ANDROID STATIC ANALYSIS REPORT

app_icon

BodBot (6.208)

File Name:	com.bodbot.trainer_128978.apk
Package Name:	com.bodbot.trainer
Scan Date:	Aug. 29, 2025, 8:28 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	14	3	1	1

FILE INFORMATION

File Name: com.bodbot.trainer_128978.apk
Size: 76.74MB
MD5: 759d8d537018abc3c5dccb0b254b0adc
SHA1: fb6ec2db6ca46892f72a8f9b1289186e1b743a21
SHA256: e1e86bf31d283e86be63745cd8f7f33bbd7b5fe761a59be763aee615295f647f

APP INFORMATION

App Name: BodBot
Package Name: com.bodbot.trainer
Main Activity: com.bodbot.trainer.BodBot
Target SDK: 34
Min SDK: 27
Max SDK:
Android Version Name: 6.208

Android Version Code: 128978

APP COMPONENTS

Activities: 8
Services: 11
Receivers: 12
Providers: 2
Exported Activities: 0
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: ST=CA, L=San Francisco, CN=Sergio Prado
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-06-07 18:15:03+00:00
Valid To: 2062-05-26 18:15:03+00:00
Issuer: ST=CA, L=San Francisco, CN=Sergio Prado
Serial Number: 0x2cc1194a
Hash Algorithm: sha256
md5: ba3bcd09becd26447746b1112b20630d
sha1: 95c0cf07d623d8cd7112321291ac102324487b3e
sha256: c76ddbabfe46d3badd8cc439522d47fc741e289a1d36fd38292e8320befd03ee
sha512: 228db55c2cee4cad6348200526ac24e75148f638c947ed356057feba9f0dc0aedf9bdf6782dce8d3ccafe19abee465daf0b24f8ddaa079f181301f88a4d25c03
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 63005b01af2e199c9c57382beec31a98c881921415df2d5a8256e314057999c4
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.providers.tv.permission.WRITE_EPG_DATA	unknown	Unknown permission	Unknown permission from android reference
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.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.android.providers.tv.permission.READ_EPG_DATA	unknown	Unknown permission	Unknown permission from android reference
com.bodbot.trainer.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

APKID ANALYSIS

FILE	DETAILS
759d8d537018abc3c5dccb0b254b0adc.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>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible VM 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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check Build.TAGS check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.bodbot.trainer.BodBot	Schemes: tvmediachannels://, https://, Hosts: www.bodbot.com, Paths: /, Path Prefixes: /Training.html, /index.html, /ad_link/,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.1, minSdk=27]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Broadcast Receiver (com.bodbot.trainer.HomeUserActionReceiver) 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.
5	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.
6	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
7	Service (com.google.android.gms.cast.tv.internal.CastTvHostService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	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: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	android/cc/fovea/PurchasePlugin.java by/chemerisuk/cordova/firebase/FirebaseMessagingPlugin.java by/chemerisuk/cordova/firebase/FirebaseMessagingPluginService.java com/bodbot/trainer/BodBot.java com/bodbot/trainer/HomeUserActionReceiver.java com/bodbot/trainer/MainActivity.java com/bodbot/trainer/MediaTVProvider.java com/bodbot/trainer/provider/VideoDetailsActivity.java com/bodbot/trainer/provider/data/VideoProvider.java com/bodbot/trainer/util/AppLinkHelper.java com/bodbot/trainer/util/DvbChannelProviderUtil.java com/bodbot/trainer/util/DvbTVProvider.java com/phonegap/plugins/barcodescanner/BarcodeScanner.java com/rjfun/cordova/plugin/nativeaudio/NativeAudio.java com/rjfun/cordova/plugin/nativeaudio/NativeAudioAsset.java com/rjfun/cordova/plugin/nativeaudio/NativeAudioAssetComplex.java de/appplant/cordova/plugin/localnotification/LocalNotification.java de/appplant/cordova/plugin/notification/AbstractRestoreReceiver.java de/appplant/cordova/plugin/notification/AssetUtil.java nl/xservices/plugins/GooglePlus.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/bodbot/trainer/BodBot.java de/appplant/cordova/plugin/notification/Builder.java
3	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/bodbot/trainer/util/DvbChannelProviderUtil.java nl/xservices/plugins/SocialSharing.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	by/chemerisuk/cordova/firebase/FirebaseMessagingPluginService.java de/appplant/cordova/plugin/notification/Notification.java nl/xservices/plugins/GooglePlus.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	nl/xservices/plugins/GooglePlus.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	com/bodbot/trainer/provider/data/VideoDbHelper.java
7	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	nl/xservices/plugins/SocialSharing.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bodbot/trainer/provider/data/VideoProvider.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	android/cc/fovea/PurchasePlugin.java by/chemerisuk/cordova/firebase/FirebaseMessagingPluginService.java com/bodbot/trainer/BodBot.java com/timetravelers/hackedme/MediaSession.java com/timetravelers/hackedme/MediaSessionNotification.java de/appplant/cordova/plugin/notification/Builder.java nl/xservices/plugins/SocialSharing.java
00013	Read file and put it into a stream	file	com/timetravelers/hackedme/MediaSession.java com/timetravelers/hackedme/MediaSessionNotification.java okio/Okio__JvmOkioKt.java
00012	Read data and put it into a buffer stream	file	com/timetravelers/hackedme/MediaSession.java com/timetravelers/hackedme/MediaSessionNotification.java
00089	Connect to a URL and receive input stream from the server	command network	com/timetravelers/hackedme/MediaSession.java com/timetravelers/hackedme/MediaSessionNotification.java de/appplant/cordova/plugin/notification/AssetUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/timetravelers/hackedme/MediaSession.java com/timetravelers/hackedme/MediaSessionNotification.java de/appplant/cordova/plugin/notification/AssetUtil.java
00092	Send broadcast	command	com/timetravelers/hackedme/MediaSession.java
00091	Retrieve data from broadcast	collection	by/chemerisuk/cordova/firebase/FirebaseMessagingPlugin.java com/bodbot/trainer/BodBot.java de/appplant/cordova/plugin/notification/AbstractClickActivity.java
00175	Get notification manager and cancel notifications	notification	by/chemerisuk/cordova/firebase/FirebaseMessagingPlugin.java de/appplant/cordova/plugin/notification/Manager.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	nl/xservices/plugins/SocialSharing.java
00022	Open a file from given absolute path of the file	file	de/appplant/cordova/plugin/notification/AssetUtil.java
00072	Write HTTP input stream into a file	command network file	de/appplant/cordova/plugin/notification/AssetUtil.java
00028	Read file from assets directory	file	de/appplant/cordova/plugin/notification/AssetUtil.java
00094	Connect to a URL and read data from it	command network	de/appplant/cordova/plugin/notification/AssetUtil.java
00108	Read the input stream from given URL	network command	de/appplant/cordova/plugin/notification/AssetUtil.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://bodbot-personal-trainer.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/848842924112/namespaces/firebase:fetch?key=AIzaSyB83aHvluVborsh09mGuPvYNMHWb8A3Wq8. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.CAMERA, android.permission.WAKE_LOCK
Other Common Permissions	6/44	android.permission.ACTIVITY_RECOGNITION, android.permission.FLASHLIGHT, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
bodbot-personal-trainer.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
commondatastorage.googleapis.com	ok	**IP:** 172.217.215.207 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.whatsapp.com	ok	**IP:** 157.240.11.53 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.bodbot.com	ok	**IP:** 98.86.3.246 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
static.bodbot.com	ok	**IP:** 18.238.109.64 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
storage.googleapis.com	ok	**IP:** 142.250.9.207 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java
name@example.com sergio@bodbot.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
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"authenticate_inputs_password" : "Password"
"authenticate_inputs_username" : "Username"

POSSIBLE SECRETS
"billing_key_param" : "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjHxaEfgvYLNliq1VaPnlK0ma9R/iQPCDEDl3BWQOe2Djfta12aOMsrv9UIsZSfk1872QHSTNF7qyb1G6Abq8jcX++mARtMW4jTNvZ4QQ+gwzmGyZnpBWOpfMTWsweJyqcyllADG+4boWlhoWejXYmf49kNfvms33Cs7mkGrH+AX5MqQfth8ljQP5hC+E9EF8gRJIHHkowRGrHt1m26dJfqKcPmHOO2NVuwnjIY08znQS/wIKKfdjebV+jIQgARdvU8C9V9uCVVh0bM0+Pfg9FeeTSI8IwIgLWBYsVn4mrSyr3D/zMftuI86ZLAHy9vAd6f2Kc1IO4NegGAPiII+iuQIDAQAB"
"firebase_database_url" : "https://bodbot-personal-trainer.firebaseio.com"
"google_api_key" : "AIzaSyB83aHvluVborsh09mGuPvYNMHWb8A3Wq8"
"google_crash_reporting_api_key" : "AIzaSyB83aHvluVborsh09mGuPvYNMHWb8A3Wq8"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
2c1352fdd8598b2fc2071b69bf573a02
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
23456789abcdefghjkmnpqrstvwxyz
c56fb7d591ba6704df047fd98f535372fea00211
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
9b8f518b086098de3d77736f9458a3d2f6f95a37

POSSIBLE SECRETS
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
cc2751449a350f668590264ed76692694a80308a

PLAYSTORE INFORMATION

Title: BodBot AI Personal Trainer

Score: 4.592141 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.bodbot.trainer

Developer Details: BodBot, 8404024925803725317, None, http://www.bodbot.com, information@bodbot.com,

Release Date: Nov 16, 2016 **Privacy Policy:** Privacy link

Description:

BodBot - AI Workout Planner & Personal Trainer Better AI, Better Workouts. Your Own AI-Powered Personal Training App BodBot delivers hyper-personalized workouts tailored to your goals, equipment, fitness level, and schedule. Whether you're training at home, weight training at the gym, or doing no equipment workouts on the go, our cutting-edge AI adapts every workout in real-time to maximize progress, efficiency, and results. Each workout, exercise and set is planned for you—from set to set and workout to workout. Train Smarter with Custom Workout Plans AI-driven workout planner: Your exercise routines evolve based on performance, recovery, and even skipped sessions Results on your terms: Build muscle with strength training, boost cardio fitness with HIIT workouts, or burn fat with weight loss workouts designed for your unique body Anytime, anywhere fitness: No gym? No problem. Get expert-level home fitness programming with bodyweight exercises or any equipment you have Intelligent Adaptation & Progress Tracking Smart fitness tracker: Your personal training app intelligently adjusts reps, sets, weight, and intensity to keep you progressing —no muscle, movement or joint left behind Lifestyle-aware coaching: Workout plans adapt to your daily activity levels, sleep, and real-world schedule. Miss a workout or go hiking on a whim? We'll adjust accordingly Seamless workout structure: Get balanced programming with circuits, supersets, and strategic recovery for maximum efficiency Personalized Exercise Coaching Step-by-step instructions and workout videos - every exercise explained in detail Smart assessments: Unlock better movement patterns with targeted mobility, strength, and posture assessments—from beginner workouts to advanced weight training techniques Your custom workout routine: No cookie-cutter fitness plans. Adjust difficulty and target specific muscles as you train Fuel Your Workouts With Intelligent Nutrition Smart meal planning: Your nutrition adapts daily based on workout intensity and recovery needs Macro tracking made simple: AI calculates optimal protein, carbs, and fats for your specific goals and training load Eat for your goals: Whether building muscle or burning fat, get meal suggestions that accelerate your results Workout-nutrition sync: Heavier leg day? More calories. Rest day? Adjusted macros. Just like having a nutritionist who watches every workout New Goal? We'll help with not only the macros but also the micronutrients The Complete Fitness App That Works For You You don't need to figure out what exercises to do-BodBot does it for you. Whether you're starting beginner fitness or you're an advanced lifter, every workout routine is optimized for maximum impact. Perfect for Every Fitness Journey: Tight hamstrings? Shoulder mobility issues? Muscle imbalances? BodBot identifies, adjusts, and helps you improve Weaker back than chest? Want to develop specific muscles like biceps or glutes? We'll address it all Home workouts, gym sessions, or bodyweight training anywhere Cardio, HIIT, strength training, and weight loss workouts all in one app Progress tracking that shows real results

And if you miss a workout session or add extra activity, your fitness plan automatically updates to keep you on track. Just as a good personal trainer creates custom workout plans, BodBot's AI coaching delivers science-based exercise routines that evolve with you. Features That Set Us Apart: Workout at home with no equipment needed Exercise videos for every movement Beginner workouts to advanced training programs Real-time workout planner that adapts daily Progress tracking for strength, cardio, and weight loss Professional & Personal training app experience at a fraction of the cost Your fitness journey, reimagined. Ready to train smarter? Download BodBot - your AI workout planner and personal training app today.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:28:29	Generating Hashes	OK
2025-08-29 20:28:29	Extracting APK	OK
2025-08-29 20:28:29	Unzipping	OK
2025-08-29 20:28:30	Parsing APK with androguard	OK
2025-08-29 20:28:30	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:28:30	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:28:33	Parsing AndroidManifest.xml	OK

2025-08-29 20:28:33	Extracting Manifest Data	OK
2025-08-29 20:28:33	Manifest Analysis Started	OK
2025-08-29 20:28:33	Performing Static Analysis on: BodBot (com.bodbot.trainer)	OK
2025-08-29 20:28:33	Fetching Details from Play Store: com.bodbot.trainer	OK
2025-08-29 20:28:34	Checking for Malware Permissions	OK
2025-08-29 20:28:34	Fetching icon path	OK
2025-08-29 20:28:34	Library Binary Analysis Started	OK
2025-08-29 20:28:34	Reading Code Signing Certificate	OK
2025-08-29 20:28:34	Running APKiD 2.1.5	OK
2025-08-29 20:28:39	Detecting Trackers	OK
2025-08-29 20:28:42	Decompiling APK to Java with JADX	OK

2025-08-29 20:28:58	Converting DEX to Smali	OK
2025-08-29 20:28:58	Code Analysis Started on - java_source	OK
2025-08-29 20:28:59	Android SBOM Analysis Completed	OK
2025-08-29 20:29:11	Android SAST Completed	OK
2025-08-29 20:29:11	Android API Analysis Started	OK
2025-08-29 20:29:21	Android API Analysis Completed	OK
2025-08-29 20:29:21	Android Permission Mapping Started	OK
2025-08-29 20:29:31	Android Permission Mapping Completed	OK
2025-08-29 20:29:31	Android Behaviour Analysis Started	OK
2025-08-29 20:29:41	Android Behaviour Analysis Completed	OK
2025-08-29 20:29:41	Extracting Emails and URLs from Source Code	OK

2025-08-29 20:29:42	Email and URL Extraction Completed	OK
2025-08-29 20:29:42	Extracting String data from APK	OK
2025-08-29 20:29:42	Extracting String data from Code	OK
2025-08-29 20:29:42	Extracting String values and entropies from Code	OK
2025-08-29 20:29:45	Performing Malware check on extracted domains	OK
2025-08-29 20:29:45	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.