ANDROID STATIC ANALYSIS REPORT

app_icon

Shotsy (1.0.0)

File Name:	com.shotsy.app_12.apk
Package Name:	com.shotsy.app
Scan Date:	Sept. 1, 2025, 8:46 a.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	15	1	1	0

FILE INFORMATION

File Name: com.shotsy.app_12.apk
Size: 61.45MB
MD5: 7948cb207740ab8237112318330d0608
SHA1: c0f326634f3a8d72df11d9dfba5d57ae8c208ebe
SHA256: 3f127f911968d8b83dcddc13e2fdabb58a2c8c490eb682f9754d525542bd9322

APP INFORMATION

App Name: Shotsy
Package Name: com.shotsy.app
Main Activity: com.shotsy.app.ui.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 1.0.0

Android Version Code: 12

APP COMPONENTS

Activities: 12
Services: 8
Receivers: 3
Providers: 4
Exported Activities: 3
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-11-27 17:39:59+00:00
Valid To: 2054-11-27 17:39:59+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe71aa0c3e938bb0bce379dd40fda8f69d8d11cf8
Hash Algorithm: sha256
md5: 1491203cb676b065856542f9980133de
sha1: 3b009dff52197676931ac7ce3cdefc17e6c8f6f3
sha256: 1d312e6fdcfd39ca384d76b343f12c181975c2f76018220e4ae9ae0ec08b3f8e
sha512: 92059da9b1fe71c99aef86ab3aa719f390c6180d71985534d734cd9439438ec4031f5dd34c1c1fb50ea2b7da13c8e93e1c3e0e952bf582148a80466dcb98c14c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: cb8408ee0b0ccaafa228e7cd2d2c0a41abb62f0d187f050aa601e1073758cd4d
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.shotsy.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
7948cb207740ab8237112318330d0608.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</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.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></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.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
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.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	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.
6	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
7	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: **5** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/caverock/androidsvg/CSSParser.java com/caverock/androidsvg/SVG.java com/caverock/androidsvg/SVGAndroidRenderer.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java com/kizitonwose/calendar/compose/CalendarState.java com/kizitonwose/calendar/compose/heatmapcalendar/HeatMapCalendarState.java com/kizitonwose/calendar/compose/weekcalendar/WeekCalendarState.java com/kizitonwose/calendar/compose/yearcalendar/YearCalendarState.java com/pairip/licensecheck/LicenseActivity.java com/pairip/licensecheck/LicenseClient.java com/revenuecat/purchases/common/DefaultLogHandler.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/revenuecat/purchases/ui/revenuecatui/helpers/Logger.java com/shotsy/app/repository/DayRecordRepository.java com/shotsy/app/repository/MedicationRepository.java com/shotsy/app/repository/ShotRepository.java com/shotsy/app/repository/UserSettingsRepository.java com/shotsy/app/ui/screens/settings/medications/EditCustomMedicationScreenKt.java com/shotsy/app/ui/screens/settings/medications/MedicationsScreenKt.java com/shotsy/app/ui/screens/summary/EstimatedLevelsChartKt$EstimatedLevelsChart$3$1.java com/shotsy/app/ui/screens/summary/EstimatedLevelsChartKt$EstimatedLevelsChart$4$1.java com/shotsy/app/ui/screens/summary/EstimatedLevelsChartKt$GraphWithFilledBezierCurveAndYAxisOnRight$3$1.java com/shotsy/app/ui/screens/summary/EstimatedLevelsChartKt$GraphWithFilledBezierCurveAndYAxisOnRight$4.java com/shotsy/app/ui/screens/summary/EstimatedLevelsChartKt.java com/shotsy/app/ui/viewmodels/AppNavigationViewModel$createCredential$1.java com/shotsy/app/ui/viewmodels/AppNavigationViewModel$deleteAccount$1.java com/shotsy/app/ui/viewmodels/AppNavigationViewModel$onLogout$1.java com/shotsy/app/ui/viewmodels/AppNavigationViewModel$onSignInWithGoogle$$inlined$CoroutineExceptionHandler$1.java com/shotsy/app/ui/viewmodels/AppNavigationViewModel$onSignInWithGoogle$2.java com/shotsy/app/ui/viewmodels/AppNavigationViewModel.java com/shotsy/app/ui/viewmodels/EditShotViewModel$observeMedications$1.java com/shotsy/app/ui/viewmodels/ShotFormStateViewModel$observeMedications$1.java com/shotsy/app/ui/viewmodels/ShotFormStateViewModel.java com/shotsy/app/ui/viewmodels/ShotViewModel$observeShots$1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/shotsy/app/ui/viewmodels/SummaryViewModel$observeShots$1.java com/shotsy/app/ui/viewmodels/SummaryViewModel.java com/shotsy/app/ui/viewmodels/UserSettingsViewModel$observeShots$1.java io/grpc/android/AndroidChannelBuilder.java io/grpc/okhttp/internal/Platform.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	coil/decode/SvgDecoder.java coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java io/grpc/PersistentHashArrayMappedTrie.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/PickFirstLoadBalancerProvider.java io/grpc/internal/TransportFrameUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	coil/decode/SourceImageSource.java
4	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	io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/PickFirstLeafLoadBalancer.java io/grpc/internal/PickFirstLoadBalancer.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/OutlierDetectionLoadBalancer.java io/grpc/util/RoundRobinLoadBalancer.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.java
6	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/revenuecat/purchases/common/UtilsKt.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.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	com/shotsy/app/ui/MainActivityKt.java com/shotsy/app/ui/screens/settings/ExportDataScreenKt.java com/shotsy/app/ui/screens/settings/SettingsScreenKt$SettingsScreen$1.java com/shotsy/app/ui/screens/settings/SettingsScreenKt.java com/shotsy/app/ui/screens/settings/SubscriptionScreenKt.java com/shotsy/app/ui/screens/settings/medications/MedicationSectionKt$MedicationSection$1$2.java com/shotsy/app/ui/screens/summary/EstimatedLevelsPaywallKt.java
00013	Read file and put it into a stream	file	coil/fetch/ContentUriFetcher.java com/revenuecat/purchases/common/FileHelper.java io/grpc/TlsChannelCredentials.java io/grpc/TlsServerCredentials.java io/grpc/util/AdvancedTlsX509KeyManager.java io/grpc/util/AdvancedTlsX509TrustManager.java okio/Okio__JvmOkioKt.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/shotsy/app/ui/MainActivityKt.java com/shotsy/app/ui/screens/settings/SettingsScreenKt.java com/shotsy/app/ui/screens/settings/SubscriptionScreenKt.java
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/shotsy/app/ui/MainActivityKt.java com/shotsy/app/ui/screens/settings/ExportDataScreenKt.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/revenuecat/purchases/common/HTTPClient.java com/shotsy/app/ui/screens/settings/ContactUsScreenKt$ContactUsScreen$sendFeedbackToZendesk$2.java
00089	Connect to a URL and receive input stream from the server	command network	com/revenuecat/purchases/common/HTTPClient.java
00109	Connect to a URL and get the response code	network command	com/revenuecat/purchases/common/HTTPClient.java com/shotsy/app/ui/screens/settings/ContactUsScreenKt$ContactUsScreen$sendFeedbackToZendesk$2.java
00162	Create InetSocketAddress object and connecting to it	socket	io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java
00163	Create new Socket and connecting to it	socket	io/grpc/android/UdsSocket.java io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java
00022	Open a file from given absolute path of the file	file	coil/disk/DiskCache.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/313099633309/namespaces/firebase:fetch?key=AIzaSyAvEfkDDnovm8S7JkoB-vRome1Py-A8SSY is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'android_summary_announce_simple_text': '{"de":"Wir suchen deutschsprachige Beta-Tester! Wenn Sie interessiert sind, senden Sie uns bitte eine Nachricht über das Kontaktformular.","_comment_pt-BR":"Estamos procurando testadores beta que falem português brasileiro! Se você tiver interesse, por favor nos envie uma mensagem através do formulário de contato."}', 'android_whatsnew_messages': '[{"date":"2025-7-28","version":"1.4.0","message":{"en":"Changes in this update:\\n* Added support for showing multiple medications on the estimated medication levels chart.\\n* Fixed a bug that occurred when changing medication visibility and then adding a shot.","de":"Änderungen in diesem Update:\\n* Unterstützung für die Anzeige mehrerer Medikamente im Diagramm der geschätzten Medikamentenspiegel hinzugefügt.\\n* Fehler behoben, der beim Ändern der Medikamentensichtbarkeit und anschließenden Hinzufügen einer Injektion auftrat.","pt":"Mudanças nesta atualização:\\n* Adicionado suporte para exibir vários medicamentos no gráfico de níveis estimados de medicação.\\n* Corrigido um bug que ocorria ao alterar a visibilidade do medicamento e, em seguida, adicionar uma aplicação."}},{"date":"2025-7-24","version":"1.3.2","message":{"en":"Changes in this update:\\n* Fixed bug where deleted or future shots were showing on the results chart.\\n* Added more Y-axis values for the results chart.\\n* Fixed bug in total change calculation on the Shots tab.\\n* Fixed bug in Color Themes.","de":"Änderungen in diesem Update:\\n* Fehler behoben, bei dem gelöschte oder zukünftige Injektionen im Ergebnisdiagramm angezeigt wurden.\\n* Mehr Y-Achsen-Werte für das Ergebnisdiagramm hinzugefügt.\\n* Fehler in der Gesamtänderungsberechnung auf der Injektionen-Registerkarte behoben.\\n* Fehler in Farbthemen behoben.","pt":"Mudanças nesta atualização:\\n* Corrigido bug onde aplicações excluídas ou futuras apareciam no gráfico de resultados.\\n* Adicionados mais valores do eixo Y para o gráfico de resultados.\\n* Corrigido bug no cálculo de mudança total na aba Aplicações.\\n* Corrigido bug nos Temas de Cores."}}]', 'latest_version_android': '1.0.0', 'min_supported_version_android': '1.0.0'}, 'state': 'UPDATE', 'templateVersion': '35'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK
Other Common Permissions	2/44	com.google.android.gms.permission.AD_ID, 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
shotsyapp.com	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.accessdata.fda.gov	ok	**IP:** 23.53.145.191 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.nejm.org	ok	**IP:** 104.18.41.121 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
shotsyapp.zendesk.com	ok	**IP:** 216.198.53.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
api.revenuecat.com	ok	**IP:** 54.88.247.37 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
errors.rev.cat	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

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	**IP:** 18.238.109.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-diagnostics.revenuecat.com	ok	**IP:** 13.216.30.250 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.revenuecat.com	ok	**IP:** 18.155.173.119 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api-paywalls.revenuecat.com	ok	**IP:** 13.216.30.250 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
assets.pawwalls.com	ok	**IP:** 18.238.96.3 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
revenuecat.com	ok	**IP:** 18.238.109.49 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
yourname@example.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
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
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyAvEfkDDnovm8S7JkoB-vRome1Py-A8SSY"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyAvEfkDDnovm8S7JkoB-vRome1Py-A8SSY"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghjkmnpqrstvwxyz
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
af60eb711bd85bc1e4d3e0a462e074eea428a8
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
36864200e0eaf5284d884a0e77d31646
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

POSSIBLE SECRETS
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
a0784d7a4716f3feb4f64e7f4b39bf04
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Shotsy - GLP-1 Tracker

Score: 4.614865 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.shotsy.app

Developer Details: Shotsy, Shotsy, None, https://shotsyapp.com, android@shotsyapp.com,

Release Date: Dec 16, 2024 **Privacy Policy:** Privacy link

Description:

Reach your goals with Shotsy – the full-featured tracker for GLP-1 medications like Ozempic®, Wegovy®, Mounjaro®, Zepbound®, Semaglutide, and Tirzepatide. Whether you're managing your journey with GLP1 medications for weight loss, tracking your shots, or analyzing your progress, Shotsy is the tool designed for you. With features to track, monitor, and plot your success, Shotsy supports your lifestyle every step of the way. KEY FEATURES GLP-1 Shot Tracker Easily log your weekly shots of Semaglutide, Tirzepatide, or other GLP-1 medications. Keep a clear history of your Zepbound, Wegovy, Ozempic, or Mounjaro shots and always stay on track. Detailed Progress Plotter Visualize your weight loss journey with detailed analytics and progress trackers. Shotsy's charts make it easy to see how your GLP1 medications like Semaglutide and Tirzepatide are helping you lose weight. Comprehensive Health Tracking Record your weight, protein intake, water consumption, and calories. Whether you're using Shotsy as a tracker for health insights or a companion to your happy scale app, you can tailor your tracking to fit your needs. Medication and Side Effect Monitoring Keep track of medication usage and side effects associated with Ozempic, Wegovy, Mounjaro, and other GLP-1 options. Gain clarity on how your medication affects your weight loss journey. WHY SHOTSY? If you're managing your health with GLP-1 medications like Zepbound, Ozempic, or Wegovy, Shotsy simplifies tracking your shots, weight, and protein intake. With its easy-to-use shot tracker and intuitive interface, Shotsy is more than an app – it's your partner in achieving weight loss success. By offering insights that help you lose weight, adjust your goals, and optimize your routine, Shotsy stands out as the tracker designed specifically for users of GLP-1 medications. It's also perfect if you use tools like MyFitnessPal or Lose It to enhance your progress. Health Disclaimer Shotsy is a tracker and educational tool only. It does not offer medical guidance or advice. Always consult your healthcare provider regarding GLP-1 medications, weight loss, and health decisions. Privacy Policy: https://shotsyapp.com/privacy-android/ Terms of Use: https://shotsyapp.com/terms/

SCAN LOGS

Timestamp	Event	Error
2025-09-01 08:46:43	Generating Hashes	OK
2025-09-01 08:46:43	Extracting APK	OK
2025-09-01 08:46:43	Unzipping	OK

2025-09-01 08:46:43	Parsing APK with androguard	OK
2025-09-01 08:46:43	Extracting APK features using aapt/aapt2	OK
2025-09-01 08:46:43	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 08:46:44	Parsing AndroidManifest.xml	OK
2025-09-01 08:46:44	Extracting Manifest Data	OK
2025-09-01 08:46:44	Manifest Analysis Started	OK
2025-09-01 08:46:44	Performing Static Analysis on: Shotsy (com.shotsy.app)	OK
2025-09-01 08:46:45	Fetching Details from Play Store: com.shotsy.app	OK
2025-09-01 08:46:45	Checking for Malware Permissions	OK
2025-09-01 08:46:45	Fetching icon path	OK
2025-09-01 08:46:45	Library Binary Analysis Started	OK

2025-09-01 08:46:45	Reading Code Signing Certificate	OK
2025-09-01 08:46:46	Running APKiD 2.1.5	OK
2025-09-01 08:46:53	Detecting Trackers	OK
2025-09-01 08:47:00	Decompiling APK to Java with JADX	OK
2025-09-01 08:47:34	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 08:47:34	Decompiling classes6.dex with JADX	OK
2025-09-01 08:47:42	Decompiling classes2.dex with JADX	OK
2025-09-01 08:47:43	Decompiling classes4.dex with JADX	OK
2025-09-01 08:47:54	Decompiling classes.dex with JADX	OK
2025-09-01 08:48:05	Decompiling classes3.dex with JADX	OK
2025-09-01 08:48:14	Decompiling classes5.dex with JADX	OK

2025-09-01 08:48:19	Decompiling classes6.dex with JADX	OK
2025-09-01 08:48:27	Decompiling classes2.dex with JADX	OK
2025-09-01 08:48:28	Decompiling classes4.dex with JADX	OK
2025-09-01 08:48:39	Decompiling classes.dex with JADX	OK
2025-09-01 08:48:50	Decompiling classes3.dex with JADX	OK
2025-09-01 08:48:58	Decompiling classes5.dex with JADX	OK
2025-09-01 08:49:03	Converting DEX to Smali	OK
2025-09-01 08:49:03	Code Analysis Started on - java_source	OK
2025-09-01 08:49:08	Android SBOM Analysis Completed	OK
2025-09-01 08:49:12	Android SAST Completed	OK
2025-09-01 08:49:12	Android API Analysis Started	OK

2025-09-01 08:49:15	Android API Analysis Completed	OK
2025-09-01 08:49:15	Android Permission Mapping Started	OK
2025-09-01 08:49:18	Android Permission Mapping Completed	OK
2025-09-01 08:49:18	Android Behaviour Analysis Started	OK
2025-09-01 08:49:22	Android Behaviour Analysis Completed	OK
2025-09-01 08:49:22	Extracting Emails and URLs from Source Code	OK
2025-09-01 08:49:25	Email and URL Extraction Completed	OK
2025-09-01 08:49:25	Extracting String data from APK	OK
2025-09-01 08:49:25	Extracting String data from Code	OK
2025-09-01 08:49:25	Extracting String values and entropies from Code	OK
2025-09-01 08:49:35	Performing Malware check on extracted domains	OK

2025-09-01 08:49:37	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.