ANDROID STATIC ANALYSIS REPORT

🤖 Macadam (5.2.0)

File Name:	com.macadamapp_249.apk
Package Name:	com.macadamapp
Scan Date:	Aug. 31, 2025, 1:44 a.m.
App Security Score:	**47/100 (MEDIUM RISK)**

B

Grade:

Trackers Detection: 16/432

FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
5	32	1	2	1

FILE INFORMATION

File Name: com.macadamapp_249.apk
Size: 74.04MB
MD5: 0088335c2392e56a60a22f4e2e8373f9
SHA1: 011776c3eb629dccc00777c4a05a392b06a7292a
SHA256: ef296f986e58bb129315c93c1faf86b56999a67ca122763208010df851650e56

APP INFORMATION

App Name: Macadam
Package Name: com.macadamapp

Main Activity: com.macadamapp.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 5.2.0
Android Version Code: 249

APP COMPONENTS

Activities: 72
Services: 34
Receivers: 30
Providers: 19
Exported Activities: 6
Exported Services: 3
Exported Receivers: 11
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-07-23 22:54:37+00:00
Valid To: 2052-07-23 22:54:37+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe6a40d4f875d15605fee2762352f60f44df0d8c9
Hash Algorithm: sha256
md5: 2d89e43df38cafd9e76753a357c9d0d8
sha1: 916129316aaab42c82dba794f0bd0e3b9a60ed03
sha256: 90248a07336dc1be6a265f44e0926efc98b5995aed5a9b71d6564690dabf2ba4
sha512: 66312f9eb6edfa7023d2d8f150230c2cb50488d9b197469e64ec1627468b884e07d26a1aa9b2798893e7d5a573ab4b25209a15e54a7c8f6bafbc2833dcb0efab
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 484720f932283688081f2e85201fa4948a990a72aa6be21d1deec2169831483b
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_HEALTH	normal	enables foreground services with health-related functionality.	Allows a regular application to use Service.startForeground with the type "health".
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.macadamapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.

🔊 APKID ANALYSIS

FILE	DETAILS	
0088335c2392e56a60a22f4e2e8373f9.apk	**FINDINGS**	**DETAILS**
	Anti-VM Code	emulator file check possible VM check

FILE	DETAILS	
assets/audience_network.dex	**FINDINGS**	**DETAILS**
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)
classes.dex	**FINDINGS**	**DETAILS**
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check
	Compiler	unknown (please file detection issue!)
classes2.dex	**FINDINGS**	**DETAILS**
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.kernel.qemu check emulator file check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)

FILE	DETAILS
classes3.dex	**FINDINGS** / **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check Compiler — unknown (please file detection issue!)
classes4.dex	**FINDINGS** / **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check SIM operator check network operator name check ro.kernel.qemu check possible VM check Anti Debug Code — Debug.isDebuggerConnected() check Compiler — unknown (please file detection issue!)

FILE	DETAILS		

	FINDINGS	DETAILS
classes5.dex	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check Build.BOARD check SIM operator check network operator name check device ID check possible VM check
	Compiler	unknown (please file detection issue!)

	FINDINGS	DETAILS
classes6.dex	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	unknown (please file detection issue!)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.macadamapp.MainActivity	Schemes: com.macadamapp://, macadam://, http://, https://, Hosts: www.macadam.app,
net.openid.appauth.RedirectUriReceiverActivity	Schemes: macadam.auth://, "macadam.auth"://,
com.moengage.sdk.debugger.MoEDebuggerActivity	Schemes: moengage://, Hosts: debugger,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,

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

🔒 NETWORK SECURITY

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: **1** | WARNING: **22** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
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 (net.openid.appauth.RedirectUriReceiverActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (com.moengage.firebase.MoEFireBaseMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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
7	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) 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.
8	Activity (com.appsamurai.appsprize.ui.AptActivity) 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	Broadcast Receiver (com.appsamurai.appsprize.service.AppsPrizeInstallReceiver) 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.
10	Broadcast Receiver (io.adjoe.sdk.internal.AdjoePackageInstallReceiver) 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.
11	Activity (com.moengage.sdk.debugger.MoEDebuggerActivity) 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	Broadcast Receiver (io.adjoe.protection.PhoneVerificationBroadcastReceiver) 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.
13	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.
14	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.
15	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.google.firebase.auth.internal.RecaptchaActivity) 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 (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.
18	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
19	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.
20	Broadcast Receiver (com.mbridge.msdk.foundation.same.broadcast.NetWorkChangeReceiver) 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.
21	Activity (app.notifee.core.NotificationReceiverActivity) 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.
22	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) 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.
23	Broadcast Receiver (com.ogury.core.internal.LogEnablerReceiver) 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.

</> CODE ANALYSIS

HIGH: **3** | WARNING: **8** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/adjust/sdk/Util.java com/applovin/impl/wj.java com/fyber/inneractive/sdk/player/exoplayer2/upstream/cache/i.java com/inmobi/media/V1.java com/mbridge/msdk/playercommon/exoplayer2/source/ShuffleOrder.java com/mbridge/msdk/playercommon/exoplayer2/trackselection/RandomTrackSelection.java g/c.java io/grpc/internal/g0.java ux/a.java ux/b.java vx/a.java
				a0/v0.java a20/c.java a5/a.java ae/e.java app/notifee/core/Logger.java bc/a.java bc/g.java bh/g.java bt/c.java bt/f.java c10/a.java c2/f.java c9/a0.java c9/l.java c9/o.java c9/s.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cb/f.java
				FileF.java
				com/adjust/sdk/sig/NativeLibHelper.java
				com/adjust/sdk/sig/Signer.java
				com/adjust/sdk/sig/d.java
				com/applovin/impl/oc.java
				com/applovin/impl/sdk/n.java
				com/bumptech/glide/load/data/b.java
				com/bumptech/glide/load/data/l.java
				com/fyber/inneractive/sdk/logger/a.java
				com/fyber/inneractive/sdk/player/cache/f.java
				com/fyber/inneractive/sdk/player/exoplayer2/extractor/mp4/q.java
				com/fyber/inneractive/sdk/player/exoplayer2/mediacodec/a.java
				com/fyber/inneractive/sdk/player/exoplayer2/mediacodec/j.java
				com/fyber/inneractive/sdk/player/exoplayer2/text/cea/a.java
				com/fyber/inneractive/sdk/player/exoplayer2/upstream/cache/l.java
				com/fyber/inneractive/sdk/player/exoplayer2/upstream/y.java
				com/fyber/inneractive/sdk/player/exoplayer2/util/b.java
				com/fyber/inneractive/sdk/player/exoplayer2/util/c.java
				com/fyber/inneractive/sdk/player/exoplayer2/util/l.java
				com/henninghall/date_picker/pickers/AndroidNative.java
				com/iab/omid/library/applovin/utils/d.java
				com/iab/omid/library/fyber/utils/d.java
				com/iab/omid/library/inmobi/utils/d.java
				com/iab/omid/library/ironsrc/utils/d.java
				com/iab/omid/library/mmadbridge/utils/d.java
				com/iab/omid/library/ogury/utils/d.java
				com/iab/omid/library/vungle/utils/d.java
				com/inmobi/media/AbstractC2905o6.java
				com/inmobi/media/C3063zb.java
				com/inmobi/media/Z2.java
				com/json/av.java
				com/json/kg.java
				com/json/l9.java
				com/json/m4.java
				com/json/mediationsdk/logger/a.java
				com/json/sdk/utils/Logger.java
				com/json/tk.java
				com/learnium/RNDeviceInfo/d.java
				com/lugg/RNCConfig/RNCConfigModule.java
				com/mapbox/common/LogBackend.java
				com/mapbox/common/Logger.java
				com/mapbox/common/MapboxMapsAndroidLogger.java
				com/mapbox/common/RunloopErrorHandler.java
				com/mapbox/common/location/compat/permissions/PermissionsManager.java
				com/mapbox/common/logger/MapboxLogger$d$1.java
				com/mapbox/common/logger/MapboxLogger$e$1.java
				com/mapbox/common/logger/MapboxLogger$i$1.java
				com/mapbox/common/logger/MapboxLogger$v$1.java
				com/mapbox/common/logger/MapboxLogger$w$1.java
				com/mapbox/common/module/provider/MapboxModuleProvider.java
				com/mapbox/maps/FontUtils.java
				com/mbridge/msdk/dycreator/bus/EventBus.java
				com/mbridge/msdk/dycreator/engine/a.java
				com/mbridge/msdk/dycreator/utils/g.java
				com/mbridge/msdk/foundation/controller/b.java
				com/mbridge/msdk/foundation/tools/l0.java
				com/mbridge/msdk/foundation/tools/o0.java
				com/mbridge/msdk/newreward/function/cache/controller/a.java
				com/mbridge/msdk/playercommon/exoplayer2/drm/ClearKeyUtil.java
				com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/PsshAtomUtil.java
				com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/TrackEncryptionBox.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mbridge/msdk/playercommon/exoplayer2/extractor/ogg/VorbisUtil.java
				com/mbridge/msdk/playercommon/exoplayer2/mediacodec/MediaCodecInfo.java
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	com/mbridge/msdk/playercommon/exoplayer2/mediacodec/MediaCodecUtil.java com/mbridge/msdk/playercommon/exoplayer2/source/chunk/ChunkedTrackBlacklistUtil.java com/mbridge/msdk/playercommon/exoplayer2/text/dvb/DvbParser.java com/mbridge/msdk/playercommon/exoplayer2/text/webvtt/WebvttCue.java com/mbridge/msdk/playercommon/exoplayer2/upstream/Loader.java com/mbridge/msdk/playercommon/exoplayer2/upstream/cache/CachedRegionTracker.java com/mbridge/msdk/playercommon/exoplayer2/util/AtomicFile.java com/mbridge/msdk/playercommon/exoplayer2/util/NalUnitUtil.java com/mbridge/msdk/playercommon/exoplayer2/util/Util.java com/mbridge/msdk/playercommon/exoplayer2/video/DummySurface.java com/mbridge/msdk/tracker/b.java com/mbridge/msdk/tracker/c.java com/mbridge/msdk/tracker/j.java com/mbridge/msdk/tracker/m.java com/mbridge/msdk/tracker/network/e0.java com/mbridge/msdk/tracker/y.java com/mbridge/msdk/widget/FeedbackRadioGroup.java com/ogury/ad/internal/r2.java com/reactnative/ivpusic/imagepicker/a.java com/reactnativecommunity/asyncstorage/c.java com/reactnativegooglesignin/b.java com/reactnativemmkv/MmkvModule.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/tapjoy/TJCurrencyParameters.java com/tapjoy/TJEventOptimizer.java com/tapjoy/TJWebViewJSInterface.java com/tapjoy/TapjoyAdIdClient.java com/tapjoy/TapjoyAppSettings.java com/tapjoy/TapjoyCache.java com/tapjoy/TapjoyCacheMap.java com/tapjoy/TapjoyCachedAssetData.java com/tapjoy/TapjoyGpsHelper.java com/tapjoy/TapjoyURLConnection.java com/tapjoy/TapjoyUtil.java com/tapjoy/d0.java com/tapresearch/tapsdk/utils/LogUtils.java com/vungle/ads/internal/util/o.java com/yalantis/ucrop/task/BitmapCropTask.java cu/e.java dw/g.java dx/c.java e10/d.java e4/d.java f4/a.java g/c.java g4/n.java gi/v.java hr/h.java hw/h0.java hw/o0.java hw/p0.java hw/v0.java i9/q.java i9/r.java io/adjoe/sdk/internal/g1.java io/adjoe/sdk/internal/o1.java io/adjoe/sdk/internal/x0.java io/invertase/firebase/app/a.java io/legere/pdfiumandroid/DefaultLogger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j9/d.java
				k0/z.java
				kl/d.java
				kt/a.java
				l5/a.java
				l7/b.java
				l9/d.java
				l9/k.java
				lb/d.java
				m10/i.java
				mk/u0.java
				n/c.java
				n20/g.java
				n5/h.java
				n8/a.java
				n9/b.java
				o10/b.java
				os/h.java
				os/j4.java
				os/j5.java
				os/m1.java
				os/q4.java
				os/w.java
				os/y0.java
				p5/a.java
				p9/a.java
				pr/a.java
				pr/k.java
				q8/a.java
				r8/d.java
				r8/e.java
				s4/b.java
				s4/d.java
				s5/a.java
				sg/b.java
				t5/k0.java
				tf/d.java
				tg/b.java
				u8/e.java
				v8/q.java
				vi/c.java
				w8/i.java
				w8/j.java
				we/k.java
				x8/i.java
				xq/p2.java
				y8/a.java
				yg/f.java
				z4/a.java
				z8/c.java
				z8/u.java
				ze/a.java
				zf/i.java
				zn/c.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	ai/a.java ci/r.java coil/memory/MemoryCache.java com/adjust/sdk/Constants.java com/applovin/impl/sdk/AppLovinSdkInitializationConfigurationImpl.java com/applovin/mediation/MaxSegment.java com/inmobi/media/C2841jc.java com/json/CachedResponse.java com/json/InitConfig.java com/json/kq.java com/json/mediationsdk/adquality/AdQualityBridgeKt.java com/json/mediationsdk/adunit/adapter/utility/AdOptionsPosition.java com/json/mediationsdk/utils/IronSourceConstants.java com/json/um.java com/macadamapp/BuildConfig.java com/mapbox/maps/ThreadChecker.java com/mapbox/maps/plugin/animation/MapAnimationOwnerRegistry.java com/mbridge/msdk/MBridgeConstans.java com/mbridge/msdk/foundation/download/core/DownloadCommon.java com/mbridge/msdk/newreward/player/imodel/IBigTempModel.java com/mbridge/msdk/newreward/player/imodel/IMoreOfferModel.java com/mbridge/msdk/newreward/player/iview/IBaseWebView.java com/mbridge/msdk/newreward/player/iview/IMetaData.java com/mbridge/msdk/newreward/player/iview/IPlayTempleView.java com/ogury/core/internal/GppConsentConstants.java com/tapjoy/TapjoyConstants.java com/tapresearch/tapsdk/models/PlacementCustomParameters.java com/tapresearch/tapsdk/storage/PreferenceManager.java com/tapresearch/tapsdk/utils/TapConstants.java com/vungle/ads/internal/l.java f6/d.java fh/b.java gn/e.java hj/b.java io/adjoe/sdk/internal/SharedPreferencesProvider.java io/grpc/internal/q2.java mk/o0.java p1/k1.java t8/g.java v8/d.java v8/p.java v8/x.java vm/b.java xq/d5.java xq/d6.java zq/d.java
4	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/fyber/inneractive/sdk/player/exoplayer2/extractor/hls/a.java com/json/mediationsdk/utils/IronSourceAES.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	eh/i.java n8/g.java zf/w.java
6	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/mbridge/msdk/playercommon/exoplayer2/util/Util.java li/c.java pr/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	com/ReactNativeBlobUtil/i.java com/json/sdk/controller/s.java com/json/sdk/utils/SDKUtils.java com/mbridge/msdk/foundation/tools/l0.java com/ogury/ad/internal/x3.java fi/m.java
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/applovin/mediation/adapters/facebook/BuildConfig.java com/applovin/mediation/adapters/google/BuildConfig.java com/applovin/mediation/adapters/inmobi/BuildConfig.java com/applovin/mediation/adapters/inneractive/BuildConfig.java com/applovin/mediation/adapters/ironsource/BuildConfig.java com/applovin/mediation/adapters/mintegral/BuildConfig.java com/applovin/mediation/adapters/ogurypresage/BuildConfig.java com/applovin/mediation/adapters/vungle/BuildConfig.java dd/a.java
9	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/json/v9.java com/mbridge/msdk/foundation/db/g.java com/mbridge/msdk/tracker/b.java com/reactnativecommunity/asyncstorage/g.java df/t0.java io/adjoe/sdk/internal/DatabaseContentProvider.java io/adjoe/sdk/internal/n2.java jl/e.java
10	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	ce/a.java com/applovin/impl/sdk/utils/StringUtils.java com/json/sdk/utils/SDKUtils.java com/tapjoy/TapjoyUtil.java os/a4.java ov/b.java ta/c.java
11	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/json/environment/IronSourceSharedPreferencesUtilities.java
12	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/fyber/inneractive/sdk/player/cache/m.java com/json/sdk/utils/SDKUtils.java com/reactnative/ivpusic/imagepicker/a.java com/tapjoy/TapjoyCache.java i7/c.java l7/a.java qa/a.java
13	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/mbridge/msdk/thrid/okhttp/internal/c.java hr/h.java
14	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/applovin/impl/adview/AppLovinWebViewBase.java os/j5.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

⛓ BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	com/mbridge/msdk/newreward/function/utils/c.java com/tapjoy/TapjoyUtil.java fh/f.java lh/a.java li/c.java
00013	Read file and put it into a stream	file	bt/e.java com/bumptech/glide/load/a.java com/fyber/inneractive/sdk/network/D.java com/fyber/inneractive/sdk/player/cache/f.java com/fyber/inneractive/sdk/player/cache/j.java com/fyber/inneractive/sdk/player/exoplayer2/upstream/f.java com/fyber/inneractive/sdk/player/exoplayer2/util/c.java com/inmobi/media/Bb.java com/mbridge/msdk/dycreator/engine/a.java com/mbridge/msdk/newreward/function/utils/c.java com/mbridge/msdk/playercommon/exoplayer2/upstream/ContentDataSource.java com/mbridge/msdk/playercommon/exoplayer2/upstream/RawResourceDataSource.java com/mbridge/msdk/playercommon/exoplayer2/util/AtomicFile.java com/reactnativecommunity/asyncstorage/c.java com/tapjoy/TapjoyUtil.java fh/f.java ie/i.java io/adjoe/sdk/internal/w1.java j20/b.java lh/a.java li/c.java m7/d.java q8/a.java z7/h.java
00094	Connect to a URL and read data from it	command network	ce/c.java com/fyber/inneractive/sdk/web/c0.java ih/a.java kl/b.java
00028	Read file from assets directory	file	com/fyber/inneractive/sdk/player/exoplayer2/upstream/C2581d.java com/mbridge/msdk/playercommon/exoplayer2/upstream/AssetDataSource.java
00030	Connect to the remote server through the given URL	network	com/adjust/sdk/AdjustLinkResolution.java com/fyber/inneractive/sdk/util/r.java com/fyber/inneractive/sdk/web/c0.java com/tapjoy/TapjoyCache.java com/tapjoy/TapjoyURLConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	agency/flexible/react/modules/email/EmailModule.java com/fyber/inneractive/sdk/util/F.java com/inmobi/media/Z2.java com/json/au.java com/reactnativebatteryoptimizationcheck/BatteryOptimizationCheckModule.java io/adjoe/sdk/internal/p0.java mk/a.java n8/b.java net/openid/appauth/c.java o6/n.java rl/a.java y00/n.java
00132	Query The ISO country code	telephony collection	com/applovin/impl/xp.java
00022	Open a file from given absolute path of the file	file	com/json/sdk/utils/IronSourceStorageUtils.java com/mbridge/msdk/foundation/download/utils/Objects.java com/reactnative/ivpusic/imagepicker/a.java com/reactnative/ivpusic/imagepicker/e.java com/tapjoy/TapjoyCache.java com/tapjoy/TapjoyUtil.java fh/f.java he/d.java i7/c.java ka/c.java m7/d.java p5/a.java qa/a.java
00012	Read data and put it into a buffer stream	file	com/tapjoy/TapjoyUtil.java m7/d.java
00089	Connect to a URL and receive input stream from the server	command network	ce/c.java com/fyber/inneractive/sdk/util/r.java com/fyber/inneractive/sdk/web/c0.java com/tapjoy/TapjoyCache.java com/tapjoy/TapjoyURLConnection.java kl/b.java mk/o0.java mk/w1.java mk/x1.java
00109	Connect to a URL and get the response code	network command	ce/c.java com/fyber/inneractive/sdk/util/r.java com/fyber/inneractive/sdk/web/c0.java com/tapjoy/TapjoyCache.java com/tapjoy/TapjoyURLConnection.java kl/b.java mk/o0.java mk/w1.java mk/x1.java
00108	Read the input stream from given URL	network command	ce/c.java com/fyber/inneractive/sdk/web/c0.java kl/b.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/fyber/inneractive/sdk/util/V.java com/inmobi/media/C3063zb.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/dylanvann/fastimage/FastImageSource.java com/json/environment/CrashProvider.java io/adjoe/sdk/internal/DatabaseContentProvider.java x6/e.java
00091	Retrieve data from broadcast	collection	expo/modules/location/services/LocationTaskService.java
00078	Get the network operator name	collection telephony	com/mapbox/maps/module/telemetry/PhoneState.java com/tapresearch/tapsdk/utils/ConnectionUtils.java jl/l.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	agency/flexible/react/modules/email/EmailModule.java com/json/au.java com/reactnativebatteryoptimizationcheck/BatteryOptimizationCheckModule.java n8/b.java rl/a.java y00/n.java
00005	Get absolute path of file and put it to JSON object	file	com/json/sdk/utils/IronSourceStorageUtils.java com/tapjoy/TapjoyCache.java com/tapjoy/TapjoyUtil.java fh/f.java
00015	Put buffer stream (data) to JSON object	file	com/tapjoy/TapjoyUtil.java
00123	Save the response to JSON after connecting to the remote server	network command	com/tapjoy/TapjoyCache.java
00163	Create new Socket and connecting to it	socket	com/mbridge/msdk/thrid/okhttp/internal/platform/g.java com/tapjoy/TapjoyCache.java
00096	Connect to a URL and set request method	command network	ce/c.java com/tapjoy/TapjoyURLConnection.java kl/b.java mk/o0.java mk/w1.java mk/x1.java
00026	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java ny/a.java ny/b.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java io/adjoe/sdk/internal/n2.java jl/e.java
00189	Get the content of a SMS message	sms	i7/c.java ta/f.java
00188	Get the address of a SMS message	sms	i7/c.java ta/f.java
00200	Query data from the contact list	collection contact	i7/c.java ta/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00201	Query data from the call log	collection calllog	i7/c.java ta/f.java
00192	Get messages in the SMS inbox	sms	i7/c.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	i7/c.java
00191	Get messages in the SMS inbox	sms	i7/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	i7/c.java io/adjoe/sdk/internal/SharedPreferencesProvider.java s4/b.java s4/d.java
00085	Get the ISO country code and put it into JSON	collection telephony	com/reactnativedevicecountry/DeviceCountryModule.java
00112	Get the date of the calendar event	collection calendar	zn/c.java
00029	Initialize class object dynamically	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00157	Instantiate new object using reflection, possibly used for dexClassLoader	reflection dexClassLoader	com/mapbox/common/module/provider/MapboxModuleProvider.java
00046	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00161	Perform accessibility service action on accessibility node info	accessibility service	g4/n.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	g4/n.java
00187	Query a URI and check the result	collection sms calllog calendar	io/adjoe/sdk/internal/SharedPreferencesProvider.java s4/d.java
00004	Get filename and put it to JSON object	file collection	com/json/sdk/utils/IronSourceStorageUtils.java
00162	Create InetSocketAddress object and connecting to it	socket	com/mbridge/msdk/thrid/okhttp/internal/platform/g.java
00202	Make a phone call	control	rl/a.java
00203	Put a phone number into an intent	control	rl/a.java

⛁ FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/2233710485/namespaces/firebase:fetch?key=AIzaSyAtaRzfHJUd3i1gzNggk7STSSJJK4vpZ04 is enabled. Ensure that the configurations are not sensitive. This 'booster_redirection_url': 'macadam://deal/booking-jr7wlvrd', 'challenges_deprecation_message': 'true', 'computer_extension_enabled': 'false', 'crashlytics_logs_enabled': 'false', 'daily_lottery_amount': '100000', 'deals_enabled': 'true', 'emails_review 'home_card_survey_image': '', 'home_deals_enabled': 'true', 'home_highlights_enabled': 'true', 'interstitial_enabled': 'false', 'interval_ad_mins_enabled': 'false', 'knock_enabled': 'false', 'list_event_disabled': '{"view": ["home","step_submit_modal","step_submit_slide","ranking_friends","balance","map_onboarding","profile","permission_notification","map_spot_wall_fame","map_spot","map_coins","app_rating_modal","step_submit_slide_freezer","step_submit_ ["step_submit_closed","native_ad_loaded","native_ad_load_failed","interstitial_ad_loaded","interstitial_ad_load_failed","interstitial_ad_clicked","interstitial_ad_displayed","interstitial_ad_hidden","ad_load_success","ad_load_failed","ad_display_succ 'location_service': 'expo', 'location_service_events_enabled': 'false', 'log_step_errors': 'false', 'map_enabled': 'true', 'max_amount_affiliate': '8000', 'max_amount_offerwall': '10000', 'max_amount_survey': '5000', 'messenger_enabled': 'false', 'mrec_e 'pre_signup_enabled': 'false', 'product_tour_enabled': 'false', 'profile_enabled': 'true', 'publish_service_enabled': 'true', 'qa_testers_idfa': '{"idfa":["E0D6257E-8919-48FA-BAC4-E7869D425E71","95466D59-B929-42DD-A167-BDD36EF2F603","10F55EF E38B104C5F0E","A0DF42AA-832E-4C52-A713-FB6B7D0EAB7D"]}', 'quests_enabled': 'true', 'referral_qr_code_enabled': 'false', 'refresh_user_position': '3', 'reviews_enabled': 'true', 'show_home_banners': 'true', 'show_install_google_fit': 'false', 'show 'use_new_deal_endpoint': 'false', 'use_new_method_steps': 'false', 'verify_email_enabled': '{"global":true,"offerwall_enabled":false}', 'watch_and_play_ads_enabled': 'false'}, 'state': 'UPDATE', 'templateVersion': '299'}

⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_CONTACTS, android.permission.CAMERA, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO
Other Common Permissions	10/44	android.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.PACKAGE_USAGE_STATS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.ACCESS_NOTIFICATION_POLICY

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
pinterest.com	ok	**IP:** 151.101.0.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
s.staging.cloud.ogury.io	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.surveyb.in	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
connect.tapjoy.com	ok	**IP:** 3.220.173.35 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
subscription.adjust.io	ok	**IP:** 185.151.204.44 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
wss.pollfish.com	ok	**IP:** 34.69.135.100 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
developers.google.com	ok	**IP:** 142.250.72.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
s-s.devc.cloud.ogury.io	ok	No Geolocation information available.
192.168.1.35	ok	**IP:** 192.168.1.35 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
app.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
app.adjust.com	ok	**IP:** 185.151.204.11 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
plus.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
s.devc.cloud.ogury.io	ok	No Geolocation information available.
gdpr.adjust.com	ok	**IP:** 185.151.204.50 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
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
s.presage.io	ok	No Geolocation information available.
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
tizen.org	ok	**IP:** 18.155.173.54 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
o-ext.mediation.unity3d.com	ok	**IP:** 18.238.96.94 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ws.tapjoyads.com	ok	**IP:** 18.238.109.83 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.250.72.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
s-s.deva.cloud.ogury.io	ok	No Geolocation information available.
exoplayer.dev	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ssrv.adjust.com	ok	**IP:** 185.151.204.2 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api.qa.appsamurai.com	ok	**IP:** 52.212.109.206 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
auth.surveyb.in	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
auth.surveyb.dev	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
subscription.s	ok	No Geolocation information available.
unif-id.ssp.inmobi.com	ok	**IP:** 35.212.40.129 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.895111 **Longitude:** -77.036369 **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

DOMAIN	STATUS	GEOLOCATION
192.168.1.105	ok	**IP:** 192.168.1.105 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
cdn2.inner-active.mobi	ok	**IP:** 151.101.195.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.mapbox.com	ok	**IP:** 18.238.96.71 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
gdpr.adjust.io	ok	**IP:** 185.151.204.1 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
crash-metrics.sdk.inmobi.com	ok	**IP:** 35.212.101.248 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.895111 **Longitude:** -77.036369 **View:** Google Map
www.mapbox.com	ok	**IP:** 199.232.192.143 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
placements.tapjoy.com	ok	**IP:** 18.155.173.104 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.adjust.io	ok	**IP:** 185.151.204.1 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
192.168.1.34	ok	**IP:** 192.168.1.34 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
prod.adjoe.zone	ok	**IP:** 3.77.12.128 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
s-s.staging.presage.io	ok	No Geolocation information available.
schemas.applovin.com	ok	No Geolocation information available.
adx.ads.vungle.com	ok	**IP:** 44.205.27.112 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
o-crash.mediation.unity3d.com	ok	**IP:** 18.238.109.72 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
gdpr.s	ok	No Geolocation information available.
spadsync.com	ok	**IP:** 34.8.2.179 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.133 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
s-s.presage.io	ok	No Geolocation information available.
api.appsamurai.com	ok	**IP:** 34.250.26.195 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
s.deva.cloud.ogury.io	ok	No Geolocation information available.
o-sdk.mediation.unity3d.com	ok	**IP:** 18.155.173.59 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.supersonicads.com	ok	No Geolocation information available.
subscription.adjust.com	ok	**IP:** 185.151.204.52 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
ssrv.adjust.io	ok	**IP:** 185.151.204.1 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api.macadam.app	ok	**IP:** 172.67.130.85 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
tech.tapjoy.com	ok	**IP:** 35.171.98.207 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
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
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sdk-monitoring.ogury.co	ok	**IP:** 52.38.239.33 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.surveyb.dev	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
ssrv.s	ok	No Geolocation information available.
aomedia.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

DOMAIN	STATUS	GEOLOCATION
console.firebase.google.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
events.ads.vungle.com	ok	**IP:** 3.226.176.24 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Adjoe	Advertisement	https://reports.exodus-privacy.eu.org/trackers/366
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
AppLovin (MAX and SparkLabs)	Advertisement, Identification, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/72
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Fyber	Advertisement	https://reports.exodus-privacy.eu.org/trackers/104
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106
Mintegral	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/200
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
MoEngage	Analytics	https://reports.exodus-privacy.eu.org/trackers/268
Pollfish	Profiling	https://reports.exodus-privacy.eu.org/trackers/305
Tapjoy		https://reports.exodus-privacy.eu.org/trackers/199

TRACKER	CATEGORIES	URL
ironSource	Analytics	https://reports.exodus-privacy.eu.org/trackers/146

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"ADJUST_APP_TOKEN_ANDROID" : "76b49p0rayv4"
"ADJUST_APP_TOKEN_IOS" : "lfl1y1szh6gw"
"ANDROID_FIREBASE_WEB_CLIENT_ID" : "2233710485-uf11vl2cqnb3esuf21ca64ds0jjdao4e.apps.googleusercontent.com"
"APPS_PRIZE_TOKEN" : "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTE5fQ.veS-GapCh2LnUkZWddiPWfb8DLEWvyE2VqA-mMKRESM"
"APP_LOVIN_MAX_KEY" : "03kXFb2-OT3BpVp1WwTB9LgFWuZbbS2TIXytsVcvBoSkKNfbAsVzSRaJLQoy0M9CKeao2JTo6PGoZ3uzP5VZDy"
"APP_SAMURAI_ANDROID_TOKEN" : "as9GqvkBR9HJZPuN3f2JKRA9hydA-2Um16NnLHoA"
"BACKGROUND_GEOLOCATION_KEY" : "ef807a385db77e8b614848147389bad2588af85680c879bb152a51477512da42"
"BITLABS_OFFERWALL_TOKEN" : "5461499f-3294-4b92-b80e-5503b344753d"
"CLEVERTAP_TOKEN" : "ccb-ca6"
"FARLY_API_KEY" : "6PpJwphuk@/RVx$T~/|$-^jp$b1DEmo7f}U_2`*(A,NczDA#SVO!+_1h[mDZE5(["
"FITBIT_CLIENT_SECRET" : "69e1b99398f8b835de860f242fa4b854"
"INBRAIN_ANDROID_API_SECRET" : "XfmvFq8DsaDVzW83aoquCVMLvmpVXM5tOLQao/8GWoCWuQn4qpObpO754aBBJv+5Geou2a6JzSVJ3BV1BKd+/w=="
"INBRAIN_IOS_API_SECRET" : "5cVYNQQyXVO/75pO0jgX/BjEkz3x6jfxEmT4FYYTeDu2PVo9ETOQdKHAhFzxGl4GkdzDt+ryNs0Y7vk3VeYlZA=="
"IRON_SOURCE_ANDROID_APP_KEY" : "16a085f2d"
"MAPBOX_TOKEN" : "pk.eyJ1IjoiamJsZXByaW5jZSIsImEiOiJjbHFFmNHJ4aXYwazQ5MmxvNDY0bXM3N3h6In0.Hb3pj0ZCEASaZZPTk4zabQ"
"MIXPANEL_PROJECT_TOKEN" : "eebf75775682bc01a5f5bb75543d4382"
"MIXPANEL_SAFARI_TOKEN" : "eebf75775682bc01a5f5bb75543d4382"
"MYCHIPS_API_KEY" : "4af792090ae04118bb859f4b487b75ab"
"POLLFISH_ANDROID_API_KEY" : "f1b5fce2-fe29-4191-89dc-bdd88dbcf350"
"POLLFISH_IOS_API_KEY" : "f8bbf868-13b0-44e4-b386-51b9717de67a"
"POSTHOG_API_KEY" : "phc_V67R8FILBW0ZPl9WQmLQOIEDdGTzQUNwX2j94iowZkq"

POSSIBLE SECRETS

"TAPJOY_ANDROID_SDK_KEY" : "30fmYRrKRKmRtB2S3A64jwECE5mQDy4lQHupqSGltpZaQ0cCmYOq5AXl5f-3"

"TAPJOY_IOS_SDK_KEY" : "uo92O58lSKq0NL6TtotKUAEB64TkhlqSMtBVZOo9EkKUeXVVnCMuSx-XPCUy"

"TAP_RESEARCH_API_KEY" : "3ae26effbccf370c4e523ac287595775"

"TAP_RESEARCH_API_KEY_ANDROID" : "e87e2e48469682b08cf444b13be9c731"

"TAP_RESEARCH_API_KEY_IOS" : "690a2f7261df34715b27de982bb5ecbd"

"THEOREM_API_KEY_ANDROID" : "421986d539ac570be1c4ca01beb4"

"THEOREM_API_KEY_IOS" : "fe7fd75eedc3a9a4b669fe8c1921"

"ZENDESK_API_TOKEN" : "whTm18x0OTQIQ7vnp84USMuhENGtDkHvRo106n2B"

"com.google.firebase.crashlytics.mapping_file_id" : "cf587d8ec46445e282d7e6db87f1db72"

"dyStrategy.privateAddress" : "privateAddress"

"facebook_client_token" : "bf71774d72c0c199b5e596dc6607e84f"

"google_api_key" : "AIzaSyAtaRzfHJUd3i1gzNggk7STSSJJK4vpZ04"

"google_crash_reporting_api_key" : "AIzaSyAtaRzfHJUd3i1gzNggk7STSSJJK4vpZ04"

"google_maps_api_key" : "AIzaSyDHxGOUTsG3jOMgIGdkehpe83qvn5k7cJl"

"session_started" : "Collecting %1$s"

i9UHFEeYKrwiWF3GKw7x6guqyhTqAOKO

HHTbuc6jJnpbFValFtkFlwv24qRilhed

ZprKdiaQVhEf0JuCZOvliqNdbLoAvnqm

oWcxHzaW6r7lBy9gASpUpQY2t5hecS1n

UNFwS5L41LHHq5BQuxA2jKAhYKXr1bOi

cXEoPWFY8ZWz1GMGWuexrOl99MIgTsP

PGh0bHWw+PGhlYWQ+CiAgICA8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlLXdpdGdhoLCBpbml0aWFsLXNjYWxlPTEiPgogICAgPHN0eWxlPgogICAgICAgIC5jb250YWluZXIgewogICAgICAgIH0KICAgICAgICAgICAgLmSZXgtY29udGFpbmVyIHsKICAgICAgICAgICAgfQogICAgICAgICAgICAgdGV4dC1hbGlnbjogY2VudGVyOwogICAgICAgICAgICAgfQogICAgICAgICAgICAgZmxleC1kaXJlY3Rpb246IGNvbHVtbjsKICAgICAgICAgICAgfQogICAgICAgICAgICBzcGFuIHsKICAgICAgICAgICAgfQogCgogICAgICAgIC5sb2FkaW5nIHsKICAgICAgICAgICAganVzdGlmeS1jb250ZW50OiBzdGFydDsKICAgICAgICB9CgogICAgICAgIC5zZHMtWXsaXBzaXMgewogICAgICAgICAgICBkaXNwbGF5OiBpbmxpbmUtYmxvY2s7CiAgICAgICAgICAgIHBvc2l0aW9uOiByZWxhdGl2ZTsKICAgICAgICAgICAgIGhlaWdodDog...

POSSIBLE SECRETS

gICAgICAgIHRyYW5zZm9ybTogdHJhbnNsYXRlKDI0cHgsIDApOwogICAgICAgICB9CiAgICAgICAgfQogICAgPC9zdHlsZT4KPC9oZWFkPgoKPGJvZHk+CiAgICA8ZGl2IGlkPSJsb2FkaW5nX3dyYXBwZXIiIHN0eWxlPSJkaXNwbGF5OiBmbGV4O2ZsZXgtZGlyZWN0aW9uOiBjb2x1bW47...
[base64-encoded data continues]

CAgICAgICAgICAgICA8ZGl2PjwVZGl2Pg0gICAgICAgICAgICA8LZRpUj4KICAgICAgICA8LZRpUj4KICAgICAgIDWVZGl2Pgu8LZRpUj4KCgU8LZJvZHk+PC90UGTsPg--

POSSIBLE SECRETS

83Bq2rwwej5lQl4xIjWhMW1frgDiuUFT

MOwQC4VnYrG9FSwrwyUZAgsxR7nFQ96o

0rHD8iYFkM5KLcEdxbz1wO1gXSem16M8

5a1nSgSc9ubjxiTpcQH3XZ5BSJHYyomE

7JLfCVxHN71IMtTwiclOJwxf6r9fSssd

zEjlxhk858iOsdYr9SgRsiKXnD8rO3VU

aBUJYB0uS7BrZTt8Q5KCQqzmSq39esRS

Fk7s6yBwWeAAqge5bF8uzhqLaOJLrhQ4

XlFlgNr5vQZ1tyGpSUziV1wK28nmqCDp

gVEIHyW2z7iU6qQnAfFVCGXDV5ZJtx1l

vGcqn5WXR3k5d8dbJ9P1g3SXUfD3IftI

QQzDcdSrE5R6m8lZGsEzAH1KwZryrNxV

UeRrU6VIZhMUvjXaMrLT2TysGAtdmGOb

VeFVBuimOKBZ6IhnkHNGVdQ2rus8nhqD

XrwELTKduoHwTv5Xe9Ueh6lc6nYoGsk4

ijVF0TjJmPEEom5xXBBS3MNokpliI9Vz

XOLeb9Yz2wj8Kp6a21le7nVhqJT2mzr6

kxqjIStyOeZmlNn9xMd3jjfND4aGb7YZ

CM8HCV1eVyulF3snUIL5CjajvzNLA86A

JTXeDaIbilWka07jjSO5NeC2nexU0fdc

M9C1QOaf2rsBVjgJKmiK14Vpxz77Nv8B

sPUJsFRJw3lzzMTWDdjyjiVEH8hW8JO7

h7KsLkfPW+xUhoPwJ7JgY7K0DkeAWrfXYN==

N1cAdaDOGYPovqFEJPANujO1ITrm1R8x

jcZWkwS564qIWYGPRhtwMiRcu2uJOsmN

XHK065n3VHEeOH2YPoqOuBkTW3Rzvopo

POSSIBLE SECRETS

lsOkAII0H3p85vNUKB6UfhRm5qanyVzp

Q1ruOHxOk6WILPvKf2GjHGHRzmp539Hk

pxSCprQoaQPuhJK6PZvvssuH3BzR25Ek

llq0nKP0GwKiYNEJRhA9Zsqqg4xJtS7q

8tunoJcFY8sdNkzTV28xZ3mFQC5lH0FH

KX8CQKcPRjr3ALAXmnNmxPsf5ZezVoBn

9U38xP8piwyhajLb0oPtN8g0SrDQbMul

YGB3OCwtMa2btxklJ7dtSCpn0L9PAA

u87jsv4Qx8TBqcflHkBU630hheaj5W5

DhDG4ysBCK9h1euDhOnTPnGquZLH8fbl

8IrZ9i3Wgz7X9CLGIW1Q1ZpEnKLSVzU5

AD9B2u3CpUm8RcifiDyOxQh6hnzeqyLc

rmUL5G3ocM8QXPjdZtuh6zbaNsDgif4G

UNrHeFRST0N9gyLTBJ6FVG6osgOV0jla

0QxzD8ZSXkCRRI3ROeoKuabFTd70p3Eq

sG6vVHTX86CLemYFR6gPDfec7Yfwaj3D

9LerROYgERLC3lU2pQvcy1JolU6pTYA4

5FlvphvUgQVU1M732kCMD6tquLVSGC6u

L8PQQ0Rvj3M4DBbwizvKN4JEZ06Jax

gok5zJYCjc2dvlikSbYtPgim2ONCGlnE

l10Uc2sObXQrfE5LSRWaITwRG6VP7m3G

6mL3lrEUp2ULAISFIzSh85ZjlbRVvlWv

C2viYzQ805EsgOX4y3n8lLHcCQmdv4Bq

OT3BpVp1WwTB9LgFWuZbbS2TIXytsVcvBoSkKNfbAsVzSRaJLQoy0M9CKeao2JTo6PGoZ3uzP5VZDy

4G6bp2JlnqCaKfrAR3d18U2njy0G4HP7

bYWrKv2GqG46pc3oh7WJWN46QVo1oXjE

POSSIBLE SECRETS

Lc6ZOpuSjj1IHjH2AmdfZtL4EvSihTxE

6RJtTYzLBnUcHRvsTatmkmWKIun16hIE

vFAyIhDjx7PQTTwycAK8iUJWbttwgSfB

VyVHRG1xUDuOqri22aozQUHlXh3udCdp

uaiMeFYOk8P5CT6awQd5iZTKLUhraaN2

lVwzbqekYbQANiPk50jGeH7RXXU9rAeI

zIgtazYEv6wIELQnc0J7ZnYrfidBuPPF

gbeo1KbNmS02dvrZyrXpgnCOAkkwIw0y

Par4AxgKHuADzZajYCYNv8eTOybwGgE2

mQm3e3EDrMVtI1xQTgCv9nJkqidgOUz3

vwYfKziuTy1RLYscQHjTEDI4uYjWuvBq

JAocLFgZR1eZV5wbskPWRgC49zmLSQ48

D4EVL43wqbYA0oDrXtmbBhqa2Bfs2J1l

1157920892103562487626974469494075735299969552241357603424222590610685120443 69

ORqZ7gMxbJJ1LCIrF8kx2625eiWSr61b

oGui3UnSaV6fb7qd5azTuEEp3mm97meQ

5XgzWWjFe0UjIKQc45EJfpyV7HOKhYUT

tWHbMLY0jEAGlYHbcSqJBIrBc18go

s6CWgTXMjjwS89lYbS7BwJEShue9hkZ

Wt9X6yajIBXU34hiGluB33HbNXSszdRF

T5D6LMII5PxeSeaFwmiiVgotr7WAYFJE

5EW0ieNDx7VK4pqGb6z6bT1osScjQsM9

0JhHJN6IXOb6Rl6r4FoMpOTStQ2rHZcY

heP9AS8gF02VUJcvkTVaFkcx4c9WIelE

n6owUrHV0UlTalMNOYWSyyNAru5hM8Vx

w1USCXg8ZjnjNvDZ7X2MerCQwxzm0Nu8

POSSIBLE SECRETS

HSA7qn06ePx53GJEFMmIpcMYLn0Jr4sG

YmrJEBKdiRZ1L6ltRDAiNut0MqgfCokc

dx2BR1y0ksYiHtLvIo7bMHcN32t5U4TZ

frsVK1FdvBngWEpFEgXb3j2VH3I0QFcs

XIj7zi9aVzSGRkWRza9PLbW8qplNkm3M

SjioWZFjItKuhqId4sWZUQTfHHPQcsy5

4GptalUYKF4Tciga7NCIJ92BgFvhnZhd

doxRQxYmnKukwMO8NbdWOtVN68TpFesA

5Jwp5xVo7ldrls8e1BLn8Q9HzbIas5MN

GapCh2LnUkZWddiPWfb8DLEWvyE2VqA

waSOeyTrnAwHOvUgKCthiNoRbzSAR0SV

Yte1vUSgji4S3VNobeKxGdrgBkFaACT

O6DgVsMjSRRAXWI9cjkKRDle2DCyXpBO

39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

2Hs1eEyuwWDgIwWONAgBlK6IqUqjA257

2sbQwT73EZw2kTLUi8M2jStfSnxhE6eL

JiFWpaVbUyZcE8LwR0m1MvC54Jb3gIYp

3ae26effbccf370c4e523ac287595775

n5PcJgzDrPqbI2Nld6vWULHVZbuOfTZA

PSO0U5rzFo7bmFbA9aIaTCLs4C45Ec76

NE0o9u3qbPEpEKxTGS4cMUcBICbCHbMr

soNl1VU97OXHQ4CjHAobgeJ4Yx1tI1qy

kleFc3GTYdmSeGzzaJMmIvt997RVj

6m9Kb2lg4QS4P0ZcGJ2XwsRwfv4UyCAv

2MJEizeCZp5uxdCnXqOwiW6KQOsM6Mkf

dzuBgE9s0LFJQmHWqmsbDjHZoDONF0gP

POSSIBLE SECRETS

mJqTstYmruZhgAwaIEL2b4JvWf0CXQMB

PfdY9h9ksw7pIrLHvaMDkidEUsYS2xix

YhTGjjkd4nQlp6zPvBFYrrZ7l65Vw2gm

OxqqmxACKcMb9rgd4flgeoqO4FLkDXK8

C95vkx1geO3cBWoagx6NE1xSoeMRhwP9

gByYkjtEEdTZs51Nu13z1IN8evpdXlXB

o2K5Iq3zbWnsvhRLVQUneLMfyrath7l2

KnBzaomJ4wFvZeITctRDF8tBR6fO5AM8

sNaJDElCp9cCYWYxYRwKU5WVGnQK3THd

t5607oHfL2MNwmRFcsOr1jnyxzutumg5

JOEGydLRZ18FabkiFWUulairw0GZ2Gkh

NTaremhH7pfVjZMHsJgugPUye2yAgFMG

7EXG0IPVOCl5nW4ISobsZsOVcrd8XJic

VVgrfIl8yumQyldYn3WSYqBvmAVi9h2x

oH0n9xAbcML0pK3kOEyCMAjio6eGJJqD

lUzsuN79KKNqdFKovZp5wJyJ63LnTGfP

Ul6ETdKi4sSCw8OfXK8DwBAUtHNMz

m2WAASCqguA1bRajQOE6ItOClvFsunSk

B0i3rKbSIcl8mqFdJDuay5LNvvemcw4

APyHxukBWXIF2vPxbwif9xgIaD7vOq8q

lDa8BWO3GNKgBVoNV1FydEibnHhzaqpi

eBV46u0KGpW8gKNBF9SaAmjhVwB3niU2

jjH4wggc1wpWWLxRj5DmyzPuqk4QCdce

NLc2w0oJuVItZcslj1CIxITo5xRh8cik

EW8hQNBuni4zfziLp651zBZrhIaSPPe

z8bmRlUG76wDgBp2wvrB0MWrv7DjKXuA

POSSIBLE SECRETS

zlx1Kp29sxoRWQT8356SM7Vgu8GAsquG

D3KVpbGnPeieQhxvT98TBR9XUfKWbPsR

mOkLH1GNKUdbhHvlcQZOnMGTeWYD6PJS

Q8xFqD15qZ9htNy6CShIJMvcdmz5frjW

TYvyTugW0LIK7CMS2wYs9G2uUGgA7Dke

I7fOo4JalOo0WGey3tlmi8nSFYyfGBZ

A4PZagHoSRM8cM4mqm2KVFoT1GUYa0fw

bCUE2z1YAZE0LvG9WsX4zUjeUwMdrUpo

iVBORw0KGgoAAAANSUhEUgAAAAwAAAANCAYAAACdKY9CAAAACXBIWXMAAAsTAAALEwEAmpwYAAAAAXNSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAABESURBVHgBzdExDQAgDETRLnjABivBLF6wAEIQQPkS2gAJl7ytIw4nchJVDajInkLHRLGWIsa/pYSFdvfD02PfDu6lLdkbCo7xk
tz5kgAAAABJRU5ErkJggg==

GZRnbLGejQQShSAr4hqHwh7J75aAFy3E

gD4OyNyezD5obJmFstdRZH3h61osYZaN

iVBORw0KGgoAAAANSUhEUgAAAA0AAAANCAYAAABy6+R8AAAAAXNSR0IArs4c6QAAAHtJREFUKBWVkksKwCAMREOh99+3y97GU3i3iTdp6tRcUoBgbJfEgCmpkF4RA2YVTo+PDbKdzCJXhBeHR8BJMxE71gGah0T/B4hqVqDbvY0QZfrF41ip3d+geZkAO89MMqV4xyTieVAW6Z3tQG6C
mP94U319dXfwT+pb9HIDwrxDUcBOiFBQAAAABJRU5ErkJggg==

lCsnFXMtzGCTFRX1SzzVAUWLGsHIck98

65yeGhez1WQhZvxg8qVLZrzPC2Ou4KSa

x98fVhayFhYIlbQQOJ9BjMfXcd34KCSx

RvezLLiD01uKKJ1jtQX7xEHNj6PkbMyI

J54PJiBLJytnlOojbjnozVdd3pHXhFgw

PNezsP2uIXfEkTtxMVhkFMGOj0OMdsbx

NeR0SJjHXwq6S99lykBHPSy65ApZKYsP

H7JbpxrghbTwVbej4vMcLROuhZC8DeWr

ZL8DSguYajuR1eoXw1hG2lJW2j5bJdo3

ulivTU6ocRt44Fi8kUKccBfI3hgmY7Iu

xiAWoJKpfkjoLWhrM4jOgBmrkR74JwPz

AVskEroBo8UlfYPInQ7Yx5KSddGfFQyi

EWWs7bfWX2zABqEPcCAhkdtns4Cu5rHI

POSSIBLE SECRETS

9ywXzXhCM32rn3RSs826HxV6thYomWUI

Ggy0EBkUq5vQG10YsWXxjCC7KKoqUJqT

Hz1lzGXaGkVdCftBSZ2HywJOuLsdaxmO

1TwObRYenAx9Xxo2pcbqEN0Hah2BLITA

2Qe1VU4DTht28N06OT2Ihgi6oEKZqtec

aXQ8cQ350VCAT2mitcvykUGHubvGx6C9

CVXSSTaTyGD8rGam3jI5MG2HGxoF6OEi

eyJ1IjoiamJsZXByaW5jZSIsImEiOiJjbHFmNHJ4aXYwazQ5MmxvNDY0bXM3N3h6In0

cn6RXotf6zZwAeB3lSiWP6IveEHpbDAc

RnCaU2E938mENSzRzPrAuXo67ZnkzA8g

01uixCM2ew1GUtPlkStbY4R3MiHKurQG

jQ6MUrNiHIuV2Q80zD0eWZ3NfiJ07L6A

F6FzT3Uj5KsGZJBmajlciX3TBepBTDoH

oHJkPKeSQUNkwlTgdbaOwJQEOAFT8Z3w

qalk034xToBy0kTaZmHtwYGALLiE8EwC

4ENs57XqgWmyHBJWN23MJhXXMCaaLz6e

Sq0yZcwOgTGXIMbLXRKfOSdr7WdDOtyr

L7s4SUBCChL0YzkanmLdnighm5pk1EfG

VwJuHcYZb6pOUF9c5fygzqO1xhwXl8

fuZWqRC62r9MuSCVvwKu5U60eWbDLskj

309211f4-eeca-4145-8676-135ea355b566

DDwCgFPJHFvA5diTm92X28ohtWZRLkNX

5Ss9iINs1N203h8UwVdzTm0B7XXAo0aC

eoagJWSpw9dhQ5uILEfDMJsGfxbL2OXR

8sSkOPQI173xL0yddX9GvFbQV9q1hctA

mMVqpqBVgrnijMcf07ELsDNcJ24OL2nP

POSSIBLE SECRETS

GOWeQyuTSoYbh2z5UHQkrSxrHOD9hfFJ

0mtXhllSXqdp9S5VgsRy7NU2TbMA8xeG

luRz3eSIkgTHKYiDYnp1YmzqTFiN9rHv

Z9dYfKMSwy4DwqfPMAiJW01558cOA1wL

nEAZXjO4i2eVoKfOQOzMBl4A0pmuVndx

ZPgmzBD45Cog9pfLf6p2hYnwtjTNY0Gq

Pi6X8Ic5BpSNrHRXVgoJ7B2wVh7XZC

SLjIMlZrt8LApw5SyAUFDc4ipDag7tTu

dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg==

KcefTCcuaU05Z9sCY8CUGAfDHno7A6Wv

qh47im7POLSb1uwOXceGvb4YvfCz05wk

JfQekQfzdw1mJ2RkSzlEvaL1jVLq96XT

NShUMjU8EFbasu9WAPG4eHHUTqko21N4

awpTB9u15TkHVvPjjOCd09Fy8dol99E

iVBORw0KGgoAAAANSUhEUgAAABAAAAAQCAYAAAAf8/9hAAAAAXNSR0IArs4c6QAAAHRJREFUOBFjYBjygBmHD0SA4puhchdxqMEpLAyUAWn6BsSWOFXhkEDW7IxDDU5hkOYLQAyymWjNjFDjmID0bSCWB+IrQPwBiPGBx0DJeCD+B9JINUCWF9BtpygQYYYhG0IwGrGFwVugSU5AfByIVWGmDmMaANyNFVTVvpxwAAAAElFTkSuQmCC

f8bbf868-13b0-44e4-b386-51b9717de67a

f1b5fce2-fe29-4191-89dc-bdd88dbcf350

HV3bjOQFG6hG19mK6btv5ZItymBNR4jb

RJC1gwIZ7rbFn6fsQqldXDA2erGgWv

PWt3UCdLmacUDAaKa7qG1WjHdRUwYQML

FTcDokCppzFM6olvGfJVNXVubstDZ8VZ

f6iKlyOeYddBSkQQnaXOCc7KzH8j

YtARcLQrDWG8KO1LLbO60FnHOktlNVTt

fXFXcHbhRt7OOsQru5ewvFqn501YUyRx

NZwRvgeKfVOQj3OAbWBZydUCa0

POSSIBLE SECRETS

an6q6r3Pxi3Yd1Uxl34WEMAekK7mvAv

0up6ixfDqbrZOotDwCZ4gMtZBiUGrTem

vAYmZT8ASJMB3FzzuSGq4ydCUrxXwpoH

7ZUqugjvimlTMP6MGoSM1hJ8SS3JK7y

OPYUEYxxfuFToCoqAJ7LijcBVLMkd

fKOq3CLbRisV2HCvxbP8DswDC3h61WtS

E45UHwgrMTIMwaLYI7blxmvG7mW9Qs1w

jE5XhhYKQHpatPcaqKauHRorLHvmx36n

OSNHTg3ADFpX6DP2tOs0qw9XaKQiTPiw

NZeIzFT7NtL3BMGbT6cfoawDteogj

UN93G5VTG9KASeEmW9fM92cjrozp12u2

sr30eG8QqeA9PTnBv5Bt4hnZqAQxDLuJ

l81c8yE1UXyvzPuTPm0IGIR5VvYUnp6F

C8lHiEVGsA1InycY308zMITezDqlCJlt

VujXzvSFrlMAu4R1I5vUAWLnq57AsPWM

686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715

jMc4mNTDFQmf2DaMzWYBnxz0IZlySjfz

kzsYhm9LKsU0BkYF5GBD4cHOfO5I2S

cz5xpykBJ1m8ZSm6Ol7HGwJnVK5b1rdS

UXOJdmjGs2LP9mzRUQfP3v2dC8BVV8MN

lcRtxCp1u16sb9wLaNGF5MQQPhmhPIjy

UWlpQQTiEDwOX7IrpEHWYNMuR1ZHkPvn

qQcG8iivYcbnleQXnFNfPBjKpUSTKwt1

nCRFoG2V5rxtp9CJ0zj2vqX2pOjohwfk

7toV51THczyutnu9dsZIYiPQpALa8FIp

AAnoVYdXRR9Z0xg61VjEQGKk3Qvi

POSSIBLE SECRETS

QZbxm3QXOF2yqMmVze25YX6oNvKBlq6Q

ewYMn9GjFuSxFQofwWKCBh7wdb0h2I2L

JRHKMDEWFLpt4s2hfuCsUWWHTwNaAfzC

ItURT5NzCCJzRXO1EoFfUiDaBsWLxBKc

iaBjp1AwQpLLyKyeruBkx6nhfTHAU7OM

T1kvqoJ1cX6i4DSx7n80qqGN8Qg91HVj

l72ITgVAaer6oLi3ZuEszNZ4Tz579Dik

gm0LtQz6WhkHdj5wX4JbuGG7BvRjVm91

22uUhJ3etkiChBnOXQGZ31CB4WVKfXWA

iNtvqmskXB4EiLFcreKpIjIsuOWl8BZN

SqVe7zamj5uHBY9dXNHGQ3Qd7KSgTA2W

qED7e7UX90QQgnHDR4FxiOt7ONkFhw8M

a7oVZcxMQNrl1fZi2h6OeAZDf6QHjYYV

m4QFNGv2UqCrxsi4qbKPCdwxAuw6y7wM

2d7Ue4OLDSzNDZ0wIaqfb27lMuRlGrEq

qO4Uq7mg6XVWSCx2fb2lLTULAXcH9HmN

2e4b65fc33a0dfab09ab54269721bbb3

4b110878-d423-4a26-a230-3d9aa194a881

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

fplWO3ygYnuHT7vj9EIqbF4EPoHQLWED

NGXmQ6vSzJX8uyjVaek6YMFly75gW1GO

Sxm2Bc4tXHoV7tL5LxeqP9KUDfvbsTCx

LV97W74qtL9kCw5aLEufLebev1Dp02F

4hX5Bu6XJriXyO1ylOVNaDjvP68bIemq

RuLyFqXzbhnlmQeuw5cGDVAvivNnSqaB

SxM7TzuiGj5mLkDPau1usW4gOWoxs80M

POSSIBLE SECRETS

bEx19V6XMUSudWAWNmFVzJXPP33hVIRX

tB3IEJBlHxhWtpYKuvAk87dclmwGEs

Xgk0OdYHTIXe2Q1HA3YZKPRbdeS7oU4D

VPsJYR6nwnKl3GGsBKT9FowhdWGAXZgf

zI20iJtpElrzvKbVLZsd1iWpdjTxU8BC

3ZIeaeVMqGSC8jDTqrHFXNca0PmxnycW

wEeRBkPfcoUTpcJss7BEDa6c0l6NXmjY

JhAlZD5OxJYpmdx1a1lzSlrIDQC8pEtq

pMqUa9o7Pi66iIAdHCcRgosi01w9m70J

xDmSay9THM0s0a1UzRtMZ3OA7t2IbfqA

4wjnoNx3VOTWdL7VvzY4PdOFwDa8aAyk

Wi1pgJHqhNt1rkC03e0JnQGSkCoA4pQ8

IUsSI7rcrCx1ERgKd0rYF5wqQshT9MFY

BuRuvxulsaJnTsptWr5C74N6kbe62CR1

q4sdjOooEVufGDgMwyNc9jWxRXQ4NKpo

oRYwVa3KjTvntAfrBK1sqTqE8vcnrhu1

lOzuqd9TjXHlivepUaRJZyovV0XRZz3Q

pPTeXoiLCEtvkN2q3qoF43bpwUDrc

U4AkfkKqs2F6cZLTDE14qhCk0AeglZbB

7EvIURBQpECqxG5jGjLOa9HKn8wbzJkS

nIUh7sEtDWkIx81Fpy5uA9wFEXEhOC2B

pgjbIMIA6qbvamypHITi6jF5BEk3eZha

te1WrCSgggsWDMNxGrks3ULWi6FlwITL

GMl1WwxQIEaOrmGnDE2kCLCvMTZHsy6h

EQhP22rcQn8uHJztvMH4f7UvmkKbnpEF

RYIhd0rxGxSYfBpuDsCOXE9retMVZXKX

POSSIBLE SECRETS

KDcDYO4g5i7d4XPLwMmGmppr610vo4rD

lpakeOCplwfUbPlWH1mKRjN93sjJNeLK

8bjSuFnY7Px2kfd2c5FIfhC79mNHlBDm

5xn2ImkHS4ATQgLTDfLLcMPpUWGwzNh4

YO0PXEoDNxNkeyj6J5zVBwlvhUUksa7C

KKvBf6HmkOg9UJ27XgqfLe6TaNBCJiNp

1TJpWQCADONb1iXZmn7rufjXlDpseMAW

qJ70LKr8xHxcQctVJa4tlMefqwiAYJOB

FO468KlqU7YYiE83Le7T5pQKY2foYhCa

znJUBPw3pDumoyQGyqs8HDKa96hSudPo

bKRxwQpiW0PmVHVfGUn2RavmyNEFkRji

Ycsm2ZrfC0lohk9KjHhsrMWfSuRqw1L2

OJIGMHO1ySc0mzACRtkWxwocBaSnW5m2

uAADS07vuTt2bWOOIRXTK9bzUqfZPQ

PHJg0XpOhfW99vW7Kex5sTOYyXlu8llY

fX9sFZGj0U97M4kLDXLqlJ6maPl5udls

a7CXWDqETze4gqUmjqRBhcRjVGu0d2y8

12WRHCRvrf7uzS15EjKhAcUJZG2MzuRW

h7KsLkfPW+xUhoPBD+QqJk2MWrfXYN==

BSNgfeEt9bBv41mFKDcPuiwW51mPbBL

IFEWDNEZ1ECVHwPAfVRji7U0Qa0phb4E

2QTGoYMpfKLSzpVAlAXt3wO29bqk4RAA

EPTevQXo6AzOyuxFlfcAvx5eJdnVP8

GFOlAA7vgdvYkzDNo5MadPPE0QeXaZAF

7fmduHKTdHHrlMvldlEqAllSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWJnxMDhlfQN0N0K2NDJg==

y6g4Ls3CGE757uBbH2iTCdPLcyck5fnI

POSSIBLE SECRETS

4KvwhmNBIb78DyW3SVt3pB4MzWrcxbsc

JDxg7tKUhtdUIhfIwWVDLdP283uC1zvF

s8oLKbIochRuLWrY7HR296xJjla

9uEWAfEbnoLYv0261NprGfBMsVVIAkoY

P0wx46ENZU7YevMRV0Bs1QgLacsNDw6Y

Q3SxFnadra2JweXV0TQ7pCIkPNwW6CrH

XdYDAAdfzTXMLa7AW4crIcJNhIryq833

iTlfKShG9zO5ZRqYxtbaM4RphnykoUGv

aAOO9yx7jRsDtZ33Oh1YUTlwgCOJU7qQ

HR23fndUBIfy3sX8NPdMDAzNZ7ikzeu

7R8f8O3Jq8ptPdlyh265i6bwGIY3AnOr

pJOGedThy6U23H0Dqr8MrVjxKTkAUTUw

RzFlIrJ9otd57SLzr7ci506FuBBONCMw

pggHvImyjq29EoPdIbNPEyFQYY47zx5L

bbLm7avGUtHkF3jUZkJgwv05OQOBaWiK

7WCwK6uLOSx7G5D82H1RtAFjcLrdRlkB

wOuQWovYJ7l8fayT1FsN6ONBeiko07KJ

dWllOszLC286Wa2jG7unkbyNU8fMVO47

TSOJfYWCxzAl33AyQiIcTNEFCW2LweGK

ghgofcX6zvMHlgudfTaqS8Nc5lCgt2E9

q5XpLTEZbHtnyzZXCKIvrGbFL2My8Wb0

Y7c14Z2TDbv/Y+xgHFeXDrcshBPUYFT=

Zf8B64fxNGGr2bfcs4J5hE6jajhXIkez

tEEVNd46OYTAYJSvyZnVijwEJ9mxfgyG

DkPtYdQTLkfAW+xUhoPwJ7JgY7K0DkeAWrfXYN==

VhoqgbC2B9SangBNTcV7FdDvnuQFXcUL

POSSIBLE SECRETS

23XjLY44GlUE0KmRGTXDOChbYzVQi08X

h25Y0rjbMuR2ypWA7lRpstXE2gsMGFZh

jUIKGw1ynNKnpAPmELSBfekQdKvvLP7N

fUjJFSbhC3MyLq7bD4XnyNju1VoRa1IS

QMIaZXPM6pynUAzwsdBa2h7UbkKjwIrX

4vfpnedVtrPjMpyfZxR38kPmdhuY8

1lFQ4Yh1vie1DVx8Y9IEXTb70qub4TNk

HJf7oQJhMr6BjfdBAkNXb1VX0FlaYu0s

eebf75775682bc01a5f5bb75543d4382

vZFktEahG3bWOXRkYAMaCi8nGdaO1v3Q

QdB4DFNTOqs3kzyCIXC3RbQ0s8ofNHfi

ioOrVGKFmPeoWtk9SUaiMK94AxkbTfSp

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAMAAAC6V+0/AAAAIVBMVEUAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABt0UjBAAAACnRSTlMAExQVLL3Q0dLTtQgh4QAAAERJREFUeAFjIAWwsDLDKARg5eJkhIFwwMwB5MIoOGCCcJnQRNkhouxkizKyAblQCq8gphiml
ZhimI7H6U3MAMEMOpIBAOSWA4VYaeadAAAAElFTkSuQmCC

Ou1dyJktpNGGcf9tDpPKvHuJxEoqg2O4

DSh0O66K0UoAsbtG5khJTMnGYv0IzoNn

80fcVnrJERY0uuv61EoOWTfKBWpdgNO

KXSmHfhq6DtFyO2I4KCsZ7pXn2h8CepA

kMwNdleMqzWVqcPvmmjgXOFb90HoR2aS

SGf6K716h04aYOies8bsBexpWYiEkey6

nC0EGBHyGvmdBobVRqQD9SZ4g56V8B8j

9GBk78KeH101Q3mSP0uttZ9ZoKvhLy8x

6J2GgEdIUlJLk3yvVentjGe1dkRWCLvM

D5Ds2N3HTc73p4rfg4KJ1tUq7xImRT2h

Er9uQMazYAvywc84qssi8CcPD5K

uo92O58lSKq0NL6TtotKUAEB64TkhlqSMtBVZOo9EkKUeXVVnCMuSx

POSSIBLE SECRETS

CoVMihrSOvAeKI017KlJ1GeUcMhjoF5o

FYvUEoMpOg3hka6RJqEpZvWO8PPoRHV2

96TNA6xbUpDgxS3VY7GPr8bnLD9hElYA

wah0xQyFlUnv3HrXTdrAvgDlPnbONWV

ycwuSagCCCN4l2dI41z3qVhXiq7PFx6V

k3yiwvHxpK5tFRY8KUaXiWkeksXbodjI

gCs3LWFTmjjaP32jtswNknURctpSvZ

3waNTwlPhtizgxjFEukxMjxslAm3KwW9

Hfw1oyg0BzWOVhb4zu8ELKkOELcM4f2B

KcMIoFUA4KOHORJmTS9CHMjc27bv2njt

yyBbFHXEa0Kbel6c5iwsjMz13YxOyOJd

tTGntKCVfgII9xqsGpGrv4L0WmyWUOUj

fICxnQOCOsz8JBbFc5EZnQUEppLIkjem

xS32wGzeebxJmdkB8qXqbLj70rQzUTrd

B2kGyn7fabtxlQFxUauI1B2uFfXVCAPw

oCsQT6uSz7ndvPMuhNCnHwcy1cykmRIP

WNsma8cFvme8ZgwSB3ik3sLylzv2AP1M

KM7boO2xaC3ZbV22lXcue9aE71LlUQ5e

NsNQiUOCEqaWjU1BLVqBIrSW7n245ODK

FasCpRA2RHhykdlBGUblwYUAQMGKU0mS

uieozUeELQJ7BnvT2m7zVxZQuFK6e7wq

ySZlw7xE2mJZGUobjeP0sD0O3cTwGa8X

B0KhbmvhQV1sBquLYa8NcmTHXN0flo

XTHqKjDvfaB7R0kK8woS2JMLPY9kkXKh

SEbmC0K2IQ7flaHMYhUIDNtJoPD

HkzwDFeD4QuyLdx5igfZYcu9xTM9NN==

POSSIBLE SECRETS

hTVEjk3rNFsg66RRpHStC4yCUn29H2cK

JxOvKTSKlNEkhUnh8wyI9NTodbLbyMe3

kSbZdYOgqhrWj8RnTgPZsuZs4QqXHZoL

K3QOntDZZViFMWU0Bvdf3H2DebaVhORR

NlYn9LsIhiHyd3xbWzs6ij1u9O30FtmN

GiKke0o7duIHnZiFD13wbUhxGmBWK7Wf

O8XwwgRKslyLqfo5O4ZQvZ7SdPHYsu5Q

rHIFlyKhXEN0aoZxnSfUJTcS8KA

66RXzOK8gCySKfU5jrDKZ2dh9bBiLsuP

deo3piwOBIkL6NX7TCyeXAL5pXVTlHho

1sEbNeEn9yAQIM08pYF4gKbNN1PUoHvf

9X5O0mohLhXJ7t6NoPERFE8nyauk6CB9

wWX707RKIRhLC7xjkiZFtTlentMuS3W

aJOeJxsM87dt105FXzNZlrhAEbJ2aQd4

3rdfmaS4Bvs6KD5DohCaazKJ5nPjrowZ

b5YZOJ5Dove32nH3VcyYtuQbqE02hip

SfnKd94fp0LIHLn5JRYBcVoydcWvvWC

emglrqM7KcB96xrWPAlCT1HSFCX

O9mPnP3CfsWUFNDjzVqrQcoADApw1Amm

w8d2diIE5BdvGUn1gxyTHp0hEgENQTV7

yK4Di7JH64WA9zfY0TMBJ08urnBzTPx7

kGRhHwEsk4pJ0bE6xku5dbDmcKAoqEqT

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

86uwoduXnLYKbsdqFVwkHHSOZ5iH2tHE

d6Mhnf64aMieM2vxsbZH8LbpuFdSo2DL

j0qb62VKLMRQ8PRw4qiKaZlPPtSv7x0h

POSSIBLE SECRETS

4lSmmc8pBcjbV0on62ZikVJFYVLsdMQp

FufaAEcqYi1G7tiijYXUMT1veLHgs7nM

sFFKCjvZ8i7qkazJexEMRuLcVG

60RqioC1jfEvrRlwJ1QlUWR9MPqv8biv

skElHJjGP8F0E9LHs3c03M6jOmkdnZrb

fY3Nz46mZ4ok68tyHpIJjbxIlrtCCt3n

9H0k66zkYNaHG7pLFG5T73JVLywfdj

DfS2nPoTWNflTHew7ejwtivrUd6Et1b1

V67R8FILBW0ZPl9WQmLQOIEDdGTzQUNwX2j94iowZkq

Oc9eC60MpRTSk1JwhF2h3JFaDWGSLdec

FQ0yrAaGYgr4mdqTvnLCAfi7gpajL

L7C8Ga0k7tlVElvjgxBYHiSOPIH52u00

zWS4lVjyDY90UUPX5QEGbfg3CKzj1elF

xXJIeuat1Un3oETUCUBgWYVlLTYdvUXR

Rv8gvV16xF14rXJa8ys12UvRM3fqPLyl

KjY4n0tPpUSoA65ieUd6JoslwFBfZm4u

toTEFRrlGK8K68MOY9fqi4QHUSJ3AT77

S4Uu90kHlMHmRsyiW8kTjlwq7rEI2

s8XR5C0JhaykpGlf4kHqosaURTbELCS3

xQTxbie1EDs9qNLRcg8m2j5qa6BjCdLv

maLtMp9QqLZF08R6t9fzDcCWwiu

WsEiqL7ZS4BTl966aPHoJ2dPx2Ea0F4l

kuAqFunmHZ8uIDSOoUkLR9MNuS1f17e5

dBAoZLypinVieBiN6OmOrWglm0mkw7Th

an5oIaHMQLp81wCZBnKMJTBSx7KtQFJf

VvWjmMzUCUeRE9wUm3LNaHxJA9d87V8N

POSSIBLE SECRETS

v8gNFDmzDFQ65UlksIc5Du22tyA8sdnr

mafT0Rfur7fS0CNoj1tBpTWo2FQFb5xI

8qSAHAaIpnwwIsCvL7AfoFTJYv1h46H2

LswLHEYKeGvbNlCvRjNUSVWZKRT8D0Zx

f4NlNCElPjJB5pPYNhX2WTR6iFmKnfGM

L7pmDhfbtl8pdMobHzydLQ1D6YOazgIb

abSMUJDaje8PZVdniKXVA7EheIgEU2Ky

6iN20dDIHc3laoZszST3X2V8JHbMwesE

F2yQzLJFEjO2XmqsM0eh8XOkYGMJUBuc

H4WTbGVyDanNwNDCQrC8WYgXSDH9x91J

GWFI2aEH9IwS9jlAmW7GhK1fzlhYxOYr

WGZsYEfxfTD4T7Cqe3yCHw86dz09xOKF

a97ad59d-711d-4df3-a3f6-e82aadda25f3

uLbNEHRnnMyyuUlqsIMZHpfsQBJ5TRv2

rt7Bq94iIT4vcXtoKSYLP1d4W6MwPUTJ

Hv8n5Vk5MDnKIrkb6r8Yx0AFcMxyPOg2

IxV2WZghQ5T6kwEibQ02uWW7iDs4uQOS

NZkFYUXBqTyLE0uJAv5x9NXUc2VI7sJS

hwWatJQYKhKE8FUxymmZjRx10ScAWIj

rdQ7fJEKRbVHtvxpiCxMwn5qtJ9qGM1n

NNB71xZWHcIAwa9uUtpvwNL455Xxeezs

2u9otpZXCk16Szcxzo3RgVsB8eWIqp2Q

wjrRPXWyt7FJOtCfXXeKbwMwqBspTzQg

u7URBkmoClRMdzvgw4WX3UmEFyKryATB

wyXr8MEnBTTKz0yAsrzUV0iU4Ibjh0Fo

sIOIMXdckNxf1vD7TuVkHKtZXYRsYSsj

POSSIBLE SECRETS

YGxjb6ZA6RtUmEF8MJ0615ZpcT73YF5q

6EmvqyT0A8GUtNQWPCztICrBXhcLnLDE

cWkBnlzylFFk2PvMzvfAX6O9wvYh3tUg

BUPkySTcvyKGzFoXb8xNfxJs2vcj6SI6

Tf0gzpE1z0DOygMknAScYVGYgxUCN6If

LHpQuNx1GJF6WPrWOoNErW9GY702stdw

DS0L0fcRoHYALrKB9SSkXSb7384LvFtu

m7KNvRLlG2HGx5CxJtjuXbqCPolwiEk2

DjfkS9z5OPUyV9QdiCBZ1KUSwMFmGRPN

d6a6e4eb-58a6-4b7f-b632-0d6bb8a1a1c0

6NcFsoITlli6jci9nvzmOwHlbJumCDg8

NFdit9VNslJwWcMc3jsN0gE8Kfr4ZGkz

nL6OAJIdW8sl7jDyOoO0QwKhwUxIf89k

QC6qUWFS60GKUUYeA4MZapqXqsMmI3vS

DbKE5eQ0SztvRB9F1cupaqpSmaw49ca0

Q2P3QGMLTw8PDNq5VpeXaAuVADEzryB4

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

RVlAHF7VxslCalKX2MZme1MZcTv0vxDz

NI1fsHbKGeRDwpNTvWuj4i2Lu559JSow

ecf9I9JqHAeutuSgOmpZliCU4Q5JYn9j

fgVvaJPNAH92mxaTJlosOWA9xsF7cqZV

Pjq84j8K1toDwE9n24Yhtzr00ksRVLD1

pSGbucuoMvma1b5VVDAxEZMYXBJBkJd7

RCnn6pCzuGmx3q71pxhPkiVufEZFhrue

V9Kuj32Ww6lLhCXMI4XEd9rHt60G9lJq

q3jgB5DsBzWTh9ofyuUcyllX5SyVXG4i

POSSIBLE SECRETS

vdh53KDEVDvYPF4U9zJ9CmemLfeqkfcW

qvLHnvd2eZmVa0k12Gn7IkXrujKfrq4G

7oIVhYtWgczHhLZ4eBK9i0jf

zUrQL7GUAFocRwXemPY3yhr7l5S0xY70

fBJq4naDVNOawpqdOhpwTAHQcatL3neF

0i5SpG4mJJwZoEfMhPDQtpKHtdTcA678

qFc9SandmZqx0yjNiQ6hc35paacWJuqv

WnfyQ5g3TOMlbPuUI1S38a6tMB

YsGjonOW8fRp2ADpBQb8BIeWFn3N4H

DkP3hrKuHoPMH+zwL+fALkK/WQc5x5zH+TcincKNNVfWNVJcVM==

wEt2AMMlWwKWRpacJrxPlGBsPjvVn5Jo

t7ZHn98FTQSdKZmdkDCbFfAfZFL04WJz

qSRAP7Al4GPL3nfNBbzCOWjKh9ZAaoHj

fegio6ElLuca0kBWCpMXWgqLCFyhlORL

cdxeXD5RiaMI9e6AO1Q2OUWCJZ0p5AOK

t11qfTcdRX3vtzWg9o3D7yzOQIlsgekI

akUHqNUioBcoPX4uDEE8eL5R4a97Fv9c

N8ai6xP5Od7TVPMs8Jay0FHFPRYirWFh

pyCuQ7D83WDNAmOGOSxjDMR9sphT9yhX

5vbywGgLU2fUNXMaCGRflqdPRLJOnOI5

NDBSvjeraksgouCWowC9mNbakqVzapXj

2Ait9FMgROtB2NZo6j3UC5dnhoYmjwMQ

6bZ3PT4hZpte9eL2tY79J7XfrRT1VGoj

UbOohqAT6hcG0r1X4DLnHOjV5CTu4rQu

XwteBG2Aw0OJWJhPb8yklLP0HTcb60fQ

e8tzsRThNax4EAToJhNq21dAKBpwgTLo

POSSIBLE SECRETS

3CmPFRqqfEz1KNHoTaFI9Gq9W7MdJSat

clibDuYBy4iZiWhBa7aDKVcHYQepg0dA

JzhYJjhyCfpGQZW0XGEf9gVBtclqQrE4

2r2XHRwXRNnyuB7hHeEjqCG0ly7MmAbM

6eVsPVOukcdBuHl172QQtpwtpqadKDAQ

2bfB3PlZj1r0tJp81OVdNUvEXeDR9P2R

3nl2uEmm3Y6v2r6DUjAJFGqyxF5bM8Tl

3J85XNytcsZ3pYJamIMiFyJCjuH41ABd

OEPmW7llGTv5RugeZAnT8CJpnv71Deb6

rfM3ikXL5SaocWaOB9TmjD2vsiJkKlJd

X0zTjQehaQj8StZrguOVf12daJe7gn3l

WGmVHEEDN9tp9RNfsq2N8TcUrFizj2Aj

m2BLFMiMxal3vAe0HMiMUws6NSaJ7WNn

tMgWvda3QkwFD9DtGaYlEy8rynMhOKHT

hjViamzirxEPLHidOwU1TOUc6K9qymfc

RnD6qsfq2PJ4GIm1AYVwkdKueb87xF36

sYPqpaaM0HqFzSjGFkcoBixd8ZNH3dn1

uDv9SVgfUW39IIs8tNcz758bHakFPicZ

C2oGTReXvdUdZ5Jz61Ig1r0mq6v7c

B3EEABB8EE11C2BE770B684D95219ECB

YCM8sGoUaU1jmh1j15M2qS0LMIJaOlkx

J0bksEA3Nc1mI6xnOvQtusRgBbL88ZUJ

ZSO21PM30lkMK5VtmFwCGRnC4HfRl6Ua

USoK2cfxb51ZJPCyGLsl1oEqVq4F5A

eBNk3oMk3zKdgPZGJWBoIC6ya78Y9W

T6gjK2QSsLcLO7czUZGr1vXDcxJirDTU

POSSIBLE SECRETS

Veg1gBO6k29QtyD4vZdw900GGcMPz1j3

a4Tt0YroJWfViDs7yV1XUKalqcZLTf7A

DRjBJdg6i5DjaqZT9xtKW9OtehwlvUrA

DAigVkrFkMuOUy14T2FK5zmWgvJcln3a

Ni0kxaOxqNIZgR2GcCdcpUbwVlUuywv5

yKBaB64vFuTn7zYoCnuYBPVEHVJ9GNEq

kxYjy8Ef8Kx8ploZbzcG0C4t5bmlcMrp

FTSoQUV14LrBCysGNfyNvfqDH1zy4Xlu

AJnFEtF8h38YXxkoJFDHCzPhEs51Q6lq

MPdgTc6Z3sPUFClC4uSLQHQa2XebDs9v

zGz2rBeihUtTfGY2pcVtSmEx1y47z9aS

Xh7ZpLnI5g0AvtHLdYA6RWKofXnumxIG

az8CKzVkexBjitPsCylcg2AVWlGeK3El

ZCUrIEQiGOY9U2nVCEFSNgqRdbKvDffQ

q35Tkz9qNjTEzRlngClyL7KdK6wO30wH

SZljZRIwDL4qj86IVN03h7W6Ja49N5

UbLf4323SSK9wFof04kcdZ3h6JYQV0q

xF0da7GYt9A5Qra0MND7i27I5BG4MHvn

hbqvlfSPUh2jdrc5qFStp6bRHKmwzne9

uH4cRPiNAtd6hIF4d2nHkiKOYdeJaHzO

WkhjXxlb50SSewekCHh9frN5EhGMAbac

0eQRRAl5wHIowgG0OxNPv3O5UqdrKzzl

nE4owr1wlu2VobktzduoSxTpcn75jZ1P

W6t2vKaLS4um3MbbUQzXnPCaVdOtQDV

QhytIBUnuaSIq9HsTJzjLcd0Gyd

Gb301YYJpOgpSDcybjg8W8RhsXLlFC2

POSSIBLE SECRETS

1rXfVnNZRCMKSBmKvXBkqyIampQHuBTT

i9ckL4hGn3OwY3VfnpnVreAjs5dC9GVS

fGRgHSleOioyqPSfalDbi2Th0ZNuk

47AxPgGepX47UnNHLVE8SY2HaawvPhh1

LdxThdi1WBKUL75ULBPBD+QqJk2MWrfXYN==

eVwJkLn66NX0DyzCMNkg9H8sjiBrfui3

e87e2e48469682b08cf444b13be9c731

5V8W8EI9U29WYa7jcvhHGtBRQdjRXn2G

kFuiftK6CrUjCipoQAB5otHUPyyIQR1T

V922PtFQPE4Rka8o3RmIKSxjMATVQg

9RASlEbgrOZWYduHYKXmEPevqLf

3K9dx3znN2rHUAZqPmMaGO8Kk3HVHL

qBfMcdZL4b2QEWRUyBulqHXnGi8Olt5r

SLLQjWjncbGd9Rz2WSR3ZqU1MRAKPCr3

IeFog7wu84ahUP8wrgQRktORVTrd36mu

ABi2fbt8vkzj7SJ8aD5jc4xJFTDFntdkMrYXL3itsvqY1QIw

e8UGMtu5263EOY4JBlmpZ4vkWui3yNma

BS0YbHQAO0VU4qHMbgdjqGwsVP1Lt8hl

elFBINX9KCZeeh3GuBtXNkrnzvQO2EpS

xRDeMM69RKfxJaGWHgM2lgB3dj0CBATA

R6VLxz3UdMSFOznv3qvHILfZYgKZO5A0

VFlryW0SGhW14tSFNmX0iOPyizAkcqk5

vvB9T8WK7bT4nFgbnm6TlGuNwpdmRtb5

NWG3TX9NYXGrD16qfhvaDq7MonVrzPIO

2MJ6dS3EV8t7lzjHOstp9BZeWuWbqqlU

DGtgBZoK51CqJxDDYeEGQpaHQi4s0SFq

POSSIBLE SECRETS

ej0x21azMZ2lcGnVvFT8lesJnsiudKto

L6Z1FseRPLChQnX48wkOINplJZHgpjkr

Q0BiPrkB2PSWzVDnLZTkEnIKaCsuaheD

VT18E82QCK2DEIowipbGw7Y7OUzTjYnd

fqSGPLRwldKX66WDmKKlg7YQ1V3cstss

ThuVKQMdtpTlOVe04IgNONUKoYEgRLHM

zTHWwR6874BSc50B06ceZtd8OhPobwtD

uvnoFswQgKsjzwr3iqz20P0mNxal25YN

gbkiAVIrvIsexfHubLTCZsCFQN6TUjvY

l0NdMuNcsvV8BIpyxAa78ogafLg9twRC

8IQX3zoxYaZjanbr90SETWyiMVFv66cT

FGlKPE9c96UBdMv9ez6ncjACQS1IUqcl

eTFhtvXuO96go1LxaU568guL4Hk8KVyX

NJXAze39VMcPW1rS6Hs2IFfOp1R86yPU

50wRnqLOESyReC73zJKGvVAEIeXW1ukc

1157920892103562487626974469494075735300861434152903141955336313088670097853951

44613e39e85bc1e738f85105bba1a9cc564976dd

BA53CFSFXKNaueAmPJEc9hkRINMpWiHX

DUz1uNpjuvZzd5dAiuCT4alZ5wEF4BPh

VoY4iRsyTVm9uFdDYrz8WEjEYD2Z3Vra

SKBAj5hBfWgpr40k574HTlm5xQmSLGYw

YLuKSEsrRIdzXIjkloLmDmBrtZDR6KFi

cMa11vJk6adNmjyXCEaOSOhGfY6WoPiz

tRVDeAYq1jPcmMGohTMj2AD5wcAJrX0H

Ro2GB40CJjXXy4HKltQfUSJDg2onAoKh

AognuA3Gp5BMXUBAwXIZSKPi0LSslNIr

POSSIBLE SECRETS

YYoW0eMgewTEbJ6HTbYGGS2KWNlxhaI9

Uaa3J2scapV8yes5b6pnu2IZk0LU1rHr

BBj2A5KlY3fbXxZGsv419mNXSY2NstKD

SrFaCaqx6zHunknjrTMn1T9PINlSt0tm

jXVZsta3c8xywNXZowgjFmkHt9o0BB1P

S07tUDZ51Jgo3YfQ92rRpWn9afvBt6KZ

2NrlLG7hqMfWnzI4aYc74QPIxJ4DJ1XR

7qjDKaDRQc0Nql42std83YrFyKnWrUw

whTm18x0OTQIQ7vnp84USMuhENGtDkHvRo106n2B

eQuD8llomM2wZCZ6oqqCRxFaVaKQS5vz

oulCgqQ5su5pKYGJ0eYJOoBckMcEv73q

Yza27yUTeZsQZywWns2Eqk9QSJgdTaNC

GogXbqDElCJhME8HyW7iX3mlv0t9khKj

VY80zOaYPxkOtyUrTAwyx7zC77lFdeof

ntSwI9JMHlRTICCMPvPKnGLbevaUr6o1

T5hdxNMEH3a8tXz2YdYKh9bF2ZTD6zRG

0M9zDLqBQAVDpkbZHtwaURqwF1mV2f1S

NxWvGXn0hRg48TcTWmDqOrJrkhvriMf4

nmoLNEgpJzlygAWMz61JvwnNXURrvdZm

X5AboSvo1lhWMpgLhiETlyUxrei9zgpK

fa5GimV0q5n2gfKUlxWuqDakVSXec8h9

69e1b99398f8b835de860f242fa4b854

R0KoAZWGaaNUWbKBmgSqKMf6V9pQtd6g

zRruk8gFetbjQnDa2F20MljfYBQnm1P6

y2cTPgBEZJ0CQAPDGqNYJyLCowU9mkWr

SP8di31m2uLOcP53jnkdZfwtPUUyGlI0

POSSIBLE SECRETS

6kStEXL0N53GFq3V1gqexDowqRHYGeCf

pY9ZXifxArCVjHBuW1cFi0dQljuE9Tf0

SoHELriMkQBcnBScVZvUK7T5g3K9Fm6N

UkFdkMsPJijR7VnNGK8H6arT

7eCrAZGCjapRaLUbK9QRGJs0olrSOuKs

0Dp8HE0WixXMfpgDKF4PEgrQKOmjSnl7

ofzRm5oD0ZehPjXAXsE4VN9RCemE2t7K

tX5KRUyTrTKIf2eU3tc1SLWDMoaFB6a3

myGvayzKyHjMQEIVnJngawcUxLve9dSw

QJblDe3wVK6feXal4ldrY3QcOGG4UkHt

rCP7fK2t8T6BPFgVAgjNGO2T1MmN1wLB

lb2Z9KtgGwzkm6WUebOJTSliuGJIKPxa

idgz8GTtDxXm2DT6Q4W8HIp0oNrYHYmb

VeQWCF02N5mb5X7ahc1LI9FSMTOHD8V3

bG0ONBuurvv92UazdjN2MWGsVI3Uiutq

7654Ro0ah2nKancwMT2DmdIGdIXFgRyE

Ts37DulPc8QB3fV2ykqejrUSGmoT8jSS

iRaMLR8dbHBCXOgyzzarEjyYAsYlFtS

WLvo7626w9dzVwCTBg7InBeeg1a7HKE3

Zpgmgw2PULMIQ945sgsvBOXkpNFyy2RR

nsPDOGo5haoHqx4MxUvN1JuyDQrM6Fdb

rzZJHS6KiH5aslcybkMmKbRCqwolmQAz

HbMMbmPQRBR0PjZnzsYHyu73qTDtUO0T

YtTqrr36IpTZEk4bgIvsBXk24JcVhmoU

DoaGgd9KcWJSkB91JveXYFzycmhzEPJ7

4HLNgzBPZBjDavwa2VUT1a0cI7AwYTVO

POSSIBLE SECRETS

kTE0MmPx9fRa1cZyXVlJ3kyazaX8qf2

1ab62d33-39de-4a43-be02-a38d57cc143b

xsd05V2KW0Qtu4gWH7wQnZjvefOmt

V8oL0A47YsiBOfzmSd9PFqBcTIBl6AWv

28QJLyNvJNS9vIUzrH1yFxCTai7z0pp

FXbZWXffVyaneTw3kEwIh8dxCOHwnV6P

e028evzEPQ1h5lDY7CAKWXrwz5QUxGwz

zfgIUpP6NOwkKkp2713xr48Icx9i2htm

VIfYmPrZv6LGyPijtMThbF852HrrLBll

Lo0unCvqAQEGTbh5Ufe2FG7hEyoPqpU0

6i20agDhmSdy9vSyuA65WoFMQBMnYQqu

iVBORw0KGgoAAAANSUhEUgAAAAgAAAANCAYAAACUwi84AAAAAXNSR0IArs4c6QAAAHlJREFUGBljZsAOBIHCu4FYC5u0GFDwAhD/B+IN6ApkgAI3oJIrgTQrsgJIlOc+VHIukGZCItQGcp5BJScCaUZkSWMg5w1UshIZAsa+A5XcCRNApwmaANKA7IYJQD6KG2Am4vUFTBHecIApQglJrHYBVYLiYhMQnwAAeiYfS1LRd+4AAAAASUVORK5CYII=

VbLm6dZxTDBAJEz4a5qL5XAV7QNWTJHt

P2K1jmtqr0f0Y5LRKLvugbgPQbCJUIld

bOBzxUCB3cvUoI573SXQe51BlLqC0MhI

Q2G372PcR6NMCVFvdcIWGsw1VZvsvBxL

iVBORw0KGgoAAAANSUhEUgAAABIAAAASCAQAAAD8x0bcAAAAgklEQVR4Ac3KtYECYRgA0UnxAqAALMl72fSrYf8M74jjKGZDOll3l4g36dDFAYXiQKkjJH6ygDxMK/WFhoLhgYPGmwM5bhgAMvV1Hjo6FIqSw0Ml5YiGBIsnOWvuTAnNeLlg44QUdCJhi4lVkMmmWiGCVJL89aaWTRqTPH9+C3vRpygZ9roDjp6hXFQAAAABJRU5ErkJggg==

BOK6fyYRMOy6Lb8Z6odzTUAxqzIsXRll

KplVD0zBVazWxl2jPlpRDfEez76Qp1Fs

3vPfkmkrA1hfyjdWVmobnDMGeBIicVYm

MmKi7b0sfZEENPZj4CT4hoOnJABUQCnv

4HA6u4Nz4keiLa8sOcHfyEhD3wtH4bT

09HtIC6J3ndQ006hR2DfsxfysqzwGQ1s

wzhVBTrm4NHLde2dsMQb3id1wgsCAtfS

jQTmnshEA3vQhZuIt4EWQ9mfUiSmLT6K

POSSIBLE SECRETS

UI7dA5vfWz5Ps8yQ7SrAKT8QjM9H5yDE

tcU6jmyapCTPAiujYKdEShZXG5LbCi0K

IWWAGEYNIxKzg9eOqlTKJuHYobxhq8aF

MpMMJFxEruer3WajkqMUDKX0biSmQw

tDclRbsxuTPzi4rfl85ylCxCUvgLsm3F

GKunEG5yOJqaNbH3mPI7oznBCVpw

SBHD4zyCYYuTUtdzO3ruR5mHrnxwLuRg

83PSjlhGPkyHWD5a17BzKCZMIovhzHLb

goVzQt2K0L2BtiDyFGHqLLcsDevd1QlQ

iDDMQnl7H0FoGDQAr6PhZLTqZy2Xncag

wZJ8kWRxyYeI3b89D2ZfjwX8MEoFWOZU

tbwfvdKmgBKRGshTqqnFkMc0Pskkyh5R

5EX4ZE8RGyFWDwwd0Tfx6XQfl6R1kt5

zrL5IKpuegwH8b9kbv5GAokwitjsOCQV

H5jmeoVh4LyksNQ25zvZiIvxmGmhytkO

d80ONhhmndH09owa4u2QAX5SlUichMvU

OQn0GSeoKkB55mmrW6XfcsGu8yTW4vwY

lMymBa1GAS6gSrjK2mQJROkXbE

ckG7PMHxRgjSmMurQ73wQaoflHipTcek

WaXRugEVfO2gUoq5HkQlmshQZztZ0bV7

ClqJ6TE5ysQtBriEUDM02SGlAUBl025g

zM61rMpjrvDScug74JUjCxPutIg5FxhC

ded99b97e60fe6d768f0e2da3b121fd8

qW6uohj2RnSHed6NlIulLWXBUQuwa2BT

PnW2R0X33A4ZX5IMwZJiE9vO4lAP96mt

LelNVzb768HYU8MfXJtnH9MoMCR0fTwa

POSSIBLE SECRETS

FzYwR6pZvRhpGGq7M5V3OlHQnA3YkzU4

ayjYK9F9Z6sDhNCNS52R1Qcr5XRGx639

t4327HI34dmOHxHgJ5Xqb1TMdgfhViRu

STqVvaQvfsIBxOWUdRx7t9fX4dhB6WaE

ZtfNba1ZWzV3M3XLiIRFTuzciE54fxB9

0iuUPmPOuoIgxX336Fp1RztEIaFVtl7B

djRU2aqvmlim9RkyPQU7a4pzcS1yn5uI

LoaGbC7dgNNPM6H7LjLEtBOJkffBiTAV

3d79787bd4f8283a7c1541d5aab32c62

UXeRQ2HNaneiXsHAoGvRBzblNiVPPyfq

lJSENTz9psORZi9A2zDcPU2PQxg7yytN

BFvJ4Vglp8cDeiQE6xUhfEubFpJPL

NcYgt8CJQWeZTs6r7gmN4DT79HnpXepC

LdxThdi1WBKUL75ULBPwJ7JgY7K0DkeAWrfXYN==

m07lALOO7DiCFWJeqD31nTybPShDem9l

SJu8u5Zh6YlgArwXrUirNpL4997vCJ

DSz0vhavMIehNnnYUsD24XzaqUk6jyxA

wvdDgPhEetLkfVyUXU5OqcDmpJOXplEG

CrKixgnMYTd0duWjm1C02lLmQdQo8tCF

4fKWUv5SQTvzMYF7waz6SD9Pf2i1NBM9

rfZkRg3bvMesL7GazOt2jRzrapFwd57m

dmw4t0heQzRKMH67OrdKuJovyCEl55Ve

CR24dGTUbsuTHAJzfoRGWGiXpvXt0s6u

RSgGKx7E1LvNImGU4MlSenI1iZojkx1y

FbpHKh3QT1SdWaw7OeCQFPuoblxH9zoB

kxld16OEBNgi84xJjJHT7l1GCW5BWB1v

POSSIBLE SECRETS

YsWjcpRBLEj4Ul19eLlIoi2JTVU6PmF7

EUYS5WQpJRPmKwOGT0we5n4rvI

5brGPIOfpSxIScBaveghLVMlb1271YeU

GcYePxlnDkyLzFZQt8gXTfFAd

686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700 5449

KWsBEUuyQyen4sbZ9JEq20dYDlqTcXTf

GbuBsSM1xhQoS8Y9reObCc9WG4REEdk3

DrtEvBPOEdCgkho9QaC1rsvic68sYnn0

4twoC8d7INBRsRXpAg06MCBSmEgkqQ0x

CI0RkYQ6Qrjuno4ZZrcsG8RAmoqr1Epb

ySHp1IuW6hVExgFmQZh21v0rDd75pKs8

eY06ibbuLK1J5UWPto3xCw2uyWnrSlTN

JMF3DYKQmRYKnieuthRXwzFPxh0qj8YI

HvWirbE21CthcAzglwYfTu8hbbodSMpt

YJmuGc85y4OuUVwghPHMw6H0hrXdCbsK

i66o8C63ky1KE2dtbuTW4TOWqloIKDrs

q9EZ5tzshMpqIiwwl1g84eKRcuYh

6wPar1yvZmOBSMEilq5oC74eJWuAafP4

2DvdeCnwUfm17kN5FHRDQx8hBER6C2qU

9gkLXGbOvBYKsW5YBwzKkub2Nn3K8ZPa

WIuZhNvv8KxyFllYsT8aGBLDwb7Qt6lT

R4DtDeY0gnGqEQjTJlumZlRTz9kcJt7M

JA9mFndCctStcDzVBolZEhplBWXHl3GV

90eRnITlqXrODLYCktUoA3f94MaN8E2n

JLdBJvlNcDpXAJRy2UXokirsyAm3AHdF

RrIU59JghBJEpeymJLqkoB6uIS3R1kvl

POSSIBLE SECRETS

xKlEfosPJh9yMYQbCpjDM6s3zVcpxbP5

J6AvcZe6YXfwvJXVFlguqZimD2oQ2oTO

lEAcrUgQN40rK9SSjAwJ22cZB26GWfbz

kCtue8tdTX7Ntsd63evdhPLil5GlGyVZ

NAMxGSXXDRlS3a9YhTQZIWUlxo26242h

1GcjrCMpoDxZbcTJPp4flsza35E3FHOH

DFK/HrQgJ+zQW+xUhoPwJ7JgY7K0DkeAWrfXYN==

N9t7LqoVZtJBHPDtx6gFeqCCQFc4aoCh

NwYbQLWQDzvN9xZwkujqy0rFcq6udtvI

QRz84tlq3wllCeb1capmh87EbVgo0fYM

uH31h0PRXTyVkIOgrCb5PcgaQIfZ1AyX

k8iQf9qcWVOKHK95vPBLm6lU2nxwg5zN

30fmYRrKRKmRtB2S3A64jwECE5mQDy4lQHupqSGltpZaQ0cCmYOq5AXl5f

Nf7MRRwZDvE8y93FmZbCxZ1qYSmL5

STlEyQPStERy8tSXGvH8F24LWNUxdBhq

MoxGygSa7eAdiXsYbQTOC3oc872WMu3f

U5QynYTJKvqXrBDteFA3kKN8MUDMbs9q

lOPEGaBOukTHor75ISwx4eUskGtuKXTT

Wp91UfiY68my4gPNmlIjqqdWX7WJ726D

eziTD2o98diJZALFyHxZflO5bO0xqfa9

az4oatOqZKbyVNpIoLDpKLWjQ80V1Ke9

LtfSHnVMNf9jD1VPw2QJdb6akNXb3KRw

H4XFnNQqwOU0BBxHSKtA4senwYzulcFS

rZKbd1qqPOm2jxQd70eAyB6uz1tOgPbY

Xwhc7JDkSZbpBXzUBO5xvnc0Yvh1Hw2q

DFK/HrQgJ+zQW+xUhoPBD+QqJk2MWrfXYN==

POSSIBLE SECRETS

jTJN86H0DvMYpZ5S4bGPoLkC3Jk4zW8z

97APORAguQeQpweI2T85fGR4lID0xZM2

s2EXwZrfzgHoO4PfEfdPmYAG5v8xH9jH

zZ2K2ZPCRMNEr6MS88VYjWdhzDoMY1p3

4IRJGuEovS11eWhLlTHcTHgAIcL0Dfrc

n82TP93wz0kvvP6hrorLqVOpldCSHKat

hqLJz7OFCqwyqI3Xl9C5Yk0lZKMX44EB

KvAzUjsGuu6UHJoTOmt3i913MHVvWe2E

MzIHyiWSWVKcGZIDQW3LWEN9ullkmdDP

WKz9sdTUAmARQIiAGrL3MFtxaOYNqSOQ

qGQ22GZNFdEfH23m47dfyhgZCsriR0f5

s31M0lMjYrtgq4OJcDKBiGgiocxpngd

iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAAXNSR0IArs4c6QAAAMRJREFUWAljYBgFoyEw0kOAmYwAcAbqmQbEQkB8igz9FGnxB+r+BcT/gfgPEAsAMd0AsuUgB5yhm81Ai9AtvwUUk6KXAwaV5TcH0ufD03JGLAkJFOdrgJgFKvcWSC8A4i9QPrnUX6DGHUB8Gp8
BHEDJD0AMyma0wF+B5qKUHUxAgQEFsGCGOeIHkBEPxLSMAlAIEwToeZ+uOQDmulFHDOqQoGtlhCsk6FodY3ME3RskMEeAmmTbgTgXJjBKj4bAaAhQEgIA28ZhUJU6FRwAAAAASUVORK5CYII=

cqlD2dZIdmZjhBfVp9VUMkw1vxAb5RnC

ykDXgz0RSMwhstOtB5XzMrmFiU4VC1of

yf4c2ua2Tfc1Hpd1iDrbnRZj0K3dC2iJ

ButKfEyieReZO2wb3N14oIodeWUfkj1h

o7T1oZxGxBAHWlRkOQbegsoO93grXIxk

Y6AdbyooKlLQqvqU7YO0Osoc2idrR8tf

Rlzv6bB7Czucpp1t79MjvCXFuIOZg8dc

690a2f7261df34715b27de982bb5ecbd

QzXzl66JDgXK1aMRt97r55ZmRT3IeIsK

Exq6DKTWLIzC5PVLQAd8YA2GF4DsQGTp

ayJKSMoIzNcUU8Q19fzYl1UxLR6MMgkq

dlMe6TUFAyxvhKGLzAxCUk9grhyb1S3t

POSSIBLE SECRETS

NmjzB0Xtr3isEon9bZHWRNmwidAWwXHD

j5XcoEcQeBll47Gmx6jJ35WP8DJmwvrw

5iaWNhSEWXdQGqHhJWYkL3vAUnXTRhmq

DFeuWkH0W+xUhoPwJ7JgY7K0DkeAWrfXYN==

8BdDEGBeUdZb1tlGAu2Ypm8i98dJIYsP

idZtcBMWKPNqKmB4YuvKnZ9J5oClLNYc

GzHB2OA1jqluXk2iMzoyOJbysCDiG3Ta

b7DBuf20fhmi4MvO4gTJDnUAFhtFn7QS

iVBORw0KGgoAAAANSUhEUgAAABIAAAATCAYAAACdkl3yAAAACXBIWXMAAABCcAAAQnAEmzTo0AAAAXNSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAADISURBVHgB3ZQxCsJAEEVnVWwsLGzSeAgrG2vBzlt4B+8gXkKxtvQGWthaWQg2VhYqimCyviVT2ATcTUiRD4+BLPOYVCcuKFBSTdWVtiuBhjEgkJkhbsYAM9CY2KjjbN2cmgJiGhcQwHlW1hECSjqamyE3xUlmvNvsoqvuYIYp1s9Xv293g0RpShpJf4DnvxDZIOzOEBT5i5byGSJSQqmbp/5iuJdBInuekk3pJC1mnAItc6KmrD22cdkyGqUybwgjXv0VXKyheH7ycYXX5AAQAAAABJRU5ErkJggg==

rsIWlKhu3J6TXEGwN5n8WqvEWNcNOt0w

uPcs22Bv4Ecng1eDU86bpHQLBlw1u

1YGAJJrzxjLCzaCnFt4GS06pgnkMjMll

YhJyuYe5vArJMmHzMuaOmLSCLmdqTU9j

egbXgGoH9YjwozG9OeqzlAo47BIpQrUt

7WihoyLotnvTQHZz2idft8ZXTVKY4zx7

4KPhJxryuqZouci8ltOnoaa6GepMOFR6

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

Kaa8VHZO9LzXf3SQPwn8McNWlttqakzD

1ZkmGDQLr4HHzESqnZwtiaJskrCoCdgr

19NDzRR0DB7SK3z9xqtaZiHwxOVs7vz5

NtNAdXJh6t2g7Pbo04GbjidImmETcndF

oJC4aegRhEHHJQ1TmbM9HekITZxf6oV

zb5q8BZfDBvmVPM7uFOoyQTMVCraB8xF

sqNpl1OaV4AX2PiDopzrEiO6zTyyi8x2

KWr2MioisOT1RP6pbxaLpNmtsO5qpX4q

POSSIBLE SECRETS

Dj15PNqThKzSJ5rgUYjkzYgIYwsmp7Zv

r5Ph5bZgG7AgDyEHuQeiaTUpJXkd

Qnd9EPcWsl8U4hISHZt2qAi8nsbxDXMp

R7n4O4sXNkY4yft8i0spMty7BWheUJ18

Rx1vO7hG8Az7i2Yj5pT4De7fyKew8lrJ

OLcmUi74zHQznPcwd2HExE6T020fWxqu

s8BhV7yvVPv9fWwhaDhts8ISKp0Ib3uz

tCQEbNaJVz0PlCRSNnPyqV4UH5k0cfLN

G44uIPn0vHKMb4gl1i6iMEVLbqSJJUyD

9kVtZpYuS1B6eNaF5MtLQpOmcikxmxeD

baZKEFvTxoHzeItuM7o3AXmynaYxTYwd

S3cqE9iPcF9hTGsbBg8LQ82o0ngu41Kq

4DPNNdejLcG9vMJExCrSPytZ3gIImbXA

5461499f-3294-4b92-b80e-5503b344753d

UHIahekmnsnG1d53o8blPpYvLvDdhHQg

7EM55IZD6WJUcGDkvpLhGBZC82NS7r4s

JgOQfSPAOiHiw6Rg9nCac4dnqR1hKwEe

0Ki4JXOncLynPK6ypbmoO1JP8yrdQeak

gBI5PCJLXGTma8ivl9EUy8DAEVjXdNbR

IGdwwTQI2iFuokxRsKC9HYA9e5TBmMKA

PK6Ri7QZ9VeoID4nNvuWqmskCo8ysON

ZuXKvCVbKiCO09p9pYqDyLAizJSm2C6Q

OCmo2WCRSteO5ntkzBQCJXTiECLA8K2u

sVEOjn8EJonDcZfN7QRvAJKGT0zqZa3R

LAzIqji4IuYx9FVtRgQH7OQvPgoyEYhN

J79m4yZ8T6gMUys2Mw9buLKZFKLQuXB5

POSSIBLE SECRETS

3HlyBddE8XVn9YWwOLwH4VSFJFUcfjL0

MOipm8XgicKDGsSG3YNTxkuPY6Ba7MyG

EbIk1BCgQ5uw3o5TzCMO1ZXZATNxIl6G

39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

HOlKa3VqrZNKzXakTySiImjoYLF1tZiN

8eASqq8qOvmTayVh8jwUHm0gJrEDzEVn

1JhoOK1lCeFzNpWXu7eAiStn9xCsTPmH

2SWBRQD5cFodCmXbUuvI5Vs4hvMM

oClOzaysC8x4DOGoit7i4h3Gpfb0OXMF

IBZtQd8oLy5hBWitakJgcXsasC5LRKBV

BIp7vzupCQc69wolM1qrlBnEL5MetbDW

DTiQjOeLHS2Pt5vxV6oLe4amAnidYBVC

F9UQYukVDOEwI1lxcupNtKixpZh4OtVr

cEMi7KsqJ6Y68dGPnFARRJAd4Z3ugaKF

WcHPi3i27m6LdaHLnkH9ENRpFxyJu3g8

XHg5TBVpct8AEYnDVgEX0lIhyoWixNuU

LlgsTT0Zui6IKPeQPgD8fSGM6QqYY5Rc

WQofXYOtPOfcZVcnLB6jDFevspEJYzJo

c8NCicdTZLmJ2inXNQ3toHzjPVonMpXv

4H5Z0LJ7wdDYVvSZnKKEqH9oXzt

kkjOWDxiYS6HSpJcTpvH6ub4oru0qlUQ

szJTv6Q1Z3W9cwFEkaj97Hf7uwsDfHCt

2WztFDsRGhQaALYpxh067UM8

UcSDNoyAd7hAuBmsZZHLguWnytii130l

0506SZgMJJ7sv8mHDOEz9KlkL25eIrXm

QaRNxGLOob9K4H7fRMkquel3h50VelkQ

POSSIBLE SECRETS

oiur5Gbx9Vkb8pNp9gZzU2heRSdk76uI

6qW7u5SP6R0wlmhQUiBuXDFp8yf

xjBfTCMiG1bFh7NB9hwMlLVXQHNbTqdl

8CaJcXxFCBt98SljWoeRspku2MSdKFfE

LTFO7rX5uSjfOX3uaTYKwhSNZ2EHHmg0

e5qOGa2bHvCngaVTbxNZ2TaAb3gIhyF7

oL2e04jbfOxdtKuwfeKQnW7E8P42I46y

XSQst8sM3v9Waw60ED5t21eOsn1IQUtw

YVrA88PsPmqtAXS24dEjb0zjZhY9NNbQ

J0QPPK8CgABCN6AkZrLHMYAzYl1dWHal

TMGBJitMUu1pxt90KbWrvOLR2BVfJ6J0

ED7ecOC6EdeJIgNMIPoHmXrwamnQGstx

nU2m6dMK7qfy4atV1JxTmvIeg7zDsgbu

B6gN4hzeX4EfdYzWeUb7VxyWyH55Crun

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

oaZzVubNOElt02WGCaqvSJ1WhomZelvc

YDpf0JUXXv3vM7KYNqlKfCs4JIrQ9MgF

fQPNbuq5zM2Vt99anBRO7vAhC8TCHPEC

iVBORw0KGgoAAAANSUhEUgAAABAAAAAaCAYAAAC+aNwHAAAAAXNSR0IArs4c6QAAAPZJREFUOBFjYCAdWAG1PADiCUDMBMQkAReg6i9A/B+KZ5Ki2w+o+AeSZpAhF4g1IBKo8Dea5utAvjQxBqQCFf1F03wOyBclRnMRmkaQs48CsQAxmuuxaN4DFOMmRnMPFs0bgWLshDSD4hUUNbBogtHLgGIshDSDFCzFonkWUIxgggE5bQMWzX1AMYIAFCi7gRjmXBjdSFAnVMFOLJqLidUM8hvIRooALi80kGIqRYEIs4iiaIQZQlFCghkConuBGBadMJqopIxsSD0WQ4jOTDCDcGVnfpgCYmiKChSYBdiKtGtASaKKNJghFBWqMEMoKtZhhqBULADcM3nkekaNxwAAAABJRU5ErkJggg==

iBPKumYfmLb65bhUzcw7T4vxhwf25kYO

nmSIAJ68DE4LOtHWgfxbIiIOKN

JPSotx28OKEE72Qpgvn7eDCIGwp5uNVo

Q5cfUKUjlAvrOqac2Z528PAxhBhncEkS

jvvklgZz86ILQho3AkuU13PaaICs87Lx

IHA7NybIhxX3WQx4UeYLmhksL6wDXcjz

POSSIBLE SECRETS

LOR0jcP8uyvbiYDNETVTqINk0FH7KZ

QPqS7MAagvQqYe50TQs3IlpOEHW3O171

5OxuqdKIp2nP9LR2zHzFDLENZioxECvO

xkYelsmw9O3RFB2zMTQOqufEggZJfpsf

HWsJryVEgJSZhaoZ2KYBbGnKIEi57XMH

6n2viGPYj5SHhnpzGoLQcwunY5cXqvEW

FqkYvgsNMANULI15i6yaohJxBf4

CbWdg7Es3Lgq62AjK6RJTjV5Dc6KX2S1

yfv8cLzmeBPWJWXBFW506HD39p2knuA3

2RTdQxHpZZ8AiQDKhWe0eMGOKfA6zgcU

edFq1RSzVbogperxRnGO2mwS9T0C3jXY

64LnU3lhwQRNyBCw5dlHSHpXej53Kco6

lqinWbZDhv0Ny2jUIa5P6Phm3DGMmF2T

djg1XP0D7NXFeZ0NOExGmhJDpZKI4dpr

CkflbgsNAkMx06fZnMm4opLTGkpn7A2i

dSWVRlyTiHf7svvh2WPzEDVR9b7sv5FM

K4oeerNs7A1VEBeDem7X4xZbHtBFCQWn

lKrFFJxvaHBIh9KU9RDmbthSOvdNTSOe

UVRdrrF5AQHdn5VM3Ax7WcOvit3GJvfg

YQomcxwQ93PK4ynsoGLiAyy456b0aprk

kVTxxC3LTF0fLMRDW8jGaPZPlig8JQO1

pXXvlweo53LEBZFO8IULCIdZyckTRG5r

hHVLoZdNuWeEAEugaul4BO4ImQQR7t2p

pWwXLaHMc2CIhW3XIuObF4bvoKv8BfMZ

ovWB89LlYvQ4xO5HZfV2GFW4RL9XN4h2

2zepy1PmZTCf4jSxyWiaVOuG1uYDUhxq

POSSIBLE SECRETS

NAQqKhMrOserh0jW3K8lxYdSIBMoHwEI

mZi1y4qoTe3Eq90wST2K5ufjmqQARasa

421986d539ac570be1c4ca01beb4

5gEoeYtHKqdKxvGOrBFQEkCXLQc4JGvi

4qUlfR9eL8Wvw2EVoaZBQCPcIiUI1e32

dBJrsGAcHV4edhw9dfAhPQoXUspDKIy9

crTnJJYSu7Bzqj8lWvsfk12r9Prdsw4f

qZW1itq9fL4xwHRJYlEkMM8FtfnBLC8V

sO2hGyIlN5zgciGhFXZ1rYz4NH0oO9ru

sUTNp2nMxY0O1vbAqz8mD0UyRSKVk6HB

TEDKkRRul1WFzr82L9WTKNimJ5QIfSph

nSSDOEXzoGvtoIqz4QDa0TtkmnPlbH1G

lO566f8c3ZpTrsgNovf1GdP6EuJ1Ihz8

7TPgv6JzmOMJusvdxeRCHMdlPjF1ygj3

0M30bmT4hYz4ZuhjE8LXlv6wVKZ562xO

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

s9HSZGEi8dFN8vFbKvf1UaL44HFpBCz2

gTtjPRse8wyQODgaJCc8oOoIzj4GdKlV

jFG3gQjXUuH0GALbmhZbm14pHMTfeDNL

J923MGmbHd249pFGu9B8ymT8z7je13tC

gVjZHTAPXXqW3paCpGTUxeCgOEd4dSxo

LkxvoQ7DD1pBAo3rq5X8aF2iImmrJAYT

wNq2gfAl4zWIB1XFoKeYdvHUl0gsJJAY

rXbUFyh56idg3rSuJ4tJQtpYdGaFTF2y

2bLZXAk3pl72OxsXhKzzangZVfhmAhBr

de5uy2BqkxnoVETaQgG6018QJ

POSSIBLE SECRETS

1t5yWCu7Rr8GJSKN0jLr3suU4yLwpLao

ZTG0qcJaBRai17vkpDLZ7jbeFwjjrIPL

fGPiNZIH9FIGNZUMCtCVq24hO8AJIHug

RIc4tTFixsMvKq90zInLLBFrOnvIp26L

vll5a2o0qWuXIFFWzt9Y9A9nrgE8UKFv

xa3iAkfTrkxPXtVHKDgHiLu9rp62G8cA

sW1q2ctPu7RNrNZv5Ej0VW9PcKYvvqLT

6FY1eZNyDjZQrv8Kxagf Jj6lvFVpVQ54

Yqk1id1iIWcVp6vlakHKZfjEHLsXJfOv

pnRx8X5Hy3x4IRuF7DDbibtYxh7eaWKw

m8f1TG9WFPBUvQLDx3K0MLj2Za0d4Euo

Dg1K6DVjcfMH4tCqXC1sgOKGeA5uth3Q

QqvGYdLSjaASY2OhI4i6KQ0w0ePoKf8h

jNVCF7hNBx7qTlxJtSxtZf62y0YMH9ti

GuBrpivSQbykanIV4Dv04bmlZ4tKSmwR

BHQbL486YclXfOG4TttSSmYhAQDicEvh

47fcOB6GOJ9GbfMYvfTnL8sz1WC6cZa5

iVxsD1Hg3ZcKsbvYTUyYIrJOOlBOlPT2

wC9e9nnwReFs9ZTI4bgFhMBKq7UfutKa

zdrgnlBB6epFGiAXytvDtgh2fpyUYHeQ

T5MrOQzei7G0RtN59lzfKQqgq2SafeDq

2yiBwXDvjLEglhUZ76UGTCKc6ACbYUli

hXJT0tWkN7S4w3G0a7yWDauM9ZCHUr7o

QkjbeLtEXK6xGgNvZ4ng7fB3y1rOF3bp

A1JfXRpmh7pGoJx4KgQXcs2DSpbOe785

iEcBvH9q7CiihZ6SUT8L1eAmSvCZtCKk

POSSIBLE SECRETS

a9uitInFNtOBWkculkeZqlUrDZJBx3st

yQnpH44oXSx8ccz3NjdKCULhtA2Hxjvh

nWHC8GobiUTV1BRDhLkuPrvX5

vvJx1YlMdzFVt9WMGmsv2mWYh0j6ZH0a

jJ62S2YkTrNcVcfPKr8ssmQcBjICfRdL

YtNF8b8ioPsgGgaDUde7WsjUMR00Jzoy

hlZJhcxljYiKc7UKHZyQNCRGeosS0rVV

ucBpJzW1cVnftjPi059PqZMmOpUXxZKe

zlzEwhsQC3FpKQNfU72ignmkxEXGlEWQ

GkKhWAhOLudlAi1KBbGzOYTYZtsrVTXq

FE9c5HnV3VVOUNIp57h4JuspLxtKtT80

YCJEv0AAmy9EO19MFuS1eY2psLita0He

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

H8DZxZg0P9MFCvur7W3rQA1KNyeBpUa4

cEFw80voMQ3YbzzTADHjyBYd9BAt2Eq9

CFAR5D2KzriYQAsOH0D7pU8M4hZwzvIf

Yhl0jQrdp33aIQ4Nx5XRCxKVIJRMQ99k

GxDga6TmLrnNDJa4WhYbU4AfHiRAiIT6

0N4cBU0BwI9IykoFTfvVsAw8l3nE

BVuPoTZp9gA5d2vDS0fzf54bf8rPPFO1

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

Iz4TXcr6fUIHp2VorFlDJLDUzyiLCaPl

LcutVO6kpZJheUIWjBQzEq2ri8qFF

iMp0vhQuApByAzd3UlzuqPNosBBIij56

xvPzB4voGkHgvzabNn8fejRwCVSwo6Ah

POSSIBLE SECRETS

Bq2StgQbD5mLPjUE1dw95ch9p648bptk

RvEZ7gkpXF5RUk3l1kihsAxfWlQybyIP

Vd3PIQVGbymKr1peOQp46bHqBe5g9xLl

dKMdYOTDZseZlVx05Wn1bVYEVd2S8aN3

GxzPigdu3bGRa23YdvFpU3mIsN0rCQhK

3L5xTrYaZHGbjsCndSxeOQfzJoqaksAO

nQvnpoALZKO0zXY3RitAVIcIBau4iEu2

4af792090ae04118bb859f4b487b75ab

h0emITNVyHPC7rvjgGvXLhCkRflG1h5g

3QHfr38dRkY9JxUpCoLwEkFMMlSloeG2

kYDrs41aRZaYTR0SA8npQuCfjZz7Tio6

v3Z7C81p3UBYKX6nY0MAEeka3DNz7RKw

wegMd5NqqvgJ45W9ANASZrnEtp1A2mXR

IRPRX55QPzo4gZSSSU3YM96DmJAcp5Ck

77nY8oBWpidVHbM4I1vmA2HaFAJ9JryL

oLzw2E9OShYSASB843fXRAiyIcSfpUGD

4SjpGfk5gALOkzJ9eVK78zFrDbXv3S0x

frFBuXumqsQze9gDO0obsB6cGwssnn2k

BRUnQfYxuNAflpssI75kRVaGcWKGRvnk

qHP9yOxEhBEQLiGQDtbNN28OigutVH7

pI4BrYZb6jEfbOR6K30piOXwM4lgsdMH

ZQcoPrIpqtUFXXAsJx1eZkXQCUYQ0RgB

cigJDFmR8APB9TZFazKvkLU6eV5xdG1z

dWX8I2VlCkDjmK6jHvJYkvPP690yaesv

rdyvRl0mnrLy9iBwCAplKJJzDaMabc0M

03i3f9u06CqTOPMXzFUkxIwTnPnoVd6c

POSSIBLE SECRETS

Da4E3gv4xQpsqKTZbnCdtwn7j4CUP

T1QHzlAro5gEiHcOkZamY04XD

MIua6DThmQIF1vqzpVDjqirjX1nsx6C7

Hr5eJHulkK4DitXKqFdG92R02ijGovUO

b81cAW5lkkuLKoB2DrgmzF0LBXDk4R48

jdLKha1Na7nbzs0Nk4YLOHAcdwecuvvy

ef807a385db77e8b614848147389bad2588af85680c879bb152a51477512da42

9B8Fyg4n1zOjDAkl95LqaeehXECnF5Gm

8Yax76Lu2a2dogjn3GzeM1tk0kWHR

gyeYb9LWXFqsSrKIVSRt0Co29LGYuhaR

BYlHqNK3eo406tllZNUH5uGyHKGLxPsS

uPRtooN1mrpPWtcIlb5668ZKfYVdzjkj

O0mirbIFzClHmiQexpJCcYhfB2GNllwd

EV4d58k22VMnbcsySNbmwKm2xbXDyfIQ

xEYdbkQkXJmqNi6lUscBQUgiZa7D0Dxz

DoSMlBJtaYqhAaTANnzLFPIy6BzbSWA6

ElxVODxrKGpjZndubW1J77FnKIhSKHYN

7rMeuqy2Hxf60lom92u6Rd8CNEVHdO75

4YWbA25kauTneX5iGtOo38Lw

qsbydxnKXALymqP4MnHEOj9tIKxnSORB

ou5H6BmOyErFNkIoNYVTqPhUeuo6kjPn

tJyNa4tKeVwhmsG7D71bzYfBkrrYu

hqnyJICqt4CMDpPSN8ZqMHnf2BtaEVhm

YyZf9NPrzEzMWmx1W7C7iqaeo0zUpAtl

GyHEsdoLJV3XEjiFxTFX6orc2Mvnrd3k

4sakcIsy6w2uz0nPxriWxgex69qzPMi1

POSSIBLE SECRETS

VPPe2MO9HED0sxCZzVAB8cvkabJHsXeP

F30RTtpMpumHuhVQJj2Sxrc5BnRJWEU6

pMT1BFzteNKtMElnfmBSO9c56WwnbBlh

cQ2wGPgO9l4ITB75rCj9hGEnqQmfMy7J

RfkEvBXgrQdDRXJFP9mAr4EwuLKmJYFp

TDiZuYUrZ6MPuX4KNh2dPAHwvpWNvxQd

aSBFun93hJrKs5fmh7DDxXeNBftzg4Tu

fiUEN16u3MZCpDGCMqSf2x4N5Q5QlPxX

EhbVD2npYjMN4Lpqgy2TDazDwa0P1ZFY

FAfgOs6oiEmG6wZbyRFeweQVagOJo3Y4

ey6hB0JJVrjTzxOQnW2QvZgefAY6GTsJ

lVdN0r5Tix7dFhz9wGL3uSfPdQIT

5QLBb0RtzLfAnzhUIvcqgNwpwZswqR66

9qyYxkloNYGFw4rMCbrwSMHZV85hWfZp

EZb49YdFLYqoOlZSlgWLmpmtHQMVBG5j

iVBORw0KGgoAAAANSUhEUgAAAAwAAAAMCAQAAAD8fJRsAAAAVklEQVR4AWMgBNgBNgYJjK8A8KJQBYK6GJ4zBDNEA0kO1ElPgIFQSCK4TWqxBcGczBtDmQhAUuGBCRoChPmZPjF8B8JfoM5QADIQYUC5EowM1xGET6HNygAkIo2DuA7sTMAAAAASUVORK5CYII=

GT6M0xAjFwvMFnv3NZosdSbEhZuyGvXt

9hzCYTVbSoKGzhiGE0INbgm8vz2Ul1tD

Pesi6L7S5NgS5H9VNXNfznCxhERgloSD

wPQqgsrO3MAOXcdZXrdV1WawN6tKhXR

fe7fd75eedc3a9a4b669fe8c1921

GGduL95yG2tM0AFXVNzOOayl6jJ8thFl

lWXZgTR79dXfBN4bKYDC9NT5SIZThBqa

ylxMzgRnic8ELdWNUfQitMVfYj0C1DI2

lQcCmoZBYA5tZudR22aEG8J8TvwruM4P

pPlbIWWtmQkYN3MHTwcOdVUNUzBLXTby

POSSIBLE SECRETS
i0gT3y5gW8KzD6GAKa0KnQ1HdBIZCzpI
Btjplq8kPAGjfXOAnbhpFCySBxhN39
Alxm9pRAksCVWi4qdGhYTOlqnuoHaQY3
jlPWqnSdxT0Usk6otqcOvu4ShZWMKlZ7
xGy6wksCbV1DRuK7mqOXpPoeqCYQ0xXA

⏵ PLAYSTORE INFORMATION

Title: Macadam, The Step Counter.

Score: 4.5007033 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.macadamapp

Developer Details: MacadamApp, MacadamApp, None, https://macadam.app/, contact@macadam.app,

Release Date: Jun 13, 2023 **Privacy Policy:** Privacy link

Description:

Discover Macadam, the revolutionary application that turns physical activity into real money. Whether you're taking a leisurely stroll or in the middle of a running workout, every step you take is converted into dollars. Macadam is compatible with connected watches and uses your phone's step counter via Google Fit to track every step you take, every calorie you burn and every metre you walk. Looking for extra motivation to reach your fitness or weight loss goals? Then you've found it. With Macadam, you're not just active, you're rewarded. Every step earns you 'coins', our virtual currency, which you can convert into real money and spend with our partners or transfer directly to your bank account. Put on your trainers, synchronise your connected watch and get started - every step counts, every step pays. Fight the sedentary lifestyle with Macadam. By encouraging and rewarding physical activity, we help you stay fit all while increase your income. Whether you're walking or sprinting, the important thing is to get moving and start earning. Your privacy is our priority. Macadam does not use your GPS data and will have no impact on your battery life. What's more, all data is anonymous - we will never sell your information. Any questions? Consult our FAQ section to find answers to all your questions about our application. Macadam is not affiliated with any other "walk to earn" application. We are a single entity, dedicated to rewarding your physical activity. Grab your trainers, hit the track or the trails and start turning your steps into cash with Macadam, the step counter that rewards you. Are you walking? We'll reward it! Download Macadam today and start earning money while you stay active.

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-31 01:44:32	Generating Hashes	OK
2025-08-31 01:44:32	Extracting APK	OK
2025-08-31 01:44:32	Unzipping	OK
2025-08-31 01:44:33	Parsing APK with androguard	OK
2025-08-31 01:44:33	Extracting APK features using aapt/aapt2	OK

2025-08-31 01:44:33	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 01:44:36	Parsing AndroidManifest.xml	OK
2025-08-31 01:44:36	Extracting Manifest Data	OK
2025-08-31 01:44:36	Manifest Analysis Started	OK
2025-08-31 01:44:36	Performing Static Analysis on: Macadam (com.macadamapp)	OK
2025-08-31 01:44:37	Fetching Details from Play Store: com.macadamapp	OK
2025-08-31 01:44:37	Checking for Malware Permissions	OK
2025-08-31 01:44:37	Fetching icon path	OK
2025-08-31 01:44:38	Library Binary Analysis Started	OK
2025-08-31 01:44:38	Reading Code Signing Certificate	OK
2025-08-31 01:44:38	Running APKiD 2.1.5	OK
2025-08-31 01:44:42	Detecting Trackers	OK
2025-08-31 01:44:49	Decompiling APK to Java with JADX	OK
2025-08-31 02:13:19	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/0088335c2392e56a60a22f4e2e8373f9/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/0088335c2392e56a60a22f4e2e8373f9/0088335c2392e56a60a22f4e2e8373f9.apk'], 999.9999858215451)
2025-08-31 02:13:19	Converting DEX to Smali	OK
2025-08-31 02:13:19	Code Analysis Started on - java_source	OK
2025-08-31 02:13:32	Android SBOM Analysis Completed	OK

2025-08-31 02:13:45	Android SAST Completed	OK
2025-08-31 02:13:45	Android API Analysis Started	OK
2025-08-31 02:13:59	Android API Analysis Completed	OK
2025-08-31 02:13:59	Android Permission Mapping Started	OK
2025-08-31 02:14:11	Android Permission Mapping Completed	OK
2025-08-31 02:14:12	Android Behaviour Analysis Started	OK
2025-08-31 02:14:27	Android Behaviour Analysis Completed	OK
2025-08-31 02:14:27	Extracting Emails and URLs from Source Code	OK
2025-08-31 02:14:31	Email and URL Extraction Completed	OK
2025-08-31 02:14:31	Extracting String data from APK	OK
2025-08-31 02:14:31	Extracting String data from Code	OK
2025-08-31 02:14:31	Extracting String values and entropies from Code	OK
2025-08-31 02:14:35	Performing Malware check on extracted domains	OK
2025-08-31 02:14:38	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.