



ANDROID STATIC ANALYSIS REPORT



 AF App (2.9.2)

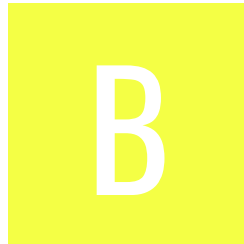
File Name: com.anytimefitness.userapp_1298.apk

Package Name: com.anytimefitness.userapp

Scan Date: Aug. 29, 2025, 7:44 p.m.






App Security Score: 52/100 (MEDIUM RISK)

Grade:



Trackers Detection: 7/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	19	2	3	2

FILE INFORMATION

File Name: com.anytimefitness.userapp_1298.apk

Size: 29.35MB

MD5: f17164709797b1ea4b56b45b027b5a2c

SHA1: 6e9e433cc92d9ed233afdcfb6834d41523028406

SHA256: 96176fa70671a85d8970915d4e3c51f287e54b637cdcb68e86ea2cf0fa1678cc

APP INFORMATION

App Name: AF App

Package Name: com.anytimefitness.userapp

Main Activity: com.anytimefitness.userapp.StartupActivity

Target SDK: 34

Min SDK: 29

Max SDK:

Android Version Name: 2.9.2

Android Version Code: 1298

APP COMPONENTS

Activities: 13

Services: 13

Receivers: 19

Providers: 3

Exported Activities: 2

Exported Services: 2

Exported Receivers: 6

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: False

v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2021-12-03 17:40:02+00:00

Valid To: 2051-12-03 17:40:02+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xdef99169f1d4a542cee31edabb9009864f05942d

Hash Algorithm: sha256

md5: 0140d69ccb3e6568189d762866ab523f

sha1: 6e1ffa9520132042485885c84bb6362029db3f25

sha256: cbe207944800cd64439e03b52040787edd4b3d4707ec5d5cf0ed305a6ab6a9d3

sha512: 6697d25ba43901de5a9b0709f4063f675813827fe3d6d6c271e89d3d0c956c6e73598969336e6c86d5978eb1764a4b468ffea3d467472b251db89389ca2b725

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: e0c74e843dfa066ba97b16dc23dcc603fcc2330537b6002eeb7af5af8a6fcb10

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_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.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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BODY_SENSORS	dangerous	grants access to body sensors, such as heart rate.	Allows an application to access data from sensors that the user uses to measure what is happening inside his/her body, such as heart rate.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_AD SERVICES_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_AD SERVICES_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.
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.anytimefitness.userapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS	
f17164709797b1ea4b56b45b027b5a2c.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check network operator name check device ID check
	Compiler	unknown (please file detection issue!)

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check SIM operator check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)
classes3.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.MANUFACTURER check Build.HARDWARE check
	Compiler	unknown (please file detection issue!)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.anytimefitness.userapp.StartupActivity	Schemes: com.anytimefitness.userapp://, https://, Hosts: *, 5qf2x.app.link, 5qf2x-alternate.app.link, 5qf2x.test-app.link, 5qf2x-alternate.test-app.link,
com.crowdin.platform.auth.AuthActivity	Schemes: crowdintest://,

NETWORK SECURITY

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

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

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: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	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.
3	Activity (com.crowdin.platform.auth.AuthActivity) 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	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
5	<p>Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.c2dm.permission.SEND [android:exported=true]</p>	warning	<p>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.</p>
6	<p>Broadcast Receiver (com.clevertap.android.sdk.pushnotification.fcm.CTFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.c2dm.permission.SEND [android:exported=true]</p>	warning	<p>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.</p>
7	<p>Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]</p>	warning	<p>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.</p>

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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.
10	Broadcast Receiver (com.contentstack.sdk.ConnectionStatus) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Broadcast Receiver (com.contentstack.sdk.ClearCache) 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	STANDARDS	FILES
				a10/h.java a9/s0.java ah/b.java aj/b.java ak/f.java ak/g.java al/a.java aq/b.java b/k.java b10/d.java b6/b0.java b6/f0.java b6/g0.java bm/c.java bo/a.java bw/b.java c3/b0.java c4/a.java c4/c.java c4/f0.java c4/h.java c4/r.java c6/f0.java c6/x.java co/b.java co/c.java com/anytimefitness/userapp/UserApp.java com/anytimefitness/userapp/modules/chat/ChatReactionLog.java com/anytimefitness/userapp/modules/onboarding/presentation/OnboardingEmailFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/onboarding/presentation/OnboardingFragment.java com/anytimefitness/userapp/modules/workoutplayer/sets/AiWorkoutEditDialogFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>com/anytimenitness/userapp/shared/vi/viService.java</div> <div>com/clevertap/android/pushtemplates/a.java</div> <div>com/clevertap/android/sdk/a.java</div> <div>com/clevertap/android/sdk/displayunits/CTDisplayUnitType.java</div> <div>com/clevertap/android/sdk/network/http/URLConnectionHttpClient.java</div> <div>com/contentstack/sdk/Asset.java</div> <div>com/contentstack/sdk/AssetLibrary.java</div> <div>com/contentstack/sdk/CSUtil.java</div> <div>com/contentstack/sdk/ContentTypesModel.java</div> <div>com/contentstack/sdk/Entry.java</div> <div>com/contentstack/sdk/Query.java</div> <div>com/contentstack/sdk/SDKUtil.java</div> <div>com/contentstack/sdk/Stack.java</div> <div>com/crowdin/platform/Crowdin.java</div> <div>com/crowdin/platform/CrowdinConfig.java</div> <div>com/crowdin/platform/ShakeDetectorManager.java</div> <div>com/crowdin/platform/auth/AuthActivity.java</div> <div>com/crowdin/platform/data/DataManager.java</div> <div>com/crowdin/platform/data/remote/CrowdingRepository\$getManifest\$1.java</div> <div>com/crowdin/platform/data/remote/CrowdingRepository.java</div> <div>com/crowdin/platform/data/remote/DistributionInfoManager.java</div> <div>com/crowdin/platform/data/remote/MappingRepository.java</div> <div>com/crowdin/platform/data/remote/StringDataRemoteRepository.java</div> <div>com/crowdin/platform/data/remote/TranslationDataRepository.java</div> <div>com/crowdin/platform/realtimeupdate/EchoWebSocketListener.java</div> <div>com/crowdin/platform/realtimeupdate/RealTimeUpdateManager.java</div> <div>com/crowdin/platform/screenshot/ScreenshotService.java</div> <div>com/crowdin/platform/util/ExtensionsKt.java</div>

NO	ISSUE	SEVERITY	STANDARDS	com/github/mikephil/charting/data/PieEntry.java FILES com/github/mikephil/charting/listener/a.java
				com/hbb20/CountryCodePicker.java com/hbb20/a.java com/launchdarkly/sdk/android/i0.java com/mikepenz/aboutlibraries/ui/LibsSupportFragment.java com/mikepenz/aboutlibraries/util/AndroidParserKt.java com/mikepenz/aboutlibraries/viewmodel/LibsViewModel\$listItems\$1.java com/muuvlabs/workoutplayer/players/WorkoutPlayerViewModel.java com/twilio/audioswitch/android/ProductionLogger.java com/twilio/util/LogWriterImpl.java com/twilio/video/Logger.java com/vi/datasdk/work/GoogleFitUploadWorker.java d4/a.java dj/i.java dk/d.java dk/f.java ds/t.java e4/g.java e4/k.java e8/b.java e8/e.java ek/b.java el/a.java em/d.java eo/b.java eo/d.java eo/e.java f4/f.java fl/a.java ft/e.java g5/a.java g8/c.java gj/a.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	gn/a.java gn/b.java gn/c.java h/f.java h/h.java ha/h.java hm/g.java i3/a.java ij/b.java il/g.java io/branch/referral/Branch.java io/branch/referral/BranchJsonConfig.java io/branch/referral/e.java io/noties/markwon/core/spans/LinkSpan.java j4/e.java j4/n.java j6/e.java j6/i.java j9/r.java ji/a.java ji/c.java jj/r.java k/f.java k4/a.java kp/u.java m/j.java m/k.java m/r0.java m/s0.java m8/a.java n4/a.java n4/b.java n4/g1.java n4/h0.java n4/o.java na/c.java net/zetetic/database/DefaultDatabaseErrorHandler.java net/zetetic/database/sqlcipher/CloseGuard.java net/zetetic/database/sqlcipher/SQLiteConnection.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				net/zetetic/database/sqlcipher/SQLiteConnectio n.java net/zetetic/database/sqlcipher/SQLiteCursor.jav a net/zetetic/database/sqlcipher/SQLiteDatabase.j ava net/zetetic/database/sqlcipher/SQLiteDebug.jav a net/zetetic/database/sqlcipher/SQLiteOpenHelp er.java net/zetetic/database/sqlcipher/SQLiteQuery.jav a net/zetetic/database/sqlcipher/SQLiteStatement. java nn/e.java o6/a.java oh/e.java p000do/c.java p8/c.java pa/b.java pa/c.java pa/g.java pa/q.java pa/s.java pa/y.java pe/e.java pk/r.java q/i.java q/m.java q/n.java q/u.java q/v.java q5/a.java qf/b.java qf/g.java r8/a.java rm/b.java rm/c.java rn/i.java rt/e.java s10/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s4/b.java s4/c.java si/f.java sj/e.java sk/j.java sk/k.java sm/g.java sm/n.java so/a.java t1/e.java t4/i.java t6/h.java t8/a.java tj/a.java tj/b.java tj/c.java tj/d.java tj/f.java tj/i.java tj/l.java tj/q.java tj/r.java tj/t.java tj/v.java tj/w.java tk/n.java tn/b.java tn/d.java tvi/webrtc/DefaultVideoEncoderFactory.java u4/b.java u5/l.java u6/g.java u6/j.java un/c.java un/d.java un/e.java us/a.java vj/d0.java vj/e.java vj/f0.java vj/s0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				vj/y0.java vn/c.java vn/d.java w4/c.java wj/a.java wj/e0.java wj/i0.java wj/m0.java wj/p.java wj/r0.java wj/t.java wj/t0.java wn/c.java ws/b.java wv/c.java xn/a0.java xn/b0.java xn/c0.java xn/e0.java xn/f.java xn/g.java xn/g0.java xn/k0.java xn/m.java xn/n.java xn/p.java xn/q.java xn/t.java xn/z.java y3/a.java yj/a.java yk/y.java yn/d.java yn/g.java yn/j.java yo/v.java yp/a.java zj/a.java zv/b.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/memory/MemoryCache.java com/anytimefitness/userapp/modules/auth/presentation/create/PhoneEntryViewModel.java com/anytimefitness/userapp/modules/auth/presentation/create/SelectAuthMethodViewModel.java com/anytimefitness/userapp/modules/auth/presentation/create/VerifyCodeModel.java com/crowdin/platform/data/model/StringData.java com/launchdarkly/sdk/LDContext.java d1/l.java g1/x0.java gr/o.java i9/d.java ir/c.java kq/c.java lb/k.java ss/b.java ss/h.java ss/n.java su/c.java v0/z.java vr/b.java
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/h.java com/anytimefitness/userapp/shared/composephoto/CameraPhotoKt.java com/anytimefitness/userapp/shared/data/SupportTicketService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/anytimefitness/userapp/modules/chat/ConversationsFragmentKt\$ConversationsScreen\$1.java hf/g.java q2/j.java
5	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/clevertap/android/sdk/inapp/f.java com/clevertap/android/sdk/inapp/j.java
6	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	c6/d0.java c6/j0.java hh/c.java hh/e.java jj/p.java jj/r.java jj/t.java jj/u.java jj/v.java jj/w.java jj/x.java jj/y.java l6/a.java pa/q.java r5/q.java w5/b.java w5/c.java y5/b.java y5/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/contentstack/sdk/SDKUtil.java la/c.java we/a.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	rm/c.java zg/v.java
9	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	f6/a.java q/n.java we/a.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	c6/m0.java com/crowdin/platform/realtimeupdate/RealTimeUpdateManager.java com/dynatrace/android/agent/data/a.java e10/d.java e10/j.java f10/x.java g0/h.java kx/a.java kx/b.java lx/a.java n6/s.java of/a.java of/c.java se/d.java se/g.java zg/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	a10/c.java a10/d.java a10/g.java a10/h.java bh/b.java com/clevertap/android/sdk/network/http/URLConnectionHttpClient.java com/launchdarkly/eventsource/a.java com/twilio/conversations/ConversationsClientImpl.java com/twilio/twilsock/util/SslContextKt.java
12	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/anytimefitness/userapp/modules/developer/presentation/ApplicationLogsFragmentKt.java com/anytimefitness/userapp/shared/composephoto/CameraPhotoKt.java com/anytimefitness/userapp/shared/conversations/DataConverterImpl.java
13	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/neovisionaries/ws/client/f.java so/a.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	ah/b.java com/anytimefitness/userapp/modules/coaching/classdetails/ClassDetailsFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/coaching/components/ReservationKt.java com/anytimefitness/userapp/modules/coaching/notoffered/ServiceNotOfferedFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/coaching/personal/PersonalScheduleFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/developer/presentation/ApplicationLogsFragmentKt.java com/anytimefitness/userapp/modules/evolt/EvoltScanResultListFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/gymdetails/GymDetailsFragment\$onCreateView\$2.java com/anytimefitness/userapp/modules/gymmembership/billinginfo/BillingInfoFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/plantab/PlanFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/servicealert/ForcedUpgradeFragment.java com/anytimefitness/userapp/modules/support/ContactSupportFragment\$onCreateView\$1.java com/clevertap/android/pushtemplates/PushTemplateReceiver.java com/clevertap/android/sdk/InAppNotificationActivity.java com/clevertap/android/sdk/inapp/c.java com/clevertap/android/sdk/inbox/a.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/CTPushNotificationReceiver.java com/crowdin/platform/auth/AuthActivity.java com/karumi/dexter/listener/SettingsClickListener.java com/mikepenz/aboutlibraries/ui/item/LibraryItem.java io/branch/referral/Branch.java io/noties/markwon/core/spans/LinkSpan.java ku/f.java of/a.java of/c.java q2/g0.java se/d.java

RULE ID	BEHAVIOUR	LABEL	td/a.java FILES com/anytimefitness/userapp/modules/coaching/classdetails/ClassDetailsFragment\$onCreateView\$1.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/anytimefitness/userapp/modules/coaching/components/ReservationKt.java com/anytimefitness/userapp/modules/coaching/notoffered/ServiceNotOfferedFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/coaching/personal/PersonalScheduleFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/evolt/EvoltScanResultListFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/gymdetails/GymDetailsFragment\$onCreateView\$2.java com/anytimefitness/userapp/modules/gymmembership/billinginfo/BillingInfoFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/plantab/PlanFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/servicealert/ForcedUpgradeFragment.java com/anytimefitness/userapp/modules/support/ContactSupportFragment\$onCreateView\$1.java io/branch/referral/Branch.java
00202	Make a phone call	control	com/anytimefitness/userapp/modules/coaching/classdetails/ClassDetailsFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/coaching/components/ReservationKt.java com/anytimefitness/userapp/modules/coaching/notoffered/ServiceNotOfferedFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/coaching/personal/PersonalScheduleFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/evolt/EvoltScanResultListFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/gymdetails/GymDetailsFragment\$onCreateView\$2.java com/anytimefitness/userapp/modules/gymmembership/billinginfo/BillingInfoFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/support/ContactSupportFragment\$onCreateView\$1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00203	Put a phone number into an intent	control	com/anytimefitness/userapp/modules/coaching/classdetails/ClassDetailsFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/coaching/components/ReservationKt.java com/anytimefitness/userapp/modules/coaching/notoffered/ServiceNotOfferedFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/coaching/personal/PersonalScheduleFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/evolt/EvoltScanResultListFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/gymdetails/GymDetailsFragment\$onCreateView\$2.java com/anytimefitness/userapp/modules/gymmembership/billinginfo/BillingInfoFragment\$onCreateView\$1.java com/anytimefitness/userapp/modules/support/ContactSupportFragment\$onCreateView\$1.java
00036	Get resource file from res/raw directory	reflection	com/clevertap/android/pushtemplates/PushTemplateReceiver.java com/clevertap/android/pushtemplates/TemplateRenderer.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/CTPushNotificationReceiver.java com/karumi/dexter/listener/SettingsClickListener.java io/branch/referral/Branch.java io/noties/markwon/core/spans/LinkSpan.java m/r0.java of/a.java of/c.java se/d.java t9/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	ba/j.java coil/disk/a.java com/airbnb/lottie/compose/d.java com/clevertap/android/sdk/inapp/images/a.java com/launchdarkly/sdk/android/e0.java com/twilio/util/LogWriterImpl.java hi/e.java la/d.java me/i.java pe/e.java yn/g.java
00094	Connect to a URL and read data from it	command network	bo/a.java
00013	Read file and put it into a stream	file	c4/c.java co/b.java com/airbnb/lottie/compose/d.java com/clevertap/android/sdk/inapp/images/a.java com/contentstack/sdk/SDKUtil.java dk/d.java f10/v.java f4/j.java g5/a.java i8/c.java la/d.java tf/f.java y5/g.java yn/g.java z00/a.java
00012	Read data and put it into a buffer stream	file	com/contentstack/sdk/SDKUtil.java g5/a.java y5/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00112	Get the date of the calendar event	collection calendar	com/contentstack/sdk/CSCConnectionRequest.java com/contentstack/sdk/SDKUtil.java
00078	Get the network operator name	collection telephony	mh/a.java pa/s.java ue/g0.java
00091	Retrieve data from broadcast	collection	com/clevertap/android/pushtemplates/PTPushNotificationReceiver.java com/clevertap/android/pushtemplates/PushTemplateReceiver.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/fcm/CTFirebaseMessagingReceiver.java ge/d.java io/branch/referral/Branch.java
00191	Get messages in the SMS inbox	sms	be/e.java m/r0.java
00162	Create InetAddress object and connecting to it	socket	a10/b.java a10/h.java ds/x.java
00163	Create new Socket and connecting to it	socket	a10/b.java a10/h.java ds/x.java
00004	Get filename and put it to JSON object	file collection	com/contentstack/sdk/ConnectionStatus.java
00175	Get notification manager and cancel notifications	notification	com/anytimefitness/userapp/modules/chat/ConversationsFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	aj/b.java io/ktor/client/engine/android/AndroidClientEngine.java la/b.java
00030	Connect to the remote server through the given URL	network	aw/a.java la/b.java
00005	Get absolute path of file and put it to JSON object	file	pe/e.java yn/g.java
00024	Write file after Base64 decoding	reflection file	ba/j.java
00147	Get the time of current location	collection location	h/h.java
00075	Get location of the device	collection location	h/h.java
00115	Get last known location of the device	collection location	h/h.java pa/s.java
00189	Get the content of a SMS message	sms	com/anytimefitness/userapp/modules/chat/ConversationsFragmentKt.java com/crowdin/platform/screenshot/ScreenshotService.java
00188	Get the address of a SMS message	sms	com/anytimefitness/userapp/modules/chat/ConversationsFragmentKt.java com/crowdin/platform/screenshot/ScreenshotService.java
00200	Query data from the contact list	collection contact	com/anytimefitness/userapp/modules/chat/ConversationsFragmentKt.java com/crowdin/platform/screenshot/ScreenshotService.java
00201	Query data from the call log	collection callog	com/anytimefitness/userapp/modules/chat/ConversationsFragmentKt.java com/crowdin/platform/screenshot/ScreenshotService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms callog calendar	com/anytimefitness/userapp/modules/chat/ConversationsFragmentKt.java com/crowdin/platform/screenshot/ScreenshotService.java
00065	Get the country code of the SIM card provider	collection	com/hbb20/CountryCodePicker.java ue/g0.java
00132	Query The ISO country code	telephony collection	com/hbb20/CountryCodePicker.java pa/s.java s6/h.java
00056	Modify voice volume	control	tvi/webrtc/audio/WebRtcAudioTrack.java tvi/webrtc/voiceengine/WebRtcAudioTrack.java
00014	Read file into a stream and put it into a JSON object	file	yn/g.java
00034	Query the current data network type	collection network	ue/x0.java
00009	Put data in cursor to JSON object	file	com/clevertap/android/sdk/pushnotification/f.java pa/q.java tf/c.java ye/b.java
00089	Connect to a URL and receive input stream from the server	command network	gz/b.java okio/internal/a.java
00183	Get current camera parameters and change the setting.	camera	com/twilio/video/CameraCapturer.java tvi/webrtc/Camera1Session.java

RULE ID	BEHAVIOUR	LABEL	FILES
00016	Get location info of the device and put it to JSON object	location collection	com/clevertap/android/sdk/inapp/evaluation/a.java com/dynatrace/agent/events/enrichment/a.java pa/g.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/a.java
00208	Capture the contents of the device screen	collection screen	tvi/webrtc/ScreenCapturerAndroid.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/825353552194/namespaces/firebase:fetch?key=AlzaSyBZxi7Gnp2-_b0X8bCEzvPykUX5Elsba-s . This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
------	---------	-------------

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	7/44	android.permission.CHANGE_NETWORK_STATE, android.permission.ACTIVITY_RECOGNITION, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, android.permission.BLUETOOTH, android.permission.MODIFY_AUDIO_SETTINGS, 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
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
privacy.anytimefitness.com	ok	IP: 45.60.12.62 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
url.com	ok	IP: 104.21.79.89 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api.crowdin.com	ok	IP: 52.0.135.149 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
pay.google.com	ok	IP: 142.250.105.92 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.amplitude.com	ok	IP: 44.252.161.144 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
login.anytimefitness.com	ok	IP: 13.248.245.245 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
afmembers.ideas.aha.io	ok	IP: 35.171.201.123 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 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

DOMAIN	STATUS	GEOLOCATION
www.allyant.com	ok	IP: 141.193.213.11 Country: United States of America Region: Texas City: Austin Latitude: 30.271158 Longitude: -97.741699 View: Google Map
accounts.crowdin.com	ok	IP: 54.88.22.105 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
play.google.com	ok	IP: 172.253.124.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
api.sebrands.com	ok	IP: 45.60.12.62 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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: 140.82.113.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
developer.android.com	ok	IP: 64.233.176.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
stage-api.sebrands.com	ok	IP: 45.60.12.62 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map

DOMAIN	STATUS	GEOLOCATION
cdn.anytimefitness.com	ok	IP: 20.60.83.227 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
www.slf4j.org	ok	IP: 159.100.250.151 Country: Switzerland Region: Vaud City: Lausanne Latitude: 46.515999 Longitude: 6.632820 View: Google Map
clientsdk.launchdarkly.com	ok	IP: 151.101.65.55 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
anytimefitness.blob.core.windows.net	ok	IP: 20.60.83.227 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mobile.launchdarkly.com	ok	IP: 3.224.167.162 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 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
www.anytimefitness.com	ok	IP: 45.60.12.62 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
distributions.crowdin.net	ok	IP: 18.238.96.23 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
bnc.lt	ok	IP: 18.238.109.50 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
static.wizrocket.com	ok	IP: 18.155.173.47 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
cdn.branch.io	ok	IP: 18.238.109.80 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
cdn-settings.segment.com	ok	IP: 18.238.93.145 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
bf83772fza.bf.dynatrace.com	ok	IP: 20.81.82.232 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
clientstream.launchdarkly.com	ok	IP: 76.223.31.44 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
ns.adobe.com	ok	No Geolocation information available.
www.googleapis.com	ok	IP: 64.233.185.95 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
demo-login.anytimefitness.com	ok	IP: 13.248.244.122 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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.
demo-api.sebrands.com	ok	IP: 45.60.12.62 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
stage-login.anytimefitness.com	ok	IP: 76.223.112.12 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
xmlpull.org	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api2.branch.io	ok	IP: 18.238.109.117 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
aim.s.twilio.com	ok	IP: 44.199.52.48 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
developers.google.com	ok	IP: 172.217.215.101 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
mikepenz.com	ok	IP: 104.21.27.65 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
clubemail@test.com	com/anytimefitness/userapp/modules/coaching/components/ComposableSingletons\$ContactGymBottomSheetKt\$lambda4\$1.java
testemail@gmail.test esttesttestemail@test.com	com/anytimefitness/userapp/modules/profile/components/ComposableSingletons\$ProfileComponentsKt.java
dev.app.logs@sebrands.com	com/anytimefitness/userapp/shared/commands/SendLogsCommand.java
mike@gmail.com jan.lasso@anytimefitness.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
CleverTap	Location, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/174
Dynatrace	Analytics	https://reports.exodus-privacy.eu.org/trackers/137
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

TRACKER	CATEGORIES	URL
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62

HARDCODED SECRETS

POSSIBLE SECRETS
"auth_login_input_password" : "Password"
"auth_login_input_username" : "Username"
"com.google.firebase.crashlytics.mapping_file_id" : "ae5dc9c5412f4f05bda4301f7ba92d94"
"google_api_key" : "AlzaSyBZxi7Gnp2-_b0X8bCEzvPykUX5Elsba-s"
"google_crash_reporting_api_key" : "AlzaSyBZxi7Gnp2-_b0X8bCEzvPykUX5Elsba-s"
"group_session_no_spots_left" : "Full"
"group_session_reserved" : "Reserved"
"group_session_today" : "Today"
"library_fastadapter_authorWebsite" : "http://mikepenz.com/"
"session_full_dialog_title" : "Sorry!"
"today_digital_key" : "Access Pass"

POSSIBLE SECRETS
0ba7ece979720efb877e1c7
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
6LdfCpAiAAAAAPvqbr2qT1siiRh1HFWOCDUu7yBF
470fa2b4ae81cd56ecbcd9735803434cec591fa
ff05b114d4dd490fa57a2bbbb140ba63
37fad9b76236f5c6faad5a1c27ddfce2
b-394e74be-caed-4dd7-9b76-82f34214acde
af60eb711bd85bc1e4d3e0a462e074eea428a8
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
2a34908ba2ef68cc767f6f241e4e9b62
36864200e0eaf5284d884a0e77d31646
9b323dabd2a93ca25a9b5688
ca4028f02c9778f9e9644d2c75080249

POSSIBLE SECRETS
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
1a477edd-60e3-4762-9ffe-74279e1442e3
a28966646d05c2c28cde608a
b-627ccc55-3a19-473c-a055-8eb48c91e22d
a59cc22b06e263270614a1e34c446daa
455cd16a710cea2118329a6db2420074
5d03c1912c9113d33a5270d8
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb
7f39321ea836250ea55c5f6f12aebd6e
b-d984991a-5a44-41f6-adb6-3e281c34057c
a0784d7a4716f3feb4f64e7f4b39bf04
d0160419f7d2727a026c9238a8ef0b0c
9ab64fa7bc2645258eebbc9f6f039f2f
516dbca3ddab4dfd9fea5c9b239b15f8

POSSIBLE SECRETS
bae8e37fc83441b16034566b
6f4545fe1797f75e71e20d89a257b3a6

PLAYSTORE INFORMATION

Title: AF App

Score: 3.6138613 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [com.anytimefitness.userapp](https://play.google.com/store/apps/details?id=com.anytimefitness.userapp)

Developer Details: Anytime Fitness, LLC, Anytime+Fitness,+LLC, None, <http://www.anytimefitness.com>, help@sebrands.com,

Release Date: Nov 22, 2022 **Privacy Policy:** [Privacy link](#)

Description:

Not just an app, the Anytime app combines a personalized plan consisting of training, nutrition, and recovery tasks, a network of 5000 gyms, and access to health and fitness services around the world to offer you the best home and gym-based services, anytime, anywhere. WHAT YOU GET WITH THE ANYTIME APP Plans — You'll get a new plan every month tailored especially to you. Want to lose weight, run further, faster, burn some fat, or tone up? The app has you covered! Your plan will consist of training and exercise, nutrition plans, educational tips, and recovery plans, and it gets better every time you use it. Coaching — Everyone needs a little help sometimes, and the Anytime app helps connect you with professional health coaching services. Our coaches pull in your current health info and learn about your goals and lifestyle information to create an ultra-personalized plan, just for you. The concierge in the Anytime app can also connect you to other services at Anytime Fitness, such as scheduling 1:1 personal training and group training classes, and much, much more! Community — Got a question? Ask questions, follow experts, and create a sense of social atmosphere outside of the four walls of the gym. In Community, you're not alone, you're surrounded by people that care and are connected to Anytime Fitness, our expert coaches, trainers, and others, just like you who have questions and want to learn more about the topic of health, fitness, training, nutrition, and recovery. Anytime app users achieve more than they ever thought possible because of the network our app and system of 5000 gyms creates — that gives you access to thousands of health and fitness professionals provides around the world.

SCAN LOGS

Timestamp	Event	Error
-----------	-------	-------

2025-08-29 19:44:20	Generating Hashes	OK
2025-08-29 19:44:20	Extracting APK	OK
2025-08-29 19:44:20	Unzipping	OK
2025-08-29 19:44:20	Parsing APK with androguard	OK
2025-08-29 19:44:21	Extracting APK features using aapt/aapt2	OK
2025-08-29 19:44:21	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 19:44:23	Parsing AndroidManifest.xml	OK
2025-08-29 19:44:23	Extracting Manifest Data	OK
2025-08-29 19:44:23	Manifest Analysis Started	OK
2025-08-29 19:44:24	Reading Network Security config from network_security_config.xml	OK
2025-08-29 19:44:24	Parsing Network Security config	OK

2025-08-29 19:44:24	Performing Static Analysis on: AF App (com.anytimefitness.userapp)	OK
2025-08-29 19:44:25	Fetching Details from Play Store: com.anytimefitness.userapp	OK
2025-08-29 19:44:25	Checking for Malware Permissions	OK
2025-08-29 19:44:25	Fetching icon path	OK
2025-08-29 19:44:26	Library Binary Analysis Started	OK
2025-08-29 19:44:26	Reading Code Signing Certificate	OK
2025-08-29 19:44:26	Running APKiD 2.1.5	OK
2025-08-29 19:44:28	Detecting Trackers	OK
2025-08-29 19:44:33	Decompiling APK to Java with JADX	OK
2025-08-29 19:44:53	Converting DEX to Smali	OK
2025-08-29 19:44:53	Code Analysis Started on - java_source	OK

2025-08-29 19:44:58	Android SBOM Analysis Completed	OK
2025-08-29 19:45:14	Android SAST Completed	OK
2025-08-29 19:45:14	Android API Analysis Started	OK
2025-08-29 19:45:29	Android API Analysis Completed	OK
2025-08-29 19:45:29	Android Permission Mapping Started	OK
2025-08-29 19:45:53	Android Permission Mapping Completed	OK
2025-08-29 19:45:53	Android Behaviour Analysis Started	OK
2025-08-29 19:46:13	Android Behaviour Analysis Completed	OK
2025-08-29 19:46:13	Extracting Emails and URLs from Source Code	OK
2025-08-29 19:46:21	Email and URL Extraction Completed	OK
2025-08-29 19:46:21	Extracting String data from APK	OK

2025-08-29 19:46:21	Extracting String data from Code	OK
2025-08-29 19:46:21	Extracting String values and entropies from Code	OK
2025-08-29 19:46:25	Performing Malware check on extracted domains	OK
2025-08-29 19:46:30	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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).