MOBSF

ANDROID STATIC ANALYSIS REPORT

MedBridge GO (4.6.3)

File Name:	com.medbridgeed.hep.go_266.apk
Package Name:	com.medbridgeed.hep.go
Scan Date:	Aug. 31, 2025, 3:13 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	19	2	3	2

FILE INFORMATION

File Name: com.medbridgeed.hep.go_266.apk
Size: 18.05MB
MD5: ead9bf19e352758ba9ec1c81449f02ae
SHA1: a319b7de1121234b8bbd20e1818e1f9deb7aef85
SHA256: bb591278637c8824b7f7f6144f5ac00a32de8a82e669cabd404fc28b16fcbaf2

APP INFORMATION

App Name: MedBridge GO
Package Name: com.medbridgeed.hep.go
Main Activity: com.medbridgeed.hep.go.activities.SplashActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 4.6.3

Android Version Code: 266

APP COMPONENTS

Activities: 33
Services: 9
Receivers: 13
Providers: 3
Exported Activities: 1
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=WA, L=Seattle, O=Medbridge Education, OU=Android Development, CN=MedBridge
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-05-24 00:20:10+00:00
Valid To: 2043-10-10 00:20:10+00:00
Issuer: C=US, ST=WA, L=Seattle, O=Medbridge Education, OU=Android Development, CN=MedBridge
Serial Number: 0x79c67830
Hash Algorithm: sha256
md5: 78b81985fb38d7ed20197b7dcf39e7ff
sha1: d158d2ecf5ef3705738d5732ec14612d3a824efe
sha256: e86fd25fd639aaa6f883185efb9dc77dae1d1a4f942639ab6563d2392bd3c444
sha512: 4dfb9e336e42611b7c6d2c0c1feb8351099c5c04e067849bd74fcba6d7c05ecd72941cbcf7b849f3aaf4505d0f0dcd3da8dd9ce81495a39b942a6aefe12cfa93
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 5af00b0b1b20c9ffad8d3956f35965ff462a01ca88f13a2acb68b28c1b862eef
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.medbridgeed.hep.go.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.

APKID ANALYSIS

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

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check Build.HARDWARE check Build.BOARD check SIM operator check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.medbridgeed.hep.go.activities.SplashActivity	Schemes: https://, http://, Hosts: *.medbridgego.com, Path Prefixes: /m,
sdk.pendo.io.activities.PendoGateActivity	Schemes: pendo-5dc2336c://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	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.
4	Activity (sdk.pendo.io.activities.PendoGateActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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: **10** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/c.java a2/a.java a2/b.java a2/h.java a2/i.java a2/j.java a5/c.java a5/f.java a5/g.java a5/o.java a5/s.java b4/l.java b6/a.java b6/d.java b7/i.java c5/c0.java c5/e.java c5/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c5/y.java com/airbnb/lottie/a.java com/github/barteksc/pdfviewer/PDFView.java com/github/siyamed/shapeimageview/mask/PorterImageView.java com/medbridgeed/core/network/d.java com/medbridgeed/core/network/e.java com/medbridgeed/core/player/PlayerFragment.java com/medbridgeed/hep/go/HepApplication.java com/medbridgeed/hep/go/activities/AccessCodeActivity.java com/medbridgeed/hep/go/activities/ChatMessagesActivity.java com/medbridgeed/hep/go/activities/ConsentActivity.java com/medbridgeed/hep/go/activities/ConsentRetryActivity.java com/medbridgeed/hep/go/activities/ExerciseActivity.java com/medbridgeed/hep/go/activities/HepGoActivity.java com/medbridgeed/hep/go/activities/HomeActivity.java com/medbridgeed/hep/go/activities/ManualEntryActivity.java com/medbridgeed/hep/go/activities/NpsActivity.java com/medbridgeed/hep/go/activities/PathologyActivity.java com/medbridgeed/hep/go/activities/ProfileActivity.java com/medbridgeed/hep/go/activities/QuickLogActivity.java com/medbridgeed/hep/go/activities/RtmSurveyActivity.java com/medbridgeed/hep/go/activities/SelectExercisesActivity.java com/medbridgeed/hep/go/activities/SelfReporting.java com/medbridgeed/hep/go/activities/SettingAct

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ivity.java com/medbridgeed/hep/go/activities/SplashActivity.java com/medbridgeed/hep/go/activities/SsoWebViewActivity.java com/medbridgeed/hep/go/activities/TelehealthActivity.java com/medbridgeed/hep/go/activities/TelehealthSurveyActivity.java com/medbridgeed/hep/go/activities/TermsActivity.java com/medbridgeed/hep/go/data/BrandManager.java com/medbridgeed/hep/go/data/DatabaseOpenHelper.java com/medbridgeed/hep/go/data/ProgramManager.java com/medbridgeed/hep/go/data/StatsManager.java com/medbridgeed/hep/go/data/Table.java com/medbridgeed/hep/go/data/table/CachedElement.java com/medbridgeed/hep/go/data/table/CachedEpisode.java com/medbridgeed/hep/go/data/table/Program.java com/medbridgeed/hep/go/data/table/Reminder.java com/medbridgeed/hep/go/data/table/Video.java com/medbridgeed/hep/go/etc/PatientAccountManager.java com/medbridgeed/hep/go/fragments/ExercisesFragment.java com/medbridgeed/hep/go/fragments/FeedbackSkippedFragment.java com/medbridgeed/hep/go/fragments/GoButtonOnboardingTooltip.java com/medbridgeed/hep/go/fragments/MessagesFragment.java com/medbridgeed/hep/go/fragments/MyActivi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tyFragment.java com/medbridgeed/hep/go/fragments/ResourceFragment.java com/medbridgeed/hep/go/fragments/ResourcesFragment.java com/medbridgeed/hep/go/fragments/SurveyFeedbackFragment.java com/medbridgeed/hep/go/fragments/SurveyStarsFragment.java com/medbridgeed/hep/go/fragments/TelehealthChatFragment.java com/medbridgeed/hep/go/model/OnboardingPageFragment.java com/medbridgeed/hep/go/network/NetworkManager.java com/medbridgeed/hep/go/network/ProgramResourceLoader.java com/medbridgeed/hep/go/network/json/v3/JsonNpsMetrics.java com/medbridgeed/hep/go/network/json/v3/episodes/SignInWithProgramResponse.java com/medbridgeed/hep/go/receivers/MbFirebaseMessagingService.java com/newrelic/agent/android/AndroidAgentImpl.java com/newrelic/agent/android/NewRelic.java com/newrelic/agent/android/SavedState.java com/newrelic/agent/android/agentdata/AgentDataController.java com/newrelic/agent/android/analytics/AnalyticsControllerImpl.java com/newrelic/agent/android/analytics/EventManagerImpl.java com/newrelic/agent/android/crash/UncaughtExceptionHandler.java com/newrelic/agent/android/harvest/Harvest.java com/newrelic/agent/android/hybrid/data/DataController.java com/newrelic/agent/android/instrumentation/io/CountingInputStream.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	com/newrelic/agent/android/logging/AndroidAgentLog.java com/newrelic/agent/android/logging/ConsoleAgentLog.java com/newrelic/agent/android/rum/AppApplicationLifeCycle.java com/newrelic/agent/android/sample/Sampler.java com/newrelic/agent/android/stores/SharedPrefsAnalyticsAttributeStore.java com/newrelic/agent/android/tracing/ActivityTrace.java com/newrelic/agent/android/tracing/TraceMachine.java com/newrelic/agent/android/util/AgentBuildOptionsReporter.java com/opentok/android/BaseVideoCapturer.java com/opentok/android/OtLog.java com/shockwave/pdfium/PdfiumCore.java e5/a.java e5/b.java e5/h0.java e5/k0.java e5/l0.java e5/m0.java e5/o0.java e5/p.java e5/q.java e5/u0.java e5/y0.java e6/i.java external/sdk/pendo/io/com/appmattus/certificatetransparency/internal/loglist/model/v2/Log$$serializer.java external/sdk/pendo/io/glide/a.java external/sdk/pendo/io/glide/gifdecoder/StandardGifDecoder.java external/sdk/pendo/io/glide/gifdecoder/d.java external/sdk/pendo/io/glide/load/data/AssetPathFetcher.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/glide/load/data/LocalUriFetcher.java external/sdk/pendo/io/glide/load/data/mediastore/ThumbFetcher.java external/sdk/pendo/io/glide/load/data/mediastore/c.java external/sdk/pendo/io/glide/load/engine/Engine.java external/sdk/pendo/io/glide/load/engine/bitmap_recycle/LruArrayPool.java external/sdk/pendo/io/glide/load/engine/bitmap_recycle/LruBitmapPool.java external/sdk/pendo/io/glide/load/engine/cache/DiskLruCacheWrapper.java external/sdk/pendo/io/glide/load/engine/g.java external/sdk/pendo/io/glide/load/engine/h.java external/sdk/pendo/io/glide/load/engine/u.java external/sdk/pendo/io/glide/load/model/ByteBufferEncoder.java external/sdk/pendo/io/glide/load/model/ByteBufferFileLoader.java external/sdk/pendo/io/glide/load/model/FileLoader.java external/sdk/pendo/io/glide/load/model/ResourceLoader.java external/sdk/pendo/io/glide/load/model/StreamEncoder.java external/sdk/pendo/io/glide/load/resource/ImageDecoderResourceDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/BitmapEncoder.java external/sdk/pendo/io/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/DefaultImageHeaderParser.java external/sdk/pendo/io/glide/load/resource/bit

NO	ISSUE	SEVERITY	STANDARDS	FILES
				external/sdk/pendo/io/glide/load/resource/bitmap/VideoDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/b.java external/sdk/pendo/io/glide/load/resource/bitmap/c.java external/sdk/pendo/io/glide/load/resource/bitmap/d.java external/sdk/pendo/io/glide/load/resource/gif/ByteBufferGifDecoder.java external/sdk/pendo/io/glide/load/resource/gif/GifDrawableEncoder.java external/sdk/pendo/io/glide/load/resource/gif/StreamGifDecoder.java external/sdk/pendo/io/glide/manager/DefaultConnectivityMonitorFactory.java external/sdk/pendo/io/glide/manager/b.java external/sdk/pendo/io/glide/request/SingleRequest.java external/sdk/pendo/io/glide/request/target/CustomViewTarget.java external/sdk/pendo/io/glide/request/target/ViewTarget.java external/sdk/pendo/io/mozilla/javascript/Interpreter.java external/sdk/pendo/io/mozilla/javascript/ScriptRuntime.java external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java external/sdk/pendo/io/mozilla/javascript/tools/idswitch/Main.java external/sdk/pendo/io/mozilla/javascript/tools/jsc/Main.java g2/k.java h5/b.java i2/a.java i5/e.java i5/m.java i7/c.java k0/a.java k0/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k7/g.java k7/n.java k8/j.java l1/a.java l1/b.java m0/o.java m0/r.java m0/u.java m0/y.java m5/b.java m8/b.java n1/c.java n1/l.java o/c.java o1/h.java o1/n.java o5/b.java o5/d.java o5/f.java o5/h.java o8/e.java org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java p1/a.java q/f.java q0/j.java q6/a.java r0/d.java r4/x.java r8/a.java s0/a.java s1/a.java s5/z.java s8/a.java s8/a0.java s8/a1.java s8/c0.java s8/d0.java s8/h.java s8/n0.java s8/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s8/u0.java s8/v0.java s8/w0.java sdk/pendo/io/PendoInternal.java sdk/pendo/io/activities/PendoGateActivity.java sdk/pendo/io/c0/j.java sdk/pendo/io/c0/k.java sdk/pendo/io/c0/m.java sdk/pendo/io/c0/n.java sdk/pendo/io/g3/c.java sdk/pendo/io/g9/a.java sdk/pendo/io/h0/a.java sdk/pendo/io/i8/e.java sdk/pendo/io/j0/a.java sdk/pendo/io/j7/g.java sdk/pendo/io/logging/PendoLogger.java sdk/pendo/io/logging/c.java sdk/pendo/io/p/a.java sdk/pendo/io/v/a.java sdk/pendo/io/w/a.java sdk/pendo/io/w/b.java sdk/pendo/io/y/b.java t6/b.java v6/i.java w/d.java w7/b.java w8/e.java w8/i.java x7/c.java y0/m.java y4/a.java y5/a.java z4/b.java z4/c.java z4/d.java z4/h.java z4/i.java z4/r.java z4/t.java z4/u.java z5/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	a4/b.java external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java sdk/pendo/io/a4/b.java sdk/pendo/io/b4/b.java sdk/pendo/io/d4/b.java sdk/pendo/io/e4/d.java sdk/pendo/io/e4/f.java sdk/pendo/io/e4/k.java sdk/pendo/io/f4/h.java sdk/pendo/io/j/b.java sdk/pendo/io/j/j.java sdk/pendo/io/k/i.java sdk/pendo/io/n3/b.java sdk/pendo/io/o3/a.java sdk/pendo/io/r3/a.java sdk/pendo/io/s3/a.java sdk/pendo/io/v3/b.java sdk/pendo/io/x3/a.java sdk/pendo/io/y3/a.java sdk/pendo/io/z3/a.java
				com/medbridgeed/hep/go/network/json/telehealth/TelehealthJoinMeetingResponse.java com/newrelic/agent/android/SavedState.java com/newrelic/agent/android/distributedtracing/TracePayload.java com/newrelic/agent/android/harvest/AgentHealth.java com/newrelic/agent/android/harvest/HarvestConfiguration.java com/newrelic/agent/android/util/PersistentUUID.java com/opentok/android/DefaultAudioDevice.java d1/d.java external/sdk/pendo/io/com/appmattus/certificatetransparency/internal/loglist/model/v2/Log.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	external/sdk/pendo/io/glide/load/engine/c.java external/sdk/pendo/io/glide/load/engine/m.java external/sdk/pendo/io/glide/load/engine/s.java external/sdk/pendo/io/mozilla/javascript/ClassCache.java external/sdk/pendo/io/mozilla/javascript/NativeError.java external/sdk/pendo/io/mozilla/javascript/NativeJavaObject.java external/sdk/pendo/io/mozilla/javascript/ScriptRuntime.java external/sdk/pendo/io/mozilla/javascript/xmlimpl/XmlNode.java p3/a.java sdk/pendo/io/actions/ActivationManager.java sdk/pendo/io/actions/FloatingVisualGuide.java sdk/pendo/io/actions/ToolTipVisualGuide.java sdk/pendo/io/actions/handlers/PendoGlobalCommandHandler.java sdk/pendo/io/d1/e.java sdk/pendo/io/m/d.java sdk/pendo/io/models/GlobalEventPropertiesKt.java sdk/pendo/io/models/StepModel.java sdk/pendo/io/n/b.java sdk/pendo/io/q/g.java sdk/pendo/io/views/custom/videoplayer/PendoYoutubePlayer.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/medbridgeed/hep/go/HepApplication.java com/medbridgeed/hep/go/data/table/Video.java com/medbridgeed/hep/go/fragments/ResourceFragment.java com/medbridgeed/hep/go/network/ProgramResourceLoader.java com/newrelic/agent/android/AndroidAgentImpl.java s8/a0.java s8/a1.java sdk/pendo/io/PendoInternal.java sdk/pendo/io/r8/a.java
5	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	s8/a0.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/medbridgeed/core/network/e.java sdk/pendo/io/f3/c.java sdk/pendo/io/f3/d.java sdk/pendo/io/f3/g.java sdk/pendo/io/f3/h.java sdk/pendo/io/k/d.java sdk/pendo/io/t4/c.java sdk/pendo/io/t4/p0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/medbridgeed/hep/go/data/DatabaseOpenHelper.java com/medbridgeed/hep/go/data/Table.java com/medbridgeed/hep/go/data/table/CachedElement.java com/medbridgeed/hep/go/data/table/CachedEpisode.java com/medbridgeed/hep/go/data/table/Program.java com/medbridgeed/hep/go/data/table/Video.java com/newrelic/agent/android/instrumentation/SQLiteInstrumentation.java m2/b0.java m2/h0.java r0/c.java
8	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/medbridgeed/hep/go/activities/SimpleWebviewActivity.java sdk/pendo/io/views/custom/videoplayer/PendoYoutubePlayer.java
9	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/medbridgeed/hep/go/activities/SimpleWebviewActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/newrelic/agent/android/util/Util.java r2/p1.java sdk/pendo/io/j3/d.java sdk/pendo/io/j3/h.java sdk/pendo/io/j4/f.java sdk/pendo/io/v4/c.java sdk/pendo/io/v4/d.java sdk/pendo/io/w2/z.java t3/y0.java t9/a.java t9/b.java u9/a.java w3/b.java
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	sdk/pendo/io/g9/m.java w7/b.java
12	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	k0/c.java m0/y.java w7/c.java
13	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	external/sdk/pendo/io/mozilla/javascript/tools/shell/Main.java
14	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	external/sdk/pendo/io/daimajia/BuildConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	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	y3/a.java
16	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	b7/w.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	b6/a.java com/vonage/webrtc/Camera1Session.java
00096	Connect to a URL and set request method	command network	com/newrelic/agent/android/agentdata/AgentDataSender.java com/newrelic/agent/android/harvest/HarvestConnection.java q4/u.java x7/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/newrelic/agent/android/harvest/HarvestConnection.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java q4/u.java x7/c.java
00109	Connect to a URL and get the response code	network command	com/newrelic/agent/android/agentdata/AgentDataSender.java com/newrelic/agent/android/crash/CrashSender.java com/newrelic/agent/android/harvest/HarvestConnection.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java q4/u.java x7/c.java
00094	Connect to a URL and read data from it	command network	com/medbridgeed/hep/go/network/ProgramResourceLoader.java com/newrelic/agent/android/harvest/HarvestConnection.java external/sdk/pendo/io/mozilla/javascript/tools/shell/Global.java q4/u.java
00108	Read the input stream from given URL	network command	com/newrelic/agent/android/harvest/HarvestConnection.java com/newrelic/agent/android/payload/PayloadSender.java q4/u.java
00022	Open a file from given absolute path of the file	file	com/newrelic/agent/android/util/OfflineStorage.java external/sdk/pendo/io/mozilla/javascript/tools/jsc/Main.java k0/c.java m0/y.java r0/d.java s0/a.java sdk/pendo/io/g9/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	external/sdk/pendo/io/glide/load/a.java external/sdk/pendo/io/glide/load/model/FileLoader.java external/sdk/pendo/io/mozilla/javascript/tools/SourceReader.java external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java external/sdk/pendo/io/mozilla/javascript/tools/idswitch/Main.java external/sdk/pendo/io/mozilla/javascript/tools/shell/Global.java m0/y.java o0/b.java okio/o.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java q4/i.java q4/j0.java s8/a0.java s8/c0.java sdk/pendo/io/g9/h.java sdk/pendo/io/p/a.java sdk/pendo/io/t4/m1.java sdk/pendo/io/t4/n0.java w7/c.java
00114	Create a secure socket connection to the proxy address	network command	sdk/pendo/io/b3/f.java
00024	Write file after Base64 decoding	reflection file	s8/a0.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/medbridgeed/hep/go/HepApplication.java com/medbridgeed/hep/go/activities/HomeActivity.java com/medbridgeed/hep/go/activities/IntroActivity.java com/medbridgeed/hep/go/activities/TelehealthActivity.java e5/b1.java k8/z.java s8/w0.java sdk/pendo/io/actions/handlers/PendoGlobalCommandHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/medbridgeed/hep/go/activities/HomeActivity.java com/medbridgeed/hep/go/activities/TelehealthActivity.java e5/b1.java s8/w0.java
00012	Read data and put it into a buffer stream	file	sdk/pendo/io/t4/m1.java sdk/pendo/io/t4/n0.java
00030	Connect to the remote server through the given URL	network	external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java q4/u.java
00078	Get the network operator name	collection telephony	com/newrelic/agent/android/util/Connectivity.java
00091	Retrieve data from broadcast	collection	com/medbridgeed/hep/go/activities/AccessCodeActivity.java com/medbridgeed/hep/go/activities/HomeActivity.java com/medbridgeed/hep/go/activities/ProfileActivity.java com/medbridgeed/hep/go/activities/SplashActivity.java
00112	Get the date of the calendar event	collection calendar	com/medbridgeed/hep/go/activities/HomeActivity.java com/medbridgeed/hep/go/activities/ManualEntryActivity.java com/medbridgeed/hep/go/activities/ProfileActivity.java com/medbridgeed/hep/go/util/CalendarView.java
00025	Monitor the general action to be performed	reflection	com/medbridgeed/hep/go/activities/SplashActivity.java
00033	Query the IMEI number	collection	com/newrelic/agent/android/util/PersistentUUID.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	com/newrelic/agent/android/util/Reachability.java sdk/pendo/io/f3/b.java sdk/pendo/io/f3/h.java sdk/pendo/io/t4/b1.java
00163	Create new Socket and connecting to it	socket	com/newrelic/agent/android/util/Reachability.java sdk/pendo/io/f3/b.java sdk/pendo/io/f3/h.java sdk/pendo/io/t4/b1.java
00132	Query The ISO country code	telephony collection	r4/z0.java
00130	Get the current WIFI information	wifi collection	sdk/pendo/io/l8/d.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	external/sdk/pendo/io/glide/load/data/mediastore/ThumbFetcher.java
00036	Get resource file from res/raw directory	reflection	com/medbridgeed/hep/go/HepApplication.java q4/j0.java
00125	Check if the given file path exist	file	com/medbridgeed/hep/go/fragments/ResourceFragment.java
00056	Modify voice volume	control	com/vonage/webrtc/audio/WebRtcAudioTrack.java com/vonage/webrtc/voiceengine/WebRtcAudioTrack.java com/vonage/webrtc/voiceengine61/WebRtcAudioTrack.java
00208	Capture the contents of the device screen	collection screen	com/vonage/webrtc/ScreenCapturerAndroid.java
00028	Read file from assets directory	file	q4/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00065	Get the country code of the SIM card provider	collection	sdk/pendo/io/l8/e.java
00102	Set the phone speaker on	command	com/opentok/android/DefaultAudioDevice.java
00014	Read file into a stream and put it into a JSON object	file	w7/c.java
00047	Query the local IP address	network collection	sdk/pendo/io/t4/e1.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://medbridge-go.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/22002218107/namespaces/firebase:fetch?key=AIzaSyBYZt2G1Y_BL4cxrN-fMw2lxGK5yBjieDk. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.RECORD_AUDIO
Other Common Permissions	5/44	android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
api.opentok.com	ok	**IP:** 168.100.106.197 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
assets.medbridge.com	ok	**IP:** 18.238.96.62 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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
plus.google.com	ok	**IP:** 142.250.75.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
medbridgeassets.s3-us-west-1.amazonaws.com	ok	**IP:** 16.15.4.171 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.409912 **Longitude:** -122.160400 **View:** Google Map
data.eu.pendo.io	ok	**IP:** 34.110.214.126 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
default.url	ok	No Geolocation information available.

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
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.189.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.medbridgego.com	ok	**IP:** 104.18.33.194 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
www.youtube.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
data.jpn.pendo.io	ok	**IP:** 34.149.195.87 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
medbridge-go.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.gstatic.com	ok	**IP:** 142.251.40.35 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.131 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
assets.medbridgeeducation.com	ok	**IP:** 18.238.109.124 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.medbridgeeducation.com	ok	**IP:** 104.18.38.51 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
data.pendo.io	ok	**IP:** 34.107.204.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
support.medbridgego.com	ok	**IP:** 104.18.33.194 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
dashif.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
us1.data.pendo.io	ok	**IP:** 34.110.177.118 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
customer.support@medbridge.com	s8/z.java
u0013android@android.com0 u0013android@android.com	a5/n.java

TRACKERS

TRACKER	CATEGORIES	URL
New Relic	Analytics	https://reports.exodus-privacy.eu.org/trackers/130
Pendo	Analytics	https://reports.exodus-privacy.eu.org/trackers/416

HARDCODED SECRETS

POSSIBLE SECRETS
"device_auth_alert_enable_ok" : "Yes"
"device_auth_alert_recommend_device_authentication_goto_settings" : "Yes"
"device_auth_cancel" : "cancel"

POSSIBLE SECRETS
"device_auth_or" : "OR"
"firebase_database_url" : "https://medbridge-go.firebaseio.com"
"google_api_key" : "AIzaSyBYZt2G1Y_BL4cxrN-fMw2lxGK5yBjieDk"
"google_crash_reporting_api_key" : "AIzaSyBYZt2G1Y_BL4cxrN-fMw2lxGK5yBjieDk"
"session_duration_calculating" : "Updating..."
"session_plus" : "+%1$s"
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1B6qsa2sbpc4CuFEjgRWez9nN
AAe901adf567cbacefdf50e40681f4f5c3d699ca23

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
410583637251521421293261297800472684091144410159937255548352563140394674012 91
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
VTdL1VbC2tejvcI2BlMkEpk1BzBZI0KQB0GaDWFLN
Vd99BKh6pxt3mXSDJzHuVrCq52xBXAKVahbuFb6dqBc

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF
32670510020758816978083085130507043184471273380659243275938904335757337482424
nvknbo5+6pBVWVZpCg5Rtpii3JUKMxOmJrccBCo7ICIqPIj/L9Nc5zmWMH2igKHLq
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF
9a04f079-9840-4286-ab92-e65be0885f95
55066263022277343669578718895168534326250603453777594175500187360389116729240
e2719d58-a985-b3c9-781a-b030af78d30e
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1 82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99 C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6 9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B 6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1 A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23 BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855 322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C 1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C 6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC 9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C 35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95 F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA 6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF
115792089237316195423570985008687907852837564279074904382605163141518161494337
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
11579208921035624876269744694940757353008614341529031419553363130886709785395l
809ba963-cb81-490e-b171-6f31945b1abe
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
7d73d21f1bd82c9e5268b6dcf9fde2cb
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

POSSIBLE SECRETS
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1 82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99 C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6 9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B 6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1 A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23 BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855 322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C 1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C 6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFF
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c1585 47f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a9 78d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E 8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA9 7B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E 7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394 2643

POSSIBLE SECRETS
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434427757837678 4
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
eyJkYXRhY2VudGVyIjoidXMxIiwia2V5IjoiOWE2YTdjMjcyZTBmYTYzYWY0NzI3ZjViN2FiNDFlYmEwMDM1YWEyNTQwMTg5NzliZjAxOTRhMzhmNmZhOTAyYTc0ZjJlMmRlMmU3NDZmZDdiMzY3NjhkZDE1ZDc3MzBiZTYyNzE5ZmM2NDYxMWFiYmEzMDE3ZWFjZDVkN2VjY2IwNmJhNDJhZTA2MTI2MjI0MWI2NGExYzM2MmE4YzAzNzVmNDU1ZmYxYWNmYjllZjEyYTQyMjEwYjU1YmYxMTQ4ZTZmZGZmNTI1ZjIwOGE4YzVkMmE2NjBiMWMzYjM2NmEuNjdjZTA3NDZjZWFmMTI4ZWE3OTFjNDg4MjhmMTNmMWIuNTI1OTc5MmE4ZTJjYTQ1NTJlNGU1ZGQ1ZjNkZmU0N2Y4MjM1OGQyYTQ3Njc4ZWNmYTJkYzg4OGEzOGVmMmExNyJ9
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
962eddcc369cba8ebb260ee6b6a126d9346e38c5
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFF
1D17C131EFFED802426472B323846B8B6CCF1FEE475419AB28107003A33E82FB
1157920892103562487626974469494075735300861434152903141955336313088670978539 48

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
389C9738-A761-44DE-8A66-1668CFD67DA1
115792089237316195423570985008687907853269984665640564039457584007908834671663
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF
OKg7Qlp4fviuTcJjAPCPwXHw79m
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148

POSSIBLE SECRETS
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
sXchDaQebHnPiGvyDOAT4saGEUetSyo9MKLOoWFsueri23bOdgWp4Dy1WlUzewbgBHod5pcM9H95GQRV3JDXboIRROSBigeC5yjU1hGzHHyXss8UDprecbAYxknTcQkhslANGRUZmdTOQ5qTRsLAt6BTYuyvVRdhS8exSZEy
FDB497E7C6F9D71A89D042B0FA5B7A4DEA5EE7938F08CFDA9F1FB58EBDF749E7
484395612939064517590525852527979142027629495260417479958440807170824046352 86
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112316
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
3071c8717539de5d5353f4c8cd59a032
9760508f15230bccb292b982a2eb840bf0581cf5
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
36134250956749795798585127919587881956611106672985015071877198253568414405109
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB

POSSIBLE SECRETS
b942b7a9a692065540a11292f2e05e6f822589c5
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFF
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbelsiqvdpzGmRF3pex4Ar1HNI
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
Ct4eTlXHBIY2EaV7t7LjJaynVJCpkv4LKjTTAumiGUIuQhrNhZLuF
eoFVMokhb4mMQ2Q3W9dbSSUT33Nhl7XxmI2IL3RMGkaTDC2OULEjN8w3uqcU3HMTPfcWnnexwgsjh4fJR2D8yoA2q8HuLo1hjuzqtDnWvJNmiY4kzlyOkG
57896044618658097711785492504343953926634992332820282019728792003956564819949
8d5155894229d5e689ee01e6018a237e2cae64cd
d67afc830dab717fd163bfcb0b8b88423e9a1a3b
726838724295606890549323807888004534353641360687318060281490199180612328166730772686396383698676545930088884461843637361053498018365439
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCv8IqRRwpH8s7EnWhLwuFqnbTA

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFF
262470350957996892686231567445669818918529234911092133878156159009255188547380500890223880539757197866508724767320 87
nMcadFr9rwxGUMGOn8qIcjLE4vr9T1rxm6DekW9IBGNAwGOynuA+ebTfpfPMYY8nO

PLAYSTORE INFORMATION

Title: Medbridge GO for Patients

Score: 4.9210525 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.medbridgeed.hep.go

Developer Details: Medbridge, Medbridge, None, https://www.medbridgego.com, patient.support@medbridge.com,

Release Date: May 15, 2017 **Privacy Policy:** Privacy link

Description:

Medbridge GO gets you moving! Powered by award-winning content and technology, Medbridge GO is the premier app for you to complete exercises as prescribed by your therapist (PT, OT, AT, or SLP). Two simple steps to get moving: 1. Enter the access code from your provider to download your program 2. Tap ‘GO’ to follow along with

the exercise videos as they play on-screen You can also set reminders, track overall progress, and view all of the Patient Education materials included by your therapist, from 3D models and explanatory exercise videos to clinician notes and PDF guides.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 03:13:45	Generating Hashes	OK
2025-08-31 03:13:50	Extracting APK	OK
2025-08-31 03:13:50	Unzipping	OK
2025-08-31 03:14:00	Parsing APK with androguard	OK
2025-08-31 03:14:00	Extracting APK features using aapt/aapt2	OK
2025-08-31 03:14:00	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 03:14:03	Parsing AndroidManifest.xml	OK
2025-08-31 03:14:03	Extracting Manifest Data	OK

2025-08-31 03:14:03	Manifest Analysis Started	OK
2025-08-31 03:14:03	Reading Network Security config from network_security_config.xml	OK
2025-08-31 03:14:03	Parsing Network Security config	OK
2025-08-31 03:14:03	Performing Static Analysis on: MedBridge GO (com.medbridgeed.hep.go)	OK
2025-08-31 03:14:08	Fetching Details from Play Store: com.medbridgeed.hep.go	OK
2025-08-31 03:14:11	Checking for Malware Permissions	OK
2025-08-31 03:14:11	Fetching icon path	OK
2025-08-31 03:14:11	Library Binary Analysis Started	OK
2025-08-31 03:14:11	Reading Code Signing Certificate	OK
2025-08-31 03:14:12	Running APKiD 2.1.5	OK
2025-08-31 03:14:20	Detecting Trackers	OK

2025-08-31 03:14:23	Decompiling APK to Java with JADX	OK
2025-08-31 03:14:43	Converting DEX to Smali	OK
2025-08-31 03:14:44	Code Analysis Started on - java_source	OK
2025-08-31 03:15:00	Android SBOM Analysis Completed	OK
2025-08-31 03:15:14	Android SAST Completed	OK
2025-08-31 03:15:14	Android API Analysis Started	OK
2025-08-31 03:15:32	Android API Analysis Completed	OK
2025-08-31 03:15:33	Android Permission Mapping Started	OK
2025-08-31 03:15:48	Android Permission Mapping Completed	OK
2025-08-31 03:15:50	Android Behaviour Analysis Started	OK
2025-08-31 03:16:04	Android Behaviour Analysis Completed	OK

2025-08-31 03:16:04	Extracting Emails and URLs from Source Code	OK
2025-08-31 03:16:10	Email and URL Extraction Completed	OK
2025-08-31 03:16:10	Extracting String data from APK	OK
2025-08-31 03:16:10	Extracting String data from Code	OK
2025-08-31 03:16:10	Extracting String values and entropies from Code	OK
2025-08-31 03:16:14	Performing Malware check on extracted domains	OK
2025-08-31 03:16:17	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.