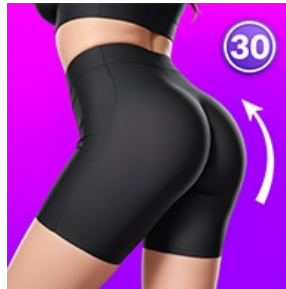




ANDROID STATIC ANALYSIS REPORT



 Buttocks Trainer (7.0.0)

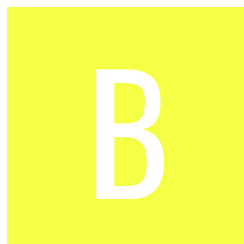
File Name: phdpan.buttocks.home.workout.trainer_7.apk

Package Name: phdpan.buttocks.home.workout.trainer

Scan Date: Sept. 1, 2025, 5:15 p.m.






App Security Score: 48/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	47	1	1	1

FILE INFORMATION

File Name: phdpan.buttocks.home.workout.trainer_7.apk

Size: 63.72MB

MD5: e3263374af6b945a1ce00a7364313d4d

SHA1: 1439c71900c4c7b89439f13dbb2aac7cc14cdc11

SHA256: 2409486e9b69864b6fc203a0be7a44fb9214a30c5a5360e5917a752424f5d0cf

APP INFORMATION

App Name: Buttocks Trainer

Package Name: phdpan.buttocks.home.workout.trainer

Main Activity: phdpan.buttocks.home.workout.trainer.ButtWorkoutSplashKkt

Target SDK: 34

Min SDK: 21

Max SDK:

Android Version Name: 7.0.0

Android Version Code: 7

APP COMPONENTS

Activities: 42

Services: 12

Receivers: 20

Providers: 4

Exported Activities: 31

Exported Services: 1

Exported Receivers: 6

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

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: 2024-06-07 12:57:28+00:00

Valid To: 2054-06-07 12:57:28+00:00

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

Serial Number: 0x120f1aadf9a2cf500c78051126faa38d1e659a11

Hash Algorithm: sha256

md5: 17643ed9adcae58631985b316b26c070

sha1: c3811a61d512277ce0785932656228d0cf80d19e

sha256: 6a5cd6a925124bb36483c623ccce1040432fadc90ad36f09288aa14323926cac

sha512: 63226571bc42716f23920ae412a2524418cc64fb4079ae2fa8167f291bf81fc2e57ec1dccebb73ffb056940c3accb9e7395a95291adb3a8d849da349170f8461

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: cca002b31d72ba53cb9e3368374a08c831757ef902a88cae07db9d1767ae4db9

Found 1 unique certificates

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.

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_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
phdpan.buttocks.home.workout.trainer.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check
	Compiler	r8

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	dragonsense.azurewebsites.net	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

Q MANIFEST ANALYSIS

HIGH: 2 | WARNING: 38 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
4	Broadcast Receiver (phdpan.buttocks.home.workout.trainer.MyApplication\$InternetConnectionReceiver) 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 (phdpan.buttocks.home.workout.trainer.utils.reminder.AlarmReceiver) 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.
6	Broadcast Receiver (phdpan.buttocks.home.workout.trainer.utils.reminder.BootReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity (phdpan.buttocks.home.workout.trainer.SplashScreenActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (phdpan.buttocks.home.workout.trainer.CustomGalleryActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (phdpan.buttocks.home.workout.trainer.HomeActivity) 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
10	Activity (phdpan.buttocks.home.workout.trainer.ChooseYourPlanActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (phdpan.buttocks.home.workout.trainer.ChooseWeightActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (phdpan.buttocks.home.workout.trainer.ChooseTargetWeightActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (phdpan.buttocks.home.workout.trainer.ChooseHeightActivity) 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.
14	Activity (phdpan.buttocks.home.workout.trainer.BMIActivity) 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.
15	Activity (phdpan.buttocks.home.workout.trainer.YourPlanActivity) 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.
16	Activity (phdpan.buttocks.home.workout.trainer.WhatsYourGoalActivity) 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.
17	Activity (phdpan.buttocks.home.workout.trainer.TurnOnWaterActivity) 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
18	Activity (phdpan.buttocks.home.workout.trainer.WellDoneActivity) 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.
19	Activity (phdpan.buttocks.home.workout.trainer.WaterTrackerActivity) 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.
20	Activity (phdpan.buttocks.home.workout.trainer.HomeDetailActivity) 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.
21	Activity (phdpan.buttocks.home.workout.trainer.ExercisesListActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	Activity (phdpan.buttocks.home.workout.trainer.FastWorkoutActivity) 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.
23	Activity (phdpan.buttocks.home.workout.trainer.FastWorkOutDetailActivity) 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.
24	Activity (phdpan.buttocks.home.workout.trainer.PerformWorkOutActivity) 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.
25	Activity (phdpan.buttocks.home.workout.trainer.RestActivity) 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
26	Activity (phdpan.buttocks.home.workout.trainer.CompletedActivity) 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.
27	Activity (phdpan.buttocks.home.workout.trainer.HistoryActivity) 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.
28	Activity (phdpan.buttocks.home.workout.trainer.AccessAllFeaturesActivity) 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.
29	Activity (phdpan.buttocks.home.workout.trainer.MyProfileActivity) 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.
30	Activity (phdpan.buttocks.home.workout.trainer.VoiceOptionActivity) 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.
31	Activity (phdpan.buttocks.home.workout.trainer.ReminderActivity) 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.
32	Activity (phdpan.buttocks.home.workout.trainer.CommonQuestionActivity) 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.
33	Activity (phdpan.buttocks.home.workout.trainer.DaysPlanDetailActivity) 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
34	Activity (phdpan.buttocks.home.workout.trainer.RecentActivity) 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.
35	Activity (phdpan.buttocks.home.workout.trainer.AboutActivity) 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.
36	Activity (phdpan.buttocks.home.workout.trainer.RestDayActivity) 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.
37	Activity (phdpan.buttocks.home.workout.trainer.EditPlanActivity) 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.
38	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.

NO	ISSUE	SEVERITY	DESCRIPTION
39	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
40	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.

NO	ISSUE	SEVERITY	DESCRIPTION
41	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: 6 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a5/g.java a6/h0.java b1/b.java b1/c.java b1/g.java b3/c.java b3/z.java b4/g.java b4/i.java b4/y.java c7/c.java c7/g.java com/bumptechnology/glide/d.java com/bumptechnology/glide/e.java com/bumptechnology/glide/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>com/bumptechnology/load/data/b.java</div> <div>com/bumptechnology/load/data/m.java</div> <div>com/bumptechnology/m.java</div> <div>com/bumptechnology/manager/q.java</div> <div>d0/b0.java</div> <div>d6/f0.java</div> <div>d9/d.java</div> <div>e0/k.java</div> <div>e2/e.java</div> <div>e2/p.java</div> <div>e4/c.java</div> <div>e4/i.java</div> <div>e4/l.java</div> <div>e4/s.java</div> <div>e4/w.java</div> <div>e4/z.java</div> <div>e6/h.java</div> <div>f/i.java</div> <div>f/u.java</div> <div>g0/g.java</div> <div>g0/k.java</div> <div>g4/g.java</div> <div>h0/d.java</div> <div>h0/k.java</div> <div>i1/a.java</div> <div>i1/b.java</div> <div>i7/a0.java</div> <div>i7/e.java</div> <div>i7/e0.java</div> <div>i7/g.java</div> <div>i7/w0.java</div> <div>i8/d.java</div> <div>j/k.java</div> <div>j1/u.java</div> <div>j4/g.java</div> <div>k/o.java</div> <div>k0/p.java</div> <div>k8/g.java</div> <div>l/g4.java</div> <div>l/h1.java</div> <div>l/k4.java</div>

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	l/m1.java l/m2.java l/o3.java l/s2.java l/s3.java l/t0.java l/y.java l2/h.java l7/j0.java m0/f.java m1/d.java m2/g.java m2/r.java m8/f.java m8/l.java m9/e.java n3/b.java o0/a1.java o0/b2.java o0/c.java o0/d1.java o0/q.java o0/v1.java o0/w1.java phdpan/buttocks/home/workout/trainer/C ompletedActivity.java phdpan/buttocks/home/workout/trainer/ HomeDetailActivity.java q1/e.java q4/c.java q9/b.java r6/b.java r6/e.java r6/f.java r6/n.java r6/o.java r7/c.java s0/u.java s1/e0.java s1/h1.java s1/m1.iava

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s1/v0.java s6/e.java s6/f.java s6/i.java s6/k.java s6/n.java s6/r.java t/a.java t3/d.java u2/f.java u3/d.java u6/e.java u6/p.java u9/a0.java u9/b0.java u9/c0.java u9/e.java u9/v.java u9/w.java u9/x.java v6/d0.java v6/e.java v6/e0.java v6/h.java v6/j0.java v6/t.java w2/f.java w2/l.java x3/a0.java x3/q.java x5/b.java x8/g.java y3/g.java y6/a.java y7/c.java z/b.java z/i.java z/m.java z6/e.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	v3/j.java x3/f.java x3/y.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	e9/i.java p5/f.java p5/o.java phdpan/buttocks/home/workout/trainer/C ompletedActivity.java phdpan/buttocks/home/workout/trainer/ HistoryActivity.java phdpan/buttocks/home/workout/trainer/R ecentActivity.java phdpan/buttocks/home/workout/trainer/d ialog/ReplaceExerciseDialogFragment.java phdpan/buttocks/home/workout/trainer/f ragments/PlanFragment.java z1/c.java
4	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	a6/p.java i7/a0.java
5	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	a6/p.java c7/i.java za/a.java
6	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	hc/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	c7/i.java q9/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	b1/g.java com/bumptechnology/glide/d.java com/bumptechnology/glide/f.java l2/e.java p3/d.java q1/b.java q1/e.java q1/j.java t/a.java t3/d.java t3/f.java ub/l.java
00079	Hide the current app's icon	evasion	w2/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00104	Check if the given path is directory	file	com/bumptech/glide/e.java
00108	Read the input stream from given URL	network command	l7/f2.java l7/m0.java
00191	Get messages in the SMS inbox	sms	l/o3.java
00036	Get resource file from res/raw directory	reflection	com/karumi/dexter/listener/SettingsClickListener.java l/o3.java s6/f.java
00096	Connect to a URL and set request method	command network	i7/b1.java
00089	Connect to a URL and receive input stream from the server	command network	i7/b1.java
00109	Connect to a URL and get the response code	network command	i7/b1.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/karumi/dexter/listener/SettingsClickListener.java s6/f.java
00003	Put the compressed bitmap data into JSON object	camera	i7/q.java
00014	Read file into a stream and put it into a JSON object	file	p3/d.java
00091	Retrieve data from broadcast	collection	phdpan/buttocks/home/workout/trainer/CompletedActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	b1/g.java
00022	Open a file from given absolute path of the file	file	hc/a.java
00112	Get the date of the calendar event	collection calendar	c5/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	s6/f.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/203360143847/namespaces/firebase:fetch?key=AlzaSyBvv7WG8WI72sMGx5jiw89Y1jlt2ai702w . This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.WAKE_LOCK

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_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
ns.adobe.com	ok	No Geolocation information available.
phdpansolutions.com	ok	IP: 194.5.156.237 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map

DOMAIN	STATUS	GEOLOCATION
fundingchoicesmessages.google.com	ok	IP: 142.250.74.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
googlemobileadssdk.page.link	ok	IP: 142.250.74.129 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
mikepenz.com	ok	IP: 172.67.141.197 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
u0013android@android.com0 u0013android@android.com	s6/p.java

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "ab9c3ef67e1b476bbd2522f8e71e6402"
"google_api_key" : "AlzaSyBvw7WG8WI72sMGx5jiw89Y1jlt2ai702w"
"google_crash_reporting_api_key" : "AlzaSyBvw7WG8WI72sMGx5jiw89Y1jlt2ai702w"
"library_AndroidIconics_authorWebsite" : "http://mikepenz.com/"

POSSIBLE SECRETS
"library_fastadapter_authorWebsite" : "http://mikepenz.com/"
"library_materialdrawer_authorWebsite" : "http://mikepenz.com/"
"library_materialize_authorWebsite" : "http://mikepenz.com/"
"user" : "User"
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c2722252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
B3EEABB8EE11C2BE770B684D95219ECB
fY7ocyET9PuMHUXxlIKP/PpFa5xsSzhwfB8mpep5FSQ=

POSSIBLE SECRETS

308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b

PLAYSTORE INFORMATION

Title: BootyFit - Workout at home

Score: 4.173913 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [phdpan.buttocks.home.workout.trainer](https://play.google.com/store/apps/details?id=com.phdpansolutions.phdpansolutions)

Developer Details: Phdpans, Phdpans, None, <http://phdpansolutions.com>, Ph.dinvelapan@gmail.com,

Release Date: Jun 7, 2024 **Privacy Policy:** [Privacy link](#)

Description:

Get ready to tone, tighten, and lift your glutes with Buttocks Home Workout Trainer! This results-oriented app for Android provides you with everything you need to achieve a stronger, more sculpted backside – all from the comfort of your own home. No gym membership required! Targeted Workouts for Maximum Results: . Variety of Butt-Blasting Exercises: Choose from a diverse library of exercises specifically designed to target your glutes and surrounding muscles. These include squats, lunges, bridges, glute raises, and more, with variations to cater to different fitness levels. . Workout Plans for Every Goal: Whether you're a beginner or a seasoned fitness enthusiast, the app offers personalized workout plans tailored to your goals. Choose from programs focused on toning, building muscle, or achieving a more rounded

shape. . High-Intensity Interval Training (HIIT): Burn calories and maximize your workout time with HIIT routines that incorporate bursts of intense activity followed by short rest periods. ☐ Key Points ☐ ♀ Butt Workout Routines ☐ Home Fitness Training ☐ Personalized Workout Plans ☐ Targeted Glute Exercises ☐ Progress Tracking ☐ Voice-guided Instructions ☐ Exercise Demonstrations ☐ Timer for Sets and Rest ☐ Strength and Resistance Training ☐ Music Integration ☐ Mobile App Accessibility ☐ Privacy Protection ☐ Workout Log ☐ Minimal Equipment Required ☐ Community Support Download Buttocks Home Workout Trainer today and transform your glutes! This app provides the motivation, guidance, and variety of workouts you need to achieve a stronger, firmer backside – all without ever leaving your home. Get ready to see and feel the difference!

☐☐☐ SCAN LOGS

Timestamp	Event	Error
2025-09-01 17:15:29	Generating Hashes	OK
2025-09-01 17:15:29	Extracting APK	OK
2025-09-01 17:15:29	Unzipping	OK
2025-09-01 17:15:29	Parsing APK with androguard	OK
2025-09-01 17:15:30	Extracting APK features using aapt/aapt2	OK
2025-09-01 17:15:30	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 17:15:33	Parsing AndroidManifest.xml	OK

2025-09-01 17:15:33	Extracting Manifest Data	OK
2025-09-01 17:15:33	Manifest Analysis Started	OK
2025-09-01 17:15:33	Reading Network Security config from network_security_config.xml	OK
2025-09-01 17:15:33	Parsing Network Security config	OK
2025-09-01 17:15:33	Performing Static Analysis on: Buttocks Trainer (phdpan.buttocks.home.workout.trainer)	OK
2025-09-01 17:15:34	Fetching Details from Play Store: phdpan.buttocks.home.workout.trainer	OK
2025-09-01 17:15:36	Checking for Malware Permissions	OK
2025-09-01 17:15:36	Fetching icon path	OK
2025-09-01 17:15:36	Library Binary Analysis Started	OK
2025-09-01 17:15:36	Reading Code Signing Certificate	OK
2025-09-01 17:15:37	Running APKiD 2.1.5	OK

2025-09-01 17:15:40	Detecting Trackers	OK
2025-09-01 17:15:41	Decompiling APK to Java with JADX	OK
2025-09-01 17:15:54	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 17:15:54	Decompiling classes.dex with JADX	OK
2025-09-01 17:16:02	Decompiling with JADX failed for classes.dex	OK
2025-09-01 17:16:02	Decompiling classes.dex with JADX	OK
2025-09-01 17:16:09	Decompiling with JADX failed for classes.dex	OK
2025-09-01 17:16:09	Some DEX files failed to decompile	OK
2025-09-01 17:16:09	Converting DEX to Smali	OK
2025-09-01 17:16:09	Code Analysis Started on - java_source	OK
2025-09-01 17:16:11	Android SBOM Analysis Completed	OK

2025-09-01 17:16:16	Android SAST Completed	OK
2025-09-01 17:16:16	Android API Analysis Started	OK
2025-09-01 17:16:21	Android API Analysis Completed	OK
2025-09-01 17:16:21	Android Permission Mapping Started	OK
2025-09-01 17:16:25	Android Permission Mapping Completed	OK
2025-09-01 17:16:25	Android Behaviour Analysis Started	OK
2025-09-01 17:16:31	Android Behaviour Analysis Completed	OK
2025-09-01 17:16:31	Extracting Emails and URLs from Source Code	OK
2025-09-01 17:16:32	Email and URL Extraction Completed	OK
2025-09-01 17:16:32	Extracting String data from APK	OK
2025-09-01 17:16:32	Extracting String data from Code	OK

2025-09-01 17:16:32	Extracting String values and entropies from Code	OK
2025-09-01 17:16:34	Performing Malware check on extracted domains	OK
2025-09-01 17:16:35	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](#).