b

Hash Algorithm: sha256

md5: cc0052a9bea4d091cbec431ff5ab0739

sha1: a1ca98e22520722afeb55ff44511457cde816472

sha256: 19df581daa89e88b919d8e57c3cce69dedcea172357e435d308a53a53c450175

sha512: 7dc9bcadb9f284c2486a5ae6f9b0bcd6df5396f479c8c8fc690553556a614fd3658a66f40b5e9924f4066cfa220d48279c735bbd62a8edcf0c8889ad56cc232b

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 122c5cd7ee55a30c1c7270d4126a4f0536d16282a0140da36794a65b8fc66c86

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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.USE_FULL_SCREEN_INTENT	normal		Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
com.cognital.audyn.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	<b>FINDINGS</b>	<b>DETAILS</b>
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.BOARD check Build.TAGS check
	Compiler	dx
classes2.dex	<b>FINDINGS</b>	<b>DETAILS</b>
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	dx

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Compiler	dx
classes4.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

## BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity	Schemes: stripe-auth://, stripe://, Hosts: link-accounts, auth-redirect, Paths: /com.cognital.audyn/success, /com.cognital.audyn/cancel, Path Prefixes: /com.cognital.audyn,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.cognital.audyn,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.cognital.audyn,



ACTIVITY	INTENT
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

## NETWORK SECURITY

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

## CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

## MANIFEST ANALYSIS

HIGH: 5 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=23]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity) is not Protected. [android:exported=true]	high	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.stripe.android.payments.StripeBrowserProxyReturnActivity) is not Protected. [android:exported=true]	high	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	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

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

NO	ISSUE	SEVERITY	DESCRIPTION
12	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: 1 | WARNING: 8 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/y.java a5/a.java a8/d0.java a9/a.java ab/f.java ac/b.java b3/c.java b4/a.java b5/a.java b5/n.java b5/o.java b5/p.java b6/a.java bc/c.java be/tramckrijte/workmanager/BackgroundWor

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ker.java c4/ee.java c8/a.java c8/a1.java c8/c.java c8/d0.java c8/d1.java c8/e1.java c8/f1.java c8/g0.java c8/h1.java c8/i.java c8/n1.java c8/q1.java c9/b.java c9/j0.java ca/i.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.jav a com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.ja va com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastH andler.java com/amazon/device/simplesignin/SimpleSignl nService.java com/amazon/device/simplesignin/a/c/b.java com/bumptechnology/glides/b.java com/bumptechnology/glides/load/data/b.java com/bumptechnology/glides/load/data/j.java com/bumptechnology/glides/load/data/l.java com/dexterous/flutterlocalnotifications/Action BroadcastReceiver.java com/revenuecat/purchases/DeviceInfoHelp er\$getDeviceInfoFetchOnly\$2.java com/revenuecat/purchases/common/DefaultL ogHandler.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java</div> <div>com/stripe/android/IssuingCardPinService.java</div> <div>a</div> <div>com/stripe/android/core/Logger.java</div> <div>com/stripe/android/core/storage/SharedPreferencesStorage.java</div> <div>com/stripe/android/core/utils/PluginDetector.java</div> <div>com/stripe/android/financialconnections/navigation/NavigationManager.java</div> <div>com/stripe/android/stripe3ds2/transaction/Logger.java</div> <div>com/stripe/android/ui/core/elements/LpmSerializer.java</div> <div>com/stripe/android/uicore/image/ImageLruDiskCache.java</div> <div>com/stripe/android/uicore/image/UiUtilsKt.java</div> <div>a</div> <div>d5/d.java</div> <div>d5/e.java</div> <div>de/l.java</div> <div>de/x0.java</div> <div>dl/j.java</div> <div>e7/c.java</div> <div>ee/c.java</div> <div>f3/a.java</div> <div>f5/c.java</div> <div>f5/e.java</div> <div>f6/c1.java</div> <div>f6/g.java</div> <div>f6/i0.java</div> <div>f6/n0.java</div> <div>f6/s0.java</div> <div>f7/e0.java</div> <div>f7/f0.java</div> <div>f7/y.java</div> <div>f8/a.java</div> <div>fb/c.java</div> <div>fb/c0.java</div> <div>fh/i1.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	fb/i0.java fb/k0.java fb/r0.java fb/u0.java fb/y.java fb/z.java fb/z0.java fe/g.java fe/i.java g5/h.java g5/i.java g5/k.java g5/q.java g5/z.java g6/c.java g6/f.java g6/g0.java g6/m.java g8/a.java g9/h.java gb/g.java gb/o.java ge/i.java h3/d.java h4/a.java h5/i.java h5/j.java h8/f.java h8/n.java hc/a.java hc/b.java hc/c.java hc/i.java i5/e.java i5/i.java ic/e.java id/a.java id/e.java io/flutter/plugins/webviewflutter/c.java io/flutter/plugins/webviewflutter/g2.java i7/v.java



NO	ISSUE	SEVERITY	STANDARDS	FILES
				j5/a.java j6/l.java jd/h.java k2/d.java k5/c.java k5/d.java k5/f.java k5/s.java k5/t.java k6/e.java k6/f.java k8/b.java le/c0.java le/e0.java le/i.java m5/a.java m6/a.java mf/b.java ml/i.java n3/c.java n5/b0.java n5/c.java n5/d.java n5/k.java n5/m.java n5/n.java n5/r.java n5/z.java o1/j0.java o3/a.java o6/f.java o6/i.java o6/l.java of/a.java p2/f.java p7/a.java p7/d.java q3/a.java q3/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q5/n.java q7/i.java q8/k.java qe/d.java qf/c.java r2/a.java r5/a.java r5/d.java r5/j.java r6/a.java ra/a.java ra/b.java ra/c.java rf/i.java t5/e.java t5/f.java t5/o.java t5/p.java t5/r.java t5/s.java t8/c.java te/b.java tf/a.java tf/b.java tf/c.java u5/d.java u9/d.java v0/c.java v0/g.java v6/d0.java v6/k0.java v6/l0.java v6/v.java v9/b.java vb/v.java w5/h.java w7/g.java wf/a.java x2/c.java x5/d.java x5/j.java x6/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x9/g.java y3/c.java y7/b0.java y7/e.java y7/g0.java y7/j.java y7/k.java y7/l0.java y7/o.java y7/x.java y8/a.java z6/c.java
				com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsSynchronizer.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java com/stripe/android/EphemeralKey.java com/stripe/android/PaymentConfiguration.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/auth/PaymentBrowserAuthActivity.java com/stripe/android/core/injection/InjectorKt.java com/stripe/android/core/injection/NamedConstantsKt.java com/stripe/android/core/networking/AnalyticsFields.java com/stripe/android/core/networking/ApiRequest.java com/stripe/android/core/networking/NetworkConstantsKt.java com/stripe/android/financialconnections/FinancialConnectionsSheet.java com/stripe/android/financialconnections/analytics/DefaultFinancialConnectionsEventReporter.java com/stripe/android/financialconnections/di/NamedConstantsKt.java com/stripe/android/financialconnections/model/FinancialConnectionsSession.java com/stripe/android/financialconnections/model/GetFinancialConnectionsAccountsParams.java com/stripe/android/financialconnections/network/NetworkConstants.java com/stripe/android/googlepaylauncher/GooglePayLauncherContract.java com/stripe/android/googlepaylauncher/GooglePayLauncherViewModel.java com/stripe/android/googlepaylauncher/GooglePayPaymentMethodLauncherContract.java com/stripe/android/googlepaylauncher/GooglePayPaymentMethodLauncherViewModel.java com/stripe/android/link/LinkActivityContract.java com/stripe/android/link/LinkActivityViewModel.java com/stripe/android/link/ui/wallet/PaymentDetailsResult.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/stripe/android/model/ConfirmPaymentIntentParams.java com/stripe/android/model/ConfirmSetupIntentParams.java com/stripe/android/model/ConfirmStripeIntentParams.java com/stripe/android/model/ConsumerSession.java com/stripe/android/model/CreateFinancialConnectionsSessionParams.java com/stripe/android/model/FinancialConnectionsSession.java com/stripe/android/model/PaymentIntent.java com/stripe/android/model/PaymentMethodCreateParams.java com/stripe/android/model/SetupIntent.java com/stripe/android/model/Source.java com/stripe/android/model/SourceParams.java com/stripe/android/model/Stripe3ds2AuthParams.java com/stripe/android/model/Stripe3ds2Fingerprint.java com/stripe/android/model/StripeIntent.java com/stripe/android/model/parsers/ConsumerSessionJsonParser.java com/stripe/android/model/parsers/EphemeralKeyJsonParser.java com/stripe/android/model/parsers/FinancialConnectionsSessionJsonParser.java com/stripe/android/model/parsers/NextActionDataParser.java com/stripe/android/model/parsers/PaymentIntentJsonParser.java com/stripe/android/model/parsers/SetupIntentJsonParser.java com/stripe/android/model/parsers/SourceJsonParser.java com/stripe/android/payments/PaymentFlowResult.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/payments/bankaccount/n egation/CollectBankAccountContract.java com/stripe/android/payments/bankaccount/ui /CollectBankAccountViewEffect.java com/stripe/android/payments/core/authentic ation/threeds2/Stripe3ds2TransactionContract .java com/stripe/android/payments/core/authentic ation/threeds2/Stripe3ds2TransactionViewMo delFactory.java com/stripe/android/payments/paymentlaunch er/PaymentLauncherContract.java com/stripe/android/payments/paymentlaunch er/PaymentLauncherViewModel.java com/stripe/android/paymentsheet/PaymentO ptionContract.java com/stripe/android/paymentsheet/PaymentS heet.java com/stripe/android/paymentsheet/PaymentS heetContract.java com/stripe/android/paymentsheet/addressesel ement/AddressDetails.java com/stripe/android/paymentsheet/addressesel ement/AddressElementActivityContract.java com/stripe/android/paymentsheet/addressesel ement/AddressLauncher.java com/stripe/android/paymentsheet/flowcontro ller/DefaultFlowController.java com/stripe/android/paymentsheet/flowcontro ller/FlowControllerViewModel.java com/stripe/android/paymentsheet/paymentd atacollection/ach/USBankAccountFormViewM odel.java com/stripe/android/paymentsheet/paymentd atacollection/polling/PollingContract.java com/stripe/android/paymentsheet/paymentd atacollection/polling/PollingViewModel.java com/stripe/android/paymentsheet/state/Pay mentSheetState.java com/stripe/android/polling/IntentStatusPoller.

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>java</div> <div>com/stripe/android/stripe3ds2/observability/DefaultSentryConfig.java</div> <div>com/stripe/android/stripe3ds2/transaction/AcsData.java</div> <div>com/stripe/android/stripe3ds2/transaction/AuthenticationRequestParameters.java</div> <div>com/stripe/android/stripe3ds2/transaction/DefaultAcsDataParser.java</div> <div>com/stripe/android/stripe3ds2/transaction/IntentData.java</div> <div>com/stripe/android/ui/core/elements/AddressType.java</div> <div>com/stripe/android/view/PaymentAuthWebViewClient.java</div> <div>e0/o0.java</div> <div>e5/g.java</div> <div>g5/d.java</div> <div>g5/p.java</div> <div>g5/x.java</div> <div>i0/r1.java</div> <div>i0/y0.java</div> <div>i6/g.java</div> <div>io/grpc/internal/m2.java</div> <div>lh/d1.java</div> <div>pb/a.java</div> <div>rb/b.java</div> <div>rb/s.java</div> <div>sb/f.java</div> <div>ub/t0.java</div>
				<div>v4/p.java</div> <div>z1/h.java</div> <div>z1/u0.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	bi/a.java ci/c.java com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java di/b.java fi/a.java gi/d.java hi/b.java ii/n.java ji/a.java jk/e.java ki/d.java li/b.java mi/f.java mj/a.java nj/b.java oj/a.java pi/c.java pi/e.java pj/a.java qi/a.java qi/c0.java qi/u.java qi/w0.java qi/x0.java qi/y0.java qi/z0.java rh/b.java ri/o.java sd/a.java uh/a.java xh/a.java yh/a.java zh/a.java



NO	ISSUE	SEVERITY	STANDARDS	FILES
4	<a href="#">The App uses an insecure Random Number Generator.</a>	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	ak/e.java ak/f.java be/tramckrijte/workmanager/BackgroundWorker.java com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java dg/e.java dg/h.java f6/r.java hc/c.java ij/f.java ik/c.java io/grpc/internal/c0.java io/grpc/internal/e0.java io/grpc/internal/z1.java j\$/util/concurrent/ThreadLocalRandom.java m8/c.java mi/e.java ug/a.java ug/b.java v6/k0.java vb/g0.java vg/a.java xf/i.java
5	<a href="#">SHA-1 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	ac/b.java com/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java e7/a.java se/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	f6/b.java f6/c1.java f6/j.java f6/p0.java f6/t0.java f7/e0.java m6/j.java s6/b.java
7	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	rf/g.java rf/i.java v6/k0.java
8	<a href="#">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.</a>	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	le/i.java qb/w3.java qb/x2.java z3/a.java
9	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	ac/c.java ol/c.java x8/b.java
10	<a href="#">This App may have root detection capabilities.</a>	secure	OWASP MASVS: MSTG-RESILIENCE-1	ca/w.java
11	<a href="#">MD5 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	g6/d.java o6/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	<a href="#">The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.</a>	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	jd/h.java
13	<a href="#">This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.</a>	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/b.java io/flutter/plugin/platform/c.java
14	<a href="#">This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</a>	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java

## SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	--------------	-------	---------	---------	------------------

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libapp.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">info</a></p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>
2	lib/arm64-v8a/libflutter.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86_64/libapp.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">info</a></p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>
4	lib/x86_64/libflutter.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi-v7a/libapp.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">info</a></p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>
6	lib/armeabi-v7a/libflutter.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">info</a></p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/arm64-v8a/libapp.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">info</a></p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>
8	lib/arm64-v8a/libflutter.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/x86_64/libapp.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">info</a></p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>
10	lib/x86_64/libflutter.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/armeabi-v7a/libapp.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">info</a></p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>
12	lib/armeabi-v7a/libflutter.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">info</a></p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

# ! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
www.ibm.com	IP: 184.31.30.212 Country: Hong Kong Region: Hong Kong City: Hong Kong

# 🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
petitparser.github.io	ok	IP: 185.199.111.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
graph.facebook.com	ok	<b>IP:</b> 31.13.80.8 <b>Country:</b> Canada <b>Region:</b> Ontario <b>City:</b> Toronto <b>Latitude:</b> 43.700111 <b>Longitude:</b> -79.416298 <b>View:</b> <a href="#">Google Map</a>
docs.revenuecat.com	ok	<b>IP:</b> 3.162.3.41 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
cognital.health	ok	<b>IP:</b> 216.239.38.21 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
bit.ly	ok	<b>IP:</b> 67.199.248.10 <b>Country:</b> United States of America <b>Region:</b> New York <b>City:</b> New York City <b>Latitude:</b> 40.739288 <b>Longitude:</b> -73.984955 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
firebasestorage.googleapis.com	ok	<b>IP:</b> 172.217.13.106 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
plus.google.com	ok	<b>IP:</b> 172.217.13.142 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
goo.gl	ok	<b>IP:</b> 67.199.248.12 <b>Country:</b> United States of America <b>Region:</b> New York <b>City:</b> New York City <b>Latitude:</b> 40.739288 <b>Longitude:</b> -73.984955 <b>View:</b> <a href="#">Google Map</a>
www.ibm.com	ok	<b>IP:</b> 184.31.30.212 <b>Country:</b> Hong Kong <b>Region:</b> Hong Kong <b>City:</b> Hong Kong <b>Latitude:</b> 22.285521 <b>Longitude:</b> 114.157692 <b>View:</b> <a href="#">Google Map</a>
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
hooks.stripe.com	ok	<b>IP:</b> 54.163.195.10 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
files.stripe.com	ok	<b>IP:</b> 54.163.195.10 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
errors.rev.cat	ok	<b>IP:</b> 67.199.248.12 <b>Country:</b> United States of America <b>Region:</b> New York <b>City:</b> New York City <b>Latitude:</b> 40.739288 <b>Longitude:</b> -73.984955 <b>View:</b> <a href="#">Google Map</a>
www.nimh.nih.gov	ok	<b>IP:</b> 137.187.52.151 <b>Country:</b> United States of America <b>Region:</b> Maryland <b>City:</b> Bethesda <b>Latitude:</b> 38.999641 <b>Longitude:</b> -77.155083 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
flyer.chat	ok	<b>IP:</b> 172.64.80.1 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
api.revenuecat.com	ok	<b>IP:</b> 3.223.234.111 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
www.revenuecat.com	ok	<b>IP:</b> 3.162.3.30 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
api.stripe.com	ok	<b>IP:</b> 34.204.109.15 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	<b>IP:</b> 172.217.13.206 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
www.github.com	ok	<b>IP:</b> 140.82.114.3 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
link.co	ok	<b>IP:</b> 3.162.3.81 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
audyn.ai	ok	<b>IP:</b> 216.239.38.21 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
flutter.dev	ok	<b>IP:</b> 199.36.158.100 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
api.flutter.dev	ok	<b>IP:</b> 199.36.158.100 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
support.stripe.com	ok	<b>IP:</b> 34.227.85.74 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
r.stripe.com	ok	<b>IP:</b> 54.187.119.242 <b>Country:</b> United States of America <b>Region:</b> Oregon <b>City:</b> Portland <b>Latitude:</b> 45.523449 <b>Longitude:</b> -122.676208 <b>View:</b> <a href="#">Google Map</a>



DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	<b>IP:</b> 104.244.42.65 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.773968 <b>Longitude:</b> -122.410446 <b>View:</b> <a href="#">Google Map</a>
www.finity.com	ok	<b>IP:</b> 45.223.28.70 <b>Country:</b> United States of America <b>Region:</b> Colorado <b>City:</b> Greenwood Village <b>Latitude:</b> 39.617210 <b>Longitude:</b> -104.950813 <b>View:</b> <a href="#">Google Map</a>
developers.facebook.com	ok	<b>IP:</b> 31.13.80.8 <b>Country:</b> Canada <b>Region:</b> Ontario <b>City:</b> Toronto <b>Latitude:</b> 43.700111 <b>Longitude:</b> -79.416298 <b>View:</b> <a href="#">Google Map</a>
developer.android.com	ok	<b>IP:</b> 172.217.13.174 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
support.link.co	ok	<b>IP:</b> 3.161.213.118 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
graph.s	ok	No Geolocation information available.
rev.cat	ok	<b>IP:</b> 52.72.49.79 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
bloclibrary.dev	ok	<b>IP:</b> 185.199.108.153 <b>Country:</b> United States of America <b>Region:</b> Pennsylvania <b>City:</b> California <b>Latitude:</b> 40.065632 <b>Longitude:</b> -79.891708 <b>View:</b> <a href="#">Google Map</a>
www.apple.com	ok	<b>IP:</b> 23.223.216.198 <b>Country:</b> France <b>Region:</b> Ile-de-France <b>City:</b> Aubervilliers <b>Latitude:</b> 48.916672 <b>Longitude:</b> 2.383330 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
errors.stripe.com	ok	<b>IP:</b> 34.192.175.142 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
github.com	ok	<b>IP:</b> 140.82.114.3 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
accounts.google.com	ok	<b>IP:</b> 172.217.13.109 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
graph-video.s	ok	No Geolocation information available.
rive.app	ok	<b>IP:</b> 3.162.3.59 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
pubmed.ncbi.nlm.nih.gov	ok	<b>IP:</b> 34.107.134.59 <b>Country:</b> United States of America <b>Region:</b> Missouri <b>City:</b> Kansas City <b>Latitude:</b> 39.099731 <b>Longitude:</b> -94.578568 <b>View:</b> <a href="#">Google Map</a>
q.stripe.com	ok	<b>IP:</b> 54.186.23.98 <b>Country:</b> United States of America <b>Region:</b> Oregon <b>City:</b> Portland <b>Latitude:</b> 45.523449 <b>Longitude:</b> -122.676208 <b>View:</b> <a href="#">Google Map</a>
pagead2.googlesyndication.com	ok	<b>IP:</b> 172.217.13.162 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
dashboard.stripe.com	ok	<b>IP:</b> 52.86.4.21 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
static.afterpay.com	ok	<b>IP:</b> 104.18.170.118 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
stripe.com	ok	<b>IP:</b> 54.186.23.98 <b>Country:</b> United States of America <b>Region:</b> Oregon <b>City:</b> Portland <b>Latitude:</b> 45.523449 <b>Longitude:</b> -122.676208 <b>View:</b> <a href="#">Google Map</a>
m.stripe.com	ok	<b>IP:</b> 44.228.215.240 <b>Country:</b> United States of America <b>Region:</b> Oregon <b>City:</b> Portland <b>Latitude:</b> 45.523449 <b>Longitude:</b> -122.676208 <b>View:</b> <a href="#">Google Map</a>
ppm.stripe.com	ok	<b>IP:</b> 3.228.62.110 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
www.cdn.stripe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
payments.cognital.health	ok	<b>IP:</b> 172.217.13.211 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
www.amazon.com	ok	<b>IP:</b> 13.225.190.76 <b>Country:</b> Canada <b>Region:</b> Quebec <b>City:</b> Montreal <b>Latitude:</b> 45.508839 <b>Longitude:</b> -73.587807 <b>View:</b> <a href="#">Google Map</a>
api-diagnostics.revenuecat.com	ok	<b>IP:</b> 3.223.234.111 <b>Country:</b> United States of America <b>Region:</b> Virginia <b>City:</b> Ashburn <b>Latitude:</b> 39.043720 <b>Longitude:</b> -77.487488 <b>View:</b> <a href="#">Google Map</a>
connect.finitycity.com	ok	<b>IP:</b> 45.223.28.70 <b>Country:</b> United States of America <b>Region:</b> Colorado <b>City:</b> Greenwood Village <b>Latitude:</b> 39.617210 <b>Longitude:</b> -104.950813 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	<b>IP:</b> 172.217.13.142 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
win32.pub	ok	<b>IP:</b> 185.199.111.153 <b>Country:</b> United States of America <b>Region:</b> Pennsylvania <b>City:</b> California <b>Latitude:</b> 40.065632 <b>Longitude:</b> -79.891708 <b>View:</b> <a href="#">Google Map</a>
firebase.flutter.dev	ok	<b>IP:</b> 199.36.158.100 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
facebook.com	ok	<b>IP:</b> 31.13.80.36 <b>Country:</b> Canada <b>Region:</b> Ontario <b>City:</b> Toronto <b>Latitude:</b> 43.700111 <b>Longitude:</b> -79.416298 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
www.facebook.com	ok	<b>IP:</b> 31.13.80.36 <b>Country:</b> Canada <b>Region:</b> Ontario <b>City:</b> Toronto <b>Latitude:</b> 43.700111 <b>Longitude:</b> -79.416298 <b>View:</b> <a href="#">Google Map</a>
www.w3.org	ok	<b>IP:</b> 104.18.23.19 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
.facebook.com	ok	No Geolocation information available.

## EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	y7/w.java
support@stripe.com	com/stripe/android/core/exception/APIConnectionException.java
support@stripe.com	com/stripe/android/core/networking/ApiRequest.java



EMAIL	FILE
email@example.com	com/stripe/android/link/ui/ComposableSingletons\$LinkAppBarKt\$lambda2\$1.java
email@example.com	com/stripe/android/link/ui/ComposableSingletons\$LinkAppBarKt\$lambda6\$1.java
example@stripe.com	com/stripe/android/link/ui/LinkButtonViewKt.java
email@me.co	com/stripe/android/link/ui/inline/ComposableSingletons\$LinkInlineSignupKt\$lambda1\$1.java
test@stripe.com	com/stripe/android/link/ui/verification/ComposableSingletons\$VerificationScreenKt\$lambda1\$1.java
support@stripe.com	com/stripe/android/networking/FraudDetectionDataRequest.java
appro@openssl.org	lib/arm64-v8a/libflutter.so
_httpparser@13463476.responsepa _customerinfo@2432493635.fromjson _double@0150898.fromintege _future@4048458.immediate _growablelist@0150898._literal teamnaji@gmail.com _link@14069316.fromrawpat _growablelist@0150898.withcapaci _growablelist@0150898._literal6 _receiveportimpl@1026248.fromrawrec _colorfilter@15065589.mode _list@0150898._ofarray _timer@1026248.periodic _growablelist@0150898._literal2 _bigintimpl@0150898.from storationinformation@55124995.fromserial _list@0150898.empty _casterror@0150898._create _invocationmirror@0150898._withtype _offering@2438197943.fromjson	

EMAIL	FILE
_rawsocket@14069316._writepipe _imagefilter@15065589.linear _storeproduct@2445169359.fromjson _uri@0150898.file _growablelist@0150898._literal1 _imagefilter@15065589.blur _growablelist@0150898._literal4 _growablelist@0150898._ofgrowabl _growablelist@0150898.of _compressednode@815137193.single _nativesocket@14069316.pipe _cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring _list@0150898.of _entitlementinfos@2433312893.fromjson _list@0150898.generate _typeerror@0150898._create _entitlementinfo@2435195990.fromjson _list@0150898._ofgrowabl _list@0150898._ofefficie spebbe@gmail.com _growablelist@0150898._ofarray support@cognital.health _growablelist@0150898._literal3 _growablelist@0150898._ofother storeproductdiscount@2444036751.fromjson _timer@1026248._internal _growablelist@0150898._literal5 _rawsocket@14069316._readpipe _socket@14069316._readpipe _list@0150898._ofother _bytebuffer@7027147._new _hashcollisionnode@815137193.fromcollis ngstreamssubscription@4048458.zoned _introductoryprice@2437433645.fromjson _storetransaction@2434339892.fromjson _assertionerror@0150898._create _nativesocket@14069316.normal _offerings@2440143891.fromjson _filestream@14069316.forstdin	lib/armeabi-v7a/libapp.so

_colorfilter@15065589.srgbtoline <b>EMAIL</b> 150898.directory _growablelist@0150898._literal8	FILE
_file@14069316.fromrawpat _package@2439483590.fromjson _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _future@4048458.zonevalue _fencematch@1864445617.frommatch _growablelist@0150898._ofefficie	
_future@4048458.immediatee appro@openssl.org	lib/arm64-v8a/libflutter.so
_httpparser@13463476.responsepa _customerinfo@2432493635.fromjson _double@0150898.fromintege _future@4048458.immediate _growablelist@0150898._literal teamnaji@gmail.com _link@14069316.fromrawpat _growablelist@0150898.withcapaci _growablelist@0150898._literal6 _receiveportimpl@1026248.fromrawrec _colorfilter@15065589.mode _list@0150898._ofarray _timer@1026248.periodic _growablelist@0150898._literal2 _bigintimpl@0150898.from storationinformation@55124995.fromserial _list@0150898.empty _casterror@0150898._create _invocationmirror@0150898._withtype _offering@2438197943.fromjson _rawsocket@14069316._writepipe _colorfilter@15065589.lineartosr _storeproduct@2445169359.fromjson _uri@0150898.file _growablelist@0150898._literal1 _imagefilter@15065589.blur	



_uri@0150898.notsimple EMAIL_growablelist@0150898._literal7 _future@4048458.zonevalue	FILE
_fencematch@1864445617.frommatch _growablelist@0150898._ofefficie _future@4048458.immediatee	

## TRACKERS

TRACKER	CATEGORIES	URL
Facebook Login	Identification	<a href="https://reports.exodus-privacy.eu.org/trackers/67">https://reports.exodus-privacy.eu.org/trackers/67</a>
Google Firebase Analytics	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/49">https://reports.exodus-privacy.eu.org/trackers/49</a>

## HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "55950a93cca49a99221789721eaf2629"
"stripe_failure_reason_authentication" : "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
"stripe_failure_reason_authentication" : "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
"stripe_failure_reason_authentication" : "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
"google_crash_reporting_api_key" : "AlzaSyBNagGQi4-RRI8PnyfCnZ0T0UOYFeSjlvk"
"stripe_failure_reason_authentication" : "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"

POSSIBLE SECRETS
"google_api_key" : "AlzaSyBNagGQi4-RRl8PnyfCnZ0T0UOYFeSjlvk"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b>□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□"
115792089210356248762697446949407573530086143415290314195533631308867097853951
14201174159756348119636828602231808974327613839524373876287257344192745939351271897363116607846760036084894662356762579528277471921224 19290710461342083806363940845126918288940005715246254452957693493567527289568315417754417631393844571917550968471078465956625479423122 93338483924514339614727760681880609734239
BDDb97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04
c469684435deb378c4b65ca9591e2a5763059a2e
24B7B137C8A14D696E6768756151756FD0DA2E5C
393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB
FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A
36DF0AAFD8B8D7597CA10520D04B
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F04699 7
004D696E67687561517512D8F03431FCE63B88F4

POSSIBLE SECRETS
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4
4099B5A457F9D69F79213D094C4BCD4D4262210B
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
9b8f518b086098de3d77736f9458a3d2f6f95a37
D09E8800291CB85396CC6717393284AAA0DA64BA
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3
E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
6b8cf07d4ca75c88957d9d670591
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259

POSSIBLE SECRETS
D6031998D1B3BBFEBF59CC9BBFF9AEE1
962eddcc369cba8ebb260ee6b6a126d9346e38c5
1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
10C0FB15760860DEF1EEF4D696E676875615175D
deca87e736574c5c83c07314051fd93a
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
010092537397ECA4F6145799D62B0A19CE06FE26AD
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkk
41058363725152142129326129780047268409114441015993725554835256314039467401291
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296



POSSIBLE SECRETS
------------------

0667ACEB38AF4E488C407433FFAE4F1C811638DF20
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
3045AE6FC8422F64ED579528D38120EAE12196D5
5F49EB26781C0EC6B8909156D98ED435E45FD59918

POSSIBLE SECRETS
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
04B8266A46C55657AC734CE38F018F2192
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
DB7C2ABF62E35E668076BEAD2088
55066263022277343669578718895168534326250603453777594175500187360389116729240
3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1

POSSIBLE SECRETS
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
22123dc2395a05caa7423daeccc94760a7d462256bd56916
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
71169be7330b3038edb025f1
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
103FAEC74D696E676875615175777FC5B191EF30
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34
6b8cf07d4ca75c88957d9d67059037a4
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F
36134250956749795798585127919587881956611106672985015071877198253568414405109

POSSIBLE SECRETS
1243ae1b4d71613bc9f780a03690e
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNIY3VyZSBzdG9yYWdlCg
295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513
FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFE73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
517cc1b727220a94fe13abe8fa9a6ee0
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
3826F008A8C51D7B95284D9D03FF0E00CE2CD723A
48439561293906451759052585252797914202762949526041747995844080717082404635286

POSSIBLE SECRETS
------------------

4A6E0856526436F2F88DD07A341E32D04184572BEB710
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148
42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437669456364882730370838934791080835932647976778601915343474400961034231316672578686920482194932878633360203384797092684342247621055760235016132614780652761028509445403338652341
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C
C49D360886E704936A6678E1139D26B7819F7E90
9B9F605F5A858107AB1EC85E6B41C8AA582CA3511EDDFB74F02F3A6598980BB9
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
1053CDE42C14D696E67687561517533BF3F83345

POSSIBLE SECRETS
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
6127C24C05F38A0AAAF65C0EF02C
659EF8BA043916EEDE8911702B22
E95E4A5F737059DC60DFC7AD95B3D8139515620C
91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28
07B6882CAAFA84F9554FF8428BD88E246D2782AE2
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNIY3VyZSBzdG9yYWdlIEFFUyBLZXkk
C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335
216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF

POSSIBLE SECRETS
7167EFC92BB2E3CE7C8AAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
07A11B09A76B562144418FF3FF8C2570B8
3086d221a7d46bcde86c90e49284eb153dab
e8b4011604095303ca3b8099982be09fcb9ae616
4D41A619BCC6EADF0448FA22FAD567A9181D37389CA
1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
3086d221a7d46bcde86c90e49284eb15
1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1
127971af8721782ecffa3
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a





POSSIBLE SECRETS
------------------

A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZlJvaWQuYXBycy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3
002757A1114D696E6768756151755316C05E0BD4
DB7C2ABF62E35E668076BEAD208B
85E25BFE5C86226CDB12016F7553F9D0E693A268
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
32670510020758816978083085130507043184471273380659243275938904335757337482424

POSSIBLE SECRETS
1E589A8595423412134FAA2DBDEC95C8D8675E58
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297
91771529896554605945588149018382750217296858393520724172743325725474374979801
115792089237316195423570985008687907852837564279074904382605163141518161494337
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
B4E134D3FB59EB8BAB57274904664D5AF50388BA
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677
41ECE55743711A8C3CBF3783CD08C0EE4D4DC440D4641A8F366E550DFDB3BB67
0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
133531813272720673433859519948319001217942375967847486899482359599369642528734712461590403327731821410328012529253871914788598993103310567744136196364803064721377826656898686468463277710150809401182608770201615324990468332931294920912776241137878030224355746606283971659376426832674269780880061631528163475887

POSSIBLE SECRETS
------------------

5EEEFCA380D02919DC2C6558BB6D8A5D
68363196144955700784444165611827252895102170888761442055095051287550314083023
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
4D696E676875615175985BD3ADBADA21B43A97E2
dcb428fea25c40e7b99f81ae5981ee6a
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315
985BD3ADBADA4D696E676875615175A21B43A97E3
03E5A88919D7CAFCBF415F07C2176573B2
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
8D91E471E0989CDA27DF505A453F2B7635294F2DDF23E3B122ACC99C9E9F1E14

POSSIBLE SECRETS
100997906755055304772081815535925224869841082572053457874823515875577147990529272777244152852699298796483356699682842027972896052747173175480590485607134746852141928680912561502802222185647539190902656116367847270145019066794290930185446216399730872221732889830323194097355403213400972588322876850946740663962
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
0095E9A9EC9B297BD4BF36E059184F
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
D2C0FB15760860DEF1EEF4D696E6768756151754
9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D759B
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECDD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928
43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136

POSSIBLE SECRETS
EE353FCA5428A9300D4ABA754A44C00DFEC0C9AE4B1A1803075ED967B7BB73F
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C
7fffffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FEFF7F2955727A
2AA058F73A0E33AB486B0F610410C53A7F132310
00F50B028E4D696E676875615175290472783FB1
E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F
115792089210356248762697446949407573529996955224135760342422259061068512044369
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a

POSSIBLE SECRETS

02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7

79885141663410976897627118935756323747307951916507639758300472692338873533959

BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985

044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97

26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294

f7e1a085d69b3ddecbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcc4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a

04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3

139454871199115825601409655107690713107041707059928031797758001454375765357722984094124368522288239833039114681648076688236921220737322672160740747771700911134550432053804647694904686120113087816240740184800477047157336662926249423571248823968542221753660143391485680840520336859458494803187341288580489525163

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB

3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4

31a92ee2029fd10d901b113e990710f0d21ac6b6

POSSIBLE SECRETS
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
10E723AB14D696E6768756151756FEBF8FCB49A9
000E0D4D696E6768756151750CC03A4473D03679
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
96341f1138933bc2f503fd44
b3fb3400dec5c4adceb8655d4c94
3E1AF419A269A5F866A7D3C25C3DF80AE979259373FF2B182F49D4CE7E1BBC8B
00689918DBEC7E5A0DD6DFC0AA55C7
0307AF69989546103D79329FCC3D74880F33BBE803CB
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACB F04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B

## POSSIBLE SECRETS

3045AE6FC8422f64ED579528D38120EAE12196D5

9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35

0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFEF2E331F296E071FA0DF9982CFA7D43F2E

8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871

cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953

038D16C2866798B600F9F08BB4A8E860F3298CE04A5798

FFFFFFFFE0000000075A30D1B9038A115

A335926AA319A27A1D00896A6773A4827ACDAC73

02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614

401028774D7777C7B7666D1366EA432071274F89FF01E718

040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F

114ca50f7a8e2f3f657c1108d9d44cfd8

7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864

C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E



POSSIBLE SECRETS
c49d360886e704936a6678e1139d26b7819f7e90
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
E87579C11079F43DD824993C2CEE5ED3
324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1
E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760
29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA
00E8BEE4D3E2260744188BE0E9C723
5FF6108462A2DC8210AB403925E638A19C1455D21
6EE3CEEB230811759F20518A0930F1A4315A827DAC
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

POSSIBLE SECRETS
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
MQVwithSHA256KDFAndSharedInfo
108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
7d7374168ffe3471b60a857686a19475d3bfa2ff
71169be7330b3038edb025f1d0f9
1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
4E13CA542744D696E67687561517552F279A8C84
115792089237316195423570985008687907853269984665640564039457584007908834671663
06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C
e4437ed6010e88286f547fa90abfe4c42212
003088250CA6E7C7FE649CE85820F7
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
6db14acc9e21c820ff28b1d5ef5de2b0

POSSIBLE SECRETS
3FA8124359F96680B83D1C3EB2C070E5C545C9858D03ECFB744BF8D717717EFC
9760508f15230bccb292b982a2eb840bf0581cf5
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
db92371d2126e9700324977504e8c90e
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
51DEF1815DB5ED74FCC34C85D709
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
03F7061798EB99E238FD6F1BF95B48FEEB4854252B
MQVwithSHA384KDFAndSharedInfo
9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D7598
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
5DDA470ABE6414DE8EC133AE28E9BBBD7FCEC0AE0FF2
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A

POSSIBLE SECRETS
DB7C2ABF62E35E7628DFAC6561C5
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9
E95E4A5F737059DC60DFC7AD95B3D8139515620F
E95E4A5F737059DC60DF5991D45029409E60FC09
0108B39E77C4B108BED981ED0E890E117C511CF072
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96
B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1

POSSIBLE SECRETS
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
cc2751449a350f668590264ed76692694a80308a
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
115792089210356248762697446949407573530086143415290314195533631308867097853948
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
0217C05610884B63B9C6C7291678F9D341
e43bb460f0b80cc0c0b075798e948060f8321b7d
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83

POSSIBLE SECRETS
6BA06FE51464B2BD26DC57F48819BA9954667022C7D03
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEE7E21340780FE41BD
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB
DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3
12511cfe811d0f4e6bc688b4d
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44
A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
7A1F6653786A68192803910A3D30B2A2018B21CD54
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
127021248288932417465907042777176443525787653508916535812817507265705031260985098497423188333483401180925999995120988934130659205614996724254121049274349357074920312769561451689224110579311248812610229678534638401693520013288995000362260684222750813532307004517341633685004541062586971416883686778842537820383

POSSIBLE SECRETS
072546B5435234A422E0789675F432C89435DE5242
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bccca2a406cb0b
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
2866537B676752636A68F56554E12640276B649EF7526267
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399

POSSIBLE SECRETS
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
74D59FF07F6B413D0EA14B344B20A2DB049B50C3
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
MQVwithSHA512KDFAndSharedInfo
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883
B99B99B099B323E02709A4D696E6768756151751
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
6C01074756099122221056911C77D77E77A777E7E7E77FCB
9162fbe73984472a0a9d0590
b8adf1378a6eb73409fa6c9c637ba7f5
8d5155894229d5e689ee01e6018a237e2cae64cd
ffffffff00000000ffffffffffffbce6faada7179e84f3b9cac2fc632551
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53



POSSIBLE SECRETS
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
020A601907B8C953CA1481EB10512F78744A3205FD
10B7B4D696E676875615175137C8A16FD0DA2211
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150

## PLAYSTORE INFORMATION

**Title:** Audyn AI Mental Health

**Score:** 3.409091 **Installs:** 1,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [com.cognital.audyn](https://play.google.com/store/apps/details?id=com.cognital.audyn)

**Developer Details:** Cognital, 7724137727297381222, Cognital UAB Konstitucijos pr. 21b 08130 Vilnius Lithuania, <https://audyn.ai>, [hello@cognital.health](mailto:hello@cognital.health),

**Release Date:** Feb 14, 2023 **Privacy Policy:** [Privacy link](#)

### Description:

Hi, I'm Audyn, your friendly mental health AI companion. Whether you're having a bad day, contemplating life choices, or simply want someone to talk to - I am here for you. Powered by natural language processing technology and uncompromised respect for your privacy, I am here to support you on your journey to mindfulness, wellness and happiness. I am able to understand and respond to a wide range of topics, but I tend to do best in conversations on mental health, relationships, lifestyle, career, anxiety, loneliness, depression. I have been trained on thousands of mental health articles, books, papers and dialogs. Some of my training sets contain handcrafted examples of real life counseling sessions, behavioral modification strategies, stress relief tools being applied through chat. The body of knowledge that I contain may help form healthy habits and improve overall well being, however I am not a medical tool nor a replacement for professional medical care. If you suffer from

a health condition please seek help with your healthcare provider. Main features: □ More than just a chatbot. An empathetic AI friend that provides emotional support, coaching and self-help strategies □ Client-side encryption of data to give you a peace of mind that no one else ever peeks into your conversations □ On-device data storage option in case you don't want to sync across devices □ AI models tuned for mental health topics in collaboration with psychologists and psychotherapists □ Evidence-based Cognitive Behavioural Therapy (CBT), Talk Therapy and other psychotherapy strategies included in model training datasets ✕ Long-term memory formation based on your conversation history to provide personalized approach and advice Limitations: □ As with all other generative AI applications, Audyn AI suffers from hallucinations, which can result in misinterpretation of dialog, bias or factually incorrect responses. Treat Audyn AI responses with caution □ Audyn AI long term memory can get polluted with an abundance of facts it picks up about you. You can reset or modify Audyn AI memory at any time About content provided through chat: Audyn AI is a generative language application. While the training datasets for Audyn AI include mental health resources and handcrafted dialogs of emotional support applied through chat, the content generated by Audyn AI may deviate from the content used during training. Content generated via chats with Audyn AI should not be used as health or medical recommendations, calculations, references, wellness reports, or diagnoses. If you suffer from a health condition please seek help with your healthcare provider. For more information about the technology used, it's abilities and limitations please visit <https://audyn.ai/#faq>

---

## Report Generated by - MobSF v3.7.9 Beta

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

© 2023 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).