ANDROID STATIC ANALYSIS REPORT

Mindbody (7.77.3)

File Name:	com.mindbodyonline.connect_24603.apk
Package Name:	com.mindbodyonline.connect
Scan Date:	Aug. 31, 2025, 4:49 a.m.
App Security Score:	**46/100 (MEDIUM RISK)**
Grade:	B
Trackers Detection:	11/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	30	3	0	2

FILE INFORMATION

File Name: com.mindbodyonline.connect_24603.apk
Size: 124.27MB
MD5: b0909df02f3392344f9cdc24baa91da5
SHA1: 3e2010d44ae69baa54515c12b187c7d9e9432a83
SHA256: 35f6d06385f16d398bfaf3791e598cd3c0a53369fcf03840412430e99cd6680e

APP INFORMATION

App Name: Mindbody
Package Name: com.mindbodyonline.connect
Main Activity: com.mindbodyonline.connect.activities.TourActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 7.77.3

Android Version Code: 24603

APP COMPONENTS

Activities: 98
Services: 15
Receivers: 24
Providers: 7
Exported Activities: 14
Exported Services: 2
Exported Receivers: 5
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=01, ST=CA, L=San Luis Obispo, O=MINDBODY Inc, OU=Electric Sheep Dreamers, CN=MINDBODY Inc
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-09-20 20:21:33+00:00
Valid To: 2038-09-14 20:21:33+00:00
Issuer: C=01, ST=CA, L=San Luis Obispo, O=MINDBODY Inc, OU=Electric Sheep Dreamers, CN=MINDBODY Inc
Serial Number: 0x2e538e62
Hash Algorithm: sha256
md5: 9db32546bc81a401d1cfd1538f5c7cc3
sha1: a5c1ac60603c5a6dc79757457ab5c9684f358016
sha256: 0011809c3201439766a24478f44ce0d915fcee9508e45de543c875d72c3da136
sha512: 453ec879c2c28de61df80bd1e350d3772eed5f8029cea5e45c235c4e1a8d205c17e312816c4131384e719689758a7bef660c67f1b70de3086682b84134e06953
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 152a8693bde6e77bd8b9d73a12d4f3e340273e5dcec4cb000180717eb5ed89a3
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.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.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.mindbodyonline.connect.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>b0909df02f3392344f9cdc24baa91da5.apk</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
subscriber ID check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
subscriber ID check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
network operator name check
subscriber ID check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes8.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table></td></tr>
<tr><td>classes9.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.mindbodyonline.connect.activities.TourActivity	Schemes: https://, mindbodyconnect://, x-mindbodyconnect-oauth-mindbody://, Hosts: get.mndbdy.ly, mindbody.app.link, mindbody-alternate.app.link, mindbody.test-app.link, mindbody-alternate.test-app.link, authcode,
com.mindbodyonline.connect.activities.workflow.FitbitAccessTokenActivity	Schemes: x-mindbodyconnect-oauth-fitbit://, Hosts: authcode,
com.mindbodyonline.connect.activities.workflow.StravaAccessTokenActivity	Schemes: x-mindbodyconnect-oauth-strava://, Hosts: authcode,
sdk.pendo.io.activities.PendoGateActivity	Schemes: pendo-42d14d29://,

ACTIVITY	INTENT
com.mindbodyonline.connect.sca.SCAAuthorizationActivity	Schemes: x-mindbodyconnect-sca://, Hosts: payment,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.mindbodyonline.connect,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.mindbodyonline.connect,

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **23** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Broadcast Receiver (com.mindbodyonline.connect.services.InstallReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.mindbodyonline.connect.activities.list.services.classes.QualifiedClassesListActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.mindbodyonline.connect.activities.workflow.PaymentMethodsActivity) 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.
6	Activity (com.mindbodyonline.connect.activities.list.services.SessionListActivity) 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
7	Activity (com.mindbodyonline.connect.activities.workflow.ReviewDialogActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.mindbodyonline.connect.activities.workflow.SignInDialogActivity) 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.
9	Activity (com.mindbodyonline.connect.activities.SettingsActivity) 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.
10	Activity (com.mindbodyonline.connect.activities.workflow.FitbitAccessTokenActivity) 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.
11	Activity (com.mindbodyonline.connect.activities.list.SupportActivity) 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.
12	Activity (com.mindbodyonline.connect.activities.workflow.StravaAccessTokenActivity) 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.
13	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.
14	Activity (com.mindbodyonline.connect.sca.SCAAuthorizationActivity) 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
15	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) 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.
16	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) 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.
17	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.
18	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

NO	ISSUE	SEVERITY	DESCRIPTION
19	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.
20	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
21	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.
22	Broadcast Receiver (com.facebook.CampaignTrackingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
23	Activity (androidx.compose.ui.tooling.PreviewActivity) 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
24	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: **0** | WARNING: **4** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				bolts/MeasurementEvent.java coil/memory/MemoryCache.java com/braze/Constants.java com/mindbodyonline/android/api/identity/model/LoginProvider.java com/mindbodyonline/android/api/sales/model/payments/PaymentMethod.java com/mindbodyonline/android/api/sales/model/pos/cart/Metadata.java com/mindbodyonline/android/api/sales/model/pos/catalog/CatalogItem.java com/mindbodyonline/android/api/sales/model/pos/deals/Deal.java com/mindbodyonline/android/api/sales/model/pos/deals/SearchItem.java com/mindbodyonline/android/api/sales/para

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/mindbodyonline/android/api/sales/params/MBSalesAccessParams.java com/mindbodyonline/android/api/subscriber/params/MBSubscriberAccessParams.java com/mindbodyonline/android/auth/okhttp/domain/model/Credentials.java com/mindbodyonline/connect/BuildConfig.java com/mindbodyonline/connect/adapters/filters/ExchangeBusinessFilter.java com/mindbodyonline/connect/adapters/filters/OnlineBookingBusinessFilter.java com/mindbodyonline/connect/stripe/StripePaymentData.java com/mindbodyonline/connect/utils/AnalyticsEventConstantsKt.java com/mindbodyonline/connect/utils/Constants.java com/mindbodyonline/connect/utils/api/gateway/serialization/GatewayResourceType.java com/mindbodyonline/data/services/OAuth2Params.java com/mindbodyonline/data/services/SalesAccessParams.java com/mindbodyonline/framework/abvariant/ABExperimentKeysKt.java com/mindbodyonline/framework/abvariant/ABFeatureVariableKeysKt.java com/mindbodyonline/framework/abvariant/FeatureFlagData.java com/mindbodyonline/ui/screen/booking/model/MarketingUiState.java com/mindbodyonline/views/compose/ConfirmationMarketingViewState.java com/newrelic/agent/android/util/Constants.java com/nimbusds/jose/HeaderParameterNames.java com/nimbusds/jose/jwk/JWKParameterNames.java com/optimizely/ab/android/sdk/OptimizelyDefaultAttributes.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-14	com/optimizely/ab/bucketing/UserProfileService.java com/optimizely/ab/config/Attribute.java com/optimizely/ab/config/EventType.java com/optimizely/ab/config/Experiment.java com/optimizely/ab/config/FeatureFlag.java com/optimizely/ab/config/FeatureVariable.java com/optimizely/ab/config/Variation.java com/optimizely/ab/event/internal/ConversionEvent.java com/optimizely/ab/event/internal/ImpressionEvent.java com/optimizely/ab/event/internal/payload/DecisionMetadata.java com/optimizely/ab/notification/TrackNotification.java com/rokt/core/ui/BaseContract.java com/stripe/android/EphemeralKey.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/NetworkConstantsKt.java com/stripe/android/core/networking/SendAnalyticsRequestV2WorkerKt.java com/stripe/android/customersheet/CustomerSheetContractKt.java com/stripe/android/model/ConfirmStripeIntentParams.java com/stripe/android/model/FinancialConnectionsSession.java com/stripe/android/model/RadarSessionWithHCaptcha.java com/stripe/android/payments/bankaccount/ui/CollectBankAccountViewEffect.java com/stripe/android/stripe3ds2/observability/DefaultSentryConfig.java com/stripe/android/stripe3ds2/transaction/A

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/stripe3ds2/transaction/AcsData.java com/stripe/android/stripe3ds2/transaction/AuthenticationRequestParameters.java com/stripe/android/stripe3ds2/transaction/IntentData.java com/tealium/core/persistence/SqlDataLayer.java defpackage/CoreConstant.java io/opencensus/metrics/AutoValue_LabelKey.java io/opencensus/trace/AutoValue_Tracestate_Entry.java
				bolts/MeasurementEvent.java com/airbnb/lottie/utils/LogcatLogger.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java com/crystal/crystalrangeseekbar/widgets/CrystalRangeSeekbar.java com/crystal/crystalrangeseekbar/widgets/CrystalSeekbar.java com/db/chart/view/ChartView.java com/j256/ormlite/android/AndroidLog.java com/j256/ormlite/logger/LocalLog.java com/jakewharton/disklrucache/DiskLruCache.java com/mindbodyonline/android/api/sales/model/payments/PaymentMethod.java com/mindbodyonline/android/api/sales/model/search/SearchModel.java com/mindbodyonline/android/util/LocaleUtil.java com/mindbodyonline/android/util/SafeGson.java com/mindbodyonline/android/util/api/BackOffPolicy.java com/mindbodyonline/android/util/log/MBLog.java com/mindbodyonline/android/views/Bitmap

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	Util.java com/mindbodyonline/connect/common/components/CurrencyEditText.java com/mindbodyonline/connect/services/InstallReceiver.java com/mindbodyonline/connect/utils/FileUtilsKtKt.java com/mindbodyonline/connect/utils/ImageUtils.java com/mindbodyonline/connect/utils/analytics/FallbackAnalyticsTrackerImpl.java com/mindbodyonline/connect/utils/api/fitnessactivity/fitbit/model/FitbitIntradayDataset.java com/mindbodyonline/connect/utils/api/gateway/model/UserPassesAttributes.java com/mindbodyonline/data/CityDb.java com/mindbodyonline/data/services/http/BackOffPolicy.java com/mindbodyonline/data/sqlcontracts/KeyCitiesJsonDBHelper.java com/mindbodyonline/domain/MobileAppVersion.java com/mindbodyonline/domain/ReviewResponse.java com/mindbodyonline/domain/TimeRange.java com/mindbodyonline/lumber/console/ErrorLog.java com/mindbodyonline/views/FbFriendListRowView.java com/mixpanel/android/mpmetrics/ConfigurationChecker.java com/mixpanel/android/mpmetrics/MPConfig.java com/mixpanel/android/mpmetrics/PersistentIdentity.java com/mixpanel/android/mpmetrics/ResourceReader.java com/mixpanel/android/mpmetrics/SessionMetadata.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mixpanel/android/mpmetrics/SystemInformation.java com/mixpanel/android/util/HttpService.java com/mixpanel/android/util/MPLog.java com/newrelic/agent/android/instrumentation/io/CountingInputStream.java com/newrelic/agent/android/logging/AndroidAgentLog.java com/newrelic/agent/android/logging/ConsoleAgentLog.java com/newrelic/agent/android/logging/Logger.java com/newrelic/agent/android/rum/AppApplicationLifeCycle.java com/newrelic/agent/android/util/AgentBuildOptionsReporter.java com/optimizely/ab/android/sdk/OptimizelyLiteLogger.java com/rokt/roktsdk/internal/util/Logger.java com/stripe/android/core/Logger.java com/stripe/android/core/storage/SharedPreferencesStorage.java com/stripe/android/core/utils/PluginDetector.java com/stripe/android/stripe3ds2/transaction/Logger.java com/stripe/hcaptcha/webview/HCaptchaWebView.java com/theartofdev/edmodo/cropper/CropOverlayView.java io/branch/referral/BranchJsonConfig.java io/branch/referral/BranchLogger.java org/slf4j/helpers/Util.java
3	[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	bo/app/r20.java com/newrelic/agent/android/util/Util.java io/opencensus/trace/SpanId.java io/opencensus/trace/TraceId.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nimbusds/jose/jwk/Curve.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/mq.java com/skydoves/balloon/BalloonPersistence.java
6	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/j256/ormlite/android/compat/ApiCompatibility.java com/j256/ormlite/android/compat/BasicApiCompatibility.java com/j256/ormlite/android/compat/JellyBeanApiCompatibility.java com/newrelic/agent/android/instrumentation/SQLiteInstrumentation.java com/optimizely/ab/android/event_handler/EventSQLiteOpenHelper.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	bo/app/pa0.java bo/app/sq.java com/airbnb/lottie/network/NetworkCache.java com/jakewharton/disklrucache/DiskLruCache.java com/mindbodyonline/android/util/api/request/multipart/MultipartFormRequestBody.java com/nimbusds/jose/util/IOUtils.java com/optimizely/ab/android/shared/Cache.java
00022	Open a file from given absolute path of the file	file	bo/app/ea.java bo/app/fa.java bo/app/ko.java bo/app/rb0.java bo/app/ug0.java bo/app/xc.java com/airbnb/lottie/network/NetworkCache.java com/braze/d0.java com/newrelic/agent/android/util/OfflineStorage.java
00089	Connect to a URL and receive input stream from the server	command network	com/mixpanel/android/util/HttpService.java com/optimizely/ab/android/shared/Client.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00096	Connect to a URL and set request method	command network	com/mixpanel/android/util/HttpService.java
00109	Connect to a URL and get the response code	network command	com/mixpanel/android/util/HttpService.java com/optimizely/ab/android/datafile_handler/DatafileClient.java com/stripe/android/payments/core/authentication/RealRedirectResolver.java
00094	Connect to a URL and read data from it	command network	com/mixpanel/android/util/HttpService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	com/mixpanel/android/util/HttpService.java com/newrelic/agent/android/payload/PayloadSender.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	bolts/AppLinks.java bolts/MeasurementEvent.java
00036	Get resource file from res/raw directory	reflection	bolts/MeasurementEvent.java
00078	Get the network operator name	collection telephony	com/mixpanel/android/mpmetrics/SystemInformation.java com/newrelic/agent/android/util/Connectivity.java
00030	Connect to the remote server through the given URL	network	com/optimizely/ab/android/datafile_handler/DatafileClient.java
00162	Create InetSocketAddress object and connecting to it	socket	com/newrelic/agent/android/util/Reachability.java
00163	Create new Socket and connecting to it	socket	com/newrelic/agent/android/util/Reachability.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://pure-genius-344.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/367590269067/namespaces/firebase:fetch?key=AIzaSyAluLwMd_hs9hSj4ckiSZ7tySRdih5DmlI is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'auto_complete_debounce_time_variable_key': '350', 'auto_complete_min_char_variable_key': '1', 'auto_suggest_sort_variable_value': '-score,distance', 'consumer_agreement_url_key': 'https://co.mindbodyonline.com/legal/consumer-agreement', 'privacy_preferences_url_key': 'https://co.mindbodyonline.com/legal/privacy-policy', 'rokt_tag_id': '2962520505079567949'}, 'state': 'UPDATE', 'templateVersion': '15'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK
Other Common Permissions	6/44	com.google.android.gms.permission.AD_ID, android.permission.READ_CALENDAR, android.permission.ACTIVITY_RECOGNITION, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
pure-genius-344.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
mobile-api.rokt.com	ok	**IP:** 23.210.216.95 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
company.mindbodyonline.com	ok	**IP:** 104.19.233.104 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
mobile-api-demo.rokt.com	ok	**IP:** 54.201.202.254 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
signin.mindbodyonline.com	ok	**IP:** 104.19.233.104 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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

DOMAIN	STATUS	GEOLOCATION
mobile-api.stage.rokt.com	ok	**IP:** 23.210.216.97 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.mindbodyapis.com	ok	**IP:** 104.16.64.230 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mindbody.io	ok	**IP:** 18.238.96.16 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.fitbit.com	ok	**IP:** 142.250.188.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dev.lymberapi.com	ok	No Geolocation information available.
js.hcaptcha.com	ok	**IP:** 104.19.229.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dpapi.mindbodyonline.com	ok	**IP:** 104.19.234.104 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.strava.com	ok	**IP:** 18.155.173.7 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
co.mindbodyonline.com	ok	**IP:** 104.19.234.104 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bit.ly	ok	**IP:** 67.199.248.11 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
support.mindbodyonline.com	ok	**IP:** 34.211.108.47 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
classpass.com	ok	**IP:** 172.64.148.102 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
signin-sandbox.staging.arcusplatform.io	ok	**IP:** 104.18.40.223 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdn.optimizely.com	ok	**IP:** 104.18.66.57 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.staging.arcusplatform.io	ok	**IP:** 172.64.147.33 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
maps.google.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.mindbodyonline.com	ok	**IP:** 104.18.37.240 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mndbdy.ly	ok	**IP:** 18.155.173.94 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
stripe.com	ok	**IP:** 54.189.200.54 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
support.mindbody.io	ok	**IP:** 34.211.108.45 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.fitbit.com	ok	**IP:** 35.244.211.136 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
account.mindbodyonline.com	ok	**IP:** 104.19.233.104 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
help.mindbody.io	ok	**IP:** 104.16.224.74 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

✉ EMAILS

EMAIL	FILE
support@stripe.com app@mindbodyonline.com flexsupport@mindbodyonline.com recommend@mindbodyonline.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
New Relic	Analytics	https://reports.exodus-privacy.eu.org/trackers/130
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412
Optimizely	Analytics	https://reports.exodus-privacy.eu.org/trackers/172

TRACKER	CATEGORIES	URL
Tealium	Analytics	https://reports.exodus-privacy.eu.org/trackers/32

HARDCODED SECRETS

POSSIBLE SECRETS
"class_pass" : "ClassPass"
"com_braze_api_key" : "ac5508c8-18e7-4239-8438-4eda9c408f39"
"com_braze_firebase_cloud_messaging_sender_id" : "367590269067"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"faux_password" : "••••••••••••"
"firebase_database_url" : "https://pure-genius-344.firebaseio.com"
"generic_username" : "User"
"google_api_key" : "AIzaSyAluLwMd_hs9hSj4ckiSZ7tySRdih5DmlI"
"google_crash_reporting_api_key" : "AIzaSyAluLwMd_hs9hSj4ckiSZ7tySRdih5DmlI"

POSSIBLE SECRETS
"mixpanel_project_token" : "8d99d3cb3912a3981289283a8db28928"
"mixpanel_project_token_dev" : "9fedd2481e37a228e10bbb1887da3a5f"
"pass" : "pass"
"pendo_api_key" : "eyJhbGciOiJSUzI1NiIsImtpZCI6IiIsInR5cCI6IkpXVCJ9.eyJkYXRhY2VudGVyIjoidXMiLCJrZXkiOiI4NGNkMWRhNDZiYjdiODhhYzZiM2JkNmMxNjQ4OTU2OTUxZTYyOWRmNjIyNjhkYjkzZGQ2MDNlMDk3M2M4YzM5MDkwMzc1OTVhNTRiMzcyY2ZlMTVjMDM0NjMwZGY1ZDZiNGI3Yjc4YTA0NDMxMTFjNzAzYTEzN2NjNGI2OTJhMDBjMjdmYzE4YWE2MjExNjNhYTljM2VhMzNkODFhNTk4LjE5NmQxNzA3OTcyM2YyNDJlMTU5ZWU2YWM5NWE1Zjc3LmNiYTJjMzZmMDBmOTIzNmQ3YWZkOWZmM2FlOTA1MzIxZDY2ZDI2NTE5N2JkZGI4MTBiNzMzMGY5ZDYxNzA1NDQifQ.mwBTWW8V494yJMRO8r-VaKMA7K4PbrH89Z1yioCb77yKejgFgptucSDcsOlhUV2eBLe4zM-KaXxd8nqOMo4SsLDagO9bhIDH01Q4KlwLXWLdfNrMoL2HJOL_URuOZT8dWVzs2lI0HQvxbl5tcRiXNCO3-eug5CeRsCBlcaorat4"
"pref_key_account" : "pref_key_account_link"
"pref_key_distance_units" : "pref_key_distance_units"
"pref_key_fitbit" : "pref_key_fitbit_link"
"pref_key_google_fit" : "pref_key_google_fit_link"
"pref_key_manage_family_accounts" : "pref_key_manage_family_accounts_link"
"pref_key_manage_notifications" : "pref_key_manage_notifications"
"pref_key_marketing_opt_in" : "pref_key_marketing_opt_in"
"pref_key_notification_phone_led" : "pref_key_notification_phone_led"
"pref_key_notification_sound" : "pref_key_notification_sound"
"pref_key_notification_vibrate" : "pref_key_notification_vibrate"

POSSIBLE SECRETS
"pref_key_notifications" : "pref_key_notifications"
"pref_key_push_notifications" : "pref_key_push_notifications"
"pref_key_ratings_reviews" : "pref_key_ratings_reviews"
"pref_key_strava" : "pref_key_strava_link"
"pref_key_sync_calendar" : "pref_key_sync_calendar"
"pref_key_user_calendar" : "pref_key_user_calendar"
"pref_key_wallet" : "pref_key_wallet_link"
"session_list_title" : "Passes"
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF
410583637251521421293261297800472684091144410159937255548352563140394674012 91
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B
32670510020758816978083085130507043184471273380659243275938904335757337482424
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF
55066263022277343669578718895168534326250603453777594175500187360389116729240
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF
6d141922977cb366235d02db78e82fcc63a41a2a99d0abd8bc9f6d91a2672e4e
115792089237316195423570985008687907852837564279074904382605163141518161494337
90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73
61d4fcde-9805-4a44-b7d8-93e6f431071c
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 9
115792089210356248762697446949407573530086143415290314195533631308867097853951

POSSIBLE SECRETS
013602400437880159360205052
26617408020502170632287687167233609607298591687569731477066713684188029449964278084915450806277719023520942412250655586621571135455709168141616373158959998 46
68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403803403728088927070054 49
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871
115792089210356248762697446949407573529996955224135760342422259061068512044369
90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D
AIzaSyCFpOClu9ApN1clR60X6XcDAtc0NpVt8G8
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
c235faf53f097f81e277aca36ec92070d13d21d2e6384d63deeb54fe8edb672a
AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
7a128b7bad5631fea812488c0646cd564ef70e86aaf11e96398c4080b42dffe3
85fe02ee70d1cf1a3baf959a25452a5602643abd
962eddcc369cba8ebb260ee6b6a126d9346e38c5
01d15abd-828a-db40-9ce9-e5dd3ac17f2e

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFF
115792089210356248762697446949407573530086143415290314195533631308867097853948
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF
115792089237316195423570985008687907853269984665640564039457584007908834671663
70665a0f2bdecec3a997721ff3dff0eed22711c28100bb5319ba6e0cd0c27476
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
38489367533689072d7cce494fc6aa7b
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
51db878fb0f26ac0cbdfedee9f4fd867
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
48439561293906451759052585252797914202762949526041747995844080717082404635286
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
9760508f15230bccb292b982a2eb840bf0581cf5
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
36134250956749795798585127919587881956611106672985015071877198253568414405109

POSSIBLE SECRETS
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFF
dcb428fea25c40e7b99f81ae5981ee6a
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
deca87e736574c5c83c07314051fd93a
8d5155894229d5e689ee01e6018a237e2cae64cd
C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE428782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562CE1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83
465a723fa7f2f379b8dbc67e696f4fd6
4a29ba44b6813ca6b7ff0247f804c589
e5e7c6eb-1189-a2c9-dda4-7d4bd6d76292

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFF
2624703509579968926862315674456698189185292349110921338781561590092551885473805008902238805397571978665087247673208 7

PLAYSTORE INFORMATION

Title: Mindbody: Fitness & Wellness

Score: 4.7958317 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.mindbodyonline.connect

Developer Details: MINDBODY Inc, MINDBODY+Inc, None, https://mindbody.io/mindbody-app, support@mindbodyonline.com,

Release Date: Oct 4, 2013 **Privacy Policy:** Privacy link

Description:

Mindbody is the world's #1 booking platform for fitness, beauty, and wellness experiences. We encourage people to try new things and find what makes them feel physically, mentally, and spiritually their best. Whether it's a class, salon service, or meditation session, we've got options. With over 40k+ studios around the world, we offer top fitness classes like yoga, Pilates, barre, dance, HIIT, bootcamp, and more. Looking for something along the lines of a massage, hair treatment, or cryotherapy? We've got that too. Plus, you'll find promoted intro offers and last-minute deals—it's all on the app. How it works: • Download the free app, then create a Mindbody account (or log in to your existing account) to get started. • Enter your location at the top of the screen to see local intro offers, price drops, and deals near you. • Looking for something in particular? Jump to the "SEARCH" icon at the bottom of the window to find businesses near you. From there, you can type in the desired service or browse popular categories. • Need to refine your results? Filter your search by business, class, date, time, distance, or category. You can also sort based on what's recommended, top-rated or closest to you. • Once you select a class or appointment, you can read up on reviews, instructor & service provider bios, and how to get there. You can also choose a business first to learn more about their amenities, schedule, services, location, and pricing. • When you're ready to secure your service, select the "Book" button in the right-hand corner. From there, you will be asked to confirm your payment information. Plug in your info, then hit "BOOK AND BUY" to make it official. Why you'll love it: Variety: You've got local fitness, beauty, salon, spa, and wellness options in the palm of your hand—you decide what works for you. Value: You'll get the best deals to try a new studio or drop-in on a fitness class without committing to a membership. Verified reviews: Know what people are saying about services before you book, with reviews from verified users. *Flexible Pricing available in the US only *Continued use of GPS running in the background can dramatically decrease battery life

SCAN LOGS

Timestamp	Event	Error
2025-08-31 04:49:19	Generating Hashes	OK
2025-08-31 04:49:20	Extracting APK	OK
2025-08-31 04:49:20	Unzipping	OK
2025-08-31 04:49:20	Parsing APK with androguard	OK
2025-08-31 04:49:21	Extracting APK features using aapt/aapt2	OK
2025-08-31 04:49:22	Getting Hardcoded Certificates/Keystores	OK

2025-08-31 04:49:25	Parsing AndroidManifest.xml	OK
2025-08-31 04:49:25	Extracting Manifest Data	OK
2025-08-31 04:49:25	Manifest Analysis Started	OK
2025-08-31 04:49:27	Performing Static Analysis on: Mindbody (com.mindbodyonline.connect)	OK
2025-08-31 04:49:27	Fetching Details from Play Store: com.mindbodyonline.connect	OK
2025-08-31 04:49:27	Checking for Malware Permissions	OK
2025-08-31 04:49:27	Fetching icon path	OK
2025-08-31 04:49:27	Library Binary Analysis Started	OK
2025-08-31 04:49:27	Reading Code Signing Certificate	OK
2025-08-31 04:49:29	Running APKiD 2.1.5	OK

2025-08-31 04:49:40	Detecting Trackers	OK
2025-08-31 04:49:50	Decompiling APK to Java with JADX	OK
2025-08-31 05:11:33	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/b0909df02f3392344f9cdc24baa91da5/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/b0909df02f3392344f9cdc24baa91da5/b0909df02f3392344f9cdc24baa91da5.apk'], 999.9999812170863)
2025-08-31 05:11:33	Converting DEX to Smali	OK
2025-08-31 05:11:33	Code Analysis Started on - java_source	OK
2025-08-31 05:11:42	Android SBOM Analysis Completed	OK
2025-08-31 05:11:55	Android SAST Completed	OK
2025-08-31 05:11:55	Android API Analysis Started	OK
2025-08-31 05:12:04	Android API Analysis Completed	OK
2025-08-31 05:12:04	Android Permission Mapping Started	OK

2025-08-31 05:12:11	Android Permission Mapping Completed	OK
2025-08-31 05:12:12	Android Behaviour Analysis Started	OK
2025-08-31 05:12:23	Android Behaviour Analysis Completed	OK
2025-08-31 05:12:23	Extracting Emails and URLs from Source Code	OK
2025-08-31 05:12:25	Email and URL Extraction Completed	OK
2025-08-31 05:12:25	Extracting String data from APK	OK
2025-08-31 05:12:26	Extracting String data from Code	OK
2025-08-31 05:12:26	Extracting String values and entropies from Code	OK
2025-08-31 05:12:30	Performing Malware check on extracted domains	OK
2025-08-31 05:12:37	Saving to Database	OK

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.