MOBSF

ANDROID STATIC ANALYSIS REPORT

Lose It! (16.6.702)

File Name:	com.fitnow.loseit_17092.apk
Package Name:	com.fitnow.loseit
Scan Date:	Aug. 29, 2025, 10:27 p.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	30	4	2	1

FILE INFORMATION

File Name: com.fitnow.loseit_17092.apk
Size: 87.08MB
MD5: 0fc1185fe46342f9d6546d67fae02b4b
SHA1: b30d33b43a14c4661663616f9aa69fccdcaf62ea
SHA256: 0a29bc5a5f2de9c41871647210903a5a7d0cba8c4f90a099aebfb9521b821bfd

APP INFORMATION

App Name: Lose It!
Package Name: com.fitnow.loseit
Main Activity: com.fitnow.loseit.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 16.6.702

Android Version Code: 17092

APP COMPONENTS

Activities: 109
Services: 21
Receivers: 20
Providers: 7
Exported Activities: 7
Exported Services: 4
Exported Receivers: 5
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=MA, L=Boston, O=FitNow, Inc., OU=Unknown, CN=Charles Teague
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-07-23 13:13:36+00:00
Valid To: 2066-04-25 13:13:36+00:00
Issuer: C=US, ST=MA, L=Boston, O=FitNow, Inc., OU=Unknown, CN=Charles Teague
Serial Number: 0x4e2ac900
Hash Algorithm: sha1
md5: be90e9a17b539402de871a2baa171ccb
sha1: 012d829a881b32666e51298cb8a2d386089d4a34
sha256: 5db75d6c38c43bb9ef440f48ed8dbb58b3bf757162dc1ed24420db95de04bfe0
sha512: 8891f8dc48a8b6b7a8b660903f3c07d963adbeed797b6463ac0e27a5a266b7e01fcf29ec05bcb314957899787057f36bcb0ebc7678fb7845da98eb421ad5990d
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 870451e95cba385e252c6f27fb95bd63606cab3fbf3ab7fbe3a44b1efc6e7714
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.fitnow.permission.LOGIN_PROVIDER	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.health.READ_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_NUTRITION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_NUTRITION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_STEPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_STEPS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.health.READ_EXERCISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_EXERCISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_ACTIVE_CALORIES_BURNED	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_ACTIVE_CALORIES_BURNED	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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_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.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.AD_SERVICES_CONFIG	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
com.fitnow.loseit.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

FILE	DETAILS
0fc1185fe46342f9d6546d67fae02b4b.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

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

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.fitnow.loseit.MainActivity	Schemes: loseit://, http://, https://, Hosts: loseit.com, *.loseit.com, url1729.loseit.com, links.loseit.com, em2.loseit.com, Mime Types: vnd.google.fitness.data_type/com.google.weight, vnd.google.fitness.data_type/com.google.calories.expended, vnd.google.fitness.data_type/com.google.nutrition.item, Paths: /get/, /settings/profile, /settings/reminders, /settings/privacy, Path Patterns: /discover/intermittent-fasting/, /discover/intermittent-fasting, /blog/.*, /articles/.*, /log/.*, /groups/.*, /shares/.*, /uni/.*, /discover/courses,
com.fitnow.loseit.social.activities.ActivityDetailActivity	Schemes: https://, Hosts: loseit.com, www.loseit.com, Path Patterns: /activities/.*,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 20 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
4	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.
5	Content Provider (com.fitnow.loseit.autologin.LoseItLoginContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (com.fitnow.loseit.application.InstallReferrerReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.fitnow.core.repositories.notifications.PushReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Activity (com.fitnow.loseit.goals2.CreateCustomGoalActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (com.fitnow.loseit.social.activities.ActivityDetailActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (com.fitnow.loseit.healthconnect.PermissionsRationaleActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity-Alias (com.fitnow.loseit.AndroidURationaleActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias 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.
12	Activity (com.amazon.aps.ads.activity.ApsInterstitialActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (com.amazon.device.ads.DTBInterstitialActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
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	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) 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.
16	TaskAffinity is set for activity (androidx.glance.appwidget.action.InvisibleActionTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
17	Service (androidx.glance.appwidget.GlanceRemoteViewsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_REMOTEVIEWS [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
18	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.
19	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.
20	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.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **4** | WARNING: **8** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c00/d.java com/amazon/device/ads/DTBAdInterstitial.java com/amazon/device/ads/DTBAdLoader.java com/amazon/device/ads/DTBAdRequest.java com/amazon/device/ads/DTBMetricsConfiguration.java com/amazon/device/ads/DtbConstants.java com/amazon/device/ads/DtbDeviceDat

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/amazon/device/ads/DtbDeviceData.java com/amazon/device/ads/DtbDeviceRegistration.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/o.java com/bumptech/glide/load/engine/t.java com/fitnow/auth/SharedAccountData.java com/fitnow/core/model/professorjson/CourseEligibilityRules.java com/fitnow/loseit/data/source/PatternsRepository.java com/fitnow/loseit/me/b.java com/fitnow/loseit/model/insights/InsightPatternJson.java com/onetrust/otpublishers/headless/Public/Keys/OTUXParamsKeys.java com/onetrust/otpublishers/headless/UI/DataModels/d.java com/onetrust/otpublishers/headless/UI/UIProperty/l.java com/singular/sdk/internal/BaseApi.java com/singular/sdk/internal/Constants.java d1/d1.java f3/g.java f3/p0.java gg/a.java m1/m1.java m1/q2.java nd/b.java pc/d2.java pc/o1.java pc/x0.java ql/a.java rd/e.java ta/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				te/n.java u8/d.java ug/a.java wq/e.java zf/PreviousMealLoggingRoute.java
				a2/f.java a8/b.java ai/onnxruntime/OrtEnvironment.java an/b.java an/c.java an/d.java an/h.java an/i.java an/r.java an/s.java an/t.java au/c.java b7/a.java b8/l0.java ba/a.java bb/h.java bn/c0.java bn/e.java bn/h.java bn/h0.java bn/i.java bn/k.java bn/t.java bn/x.java bu/d.java c5/b.java ca/a.java co/i1.java com/amazon/device/ads/AdRegistration.java com/amazon/device/ads/DTBAdMRAIDController.java com/amazon/device/ads/DTBAdMRAIDExpandedController.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazon/device/ads/DTBAdMRAIDInterstitialController.java com/amazon/device/ads/DTBAdNetworkInfo.java com/amazon/device/ads/DTBAdRequest.java com/amazon/device/ads/DTBAdResponse.java com/amazon/device/ads/DTBAdUtil.java com/amazon/device/ads/DTBInterstitialActivity.java com/amazon/device/ads/DTBMetricReport.java com/amazon/device/ads/DTBMetricsConfiguration.java com/amazon/device/ads/DTBMetricsProcessor.java com/amazon/device/ads/DTBTimeTrace.java com/amazon/device/ads/DtbAdRequestParamsBuilder.java com/amazon/device/ads/DtbAdvertisingInfo.java com/amazon/device/ads/DtbCommonUtils.java com/amazon/device/ads/DtbDebugProperties.java com/amazon/device/ads/DtbDeviceData.java com/amazon/device/ads/DtbDeviceRegistration.java com/amazon/device/ads/DtbFireOSServiceAdapter.java com/amazon/device/ads/DtbGeoLocation.java com/amazon/device/ads/DtbGooglePlayServices.java com/amazon/device/ads/DtbGooglePlayServicesAdapter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazon/device/ads/DtbHttpClient.java com/amazon/device/ads/DtbLog.java com/amazon/device/ads/DtbMetrics.java com/amazon/device/ads/DtbOmSdkSessionManager.java com/amazon/device/ads/DtbPackageNativeData.java com/amazon/device/ads/DtbSharedPreferences.java com/amazon/device/ads/DtbThreadService.java com/amazon/device/ads/WebResourceService.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/j.java com/bumptech/glide/load/engine/v.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/c0.java com/bumptech/glide/load/resource/bitmap/f.java com/bumptech/glide/load/resource/bitmap/f0.java com/bumptech/glide/load/resource/bit

NO	ISSUE	SEVERITY	STANDARDS	FILES
				map/p.java com/bumptech/glide/load/resource/bitmap/q.java com/bumptech/glide/load/resource/bitmap/u.java com/fitnow/core/database/googlefit/GoogleFitSyncWorker.java com/fitnow/loseit/application/InstallReferrerReceiver.java com/fitnow/loseit/application/JSWebViewFragment.java com/fitnow/loseit/food_search/a.java com/github/mikephil/charting/charts/a.java com/github/mikephil/charting/charts/b.java com/github/mikephil/charting/charts/c.java com/iterable/iterableapi/e.java com/iterable/iterableapi/w.java com/onetrust/otpublishers/headless/Internal/Log/OTLogger.java com/onetrust/otpublishers/headless/Public/OTPublishersHeadlessSDK.java com/pairip/SignatureCheck.java com/pairip/VMRunner.java com/pairip/licensecheck/LicenseActivity.java com/pairip/licensecheck/LicenseClient.java com/samsung/android/sdk/healthdata/HealthDataObserver.java com/samsung/android/sdk/healthdata/HealthDataStore.java com/samsung/android/sdk/healthdata/HealthPermissionManager.java com/samsung/android/sdk/internal/database/BulkCursorToCursorAdaptor.java com/samsung/android/sdk/internal/he
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	

NO	ISSUE	SEVERITY	STANDARDS	FILES
				althdata/HealthResultHolderImpl.java com/singular/sdk/Singular.java com/singular/sdk/internal/DeviceInfo.java com/singular/sdk/internal/ExternalAIFAHelper.java com/singular/sdk/internal/LicenseChecker.java com/singular/sdk/internal/SingularInstance.java com/singular/sdk/internal/SingularLog.java com/singular/sdk/internal/SingularRequestHandler.java cp/a.java d0/c.java dq/a.java dq/b.java dq/c.java e4/d.java ec/d.java ee/b.java en/a.java ep/d.java f5/d.java f5/e.java f5/f0.java f5/g.java f5/j0.java f5/o.java f5/s0.java f5/v.java fa/b.java fb/a.java fb/d.java fb/j.java fp/b.java g/e.java g3/j0.java g7/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ga/d.java gk/d.java h4/t.java h7/a.java h7/m.java h8/a.java h8/e.java hb/e.java hb/q.java hb/r.java hj/d.java hn/b.java hp/g.java ib/d.java in/g.java in/t.java in/u.java j5/a.java j5/c.java j8/f.java j8/o.java jk/a.java k4/c.java kb/j.java kj/a.java ks/l.java l4/p.java l4/t0.java la/a.java lb/d.java lb/k.java lj/l.java lm/q.java ln/d.java m1/b.java m3/c.java ma/c.java mo/a.java n/c.java nb/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				no/a.java np/j.java o8/a.java oq/f.java oq/n.java or/b.java org/tensorflow/lite/task/core/TaskJniUtils.java p8/p.java pa/a.java pb/a.java pr/c.java ps/m.java ps/o.java q3/p.java q7/m.java qa/d.java qa/e.java qd/k.java qo/g.java qt/c.java r3/d.java r4/c.java rj/a.java rn/c.java rq/f.java rs/c.java rt/d.java s6/c.java s7/r.java s7/x.java se/h.java t00/b.java t3/c.java t3/o.java t6/a.java ts/e.java ts/f.java tz/e.java u2/m0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u3/e.java u7/a.java u9/c.java ua/c.java ua/e.java uj/g.java un/l.java uq/r.java ur/g.java ur/k.java ur/n.java vr/a.java w3/f.java w7/h.java w9/d.java wa/i.java wa/j.java wr/c.java x7/d.java xa/e.java xa/i.java y3/a.java y3/c.java y3/d.java y3/f.java y7/a.java ya/a.java ym/g.java z00/a.java za/c.java za/d.java za/f.java za/j.java za/l.java zu/d.java
3	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/darrow/loseit/me/debug/AppMan DebugPromoGroupFragment.java com/darrow/loseit/widgets/ShareDialog Fragment.java com/intrust/otpublishers/headless/UI /fragment/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	pc/q.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/amazon/device/ads/DtbDeviceData.java com/singular/sdk/internal/Utils.java or/b.java pc/o2.java pc/q.java qb/a.java xu/c.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	sz/c.java sz/d.java sz/i.java sz/j.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/iterable/iterableapi/k0.java com/iterable/iterableapi/m.java com/singular/sdk/internal/OfflineEventsMigrator.java com/singular/sdk/internal/SQLitePersistentQueue.java ga/f.java nk/m0.java nk/t0.java uk/b.java uk/c.java x7/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	iu/z.java
9	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/amazon/device/ads/DTBMetricsConfiguration.java com/amazon/device/ads/WebResourceService.java or/c.java s7/x.java we/o.java
10	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	ba/a.java ba/b.java dc/g.java tl/s.java yv/a.java yv/b.java zv/a.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	np/v.java uq/i.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	jg/f.java we/o.java
13	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/fitnow/loseit/MainActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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	wl/a.java
15	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	cg/r.java
16	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	xu/c.java
17	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	xu/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	aa/c.java bf/b.java bn/f.java com/amazon/aps/ads/util/adview/m.java com/amazon/device/ads/DTBAdMRAIDController.java com/amazon/device/ads/DTBAdUtil.java com/fitnow/core/repositories/notifications/b.java com/fitnow/loseit/LoseItActivity.java com/fitnow/loseit/application/AuthenticatingWebView.java com/fitnow/loseit/application/ConfigureLoseItDotComPromoView.java com/fitnow/loseit/application/JSWebViewFragment.java com/fitnow/loseit/application/buypremium/BuyCourseFragment.java com/fitnow/loseit/application/surveygirl/SurveyActivity.java com/fitnow/loseit/charlie/CharlieFragment.java com/fitnow/loseit/healthconnect/HealthConnectFragment.java com/fitnow/loseit/me/recipes/RecipeBuilderPlainTextEntryFragment.java com/fitnow/loseit/me/recipes/RecipeBuilderUrlEntryFragment.java com/fitnow/loseit/more/apps_and_devices/ConnectGoogleFitFragment.java com/fitnow/loseit/more/apps_and_devices/SamsungHealthConnectFragment.java com/fitnow/loseit/more/configuration/EditUserProfileActivity.java com/fitnow/loseit/more/configuration/LoseItDotComBackupOrRestoreActivity.java com/fitnow/loseit/more/insights/DnaInsightFragment.java com/fitnow/loseit/social/inbox/ConversationFragment.java com/iterable/iterableapi/a0.java com/iterable/iterableapi/e.java com/samsung/android/sdk/healthdata/HealthConnectionErrorResult.java h7/a.java h7/m.java jg/f.java pp/c.java qg/t.java re/y1.java zu/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/fitnow/loseit/LoseItActivity.java com/fitnow/loseit/application/WebViewActivity.java com/fitnow/loseit/log/meal_summary/MealSummaryActivity.java com/iterable/iterableapi/c0.java com/iterable/iterableapi/g.java
00109	Connect to a URL and get the response code	network command	com/amazon/device/ads/DtbHttpClient.java com/bumptech/glide/load/data/j.java com/fitnow/loseit/onboarding/VerifyAccountActivity.java com/iterable/iterableapi/h0.java com/singular/sdk/internal/SingularExceptionReporter.java com/singular/sdk/internal/SingularRequestHandler.java e9/b.java g9/f.java pr/c.java ym/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	br/a.java com/amazon/device/ads/DTBAdUtil.java com/amazon/device/ads/DtbDebugProperties.java com/amazon/device/ads/WebResourceService.java com/bumptech/glide/load/a.java com/iterable/iterableapi/n0.java com/samsung/android/sdk/healthdata/HealthDataStore.java dc/g.java dg/a.java dg/i.java ec/i.java jg/k.java lm/b.java o00/a.java or/c.java org/tensorflow/lite/task/core/TaskJniUtils.java pa/a.java s7/x.java sv/g.java sv/i.java t4/l.java u7/b.java uq/a0.java vq/d.java xz/q.java za/g.java zq/e.java
00016	Get location info of the device and put it to JSON object	location collection	ga/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	br/a.java com/amazon/device/ads/DtbDebugProperties.java dc/g.java ec/i.java or/c.java vq/d.java
00022	Open a file from given absolute path of the file	file	ai/onnxruntime/OnnxRuntime.java com/amazon/device/ads/DTBAdUtil.java com/amazon/device/ads/DTBMetricsConfiguration.java com/amazon/device/ads/WebResourceService.java com/fitnow/loseit/worker/FoodDatabaseDownloadWorker.java s7/x.java t4/l.java vq/d.java we/o.java x7/d.java z9/c.java
00005	Get absolute path of file and put it to JSON object	file	vq/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	aa/c.java bn/f.java com/amazon/aps/ads/util/adview/m.java com/amazon/device/ads/DTBAdMRAIDController.java com/amazon/device/ads/DTBAdUtil.java com/fitnow/loseit/application/AuthenticatingWebView.java com/fitnow/loseit/healthconnect/HealthConnectFragment.java com/fitnow/loseit/more/apps_and_devices/ConnectGoogleFitFragment.java com/fitnow/loseit/more/apps_and_devices/SamsungHealthConnectFragment.java com/iterable/iterableapi/e.java h7/a.java jg/f.java
00036	Get resource file from res/raw directory	reflection	bn/f.java com/amazon/device/ads/DTBAdUtil.java com/iterable/iterableapi/a0.java com/iterable/iterableapi/e.java com/onetrust/otpublishers/headless/Internal/c.java com/singular/sdk/internal/DeviceInfo.java com/singular/sdk/internal/Utils.java jg/f.java pp/c.java zu/d.java
00114	Create a secure socket connection to the proxy address	network command	oz/f.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	ua/c.java
00026	Method reflection	reflection	qw/a.java qw/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/singular/sdk/internal/DeviceInfo.java
00034	Query the current data network type	collection network	g9/b.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	we/g.java
00183	Get current camera parameters and change the setting.	camera	com/fitnow/loseit/widgets/CameraPreview.java
00115	Get last known location of the device	collection location	com/amazon/device/ads/DtbGeoLocation.java ga/h.java
00089	Connect to a URL and receive input stream from the server	command network	com/amazon/device/ads/DtbHttpClient.java com/bumptech/glide/load/data/j.java com/fitnow/loseit/shared/push/LoseItFirebaseMessagingService.java com/iterable/iterableapi/h0.java com/singular/sdk/internal/SingularRequestHandler.java pr/c.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java com/fitnow/loseit/onboarding/VerifyAccountActivity.java com/fitnow/loseit/shared/push/LoseItFirebaseMessagingService.java com/singular/sdk/internal/SingularExceptionReporter.java com/singular/sdk/internal/SingularRequestHandler.java
00023	Start another application from current application	reflection control	com/amazon/device/ads/DTBAdMRAIDController.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/iterable/iterableapi/h0.java com/singular/sdk/internal/SingularExceptionReporter.java com/singular/sdk/internal/SingularRequestHandler.java pr/c.java
00015	Put buffer stream (data) to JSON object	file	ec/i.java
00004	Get filename and put it to JSON object	file collection	com/singular/sdk/internal/ApiManager.java ec/i.java
00012	Read data and put it into a buffer stream	file	ec/i.java
00189	Get the content of a SMS message	sms	yb/a.java
00188	Get the address of a SMS message	sms	yb/a.java
00200	Query data from the contact list	collection contact	yb/a.java
00187	Query a URI and check the result	collection sms calllog calendar	yb/a.java
00201	Query data from the call log	collection calllog	yb/a.java
00078	Get the network operator name	collection telephony	com/amazon/device/ads/DtbDeviceData.java ga/h.java
00162	Create InetSocketAddress object and connecting to it	socket	sz/b.java sz/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	sz/b.java sz/j.java
00094	Connect to a URL and read data from it	command network	fa/b.java yq/a.java
00123	Save the response to JSON after connecting to the remote server	network command	com/fitnow/loseit/onboarding/VerifyAccountActivity.java com/singular/sdk/internal/SingularExceptionReporter.java com/singular/sdk/internal/SingularRequestHandler.java
00137	Get last known location of the device	location collection	ga/h.java
00132	Query The ISO country code	telephony collection	ga/h.java lm/o0.java
00125	Check if the given file path exist	file	com/amazon/device/ads/DTBAdUtil.java com/samsung/android/sdk/healthdata/HealthDataStore.java
00161	Perform accessibility service action on accessibility node info	accessibility service	h4/t.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	h4/t.java
00009	Put data in cursor to JSON object	file	com/singular/sdk/internal/OfflineEventsMigrator.java ga/f.java
00104	Check if the given path is directory	file	com/amazon/device/ads/DTBAdUtil.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://com-loseit.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/160910807917/namespaces/firebase:fetch?key=AIzaSyAxioaByH_rCRLZIGMr_cBP0AodFLCeeeY is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'DisplayCannonAndroid': '200'}, 'state': 'UPDATE', 'templateVersion': '4'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.CAMERA, android.permission.GET_ACCOUNTS, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	6/44	android.permission.BLUETOOTH, android.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
images.loseit.com	ok	**IP:** 18.238.96.118 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
mountainous-galette-5e4.notion.site	ok	**IP:** 208.103.161.32 **Country:** United States of America **Region:** South Carolina **City:** Mount Pleasant **Latitude:** 32.794071 **Longitude:** -79.862587 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
amplitude.loseit.com	ok	**IP:** 18.238.109.26 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
prod.tahoe-analytics.publishers.advertising.a2z.com	ok	**IP:** 52.11.154.73 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
us-central1-com-loseit-data-science.cloudfunctions.net	ok	**IP:** 216.239.36.54 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.amplitude.com	ok	**IP:** 54.245.125.82 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.eu.iterable.com	ok	**IP:** 34.254.102.241 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
mobileweb.loseit.com	ok	**IP:** 104.18.33.83 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
assets.loseit.com	ok	**IP:** 104.18.33.83 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 172.253.124.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sdk-api-v1.singular.net	ok	**IP:** 23.220.73.57 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 74.125.136.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
exceptions.singular.net	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.android.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
foodsearch.loseit.com	ok	**IP:** 18.155.173.52 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
dsar.loseit.com	ok	**IP:** 23.1.237.64 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
labs.loseit.com	ok	**IP:** 172.64.154.173 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.aboutads.info	ok	**IP:** 172.67.72.200 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
foodcreate.loseit.com	ok	**IP:** 52.1.183.200 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
food-search.int.fitnowinc.com	ok	**IP:** 172.64.154.119 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
help.loseit.com	ok	**IP:** 216.198.54.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
geolocation.1trust.app	ok	**IP:** 104.18.36.7 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
loseit.com	ok	**IP:** 104.18.33.83 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
food-search.prod.fitnowinc.com	ok	**IP:** 172.64.154.119 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.loseit.com	ok	**IP:** 172.64.154.173 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
com-loseit.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
accounts.google.com	ok	**IP:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
loseit.live	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
c.amazon-adsystem.com	ok	**IP:** 18.238.105.193 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
loseitblog.com	ok	**IP:** 104.18.43.216 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
tagan.adlightning.com	ok	**IP:** 18.155.173.27 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
local.adsbynimbus.com	ok	No Geolocation information available.
barcodesearch.loseit.com	ok	**IP:** 54.146.28.150 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
int.loseit.com	ok	**IP:** 104.18.33.83 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hub.samsungapps.com	ok	**IP:** 54.73.22.117 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
sync.loseit.com	ok	**IP:** 172.64.154.173 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.137 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
gateway.loseit.com	ok	**IP:** 54.175.38.19 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api.iterable.com	ok	**IP:** 44.215.217.155 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.251.40.42 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
social-feed.loseit.com	ok	**IP:** 18.238.96.129 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 142.250.9.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
prod.cm.publishers.advertising.a2z.com	ok	**IP:** 52.12.245.57 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
d21zgfprgikg74.cloudfront.net	ok	**IP:** 18.155.173.47 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
mobile-data.onetrust.io	ok	**IP:** 104.18.32.25 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.amazon.com	ok	**IP:** 18.238.90.46 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cookies2-ds.dev.otdev.org	ok	No Geolocation information available.
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	bn/s.java
back+android_premium@loseit.com feedback+android@loseit.com	com/fitnow/loseit/model/c.java

TRACKERS

TRACKER	CATEGORIES	URL
Amazon Advertisement		https://reports.exodus-privacy.eu.org/trackers/92
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
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
Singular	Analytics	https://reports.exodus-privacy.eu.org/trackers/251

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"compass" : "Compass"
"exercise_category_hockey" : "Hockey"
"firebase_database_url" : "https://com-loseit.firebaseio.com"
"foods_turkey" : "Turkey"
"foundation_api_key" : "70D980AE-FEA1-4058-82EC-E5C5FC229647"
"google_api_key" : "AIzaSyAxioaByH_rCRLZIGMr_cBP0AodFLCeeeY"
"google_crash_reporting_api_key" : "AIzaSyAxioaByH_rCRLZIGMr_cBP0AodFLCeeeY"
"key" : "Key"
"password" : "Password"
"singular_api_id" : "6147e6a0095b79ec6a6e2986ecc18125"
"singular_api_key" : "fitnow"
"str_private" : "Private"
"thumbor_security_key" : "p8LZzf8R4CQh3NuF"

POSSIBLE SECRETS
E3062B5C-7C4F-48F2-ACAB-682F6F118162
21631cfc-a9e1-4c17-8e35-3d523e6442c6
3f468031-c704-408e-a76e-8e332ade43b2
9douHjmTTjq3N4YYUdzzHaKyxIqsB5K92p8t26vKQB1HahpVak+32YHan4LmgLPE
d35684c0-c108-4305-9a44-c33f8171638d
610A202A-C460-46BA-BE1A-BE48BF65326D
1CCCFA3F-3D03-4CD5-9384-41430EC3FF3C
1VeJuVnEfsh9S8+TnOEDCfIzscTATtniwvJaQ7/W6I8=
BFF80C7E54CE454BBDFEF88BE9E1F0AF
joxZSCFIfSio2J1Z0g3HMtlcDGNvogfMyrj1e2b+qPNv6DXnDVXfwkgCXW9zFWFC
3d604b88-d49a-4d98-b448-138cdaa17c86
D9061E13-E047-42ED-9108-26D50A3D1219
1F3E44908772476EAC4315DD644CC807
a6d66644-71e0-477a-a762-f553dd1d862f
fd614abd-3017-439f-973f-e51e1aea065e

POSSIBLE SECRETS
04DF6DDC3E6B450BAFA802D912339A55
27104382-f3b1-4a10-824a-0ff1af5086bb
JAIugkcNQRXP51pRzjbhWzeihtmzLSCJCmT0+GTbkts=
29a67125-d89c-492f-9395-1367eb552af6
C030E27C-5E1E-4537-AC70-CEC353C922E4
avDZD6/xoSbFYvWCy23XLncB75oD5DxKdrTKFY2O0hY=
c30a192e-4d87-462a-88ab-f564aa705ab9
Kx8fghNUQq+sA+EfmK6qh0KjuKvw753ECuaCFV8szVM=
5e190319-8c57-48c4-8604-a7f6bfa3f8e9
c1b339a9-1454-43b8-b3b8-e73922c98a3c
c499c8f2-392d-4124-a3f4-019627f880e9
6JHAw9/xzu8LcH4q9f7Udi9sTntehS9dfukXhX8DEHhp54WYBhd6ZhWkqnOAMGmY
de1f934c-49f4-4da0-a5e9-3dfcc873eeca

POSSIBLE SECRETS
308201e53082014ea00302010202044f54468b300d06092a864886f70d0101050500303731 0b3009060355040613025553311 0300e060355040a1307416e64726f69643 1163014060355040313 0d416e64726f6964204465627567301e170d313230333035303435323237 5a170d343230323236303435323237 5a3037310b300906035504061 30255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567 30819f300d06092a864886f70d010101050003818d003 08189028181008a53be36d02befe1d152724281630bd1c42eff0edf5fdca8eb944f536ab3f54dca9b22cfb421b37706a4ad259101815723202b359250cf6c5990503279827 3462bfa3f9f1881f7475ee5b25849edefac81085815f42383a44cb2be1bfd5c1f049ef42f5818f35fe0b1131c769cee347d558395a5fa87c3d425b2b9c819cf91870203010001 300d06092a864886f70d0101050500038181000512992268a01e0941481931f3f9b6647fbe25ee0bc9648f35d56c55f8cfa6c935fb3d435125fd60ef566769ac7e64fe28234 09461ca7a04570c43baaab3fb877bf3a6a8dd9ef7e69944f65b0e5e36f2ac2bf085fdeda063898855ea2ce84c60655d824844fe1659a77c12604c3fb84d41df6f1a7705a1b9 962ac2fdc9933122
42aca610-14bb-48c2-8681-13e6f32fbc55
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
ngqbGKXcQCvq0ft27xRzOzNoEVN+ei+Vq2+CNx9QQMc=
00b66220-29cc-45af-950a-fe8f06f16593
5561CFDB-B5BB-4BC4-B996-F95E9A1A7325
bFK3lRg0oaTUwYDrSsMiLa/j4LG9nRlI5KKEyt63x08=
75a9970d-509f-45f2-88e1-b4b349e758a8
7e8085e1-a5ae-4437-b59d-ee723197b730
311569B4-D5AC-4FD0-82DF-6F0AE669A697
F010ECD96F8A47E8A495DA6616054F3C
l4qa5EABhdRHJHltXD4U8dy0wNZl4oyoZ9TbFONnMI4=

POSSIBLE SECRETS
6c19697c-11be-46ce-b004-c55112f6cb7f
593b89b6-faba-410f-8790-a63eb054ba1e
CF337232-47C0-4742-AC90-252421E3AC84
5kY1EQ+6snGNdZX1BEywItRy0EAwZ4DbRiPucqHAgfZR8kr75HzXIMEIf0cE9z11
0njjbCFUq6vJ1UgnErUI7KEtLgZLN7V9IJ5yZ3QtzXmjMaTjzKInpeDNakYTgh0P
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
7ffb01ba-ed30-4161-a527-2528c55c8d2c
737A3BAF69884921BC223CDEE4477BFB
8C7A337D59784A87AAC875CC485C3047
369E5A76-5AB8-4B75-8CD0-F2808FC482E6
03f2618d-ab50-4dcf-aa21-24e7d2e32c03
E7EAD450-DB47-40A3-9BEE-6027B96EF723
e8d63425-418b-4e18-a69b-e21ef122ee87
23f76b1d-31e3-4941-9194-1317f46c8871
JLulXGPEHVwHK+0FG96HP9my+NvwpTQbwIaIZrjn9OU=

POSSIBLE SECRETS
nVNp1WYfnkUt4CgZM9ftj8WNocg8ldySiFlqCJaJia4=
DC730E24B55F454BAE352628BCBF7FAF
Cv0JAL9ptzpRvgIi9AFTFGn0l5MhpPgpRN4VfZybymKMuiqBn9AG0bgJaX/QotAk
a40b47ca-3f8d-4b3c-8c4d-b894524180f1
SKSJAjN3UKeguXyEasCGg04d/yJuUN8XZYgactMp4rfMtHclJcD0mydl5RKvI49M
553da004-99c0-491d-825f-76c0e753545e
XbddbDjEO7nvRA9I7Y27WLO/dXFi3B7SRCDbld4Ev+A=
43259bf1d443a57ba35efab6aff422c8
1cd24942-5af2-46e5-848b-7402f3b077bc
19AC4737-5AC6-42F5-AE99-1F776552B70C
CB9F472BDEF646DABF0A6D5731717961
11754a52-2d41-4efc-8c6a-740f162370dd
CFDAB6F4-1EEB-4DE7-AD50-22C0B0C89B75
8253d599-cf86-41e0-9a68-a0d51d11b870
TvLSh+Eka5RyCXMK4IvAvP4vfksx/KqJwxjzSKu7qQs=

POSSIBLE SECRETS
1c588434cda8295f170319df5cb8895f
iJiFXDBrMwFOGpG8WmWNKc3sGwXbWv8N6fPQac0mMm0=
7e37985e-7300-4962-8d7a-ad92aecefb89
cb89d87e-7e56-431b-8dbb-ef5a5d6eb906
598AE576FBDC449FA630452BFDBFD670
8378a28b-5b8f-4906-aee2-86c9055a25ed
D5C27B7B-7A54-4DA5-89B1-EB3413BF7DE4
E4E377D8335443F5AE3E8AA78F2862A9
F12B1200-0000-46C7-AC6F-23CDFC72E51F
f8e2473c-8805-45db-adf2-b1de1230b5ae
93BED36F7789419D99535E80CBFA02D7
1yJaDnXEM3em29nHb3kYjIOvpW6Mkce5Fji3syGd7T0=
0e086e34-8701-4e56-9677-dc054824be16
9556489b-aa91-4255-b81e-5017ee4dd98a
79d85fb9-f8b5-4c5d-b6b3-a4cd8256c44d

POSSIBLE SECRETS
1660E19F-647D-4898-A977-72C04F2BA9A0
D1D2B0CBB26442CB9C01CCD523974338
a578b1be-69f5-4c00-9d3e-22820ae738ac
cf5c8e95-5b58-4981-8f34-5b222f3137ec
da549402-e641-4369-9294-7219e6363fb9
142D50F623B94275A7E03D7341866907
1B60DF18214D406B90B9E83A9F22859A
608ff2a5-887c-4625-8000-748fa066366f
cde83ddd-4be7-45e7-a71e-b13ba8dfab05
2b620ab4-14e2-474d-bbc8-ad43b74f094d
EB3DF8444DED4206AB470B2BF8C1C766
8Xr1ilYJHo+oWZQAYAG91DIHBuqEmXK8yHtxL6KkyfU=
sjYkfzJTuYKxh1jvZaP9n5dx9JGmzJotOUC/vdvgi4M=
6260fe6a-0f9a-41af-b6b4-94a956d7e46b
83966b5d127f484132a8562a4bce23dc

POSSIBLE SECRETS
Ls+ZUCEdSGy+47NpfWc5WNy2WCTB2lhysvWY8PCvkdyqiw8HkO3XVSxwPIsY4tvv
8253d564-3f57-48a2-a7e6-84daca7c58d3
9ObkV+9nuY0gPBNLH25GoxM7YATuF1pi7lORvVFb3+Q=
49237401-2813-4805-8D8E-8868EAEA5EA1
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
0C365959-0587-49B0-B592-8BB102062551
Vn3kj4pUblROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=
35733D96-FF7B-414F-8F3A-1213D6125E33
38d02249-7d5b-4a68-8e10-9b99d4b04fc0
e4d7c86b-952e-4b99-8103-fd2d94b7bd01
9E919C0C-77E4-4D5C-A8B1-28BEDDCBBB1A
06AD1F226D66484F85530B0724875342
7192f7a9-a9e3-44ac-aacb-f0176b6c7e3a
F223D8F5-1EA8-429D-8F8F-042BBF865273
8186fe38-483e-456a-b37d-8e9fd3d99252

POSSIBLE SECRETS
86B004F0-D118-46F0-AB07-440CCD8C188F
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
83421FAC5AB04134B0D2749F851E3667
1e56524d-f060-4636-8633-5be1f8a7faf7
5FBA8F0BF6CC470BBA78AD2460BCD508
71c8d39e-8322-4227-bde9-c0d0b0e18f9a
gYPijpNio6OwLgbzbH6IuWSNtvp7bCV5UMbKZJCVNdg=
f949ee05-549c-43a7-bd83-de8965df6ed7
d7YRusR2mxxBt1bBYjK2gXVvJl/MfqFw2IiZZVeFOFqksQBErGXLOKgf56kYtWpK
9ff5a942-d19d-461d-8fef-1158e7ed7f94
30e7017a-fc14-4168-be0a-255b9c10c6d2
3884e10d-12df-4c4e-8ff1-d02edb92991b
FF16A3DD96724EEC8DD96F8CEF974AB6
ffccc736-0e61-44f3-b2aa-1613deff0126

POSSIBLE SECRETS
29336ea4-ac1f-4a01-9432-2fdb395cb627
AAC04B8D-70C3-4DB7-9352-BBC86EC674EC
98ab6deb-0d40-4e3b-8de3-6153fc5c6858
SkMlFTLt8H3eQLYvgf87g2pXBfp4xPpxL3RMs974XSU=
24f7+wNdQe8HQwz0gPH2QlzxUp8iQNA20yBU7Dg74Sc=
0d01e756-7bbc-4478-b169-1b989b66937b
E8537C9B-A5F0-417E-A62F-58614950A4FA
b1f96862-3f24-4f27-bd63-fc12a914ac9d
EE927EC9E6D742F4A1B8F8F7D4293E8A
2a9b72e3-c563-4901-b99e-c0d597258c0c
9rXsTdb/WXYONX554dN5CJ2eqpcy9gFPMPi8uAjaHTA=
6ba7b812-9dad-11d1-80b4-00c04fd430c8
7d802ce8-b65a-401d-b667-eeeb4d58cf70
dd7f359b-7b0f-46db-8ab5-692f4f90e956
141bd962-fe18-4adf-815b-a28951fc6518

POSSIBLE SECRETS
F7963EC8CCC443B5A2FFD4682CFBB84C
fc15b56c-a324-4507-989d-ca1b4049671b
37a0cd21-4947-4fba-a415-cd18c3c84ac3
6ba7b811-9dad-11d1-80b4-00c04fd430c8
17a5b7b4-45e3-4b50-9a8f-d3155818d1f8
AZwRbSS9Tjg/vY6NNyDfd3mU35mZBbQduzRpliDRt3qUNjlKylmreq0JkiCiO6dF
09b0b413-e68b-416d-849a-99d124365ef8
C6OPKdOx6rUdfDdOmaUimt8yM1FrOv7bKCITdJ0Uo74WwXDfvXouJ4oz4kHBjTSk
75412329-ec65-46a1-b297-7902c90a9b5c
7d73d21f1bd82c9e5268b6dcf9fde2cb
17eb370a-4feb-4125-ba6c-3f2a4e32e0eb
25BA15C930FE4C2881F78FFF6F465C80
hwvIMOeohSBrCWT4pVkQok22g/l0cZbbqOTmNbjObWwcwhLlaFMNibQmd2cIB1Vb
a0784d7a4716f3feb4f64e7f4b39bf04

POSSIBLE SECRETS

308204d4308203bca003020102020900d20995a79c0daad6300d06092a864886f70d01010505003081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d313130363232313232323531325a170d333831313037313232323531325a3081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100c986384a3e1f2fb206670e78ef232215c0d26f45a22728db99a44da11c35ac33a71fe071c4a2d6825a9b4c88b333ed96f3c5e6c666d60f3ee94c490885abcf8dc660f707aabc77ead3e2d0d8aee8108c15cd260f2e85042c28d2f292daa3c6da0c7bf2391db7841aade8fdf0c9d0defcf77124e6d2de0a9e0d2da746c3670e4ffcdc85b701bb4744861b96ff7311da3603c5a10336e55ffa34b4353eedc85f51015e1518c67e309e39f87639ff178107f109cd18411a6077f26964b6e63f8a70b9619db04306a323c1a1d23af867e19f14f570ffe573d0e3a0c2b30632aaec3173380994be1e341e3a90bd2e4b615481f46db39ea83816448ec35feb1735c1f3020103a382010b30820107301d0603551d0e04160414932c3af70b627a0c7610b5a0e7427d6cfaea3f1e3081d70603551d230481cf3081cc8014932c3af70b627a0c7610b5a0e7427d6cfaea3f1ea181a8a481a53081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900d20995a79c0daad6300c0603551d130405300301 01ff300d06092a864886f70d0101050500038201010032960 1fe40e036a4a86cc5d49dd8c1b5415998e72637538b0d430369ac51530f63aace8c019a1a66616a2f1bb2c5fabd6f313261f380e3471623f053d9e3c53f5fd6d1965d7b000e4dc244c1b27e2fe9a323ff077f52c4675e86247aa801187137e30c9bbf01c567a4299db4bf0b25b7d7107a7b81ee102f72ff47950164e26752e114c42f8b9d2a42e7308897ec640ea1924ed13abbe9d120912b62f4926493a86db94c0b46f44c6161d58c2f648164890c512dfb28d42c855bf470dbee2dab6960cad04e81f71525ded46cdd0f359f99c460db9f007d96ce83b4b218ac2d82c48f12608d469733f05a3375594669ccbf8a495544d6c5701e9369c08c810158

POSSIBLE SECRETS
308204d4308203bca003020102020900e5eff0a8f66d92b3300d06092a864886f70d01010505003081a2310b30090603550406130 24b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d313130363232313232353133 5a170d333831313037313232353133 5a3081a2310b30090603550406130 24b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100e9f1edb42423201dce62e68f2159ed8ea766b43a43d348754841b72e9678ce6b03d06d31532d88f2ef2d5ba39a028de0857983cd321f5b7786c2d3699df4c0b40c8d856f147c5dc54b9d1d671d1a51b5c5364da36fc5b0fe825afb513ec7a2db862c48a6046c43c3b71a1e275155f6c30aed2a68326ac327f60160d427cf55b617230907a84edbff21cc256c628a16f15d55d49138cdf2606504e1591196ed0bdc25b7cc4f67b33fb29ec4dbb13dbe6f3467a0871a49e620067755e6f095c3bd84f8b7d1e66a8c6d1e5150f7fa9d95475dc7061a321aaf9c686b09be23ccc59b35011c6823ffd5874d8fa2a1e5d276ee5aa381187e26112c7d5562703b36210b020103a382010b30820107301d0603551d0e041604145b115b23db35655f9f77f78756961006eebe3a9e3081d70603551d230481cf3081cc80145b115b23db35655f9f77f78756961006eebe3a9ea181a8a481a53081a2310b30090603550406130 24b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900e5eff0a8f66d92b3300c0603551d13040530030101ff300d06092a864886f70d01010505000382010039c91877eb09c2c84445443673c77a1219c5c02e6552fa2fbad0d736bc5ab6ebaf0375e520fe9799403ecb71659b23afda1475a34ef4b2e1ffcba8d7ff385c21cb6482540bce3837e6234fd4f7dd576d7fcfe9cfa925509f772c494e1569fe44e6fcd4122e483c2caa2c639566dbcfe85ed7818d5431e73154ad453289fb56b607643919cf534fbeefbdc2009c7fcb5f9b1fa97490462363fa4bedc5e0b9d157e448e6d0e7cfa31f1a2faa9378d03c8d1163d3803bc69bf24ec77ce7d559abcaf8d345494abf0e3276f0ebd2aa08e4f4f6f5aaea4bc523d8cc8e2c9200ba551dd3d4e15d5921303ca9333f42f992ddb70c2958e776c12d7e3b7bd74222eb5c7a
a5c71f6aff54eb34c826d952c285eaf0650b4259c83ae598962681a6429b63f6
93bee74b-c7c6-4e3e-b908-1124d7eab886
6ADE33CF-FFE2-4BAC-8330-DE9EEBDA60C0
c7828f23-8595-479d-8cfe-3a6fb3d8273c
3ee87eeb-a8ac-40a9-ba44-02f252ecd402
eUrWQVF8FAlcOLX3Auj55rxdEWjF+0P5JAPLCHVKKQw=
DDAB788A-475B-4AAD-91C2-12B72ADA3FE6

POSSIBLE SECRETS
3314E1E6-2B28-4651-9715-2A069C09921E
4cf3e952-eb3d-4bf0-9c4c-61937b2504c8
8CB7CF08-0711-4665-A519-F88F8651FD90
5e91a27f-a45b-48cc-aea6-f2f49a88ac03
BCE0A7C5F3F542BB91682B07421F2717
651f3038f6e34dfab3664f57885d0454
63842ed3-d1b8-4fd0-8e59-2295ceed0248
561f8c7a-6adb-460f-a08c-664c7c47f35e
BAF37E00-C154-4DCF-9783-3FF071CCE0A3
af60eb711bd85bc1e4d3e0a462e074eea428a8
5490D38C1FD44727AE713C84F0A46D7E
6f19f9cc-2a93-49eb-9bb5-300c800f8cf4
04854fdb86a3434b654eef9330fd3bf6
ABF6FD21-B50A-4042-A864-C42265B353E0
479bad87-a5d7-4521-bfbe-d8f5e3a112be

POSSIBLE SECRETS
678C5EF3-EB76-42AA-9C1C-596143BA57B0
52860D01-3346-4772-9E5E-647813531F95
AB763EF28B584D9F956D64E2DA51128B
3a4e651f-aa1d-46a2-86e4-df31b9bf6f3b
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
RKC3mFMqGi7xOgQ7s39JMoZe9bnzGCFipcdUUf0vlgHDkBg7SvMkVmBGpwLs06ia
uJ6tafbdnitpIiJcEDt3zh4lzBZEYeFsW45S60suhbKyZNy2K2MuNEbuksualim4
8463ACCEE2F1463EBEBEDD6A360EF0CD
05068d71-069e-4eef-92e0-72fad95b0887
a90b2421-8123-41f9-94c5-f55336315157
e41fb79f-c6df-43fe-adcd-8526b383a3f5
FC91FB879B3C4DDFB402A2C88EFA2A06
0ccf0b7b-544e-49c3-b9d4-7f43193c4a35
70AADAE8-FC19-4364-96CF-30C3FB9801F8
6849E623-8906-4728-8337-A14732B0AC2A

POSSIBLE SECRETS
3B75A66F84594F92A36053DE4576992E
84E3224DA83E45299BE2606B0A531ADD
D801ADB4-C5AC-4CB1-8800-8C922932D125
9ca12223-e1bf-4bfb-92ae-68fed66bc8f3
O+vmm8flr2e7ZrTWUx/T8ClWwcEwLlJlfjM8sMGjZbg=
b3188ba8-5011-4681-9e5a-5efe041c3487
2dc0c0cf-901e-4ba9-826f-80023da6a316
758713f8-41a7-4f98-b6d2-62ba642db6f9
6ba7b810-9dad-11d1-80b4-00c04fd430c8
d3df5398-bc36-4f78-8c87-c2f26f34ca79
546c83c3-0b01-498f-bd0c-3538885b1e57
6cf38b16-4948-437b-be89-71dcf0ce1964
51B8B60832294BF5A607FCE587163BA5
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
tVSI3GZQAGRITfe/VNiB0JAqJe5Pfq0lPruET3IJQ2F3N6dl8hPg+ZOAK3nXD45u

POSSIBLE SECRETS
acb7fad3-1df4-47bc-976f-12bca586e2b3
1521b62c-695c-4eb5-98cf-c4c2fdd2ee37
825A7E71-AADA-4A5A-843E-120BCE278C97
A8C823A56D4242A2A61ADA52A53C776E
r0MNv9zqwvoUwASL1pBJjOA1OkDa8Kcs5NaA6VOkJEI=
653BB7E4-736F-43FA-9FF0-B623D3418CCE
16E48D56E93D4389900F464B873BB956
073B6EAF-E8D6-44BA-87F5-E0649BF6377A
CE3C251CFED1473FBB5195FDFACB9DDB
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
23f1ef15-fa60-4247-9de0-99baecb292b4
0f94484e-2512-407f-bb4d-2a7d6eaf2d6d
8E4cUkgIY9w8/0qt+Oeyh9wfu9tQKpeKsR+Ou+hsYewuB4uFdKW1FI4W+bAZwe0B
164A8A571BB148C9A42D577555AE891C
38B536F1151B45F2B8BB32A458730963

POSSIBLE SECRETS
E7230E337EA242F9B683CBAE3EF460FC
b480b98b-8a51-4396-ac60-e221c98233c3
61F6B4ADD3AA4CA4ADE2B8F6B04955D1
b60df8ac-d695-4d3d-bd1d-8ec57e1815b2
c43fcfc3-019a-4f2e-b082-692388a28b9e
6e486bd2-a9df-49b0-8036-c807b3b91904
52D0DE09-DD09-4F21-9E9E-516B8656237A
D5C6EC5742CB4D68A6810AA222246C88
875959cd-6580-4f53-9e9c-b498dd076030
411b8ca7-0f96-4875-ae52-2277761d7e0d
B02682C3-2CA5-489C-AC27-9BB45799AC79
F3B439FE-4F09-48C1-B615-AF3ACB36F1CA
X9PgbTHLX0FFxbl3gdPDuVwcglfXy5CDrzo8siaVNaH+OIJ6JI34Wu3QK5rLega4
cf821a9b-a62e-4140-8cf2-cbddcd1d5b0b
ce3c79aa-9bab-4b9e-971b-d3c8d196a977

POSSIBLE SECRETS
NtWyZSC7qBNyKPaXbOjRpNaZGUUAwpDpvYkB4v1ZH9M=
0yxvRSsGg+/BBPRqwe1F54W0T+vv1NRnE+jebtT36Vo=
0193da76-9f40-49fa-b2e1-64f15b0a2f24
iz9pI8M74OdFMOjBXhk6CVKK/c29GtinDT3TfbuphLdYOSnoV+Rg8WuW9whaa7rD
A255894C9B1A4A87927979B5666321E9
HeBkX9XaSpC6sV82I6X2HUgm82vH8VhIWt26LGkrI3A=
9503a3de-c487-411a-b9ce-794131344907
4e80cf46-4d3e-4290-b853-cc2b639e9e0a
6C02BC3F-167B-46A9-A983-C73377355C17
436e6598-67dd-49e0-a9ee-fe799d62c8e1
0AF5E4CAC5754393A674721847A3F90B
b5d21a38-75a9-4a39-8320-be677b183ee2
f3a2bd92-5813-40a4-a613-53e4a8eba3a3
b5990835-eb6f-48d3-b2f1-b6800a2e239d
b350d36e-11da-48e4-be44-89d5143f7491

POSSIBLE SECRETS
D8B247223FE14963A872114C585E392F
LYoHKR17UvbUNibqKPKJklawQJNaw1zk7CnhZAC68YBTzC7x4MYQVXp9Sihs98Ok
a0919710-71a7-43c5-a73f-1eb5305eefde
B3EEABB8EE11C2BE770B684D95219ECB
83a495fc-cfbf-4763-aa5a-51fcae050152
722EAEAE465948ED9BAE37A48D5F15D9
6A3B9357C2344884B1284C99947321D0
ebe7c6d0-6b3a-4c95-9e03-0cdc8ca97d8b
lnMUlT0qopStslq/RfZHkyvg0xAUTVuMPsMot4SEaYA=
f85668ef-51e9-4354-ac9c-7db960faa1ca
E9339958-606A-443B-80FA-E64D7092C13D
97DAD616B31C428C9B2B045DEB8DDC8C

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b13 07416e64726f69643110300e06035504031307416e64726f6964312302006092a864886f70d0109011613 616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930 3130323333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f72 6e69613116301406035504071307
488d6d1f-5449-4d96-910d-5f72aa33d9a1
410bd505-a42e-4cab-8026-3008e046eab9
SxHy+zpC+eGmQUPW4BYYcldQdVxiSSVnY0gIrWauGKU=
02555aec-0743-41fd-9f1e-3ada707534db
E9C33371-46BD-4538-B2B7-B85749A8E62C
BD56F9EBADD346AC85E94E8234DFBBCA
2F38216E44284FF19F74CCE78DB29285

POSSIBLE SECRETS
99bcb982-3b9a-404a-983c-4de786703e2e
44cf8f4a-949e-49c5-a1a3-c00994da23a9
8E8F4F3E9F4C4052A934799D1C58DF60
18022967B20143A8B9503C6AB1038E24
e4789745-ae62-4af7-b82f-2cccfbe24107
62a7cfd4-42a2-444a-9c6f-266ebaf306d8
vpqgk7W2OO4+emKKnTSxckIsP1c64LGVSWcdsnDvr3w=
3e659fb3-8688-4ed8-b84d-ff00bc8ad381
V8P78mWO+MxnWR283vMX+BSDXEvrm8XlQCYXMpvUe5w=
e9026ffd475a1a3691e6b2ce637a9b92aab1073ebf53a67c5f2583be8a804ecb
f744eb1f-df85-4ff3-b9a4-ecd974df7ebb
4033D2EBAE194FCBB05AD9404511399B
a12a08c9-e2be-458d-b9ee-56aef61c0bd2
o5W1eROpLyVNcsDGW3Y0lGc2x/V+mDPvMXouv3gbW6M=
9F51392D-CF5F-4C98-8766-26C79C20CBF1

POSSIBLE SECRETS
2ee5b8be-62e7-45d4-8504-395b4877e66f
4FA5D52B-8AE1-4F91-9EB5-19810CAA144E
3fysZeGzwX+hqd2f4+qtlSho+oF+DeFl9kzKrTFOSWo=
69f1904c-6e76-4e06-87c8-6b1a3b8718af
39DB3E5162E6436EB76022C8C7A00520
f53c0fe2-5eb8-4970-aafa-c3f827d76fbd
1F5C37F5-F128-466C-BEE1-08BD9DF1DC0C
eb923b84-1b30-4c09-9e96-1119c1edc137
e17c510d-88bc-4fd9-a5dd-f5b2f2e20a0d
3af2c83a-1344-4551-9725-cc5d95d698ef
E060B67A54C84A67A96CDAF0C40674CC
Rx5KxmHu63h8QT7T4cYR2mu7F4LQnYkocG/Azb9HP8ZHyjUHnRxxCuB99BIp3kbl
hhtrMjcGMTQSGdrv1+l2gakNTe0Pfchc8VT5kRHtsehlafuJ8JEE4iewNV4y5I/U
A0E982C9-5A7C-4A57-A46F-442804BDC92F
24166c40-fe20-475c-8902-137b42ae20c6

POSSIBLE SECRETS
05571B2DC6014B25B714C565F53AB29F
3DC4B76E054E45B9972C2D632906ACAD
dd996d29-8816-47b1-a638-4e01928c852c
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
A6A429C4-3B19-43A7-819A-443D876F4E81
02a9b1cc-7662-40eb-8677-13f35b56fa09
w1mRpvC09hSNbQ10UvFXagm2P4TWR/T2KztJ+buPFQZnRnjxpdFVScAm9trUP6jM
359c2e74-aba1-4a06-8ccb-547086b7b0ec
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
a69103ac-20a2-4bdc-8195-fb3cfbdb431b
2d1f6b8e-1d4d-47ca-b6f6-40f2a8335b6b
SfaCE2ReDSQ3+KDKcvA6SSrX7nuWYsM/FN3ZFmlH0dA=
38ea8d37-f4d4-4936-88a3-82f081938dd1
ccbedb66-7c7d-417c-9cdb-9d69b179a58f
4261606d-7d15-4278-a516-ea3334da7aab

POSSIBLE SECRETS
u7Ufq5yuXkEXg69T8jpWuOOX55Q9g2DSVI1gtbNUvY8=
9F6A21B778ED4782B9940201B88F8A1F
f7a8d7c8-44e3-4b2a-9c72-0cc8d8555417
21fb2c11-4c42-444d-8482-d056315d1c73
0366bdc3-9ff1-4a32-ba74-cc075787c63d
F6DF6C5CF7A144109E1C1968E2868C4B
a08f6bef-7480-43a9-8904-e3f91eb0ec5b
ZdMwT5n8r4APV4u4GhQlb1VCwOIVHkTm7kF7LnArEpyZnsv+C3G3q6fVFgtTcqcc
86971ac1-8ccf-4ad2-812f-abad56ef51b8
b3f5f60f-3595-4813-a416-d28defbc055b
016EA38E-2113-465D-B7DD-261A76A587F2
0DA599B6EBBE4F739B74CF5BCB1375C2
12a2697d-79fd-44e7-a9a8-1bd7293ce230
0B5C7B99-80CC-40ED-94B8-6F73B148886B
2DF902EAFF684E4FBDF2A34438A3468C

POSSIBLE SECRETS
8ffbcc3f-53ae-4df3-bd15-b9b58cad390b
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
c6fd76e4-7c42-4b47-b07d-8d352cdd3795
6ba7b814-9dad-11d1-80b4-00c04fd430c8
1059af00-1f2a-4b44-969d-53ce7ab49b51
308204a830820390a003020102020900b3998086d056cffa300d06092a864886f70d01010405003081943 10b30090603550406130255533113301106035504081 30a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100 9c780592ac0d5d381cdeaa65ecc8a6006e36480c6d7207b12011be50863aabe2b55d009adf7146d6f2202280c7cd4d7bdb26243b8a806c26b34b137523a49268224904dc 01493e7c0acf1a05c874f69b037b60309d9074d24280e16bad2a8734361951eaf72a482d09b204b1875e12ac98c1aa773d6800b9eafde56d58bed8e8da16f9a360099c37 a834a6dfedb7b6b44a049e07a269fccf2c5496f2cf36d64df90a3b8d8f34a3baab4cf53371ab27719b3ba58754ad0c53fc14e1db45d51e234fbbe93c9ba4edf9ce54261350e c535607bf69a2ff4aa07db5f7ea200d09a6c1b49e21402f89ed1190893aab5a9180f152e82f85a45753cf5fc19071c5eec827020103a381fc3081f9301d0603551d0e041604 144fe4a0b3dd9cba29f71d7287c4e7c38f2086c2993081c90603551d230481c13081be80144fe4a0b3dd9cba29f71d7287c4e7c38f2086c299a1819aa48197308194310b30 0906035504061302555331133011060355040813 0a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900b3998086d056cffa300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100572551b8d93a1f73de0f6d469f86d ad6701400293c88a0cd7cd778b73dafcc197fab76e6212e56c1c761cfc42fd733de52c50ae08814cefc0a3b5a1a4346054d829f1d82b42b2048bf88b5d14929ef85f60edd12 d72d55657e22e3e85d04c831d613d19938bb8982247fa321256ba12d1d6a8f92ea1db1c373317ba0c037f0d1aff645aef224979fba6e7a14bc025c71b98138cef3ddfc0596 17cf24845cf7b40d6382f7275ed738495ab6e5931b9421765c491b72fb68e080dbdb58c2029d347c8b328ce43ef6a8b15533edfbe989bd6a48dd4b202eda94c6ab8dd5b8 399203daae2ed446232e4fe9bd961394c6300e5138e3cfd285e6e4e483538cb8b1b357
1330093f-bdf4-4899-bf51-cffeb9e3b45d
ef4a4496-71ef-4146-a38c-ab285589b7b2

POSSIBLE SECRETS
b360b31b-e630-4583-95de-400bcda2e47e
2ee7d4a1-1771-4838-bb7a-159dced4737e
0A509EFE4E154E5CBDF623C22FECC0E9
5E2FC893-222C-4127-A1FA-BBA725168841
FLgp79R6LGLnWDio6G1XBjsjORgKSjLkdakyn5bigQludVyQtVZMhDAlppvakfKf
bae8e37fc83441b16034566b
1tXSieficgPhud4YihA+CzunTIb+yA05iyb1BkAzMoc=
163b715f-5279-45eb-b826-401c31cecc83
74637323-6325-4A3C-956A-0ADF18C76AEB

POSSIBLE SECRETS
308204a830820390a003020102020900936eacbe07f201df300d06092a864886f70d01010505003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e 64726f69643110300e06035504031307416e64726f6964312302006092a864886f70d0109011613616e64726f 696440616e64726f69642e636f6d301e170d303830323232393031333334365a170d3335303731373031333334 365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406 03550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355 040b1307416e64726f69643110300e06035504031307416e64726f6964312302006092a864886f70d0109011 613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00 308201080282010100d6931904dec60b24b1edc762e0d9d8253e3ecd6ceb1de2ff068ca8e8bca8cd6bd3786ea70 aa76ce60ebb0f993559ffd93e77a943e7e83d4b64b8e4fea2d3e656f1e267a81bbfb230b578c20443be4c7218b 846f5211586f038a14e89c2be387f8ebecf8fcac3da1ee330c9ea93d0a7c3dc4af350220d50080732e0809717 ee6a053359e6a694ec2cb3f284a0a466c87a94d83b31093a67372e2f6412c06e6d42f15818dffe0381cc0cd444 da6cddc3b82458194801b32564134fbfde98c9287748dbf5676a540d8154c8bbca07b9e247553311c46b9af76 fdeeccc8e69e7c8a2d08e782620943f99727d3c04fe72991d99df9bae38a0b2177fa31d5b6afee91f020103a38 1fc3081f9301d0603551d0e04160414485900563d272c46ae118605a47419ac09ca8c113081c90603551d2304 81c13081be8014485900563d272c46ae118605a47419ac09ca8c11a1819aa48197308194310b300906035504 0613025553311330110603550408130a43616c69666f726e69613116301406035504071307 4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e 64726f69643110300e06035504031307416e64726f6964312302006092a864886f70d0109011613616e64726f 696440616e64726f69642e636f6d820900936eacbe07f201df300c0603551d13040530030101ff300d06092a86 4886f70d01010505000382010100 7aaf968ceb50c441055118d0daabaf015b8a765a27a715a2c2b44f221415ffdace03095abfa42df70708726c2069 e5c36eddae0400be29452c084bc27eb6a17eac9dbe182c204eb15311f455d824b656dbe4dc2240912d7586fe88 951d01a8feb5ae5a4260535df83431052422468c36e22c2a5ef994d61dd7306ae4c9f6951ba3c12f1d1914ddc 61f1a62da2df827f603fea5603b2c540dbd7c019c36bab29a4271c117df523cdbc5f3817a49e0efa60cbd7f741 77e7a4f193d43f4220772666e4c4d83e1bd5a86087cf34f2dec21e245ca6c2bb016e683638050d2c430eea7c26 a1c49d3760a58ab7f1a82cc938b4831384324bd0401fa12163a50570e684d
4222da5b-5f7d-4ae3-971f-c5e6051b5c9f
470fa2b4ae81cd56ecbcda9735803434cec591fa
136ed544-4ca2-4509-8388-fdbb678d0d50
AMztxBQmasdCMrU1nlH2RhtlfSPsjcYFxTHFmKvCDYM=
AC312C392FB7474D852F8AA2143F4EE8
e6063b97-e007-4886-b246-82f06b67028c
63bbbabc-4ee4-4bb0-a661-6c8d43674c82

POSSIBLE SECRETS
7461E5EE33534E73B5F17E11285B7296
CC9A331F996446EAB9050BD6A1C0BD49
EE0D6762-6E2A-4D34-BF3E-4F030371C5A6
6db669c0-c966-49e7-b770-39b07d2cf4ef
135ed276-612e-4e9a-9f42-501c37e80bd9
5B0CA40B-EB65-4CDB-93A2-E99D78B93BED
90E98415-D169-4BB5-9213-059073AFD423
0AFB8E30-6A82-42D4-91C7-DF4BFC11D5A6
92ca152e-6897-46f3-9a9e-03a0017b23ad
6jGSPrUM0+2YrTO2vsTOKq3+XL/IfUFs5oxZaSEvsQg=
291099ec-3876-4a14-90da-808c2697beba
2ecb766c-f682-4694-91c5-2144c40ed959
4DF95B84-FDF5-447A-AC6B-F447DC1509BA
32ada2d8-d3d6-4178-b6ad-350abec21909
5HcA415u1KU8m2yVlDZBhQQK+0IFNRmmWPxuAq0DnfPzSdJ/uWlnYMD1kKfkH6cZ

POSSIBLE SECRETS
edc644a0-e946-4efb-abd9-9db5c6d6a3fa
M2RhhRYJhjrQUa7n9jg23IBcTQvCkUFLA/9ZbQYvHFo=
B1298867-F926-4F91-9CB5-724DD6EEA72A
6f6ca4a6-d159-47bf-b09a-593d9519d3e0
B7A3B4F805234125BFB7754F4AD58A7A
22242D4F-751E-4523-89BB-F82F71E48D7F
b3e91532-3da4-4797-82e1-97e197574beb
70fa635a-0f8c-47e6-bcca-9cb5d708a1be
AC18479AACE140E69BB66DB14A35C947
sdX902x/AS9226TxUXaqji9wP1uHqRQA8nkg2YMN1TcruTTaw008l9z5V3jZGjLO
3ab99bcc-94fa-4390-9d29-af346cac58f5
EEA182C2C33F402791541D37C8D2FE02
dfb9d54f-a0cb-4056-9201-f9bf99b1d17a
XFxH1z0dBuMDP7aWA+P/3WKwW9qr8sC2ASjEfciaKHfSLryjCNl4cmJgfsh2Tylb
1ee668a4-a5ab-469c-8baa-660c1c9d5458

POSSIBLE SECRETS
9e9144e0-cc7c-40bf-9177-72b51ad484ac
21B371E6C35B4C269FF32409A8279D7F
SHfJbyMgI7MrHewwYoTmYsM7CTkziBSZ0pvzhPCRWcLGoNw6AaEZWLqlKa0dpKuD
tPxcLkiesd8JzrYlyuRbLGxWAQfsX+C1jrJaS2rsRu6lU/ve1b9hEzSSzo6VwqXx
5265CB80-F85F-441D-9CA1-2860D2A85796
53DB47F0-938B-452D-AC3F-AE17A95E25F6
0AF16B5F5A85459B8834BDDDE494BD42
g3h/WBQ8k1SqFyNwcX6aXlyabMyZPKS0QgL4qcVfix1XI+70++CdiHkDZKRlUPQw
CBBA81585D1348B094D161D4B9F1D685
7f171e56-8c71-43d7-8f39-c906d2e77392
0BC5B361361B44D7805916F30E3496D8
mkunJHFc5vhTAVOcsaNSYx7OvFB6slgbORGrA/joIDO0IYq5rQvDcAbp2AI6CPUh
52FF59E9-D8BF-4887-BDC2-E1E9B792D756
02E9A8C1BD784E138D852DF64C1DCFC1
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

POSSIBLE SECRETS
22b03a9d-dd6a-40df-8895-991cadf20320
F99E6F271DC944BDBDD62D33052DDEF6
26ade974-c91d-498a-a23d-ab70ab73f8c7
bf565ac7-dbb3-4602-9481-bafe6f7fd971
824d13f3-0f82-4815-ba2f-871572421c69
d362185a-655f-4445-a4b9-0fcb0c0455f9
36864200e0eaf5284d884a0e77d31646
2A9039DD9E9F48BCBC4873CAD2D57E40
93439339-e4e4-4f79-80b2-ecb9958f7ac4
8d58969a-ca34-4f8e-8b60-5cb85e330bd3
QcEEfK1PwFv2Eb+NZQ+4kWKAUUVvycYqoBzmAjBexJV/sKEjaFlajeD5MAZYWXy5
82e053f5-2860-4971-9e08-f9b291406ee9
02529299-c31c-495e-b404-e8835e78b202
768D67FB-2439-412D-89ED-721E0FE16DB2
4a4ec024-835b-416a-a8d6-6fd4aeaface0

POSSIBLE SECRETS
3A9C092D3B704171B163219360645AC8
6870BB7C-81D9-402C-BAF7-3198F1832908
a3ad6b9d-49cc-48ab-8d34-c6e0c965b216
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
53eb3e9c-c153-4ff2-b814-5a9d698bc922
6LfuWNElAAAAAH1QvfazO3qTevBrGdBuAlYTcBdM
f584372c-991a-4d93-b706-0ca2130e9582
k8GEQUoJxJPI/0jAlfeUix8QD7WaaXAfMcSQAzrpgrU=
Cv/m6MvBjdOit7tT7cC+xPCpFEqovwYj4XIOcXUxCMs=
t+CAjrsoEFEWDgC/oCfdqxFl31lIReQPqb6CaFb+1Y0=
712922bb-b4bf-4cb7-bc26-02ac76762d3b
fHaUCxrr3fcbpdQPVJw6OSoHeHoizr6wmxmAsnLvDUhuNG2u8ebKX4VPxAoXSx4W
47764279-c8ea-444c-9f38-413eb007e828
19377f50-af4c-4d69-9cf2-e4615ec6dc18
EF74C588ABF84984B702FFB1A37C5DC8

POSSIBLE SECRETS
cde8b405-f4c0-4528-a7b9-50bf7ea19a46
0C40E5BF02A6422198B8C99B50444A28
4f1c6ada-5f16-4f6b-98c3-46ec86813796
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
vvYcBqgI4aoC3GZZ7n1bdLp71k52s6EJLh0/nA6ME39LmvOZf3TBZ+H4xg1YfQXg
6D6DBDF0-A7AA-4F3D-BB56-63FC28D1D46C
z3i9M2k4RJ/f7GArNBcGbUcpUFpuRmLev6S20UO7Vqs=
0FE01A60-6BE6-48F2-9F9A-50943D62C5E6
1b03c523-7879-4079-83c5-a62c4b603827
1e30d1ad-0124-4ced-90d8-61bcd508cc52
31067426-4C53-4903-B01C-1260F4953F62
5e479aab-f847-4486-9690-82905539841c
KvkOAoII09ZSAixqGUOtipMDBdKXVlslzVnQOpfDZOEJW+xbFKrK173Gu3h1RVkI
BFE65309-321C-405D-B7CC-9F94C8566236
124fece9-7450-4c48-a8b0-f9b8985e0ce0

POSSIBLE SECRETS
FF0150C8-5917-4965-A1D4-DF37D3CE5A60
cfc7a444-304a-4233-8740-566d40aeffb8
cZ2qwY2ZIJRch325gepGJtH7dQ9IcqmfWvaHdfiFi6Y=
B868EF4EAAD94810AD50FA4FCFAB5A07
6f509c25-32c1-477b-8631-d06e096e50be
d-a310dc5204514027ba83dfc500b9ad47
01219961-4225-47BB-932D-DCB0A2C67303
26c1f159-5318-468e-96d1-738a20a515cb
3LpdW89cIASEFv5WvS5ZDEWsiVGQitP33SL3WZgJ6zE=
9bd7a10f-ab45-404e-9cb3-04203530ffea
7cd596d8-ce4d-4163-8963-19489d5e1cc3
e3dc92c8-b3d7-492c-b67e-cbad5a5b7753
tnRfJM39LV6MDlXml8e8fAfi5JhKcsRyFSmagsP97rbE/0XgA5fRVLlLbAYUcu57
50E6A90FB0A74858B81CEA1353175355
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

POSSIBLE SECRETS
1ed4977d-3918-4822-ad23-7184985b037e
5194A31F-FE57-4543-804B-6FB64377DFD8
D24CD7FA-A2F8-44BF-A8BC-1C984B8984DB
4C19A59F-3407-48E9-8038-6850C2C6FAFA
lsjUo68NMWNsPUz4dBIEYtWAZHRXaEljQLBgt48XQs4=
Kq6mcF8LH4HqXGyg5/DR3VvLtDExNTPXoCRIPhkdOGM=
ECAB6F13-79A5-48D5-B5DC-AFB04E038243
5f21c2e4-a2dd-4235-a055-2fda8162b27c
b6cfcebe-b8c8-4e73-8bb7-c7896f28d28d
17d8d968-6cbc-4e61-8e60-9b92f3aa2add
6vt+8E5GP5AwoxquDM0Y7lVJzS23/VCjNo5D8xB8rgAaaF6IhToGZhlIAUkgigHl
E56BCB9A-7414-46E5-89F3-42930FA9D540
GC4CZUnPsyUcm5NrWw7C8gSktjb/gtBCDrSKBLlqImuOnQy7zHyo6XlIzkH3EMVH
851edeb0-c033-40f9-b8d6-0de4e7796242
0A6639B16FE64704B12EB75BB97B8843

POSSIBLE SECRETS
c519372a-c4ac-499a-a337-ad73abf62e97
d24594fb-836f-468d-9984-0264d1f00d94
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
gYgEHbtWs2qrOou4Pi9x8/evNQKl7xufkAwk8FBwpKpll2nmAbj5wvKo77J2SETY
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
B0A22220F85442F68BA5433D265BFDEC
3349a41e-4991-4dd4-bbe4-694ff5dcb8e7
98614D8B-7B4C-4109-93B4-BCCDBB296482
F2CEEFAC1A9D4B6F8D2F6365106EB243
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
5BhEc19mhLCb3gixLpO/usqpdcrz8iDHUvKRNr8tUAX9rUzF0wog6vEOJrftvcpW
6CWPidOWJZFxRWI8V7yi3OiMbOhIWZX/jTayTGRwqCM0W8dtKHQOPe60TuQicfhG
3071c8717539de5d5353f4c8cd59a032
613cac3f-6dda-49be-9c20-1d1e16311e76
03EAA1B1-2A1D-4EEE-BC47-C0D1F42F9433

POSSIBLE SECRETS
WfvM4SeNDVyFarUKUVpVTE2MRQkjnaN4GpgwC5lMrmyQkCennlTSSkgCAZvzOVXK
512F722A42854EDA94FE7FD9985D8E5A
2ab4a67d-bd5a-4812-9ab6-5671dac23865
uxIInGM9FQ+1gujg5A7z9IJxIqStl6tvqqzSbuEi494=
K/sgHSTVeE1LLZ4HP+m5KF6ND+k7W4ID3M3VTul8bAI=
7800bb44-5ca3-4da1-99ed-712daf52970e
9A6974C3-1898-4326-BA50-895BFF2CE835
d8345f83-c5b7-4a01-8a25-80eea7cdc1bc
774635E273FD4CFF9A5AD673E9E181DF
57C4560B5D96412EAEEA72E306F1802E
d92c9e4b-2d24-41b6-b59d-bcd93d071a92
2D10CFF4-89C0-4813-9C6F-C979D9CC1C0B
f3f38976-3da3-4bc6-ade4-9eb46974ee64
33692334-9b4d-4aee-81d0-38e812a2a6d1
6749AF4D-B459-4B2F-835A-086F918838BE

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a4361 6c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b300906035504061302 5553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
9AB44D85DB264449AA30FED6C1108C3C
b2f88c1b-7e56-4ab9-8e72-3f1c91d204f6
014c0f8a-a401-41d3-8632-4794ea100859
eee6ea52-8f5d-470c-8e1e-a345932b226e
526d5c77-510c-4ec8-af02-db6015ca093c
285c97f1-4f97-48e6-a91b-3165ba5db96a
185a16a3-eeb2-48bc-9107-3bf92b65aeee
40add1df-2b52-4ab2-a874-9ffedc97314c

POSSIBLE SECRETS
f848cf8e-4516-4437-b976-c0b882f5a797
ee30d007-412c-4afe-b890-f78241cd8718
F58D617AADBF470B827DE10906811D1F
C4BCF66C3EEA4C49990FEE67C24B4E80
5631C5D9-0D6C-4615-A6A6-77EC64EDF39C
ysEnh8zkgcN8WwINs5FP7vGybZW2TtVSX36HO6emvdUrcCkVbC9hrF5Pe5ZSZx3i
03511426-7b37-464a-a0ea-3dc17e8ad2e9
3ad2205b-942b-4cdb-ad26-2e3709586978
11484809-4757-4ab3-8f08-6d0077b6522d
25e7f1d5-6e53-44e2-94cf-7047569896c1
xcWDoPM3ZfO4P10VSUmZKRTMvsXPXnglJL31bwAJBgJGdSUy2IQG17s4MILOncV2
b19edef2-f247-4f15-bab2-2ce789784a4d
512C00C3-B4EC-45F2-895B-9202E3AEBA2E
CkzLLxV5zSb+jeaEDnt9Q3eBrpVMtqnw6wBKNocN2YzoApdHEqHkRi4x0VOMDtd4
89031fad-8d53-4581-98f8-10c28b912aca

PLAYSTORE INFORMATION

Title: Calorie Counter by Lose It!

Score: 4.6661506 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.fitnow.loseit

Developer Details: FitNow, Inc., FitNow,+Inc., None, http://www.loseit.com, android@loseit.com,

Release Date: Jul 24, 2011 **Privacy Policy:** Privacy link

Description:

Lose It! is a calorie counter and weight loss diet app that helps you stick to your diet and reach your weight loss goals! Simply set your weight loss goals then track your diet, food and exercise to lose weight. Lose It! is more than just a free calorie tracker. You can track your nutrition, macros, carb and calorie intake, and plan your intermittent fasting schedule. Counting calories, tracking your food and losing weight has never been easier! SIMPLIFY YOUR WEIGHT LOSS JOURNEY Lose It! uses the proven principles of calorie counting, food tracking, calorie deficit and diet tracking to help you succeed. To get started on your weight loss journey, input your profile details and we'll calculate the daily calorie budget. Then, easily track your food, weight, and activity to celebrate your weight loss victories. Change your calorie and dieting habits while learning about your nutrition needs to set achievable goals. AI VOICE & PHOTO MEAL LOGGING Quickly and accurately log meals using your voice or a photo. Just speak into your phone or tap the camera icon to track food and count calories in seconds. Snap a photo, log a meal and make your weight loss journey simple! LOSE IT! BASIC FEATURES • Calorie Tracking – Utilize the calorie counter to it easy to track meals and exercise directly from your phone • Weight Loss Plan – Build a weight loss plan based on your unique body composition, activity level and habits • Community Support – Add your friends and join support groups to stay motivated PREMIUM PLAN FEATURES • Photo Meal Logging – "Snap It" lets you log meals by taking a picture • AI Voice – Just say "I had 2 eggs, toast with butter and jam." to log your meal • Barcode Scanner – Scan food barcodes or search our database of items and recipes • Advanced Tracking – track more than just calories including macronutrients like protein, carbs, fat, sugar; as well as blood pressure, body measurements, sleep cycles and more • Intermittent Fasting - set your intermittent fasting plan and track your fasts in the same app where you track your food • Meal Planning & Targets – meal targets help you calculate suggested nutritional content including macro, carb, protein and overall calorie intake. Customize your diet and eating for personalized weight loss! • Weight Loss Diet Plans – learn about your food and calorie intake habits with our exclusive personal insights to identify what is hindering or helping your weight loss progress • Fitness App Syncs – connect fitness trackers, workout apps, and devices like Fitbit trackers, Misfit trackers, Garmin trackers, Withings scales, Google Fit, Healthkit, and more to maximize your weight loss, gain or maintenance goals Since our launch in 2008 we have been featured in The Wall Street Journal, The Today Show, Men's Health, Women's Health, CNET, Buzzfeed, CNN, Shape, Good Morning America, and more. Lose It! has helped over 57 million users lose more than 150 million pounds. With a global food database of 56+ million items and recipes, tracking what you eat is simple and accurate. Choose from over 25 health goals—including macros, carbs, protein and calories—and start seeing results in just three days of consistent tracking. Download Lose It! and join our weight loss community, full of members helping us reach our mission to mobilize the world to achieve a healthy weight. No matter your diet needs or weight loss goals, Lose It! can help you find weight loss that fits! Should you choose to purchase a Premium or Boost subscription, subscription purchase will be charged to your iTunes account. The yearly subscription will automatically renew unless the auto-renew is turned off at least 24 hours before the period subscription ends. Your premium subscription auto-renew can be turned off or managed in your iTunes account settings. Any unused portion of the free trial is forfeited after purchase. Full terms: http://loseit.com/terms

SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:27:10	Generating Hashes	OK
2025-08-29 22:27:10	Extracting APK	OK
2025-08-29 22:27:10	Unzipping	OK
2025-08-29 22:27:15	Parsing APK with androguard	OK
2025-08-29 22:27:15	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:27:16	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:27:22	Parsing AndroidManifest.xml	OK
2025-08-29 22:27:22	Extracting Manifest Data	OK
2025-08-29 22:27:22	Manifest Analysis Started	OK
2025-08-29 22:27:25	Reading Network Security config from network_security_config.xml	OK

2025-08-29 22:27:25	Parsing Network Security config	OK
2025-08-29 22:27:25	Performing Static Analysis on: Lose It! (com.fitnow.loseit)	OK
2025-08-29 22:27:26	Fetching Details from Play Store: com.fitnow.loseit	OK
2025-08-29 22:27:27	Checking for Malware Permissions	OK
2025-08-29 22:27:27	Fetching icon path	OK
2025-08-29 22:27:27	Library Binary Analysis Started	OK
2025-08-29 22:27:27	Reading Code Signing Certificate	OK
2025-08-29 22:27:28	Running APKiD 2.1.5	OK
2025-08-29 22:27:40	Detecting Trackers	OK
2025-08-29 22:27:47	Decompiling APK to Java with JADX	OK
2025-08-29 22:28:27	Converting DEX to Smali	OK

2025-08-29 22:28:27	Code Analysis Started on - java_source	OK
2025-08-29 22:28:39	Android SBOM Analysis Completed	OK
2025-08-29 22:29:30	Android SAST Completed	OK
2025-08-29 22:29:30	Android API Analysis Started	OK
2025-08-29 22:30:14	Android API Analysis Completed	OK
2025-08-29 22:30:14	Android Permission Mapping Started	OK
2025-08-29 22:31:07	Android Permission Mapping Completed	OK
2025-08-29 22:31:37	Android Behaviour Analysis Started	OK
2025-08-29 22:32:20	Android Behaviour Analysis Completed	OK
2025-08-29 22:32:20	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:32:28	Email and URL Extraction Completed	OK

2025-08-29 22:32:28	Extracting String data from APK	OK
2025-08-29 22:32:29	Extracting String data from Code	OK
2025-08-29 22:32:29	Extracting String values and entropies from Code	OK
2025-08-29 22:32:37	Performing Malware check on extracted domains	OK
2025-08-29 22:32:42	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.