MOBSF

ANDROID STATIC ANALYSIS REPORT

Geocaching (9.67.0)

File Name:	com.groundspeak.geocaching.intro_1454.apk
Package Name:	com.groundspeak.geocaching.intro
Scan Date:	Aug. 29, 2025, 11:20 p.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	23	3	1	1

FILE INFORMATION

File Name: com.groundspeak.geocaching.intro_1454.apk
Size: 31.37MB
MD5: 514c11b86102d35c405376a607587df4
SHA1: 02068356b48eec0ebf56bbc45471bacdee3d9829
SHA256: a5c30fd60a580adb0aad1f582964262c63c8787843c1cb3301965c6f033a1013

APP INFORMATION

App Name: Geocaching
Package Name: com.groundspeak.geocaching.intro
Main Activity: com.groundspeak.geocaching.intro.main.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 9.67.0

Android Version Code: 1454

APP COMPONENTS

Activities: 76
Services: 15
Receivers: 15
Providers: 5
Exported Activities: 7
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=WA, L=Seattle, O=Groundspeak, OU=Groundspeak, CN=Groundspeak
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2009-12-29 12:29:25+00:00
Valid To: 2037-05-16 12:29:25+00:00
Issuer: C=US, ST=WA, L=Seattle, O=Groundspeak, OU=Groundspeak, CN=Groundspeak
Serial Number: 0x4b39f625
Hash Algorithm: sha1
md5: 5611696881d4deb31c02716008811ba7
sha1: 9c10d82bd0317d11af79d9e70a32ba3f88d53223
sha256: 7f000458070a8272e5960f2b3c9d3348372f31b0e600c86af34fc06e85f8db8c
sha512: 7e73f0e7d4d9d2535cd78d90baa179f08ca8c755c9567106717c4e6f6ee56f40262a27a23b42987ac1a8edf161d07b3fae21b51aec8df83fa6fa9c5f4f5832d7
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 60875e5823bb4bb1c7728474e7f929edf1fa25a8e5b21c707cc05b3848806ec4
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.HIGH_SAMPLING_RATE_SENSORS	normal	Access higher sampling rate sensor data	Allows an app to access sensor data with a sampling rate greater than 200 Hz.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.groundspeak.geocaching.intro.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

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_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.

APKID ANALYSIS

FILE	DETAILS
514c11b86102d35c405376a607587df4.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes3.dex	

FINDINGS	DETAILS
yara_issue	yara issue - dex file recognized by apkid but not yara module
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.MODEL check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
Compiler	unknown (please file detection issue!)

<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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.groundspeak.geocaching.intro.main.MainActivity	Schemes: http://, https://, inApp://, Hosts: www.geocaching.com, staging.geocaching.com, MainActivity, coord.info, www.coord.info, staging.coord.info, Paths: /dl/profile, /PROFILE, /dl/milestonesmobile, /dl/friendrequests, /dl/friends, /dl/statistics, /dl/upgrade, /dl/souvenirs, /dl/settingsmobile, /dl/experimental, /dl/emailprefs, /dl/lists, /LISTS, /dl/messagecenter, /MESSAGE_CENTER, /dl/nearbycaches, /MAP, /dl/nearbycacheslist, /dl/filters, /dl/filtersmobile, /dl/search, /dl/quickguide, /dl/helpatgz, /dl/more, Path Prefixes: /dl/navigate/, /SEARCH/, /,

ACTIVITY	INTENT
com.groundspeak.geocaching.intro.validation.UserValidationActivity	Schemes: http://, https://, Hosts: staging.geocaching.com, geocaching.com, www.geocaching.com, coord.info, staging.coord.info, Path Prefixes: /account/join/validateaccount,
com.groundspeak.geocaching.intro.activities.linkaccount.LinkAccountActivity	Schemes: https://, Hosts: www.geocaching.com, Path Prefixes: /dl/profile,
com.groundspeak.geocaching.intro.premium.upsell.PremiumUpsellActivity	Schemes: geocachingscreentrigger://, Hosts: upgradescreen,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.groundspeak.geocaching.intro,
com.groundspeak.geocaching.intro.activities.DeepLinkActivity	Schemes: http://, https://, Hosts: staging.geocaching.com, geocaching.com, www.geocaching.com, Path Prefixes: /hqpromo,

NETWORK SECURITY

HIGH: 1 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	static.geocaching.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

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: 3 | WARNING: 13 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	App Link assetlinks.json file not found [android:name=com.groundspeak.geocaching.intro.validation.UserValidationActivity] [android:host=http://geocaching.com]	high	App Link asset verification URL (http://geocaching.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 302). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
4	App Link assetlinks.json file not found [android:name=com.groundspeak.geocaching.intro.validation.UserValidationActivity] [android:host=https://staging.coord.info]	high	App Link asset verification URL (https://staging.coord.info/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
5	App Link assetlinks.json file not found [android:name=com.groundspeak.geocaching.intro.validation.UserValidationActivity] [android:host=https://geocaching.com]	high	App Link asset verification URL (https://geocaching.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 302). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
6	Activity (com.groundspeak.geocaching.intro.validation.UserValidationActivity) 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.
7	Activity (com.groundspeak.geocaching.intro.activities.linkaccount.LinkAccountActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.groundspeak.geocaching.intro.premium.upsell.PremiumUpsellActivity) 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
9	Activity (com.facebook.CustomTabActivity) 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.groundspeak.geocaching.intro.activities.DeepLinkActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (com.groundspeak.geocaching.intro.campaigns.digitaltreasure.DigitalTreasureCampaignNavHost) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	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
13	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.
14	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
15	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.
16	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

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

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a5/a.java b2/c.java b2/d.java b2/h.java b6/c.java c5/a.java com/airbnb/lottie/utils/d.java com/bumptech/glide/b.java com/bumptech/glide/gifdecoder/d.java com/bumptech/glide/gifdecoder/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/data/mediastore/c.java com/bumptech/glide/load/data/mediastore/e.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_recycle/i.java com/bumptech/glide/load/engine/bitmap_recycle/j.java com/bumptech/glide/load/engine/cache/e.java com/bumptech/glide/load/engine/cache/i.java com/bumptech/glide/load/engine/executor/a.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/w.java com/bumptech/glide/load/model/c.java com/bumptech/glide/load/model/d.java com/bumptech/glide/load/model/g.java com/bumptech/glide/load/model/t.java com/bumptech/glide/load/model/u.java com/bumptech/glide/load/model/v.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/d.java com/bumptech/glide/load/resource/bitmap/h.java com/bumptech/glide/load/resource/bitmap/i.java com/bumptech/glide/load/resource/bitmap/l.java com/bumptech/glide/load/resource/gif/a.java com/bumptech/glide/load/resource/gif/d.java com/bumptech/glide/load/resource/gif/j.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/q.java com/bumptech/glide/manager/r.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/util/pool/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/groundspeak/geocaching/intro/activities/CreateNewMessageActivity.java com/groundspeak/geocaching/intro/activities/EditWaypointActivity.java com/groundspeak/geocaching/intro/analytics/crashlytics/a.java com/groundspeak/geocaching/intro/analytics/launchdarkly/LaunchDarkly.java com/groundspeak/geocaching/intro/api/igc/service/IgcApi.java com/groundspeak/geocaching/intro/api/service/TrackableApi.java com/groundspeak/geocaching/intro/billing/BillingRepository$getProductsWithExtras$2.java com/groundspeak/geocaching/intro/billing/BillingRepository.java com/groundspeak/geocaching/intro/campaigns/CampaignRepositoryKt$fetchCampaignsFromNetworkAndDeferToDB$2.java com/groundspeak/geocaching/intro/campaigns/digitaltreasure/DigitalTreasureCampaignRepoKt.java com/groundspeak/geocaching/intro/db/tables/q.java com/groundspeak/geocaching/intro/debug/DebugCampaignsResponsePresenter$onFragmentDisplayed$1.java com/groundspeak/geocaching/intro/drafts/DraftsViewModel$postLog$1.java com/groundspeak/geocaching/intro/drafts/repos/DraftRepository$syncDraftsFromServer$2.java com/groundspeak/geocaching/intro/drafts/repos/DraftRepository.java com/groundspeak/geocaching/intro/drafts/repos/DraftWorkerRepository$postDraftImages$2.java com/groundspeak/geocaching/intro/drafts/repos/DraftWorkerRepository$postDrafts$2.java com/groundspeak/geocaching/intro/experimentalfeatures/e0.java com/groundspeak/geocaching/intro/ext/MapTileUtilsKt.java com/groundspeak/geocaching/intro/fragments/dial

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	ogs/b.java com/groundspeak/geocaching/intro/fragments/dialogs/h.java com/groundspeak/geocaching/intro/fragments/settings/MessageCenterSettingsFragment.java com/groundspeak/geocaching/intro/fragments/settings/NewsletterSettingsFragment.java com/groundspeak/geocaching/intro/fragments/settings/SettingsViewModel.java com/groundspeak/geocaching/intro/injection/g5.java com/groundspeak/geocaching/intro/main/MainActivity.java com/groundspeak/geocaching/intro/mainmap/map/NewMapFragment$onCreate$1.java com/groundspeak/geocaching/intro/mainmap/map/NewMapFragment$onCreate$2.java com/groundspeak/geocaching/intro/messagecenter/ConversationActivity.java com/groundspeak/geocaching/intro/model/CacheDetailsFetcher.java com/groundspeak/geocaching/intro/model/z0.java com/groundspeak/geocaching/intro/navigationmap/NavigationMapPresenter.java com/groundspeak/geocaching/intro/navigationmap/NavigationViewModel.java com/groundspeak/geocaching/intro/network/api/campaigns/CampaignsApi.java com/groundspeak/geocaching/intro/network/api/drafts/DraftsApi.java com/groundspeak/geocaching/intro/network/api/friends/FriendsApi.java com/groundspeak/geocaching/intro/network/api/geocaches/GeocacheApi.java com/groundspeak/geocaching/intro/network/api/geocaches/logs/GeocacheLog$$serializer.java com/groundspeak/geocaching/intro/network/api/geocaches/logs/GeocacheLog.java com/groundspeak/geocaching/intro/network/api/geocaches/logs/GeocacheLogsApi.java com/groundspeak/geocaching/intro/network/api/g

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/groundspeak/geocaching/intro/network/api/geocaches/logs/GeocacheLogsResponse$Log$$serializer.java com/groundspeak/geocaching/intro/network/api/geocaches/logs/a.java com/groundspeak/geocaching/intro/network/api/images/ImagesApi.java com/groundspeak/geocaching/intro/network/api/iterable/GeocacheIterableUtilKt$fetchIterableJWT$1.java com/groundspeak/geocaching/intro/network/api/launchdarkly/LaunchDarklyApi.java com/groundspeak/geocaching/intro/network/api/lists/GeocacheLog$$serializer.java com/groundspeak/geocaching/intro/network/api/lists/GeocacheLog.java com/groundspeak/geocaching/intro/network/api/lists/ListRepository$downloadRasterTiles$2$1$1$element$1.java com/groundspeak/geocaching/intro/network/api/lists/ListRepository$downloadRasterTiles$2.java com/groundspeak/geocaching/intro/network/api/lists/ListRepository.java com/groundspeak/geocaching/intro/network/api/lists/ListsApi.java com/groundspeak/geocaching/intro/network/api/milestones/MilestonesApiKt.java com/groundspeak/geocaching/intro/network/api/oauth/OAuthApi.java com/groundspeak/geocaching/intro/network/api/payments/PaymentsApi.java com/groundspeak/geocaching/intro/network/api/profile/ProfileApi.java com/groundspeak/geocaching/intro/network/api/push/DeviceRegistrationApi.java com/groundspeak/geocaching/intro/network/api/settings/SettingsApi.java com/groundspeak/geocaching/intro/network/api/stats/StatsApi.java com/groundspeak/geocaching/intro/network/api/user/UserApi.java com/groundspeak/geocaching/intro/network/api/u

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/groundspeak/geocaching/intro/network/api/user/finds/FindsApi.java com/groundspeak/geocaching/intro/network/api/user/hides/HidesApi.java com/groundspeak/geocaching/intro/network/api/utilities/UtilitiesApi.java com/groundspeak/geocaching/intro/network/api/waypoints/WaypointsApi.java com/groundspeak/geocaching/intro/network/souvenirs/SouvenirApi.java com/groundspeak/geocaching/intro/notifications/AwardMomentWindow.java com/groundspeak/geocaching/intro/premium/upsell/PremiumUpsellFragment.java com/groundspeak/geocaching/intro/profile/ProfileFragment.java com/groundspeak/geocaching/intro/profile/friends/FriendsFragment.java com/groundspeak/geocaching/intro/profile/hidesandfinds/HideCacheApi.java com/groundspeak/geocaching/intro/search/SearchRepository.java com/groundspeak/geocaching/intro/services/ListDownloadService$downloadCaches$1.java com/groundspeak/geocaching/intro/services/ListDownloadService$stopCurrentDownload$1$1.java com/groundspeak/geocaching/intro/services/ListDownloadService.java com/groundspeak/geocaching/intro/tasks/TrackableLogTask.java com/groundspeak/geocaching/intro/trackables/services/TrackableLogQueueWorker.java com/groundspeak/geocaching/intro/trackables/work/TrackablesLogUploadWorker.java com/groundspeak/geocaching/intro/types/PostTrackableLog.java com/groundspeak/geocaching/intro/types/TrackableLogType.java com/groundspeak/geocaching/intro/ui/compose/y0.java com/groundspeak/geocaching/intro/util/ImageUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				java com/groundspeak/geocaching/intro/util/SettingsSharedPrefs.java com/groundspeak/geocaching/intro/util/SyncingMonitorKt$monitorDraftImageSyncingTables$1.java com/groundspeak/geocaching/intro/util/SyncingMonitorKt$monitorDraftImageSyncingTables$2.java com/groundspeak/geocaching/intro/util/SyncingMonitorKt$monitorDraftSyncingTables$1.java com/groundspeak/geocaching/intro/util/SyncingMonitorKt$monitorDraftSyncingTables$2.java com/groundspeak/geocaching/intro/util/SyncingMonitorKt$monitorDraftSyncingTables$3.java com/groundspeak/geocaching/intro/util/SyncingMonitorKt$monitorGeocacheLogsSyncingTables$1.java com/groundspeak/geocaching/intro/util/UtilKt.java com/groundspeak/geocaching/intro/util/e1.java com/iterable/iterableapi/t0.java com/willowtreeapps/signinwithapplebutton/view/SignInWebViewDialogFragment.java h2/l.java h5/d.java ha/a.java i1/a.java i2/d.java j0/c.java k2/n.java k3/h.java l9/o.java m2/c.java m3/a.java p5/l.java q5/c.java q5/d.java retrofit/Platform.java rx/internal/util/g.java rx/plugins/c.java s7/g.java t6/a.java t7/a.java t9/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t9/c.java u5/a.java u6/c.java w1/b.java y8/a.java z4/a.java z6/g.java
2	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/groundspeak/geocaching/intro/fragments/dialogs/y.java d8/i0.java
3	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	aa/a.java com/groundspeak/geocaching/intro/db/tables/GeocacheNoteTable.java com/groundspeak/geocaching/intro/db/tables/a.java com/groundspeak/geocaching/intro/db/tables/b.java com/groundspeak/geocaching/intro/db/tables/c.java com/groundspeak/geocaching/intro/db/tables/f.java com/groundspeak/geocaching/intro/db/tables/g.java com/groundspeak/geocaching/intro/db/tables/h.java com/groundspeak/geocaching/intro/db/tables/i.java com/groundspeak/geocaching/intro/db/tables/j.java com/groundspeak/geocaching/intro/db/tables/k.java com/groundspeak/geocaching/intro/db/tables/l.java com/groundspeak/geocaching/intro/db/tables/m.java com/groundspeak/geocaching/intro/db/tables/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/groundspeak/geocaching/intro/db/tables/o.java com/groundspeak/geocaching/intro/db/tables/q.java com/groundspeak/geocaching/intro/db/tables/r.java com/groundspeak/geocaching/intro/db/tables/s.java com/iterable/iterableapi/f1.java com/iterable/iterableapi/y.java t7/a.java u7/a.java u7/b.java u7/c.java u7/d.java
				coil/memory/MemoryCache.java coil/request/l.java com/bumptech/glide/load/d.java com/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/n.java com/bumptech/glide/load/engine/u.java com/geocaching/api/type/ProfileResponse.java com/groundspeak/geocaching/intro/api/service/TrackableProfileSummary.java com/groundspeak/geocaching/intro/geocacheactivity/f2.java com/groundspeak/geocaching/intro/network/ProfileTest.java com/groundspeak/geocaching/intro/network/api/friends/Friend.java com/groundspeak/geocaching/intro/network/api/friends/FriendRequestUser.java com/groundspeak/geocaching/intro/network/api/geocaches/GeocacheOwner.java com/groundspeak/geocaching/intro/network/api/geocaches/LiteGeocache.java com/groundspeak/geocaching/intro/network/api/geocaches/ValidationProfileResponse.java com/groundspeak/geocaching/intro/network/api/g

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eocaches/logs/GeocacheLog.java com/groundspeak/geocaching/intro/network/api/geocaches/logs/GeocacheLogsResponse.java
4	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/groundspeak/geocaching/intro/network/api/lists/GeocacheLogOwner.java com/groundspeak/geocaching/intro/network/api/lists/GeocacheOwner.java com/groundspeak/geocaching/intro/network/api/oauth/OAuthCreateAccountBody.java com/groundspeak/geocaching/intro/network/api/oauth/OAuthLinkAccountRequestBody.java com/groundspeak/geocaching/intro/network/api/profile/ActivityLogOwner.java com/groundspeak/geocaching/intro/network/api/profile/OwnProfileResponse.java com/groundspeak/geocaching/intro/network/api/profile/UserLoginRequestBody.java com/groundspeak/geocaching/intro/network/api/profile/UserLoginResponse.java com/groundspeak/geocaching/intro/network/api/profile/UserProfileResponse.java com/groundspeak/geocaching/intro/network/api/user/CreateUserBody.java com/groundspeak/geocaching/intro/network/api/user/hides/LiteGeocacheOrdered.java com/groundspeak/geocaching/intro/profile/friends/b.java com/groundspeak/geocaching/intro/profile/hidesandfinds/y2.java com/groundspeak/geocaching/intro/profile/i2.java com/groundspeak/geocaching/intro/profile/j2.java com/groundspeak/geocaching/intro/profile/x2.java com/groundspeak/geocaching/intro/push/DeserializedPushNotification.java com/groundspeak/geocaching/intro/types/igc/ParticipantPayload.java e9/a.java io/grpc/internal/j2.java y3/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ec/x.java lf/c.java lf/d.java lf/i.java lf/j.java
6	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	bf/b.java de/a.java ef/a.java ef/b.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/b0.java io/grpc/internal/j1.java io/grpc/internal/l1.java io/grpc/internal/t1.java io/grpc/okhttp/g.java io/grpc/util/h.java io/grpc/util/j.java nl/dionsegijn/konfetti/emitters/RenderSystem.java
7	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	g6/a.java io/ktor/util/NonceKt$nonceGeneratorJob$1.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/iterable/iterableapi/s0.java v5/b.java
9	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/groundspeak/geocaching/intro/util/ImageUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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/groundspeak/geocaching/intro/util/ImageUtils.java ua/a.java
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	ec/l.java
12	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	w4/f.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/groundspeak/geocaching/intro/activities/DeepLinkActivity.java com/groundspeak/geocaching/intro/activities/MessageUserActivity.java com/groundspeak/geocaching/intro/activities/VideoActivity.java com/groundspeak/geocaching/intro/activities/s0.java com/groundspeak/geocaching/intro/base/BaseMapFragInjected.java com/groundspeak/geocaching/intro/debug/DebugMenuFragment.java com/groundspeak/geocaching/intro/debug/LaunchDarklyOverrideFragment.java com/groundspeak/geocaching/intro/fragments/LegalFragment.java com/groundspeak/geocaching/intro/fragments/QuickGuideFragment.java com/groundspeak/geocaching/intro/fragments/g1.java com/groundspeak/geocaching/intro/geocachedetails/GeocacheDetailsActivity.java com/groundspeak/geocaching/intro/main/MainActivity.java com/groundspeak/geocaching/intro/more/MoreFragment.java com/groundspeak/geocaching/intro/navigationmap/NavigationMapActivity2.java com/groundspeak/geocaching/intro/onboarding/OnboardingMapActivity.java com/groundspeak/geocaching/intro/profile/hidesandfinds/HidesListFragment.java com/groundspeak/geocaching/intro/profile/hidesandfinds/OtherHidesListFragment.java com/groundspeak/geocaching/intro/search/SearchLandingFragment.java com/groundspeak/geocaching/intro/souvenirs/SouvenirDetailsActivity.java com/groundspeak/geocaching/intro/trackables/TrackableDetailsActivity.java com/groundspeak/geocaching/intro/trackables/TrackableEducationActivity.java com/groundspeak/geocaching/intro/trackables/logs/CreateTrackableLogActivity.java com/groundspeak/geocaching/intro/trackables/logs/n.java com/groundspeak/geocaching/intro/util/UtilKt.java com/groundspeak/geocaching/intro/util/j0.java com/groundspeak/geocaching/intro/util/w0.java com/groundspeak/geocaching/intro/util/w1.java com/iterable/iterableapi/o.java com/iterable/iterableapi/x0.java h7/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/groundspeak/geocaching/intro/debug/DebugMenuFragment.java com/groundspeak/geocaching/intro/fragments/LegalFragment.java com/groundspeak/geocaching/intro/main/MainActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/groundspeak/geocaching/intro/profile/hidesandfinds/HidesListFragment.java com/groundspeak/geocaching/intro/profile/hidesandfinds/OtherHidesListFragment.java com/groundspeak/geocaching/intro/search/SearchLandingFragment.java com/groundspeak/geocaching/intro/util/j0.java com/iterable/iterableapi/o.java h7/d.java
00036	Get resource file from res/raw directory	reflection	com/groundspeak/geocaching/intro/activities/s0.java com/groundspeak/geocaching/intro/util/j0.java com/iterable/iterableapi/o.java com/iterable/iterableapi/x0.java i4/e.java
00013	Read file and put it into a stream	file	a5/a.java com/bumptech/glide/load/b.java com/bumptech/glide/load/model/g.java com/iterable/iterableapi/i1.java j3/b.java okio/w.java retrofit/mime/TypedFile.java s5/i.java v5/a.java w4/f.java w4/g.java z5/j.java
00191	Get messages in the SMS inbox	sms	com/groundspeak/geocaching/intro/messagecenter/MessagesAdapter.java
00003	Put the compressed bitmap data into JSON object	camera	p5/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	io/ktor/network/sockets/SocketImpl.java lf/b.java lf/j.java
00163	Create new Socket and connecting to it	socket	io/ktor/network/sockets/SocketImpl.java lf/b.java lf/j.java
00047	Query the local IP address	network collection	io/ktor/network/sockets/SocketImpl.java
00022	Open a file from given absolute path of the file	file	coil/disk/a.java com/airbnb/lottie/q.java com/groundspeak/geocaching/intro/util/ImageUtils.java retrofit/mime/TypedFile.java ua/a.java w4/f.java w4/g.java
00091	Retrieve data from broadcast	collection	com/groundspeak/geocaching/intro/activities/EditWaypointActivity.java com/groundspeak/geocaching/intro/activities/FullTextActivity.java com/groundspeak/geocaching/intro/activities/GeocacheDTSActivity.java com/groundspeak/geocaching/intro/main/MainActivity.java com/groundspeak/geocaching/intro/messagecenter/ConversationActivity2.java com/groundspeak/geocaching/intro/trackables/inventory/TrackableInventoryActivity.java com/groundspeak/geocaching/intro/trackables/logs/CreateTrackableLogActivity.java com/iterable/iterableapi/q.java com/iterable/iterableapi/ui/inbox/IterableInboxActivity.java com/iterable/iterableapi/z0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/groundspeak/geocaching/intro/util/Util.java com/iterable/iterableapi/d1.java io/ktor/client/engine/android/AndroidClientEngine.java retrofit/client/UrlConnectionClient.java w4/b.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/j.java com/groundspeak/geocaching/intro/profile/qr/QRCodeViewModel.java com/iterable/iterableapi/d1.java g6/c.java retrofit/client/UrlConnectionClient.java ua/a.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/j.java com/groundspeak/geocaching/intro/util/Util.java com/iterable/iterableapi/d1.java io/ktor/client/engine/android/AndroidClientEngine.java retrofit/client/UrlConnectionClient.java ua/a.java
00014	Read file into a stream and put it into a JSON object	file	s5/i.java v5/a.java z5/j.java
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/q.java
00004	Get filename and put it to JSON object	file collection	d6/a.java
00094	Connect to a URL and read data from it	command network	com/groundspeak/geocaching/intro/util/Util.java ua/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	k2/n.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java com/groundspeak/geocaching/intro/profile/qr/QRCodeViewModel.java w4/b.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/c.java
00072	Write HTTP input stream into a file	command network file	ua/a.java
00108	Read the input stream from given URL	network command	ua/a.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/1035398089347/namespaces/firebase:fetch?key=AIzaSyAbjnGKC7IlAfUF74AkaXMCcMQ9PadrcAA is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'shop_link_presentation': '{"isHidden":false,"shopImageLink":{"imageUrl":"https://firebasestorage.googleapis.com/v0/b/geocaching-production-1.appspot.com/o/Shop%20link%20images%2FFall%20Equinox%20Coin%20GC%20Mobile%20App%20Hero%20Banner.png?alt=media&token=c0fb0e42-ac75-4b2e-87aa-fa93627db7e0","imageAltText":"September equinox geocoin now available at Shop Geocaching.","copy":"Everything you need to hide, play, and share","linkUrl":"https://shop.geocaching.com/?utm_source=geocaching_app&utm_medium=more&utm_campaign=2024_signal_plush&utm_content=banner"}}'}, 'state': 'UPDATE', 'templateVersion': '139'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
www.maptiler.com	ok	**IP:** 104.17.246.40 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
img.geocaching.com	ok	**IP:** 63.251.163.214 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map
www.nasa.gov	ok	**IP:** 192.0.66.108 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.748425 **Longitude:** -122.413673 **View:** Google Map
appleid.apple.com	ok	**IP:** 17.23.96.16 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
communication-service.geocaching.com	ok	**IP:** 63.251.163.216 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map
support.google.com	ok	**IP:** 64.233.177.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.eu.iterable.com	ok	**IP:** 52.31.143.172 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
api.groundspeak.com	ok	**IP:** 63.251.163.198 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
thumbs.dreamstime.com	ok	**IP:** 151.101.129.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
payments.geocaching.com	ok	**IP:** 63.251.163.194 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
coord.info	ok	**IP:** 63.251.163.213 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map
www.geocaching.com	ok	**IP:** 63.251.163.200 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
shop.geocaching.com	ok	**IP:** 23.227.38.74 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map
apidevelopers.geocaching.com	ok	**IP:** 63.251.163.238 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map
www.youtube.com	ok	**IP:** 172.253.124.190 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
maptiles-test.geocaching.com	ok	**IP:** 63.251.163.242 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dgalywyr863hv.cloudfront.net	ok	**IP:** 18.238.92.212 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
maptiles.geocaching.com	ok	**IP:** 63.251.163.204 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map
oauth.geocaching.com	ok	**IP:** 63.251.163.200 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map
api.iterable.com	ok	**IP:** 54.164.170.125 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
static.geocaching.com	ok	**IP:** 18.238.92.193 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.openstreetmap.org	ok	**IP:** 172.67.173.161 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
ktor.io	ok	**IP:** 13.224.53.103 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
forums.geocaching.com	ok	**IP:** 63.251.163.241 **Country:** United States of America **Region:** Washington **City:** Silver Firs **Latitude:** 47.866020 **Longitude:** -122.155098 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
d17wd0umvxxjds.cloudfront.net	ok	**IP:** 18.238.92.203 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
adventurelab.page.link	ok	**IP:** 142.250.105.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
confluence.hq.groundspeak.biz	ok	**IP:** 66.150.167.130 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.615700 **Longitude:** -122.344498 **View:** Google Map

EMAILS

EMAIL	FILE
contact+mobile@geocaching.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"apple_oauth_provider" : "Apple"
"com.google.firebase.crashlytics.mapping_file_id" : "0262b526a8164947939b540ce2a55344"
"compass" : "Compass"
"dev_oauth_label" : "OAuth"
"facebook_client_token" : "3230689c61ccd5479e9ac64038670613"

POSSIBLE SECRETS
"facebook_oauth_provider" : "Facebook"
"google_api_key" : "AIzaSyAbjnGKC7IlAfUF74AkaXMCcMQ9PadrcAA"
"google_crash_reporting_api_key" : "AIzaSyAbjnGKC7IlAfUF74AkaXMCcMQ9PadrcAA"
"google_oauth_provider" : "Google"
"iterable_client_token" : "d5c3834176a54cfc8dd8fbd2c479e21e"
"key_ed_and_promo" : "com.groundspeak.geocaching.intro.db.UserSettings.ED_AND_PROMO"
"key_language" : "com.groundspeak.geocaching.intro.db.UserSettings.LANGUAGE"
"key_mentions" : "com.groundspeak.geocaching.intro.db.UserSettings.MENTIONS"
"legal_url_authorized_developers" : "https://apidevelopers.geocaching.com"
"password" : "Password"
"username" : "Username"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghjkmnpqrstvwxyz
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51

POSSIBLE SECRETS
759efbdb-e9f5-4e95-96c0-58e72f23311a
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
b8cdd85e-956f-4771-9692-252ad1d9e38b
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
c56fb7d591ba6704df047fd98f535372fea00211
a-95ed6082-b8e9-46e8-a73f-ff56f00f5d9d
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9b8f518b086098de3d77736f9458a3d2f6f95a37
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
ZjAxZWZlZDUtMWYyNi00MTQzLWI4YTAtNjEyZmI5YjNlN2FmOkRuQnlRdzJSdmFxNHpZNDlXWjR3Mlh4OGUyYlNEcg==

POSSIBLE SECRETS
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
86254750241babac4b8d52996a675549
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
cc2751449a350f668590264ed76692694a80308a
68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403803403728088927070054 49
38cf4c50-8eeb-4c01-85e9-5d78acab7b6a
1cbd3130fa23b59692c061c594c16cc0
a7967d2a7e2d2d1692074a14d9837cad
D72FD950-5342-4402-8811-17E49585CAD9
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
115792089210356248762697446949407573529996955224135760342422259061068512044369

POSSIBLE SECRETS
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
3acaaac89ab7e7d66e2cfcf190c05669
bbd9d645-f17e-4f8d-90e2-5d4b021b1056

PLAYSTORE INFORMATION

Title: Geocaching®

Score: 4.5909777 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.groundspeak.geocaching.intro

Developer Details: Groundspeak Inc., Groundspeak+Inc., None, http://www.geocaching.com/help, contact@geocaching.com,

Release Date: Apr 15, 2014 **Privacy Policy:** Privacy link

Description:

Discover the World's Largest Treasure Hunt with Geocaching® Embark on real-world treasure hunts with Geocaching, the ultimate outdoor adventure app! Join millions of players worldwide in a game of hide-and-seek using GPS coordinates. Whether you enjoy camping, hiking scenic trails, exploring nature while biking, or getting your heart rate up while running, geocaching adds a fun and rewarding dimension to your favorite outdoor activities. Explore the outdoors and discover hidden geocaches tucked away in parks, cities, forests, and scenic places all around the world! To celebrate the 25th year of geocaching, we have introduced digital Treasures, a new way to enhance your geocaching experience! These themed Treasure collections add a fresh layer of excitement to every adventure. Show off your collected Treasures in the app and challenge yourself and your friends to collect them all! Geocaching isn’t just about finding hidden treasures—it’s also about creating them! The global geocaching community is built by players who hide geocaches for others to find. Hiding a geocache connects you to a community of millions, all from a set of coordinates! Share your favorite scenic spots, historical points of interest, or your creatively designed container. Read messages from players who discover and log your cache, and challenge friends and family to find your hidden gem. How Geocaching Works: • Find Geocaches on the Map: Use the app's map to locate hidden containers (geocaches) near your current location or plan adventures on your favorite hike or trail. • Navigate to the Cache: Follow the app’s GPS-guided directions to get within a short distance of the hidden treasure. • Start Searching: Use your observation skills to uncover cleverly disguised caches that could look like anything. • Sign the Logbook: Write your name in the logbook inside the geocache and log it in the app. • Trade SWAG (Optional): Some geocaches contain coins, trackable tags, and trinkets for trading. • Return the Geocache: Place the geocache back exactly where you found it for the next explorer to find. Why You'll Love Geocaching: • Explore the Outdoors: Discover new places and hidden gems in your neighborhood and beyond. • Fun for Everyone: Enjoy geocaching with family, friends, or solo. It's a great activity for all ages and fitness levels. • Global Community: Connect with other geocachers at local events and online. • Endless Adventure: With millions of geocaches hidden worldwide, there's always a new treasure to find. • Hide Your Own Cache: Showcase your favorite scenic spots or design your own creative container to hide. • New Digital Treasure: You can now collect digital Treasure from logging qualifying caches! Go Premium for the Ultimate Geocaching Experience: Unlock all geocaches and exclusive features with Geocaching

Premium: • Access all Geocaches: Discover every cache type, including premium-only caches. • Offline Maps: Download maps and cache details for offline use, perfect for remote adventures. • Trail Maps: Access the Trails map for offline or off-road outings. • Personalized Statistics: Monitor your progress and achievements with streaks, milestones and more! • Advanced Search Filters: Find specific geocache types, sizes, and difficulty levels. Download Geocaching® today and start exploring! You can buy a Premium membership subscription through your Google Play account. Premium membership is available with a monthly or annual subscription. You can subscribe and pay through your Google Play account. Your subscription will automatically renew unless canceled at least 24 hours before the end of the current period. Terms of use: https://www.geocaching.com/about/termsofuse.aspx Refund policy: https://www.geocaching.com/account/documents/refundpolicy

SCAN LOGS

Timestamp	Event	Error
2025-08-29 23:20:34	Generating Hashes	OK
2025-08-29 23:20:34	Extracting APK	OK
2025-08-29 23:20:34	Unzipping	OK
2025-08-29 23:20:35	Parsing APK with androguard	OK
2025-08-29 23:20:35	Extracting APK features using aapt/aapt2	OK
2025-08-29 23:20:35	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 23:20:38	Parsing AndroidManifest.xml	OK

2025-08-29 23:20:38	Extracting Manifest Data	OK
2025-08-29 23:20:38	Manifest Analysis Started	OK
2025-08-29 23:20:40	Reading Network Security config from network_security_config.xml	OK
2025-08-29 23:20:40	Parsing Network Security config	OK
2025-08-29 23:20:40	Performing Static Analysis on: Geocaching (com.groundspeak.geocaching.intro)	OK
2025-08-29 23:20:40	Fetching Details from Play Store: com.groundspeak.geocaching.intro	OK
2025-08-29 23:20:41	Checking for Malware Permissions	OK
2025-08-29 23:20:41	Fetching icon path	OK
2025-08-29 23:20:42	Library Binary Analysis Started	OK
2025-08-29 23:20:42	Reading Code Signing Certificate	OK
2025-08-29 23:20:42	Running APKiD 2.1.5	OK

2025-08-29 23:20:44	Detecting Trackers	OK
2025-08-29 23:20:49	Decompiling APK to Java with JADX	OK
2025-08-29 23:21:11	Converting DEX to Smali	OK
2025-08-29 23:21:11	Code Analysis Started on - java_source	OK
2025-08-29 23:21:18	Android SBOM Analysis Completed	OK
2025-08-29 23:21:26	Android SAST Completed	OK
2025-08-29 23:21:26	Android API Analysis Started	OK
2025-08-29 23:21:34	Android API Analysis Completed	OK
2025-08-29 23:21:35	Android Permission Mapping Started	OK
2025-08-29 23:21:42	Android Permission Mapping Completed	OK
2025-08-29 23:21:43	Android Behaviour Analysis Started	OK

2025-08-29 23:21:53	Android Behaviour Analysis Completed	OK
2025-08-29 23:21:53	Extracting Emails and URLs from Source Code	OK
2025-08-29 23:21:57	Email and URL Extraction Completed	OK
2025-08-29 23:21:57	Extracting String data from APK	OK
2025-08-29 23:21:57	Extracting String data from Code	OK
2025-08-29 23:21:57	Extracting String values and entropies from Code	OK
2025-08-29 23:22:01	Performing Malware check on extracted domains	OK
2025-08-29 23:22:07	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.