MOBSF

ANDROID STATIC ANALYSIS REPORT

DietAI (1.1.3)

File Name:	dietaiplan.calorietracker.app_1013.apk
Package Name:	dietaiplan.calorietracker.app
Scan Date:	Sept. 1, 2025, 1:08 p.m.
App Security Score:	53/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	20	2	2	1

FILE INFORMATION

File Name: dietaiplan.calorietracker.app_1013.apk
Size: 21.97MB
MD5: 1a0c74376ac359c5670576ac24584a4a
SHA1: 530baa3728c59cf06728ee0f395c97110ad51d92
SHA256: 221344ffbee8469b61510c302e76ce9286960174933826a9fa0cb8b36d4c315b

APP INFORMATION

App Name: DietAI

Package Name: dietaiplan.calorietracker.app
Main Activity: diet.dietai.app.publicpage.SplashActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 1.1.3
Android Version Code: 1013

APP COMPONENTS

Activities: 11
Services: 17
Receivers: 13
Providers: 6
Exported Activities: 3
Exported Services: 2
Exported Receivers: 3
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-09-25 12:03:32+00:00
Valid To: 2054-09-25 12:03:32+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x2b744b998a915b2d6a5dde66fcbb292617c2aeb9
Hash Algorithm: sha256
md5: 9db164601434f1b1566b58a6fe57d3a5
sha1: 116f4ecdb422a1239cde762cc90baf7426f021ab
sha256: 6b1293c8dcba68337f61387652ef1f5de119b1193e6be345b69eed3a60542d78
sha512: a02f2815f71a0eed74a65fdc0aabfe1b0fb3f92ba09f1daadfd2a4bfe19108833a89efd9d8e9871c3f9dab8957c47ce872073a35127f5e0f60b0551ac29e9dbd
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 7551596b76630d00db2f8f9804538e8269d7b2880082286ceb3f4238b712a342
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.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.
homeworkout.fitness.app.READ_DATA	unknown	Unknown permission	Unknown permission from android reference
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.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
dietaiplan.calorietracker.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>1a0c74376ac359c5670576ac24584a4a.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></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
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</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.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

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

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	127.0.0.1 localhost 10.0.2.2	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 can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.
3	Activity (diet.dietai.app.MainActivity) 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	Content Provider (diet.dietai.app.dfprovider.DFContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	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.
6	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.
7	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.
10	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.
11	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: **7** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A0/g.java A4/b.java B1/A.java B1/C0009b.java B1/P.java B1/RunnableC0018k.java B1/a0.java B1/f0.java B3/b.java B4/AbstractC0040h.java B4/C.java B4/C0043k.java B4/E.java B4/EnumC0039g.java B4/G.java B4/I.java B4/J.java B4/o.java B4/p.java B4/r.java B4/t.java B4/v.java B4/w.java B4/x.java B4/y.java B4/z.java C0/d.java C0/i.java C0/j.java C0/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				C0/p.java C2/b.java C4/d.java C4/g.java C4/m.java C4/n.java C4/q.java C5/d.java D/e.java D/g.java D/i.java D/o.java D/w.java D2/k.java D5/c.java D5/r.java F/b.java G/e.java G0/C0099f.java G0/h.java G1/a.java G4/a.java G4/c.java H/e.java H0/f.java H0/h.java H4/c.java H4/d.java J0/b.java J0/o.java J2/d.java J2/j.java J5/j.java J5/k.java K0/h.java K0/k.java L0/c.java L1/f.java L5/a.java L5/c.java L5/f.java O0/l.java O3/b.java P0/a.java P0/b.java P1/d.java P2/b.java P2/c.java Q1/f.java R1/f.java R1/k.java R1/l.java R3/d.java S3/a.java T0/C0113b.java T0/C0125n.java T0/E.java T0/P.java T0/j0.java T0/k0.java T0/o0.java T4/a.java U3/g.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	U5/g.java U5/a.java W3/e.java W4/e.java W4/h.java W4/i.java W4/j.java X/e.java X2/d.java X2/i.java Y0/b.java Y2/b.java Y2/d.java Y2/f.java Y2/g.java Y2/j.java Y2/k.java Y2/l.java Y2/m.java Y2/n.java Z0/r.java Z2/e.java Z2/f.java Z2/g.java Z2/h.java Z2/j.java Z2/m.java Z2/p.java Z2/s.java Z4/b.java a/AbstractC0140a.java a4/d.java a4/f.java a5/b.java b/g.java b4/C1488g.java b4/ServiceConnectionC1491j.java b5/c.java c/e.java c3/C1500a.java com/pairip/SignatureCheck.java com/pairip/VMRunner.java com/pairip/licensecheck/LicenseActivity.java com/pairip/licensecheck/LicenseClient.java d4/AbstractC1885c.java d4/C1902t.java diet/dietai/app/MainActivity.java diet/dietai/app/di/e.java diet/dietai/app/notification/d.java diet/dietai/app/publicpage/SplashActivity.java diet/dietai/app/s.java diet/dietai/auth/s.java diet/dietai/core/ui/auth/o.java diet/dietai/core/ui/common/B.java diet/dietai/core/ui/common/B0.java diet/dietai/core/ui/common/C2024z0.java diet/dietai/core/ui/common/D.java diet/dietai/data/remoteconfig/h.java diet/dietai/data/remoteconfig/i.java diet/dietai/data/remoteconfig/j.java diet/dietai/data/remoteconfig/k.java diet/dietai/dbilling/e.java diet/dietai/dbilling/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				diet/dietai/dbilling/o.java diet/dietai/dbilling/p.java diet/dietai/homepage/main/B.java diet/dietai/homepage/main/tabscreenmodel/r.java diet/dietai/logfood/logscreen/C2324z.java diet/dietai/logfood/logscreen/h0.java diet/dietai/navigation/l.java diet/dietai/network/callables/m.java e/e.java e/i.java e/k.java e/r.java e/u.java f1/C2376c.java f5/AbstractC2389e.java f5/C2383A.java f5/D.java f5/F.java f5/RunnableC2384B.java f5/g.java f5/i.java f5/j.java f5/p.java f5/t.java f5/u.java f5/v.java f5/w.java f5/z.java h/h.java h/i.java h3/C2418a.java h5/c.java i/MenuC2442l.java i/ViewOnKeyListenerC2436f.java i2/o.java i3/AbstractC2464c.java i3/f.java i4/AbstractC2466b.java i4/C2469e.java i4/g.java j/AbstractC2508b0.java j/C2516f0.java j/C2542t.java j/C2546v.java j/D0.java j/I0.java j/J.java j/P.java j/P0.java j1/C2558b.java j1/C2559c.java j1/C2563g.java j5/C2570c.java j5/C2572e.java j5/RunnableC2569b.java j5/n.java l1/AbstractComponentCallbacksC2748q.java l1/AnimationAnimationListenerC2737f.java l1/C2715E.java l1/C2718H.java l1/C2722L.java l1/C2725O.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				l1/C2728S.java l1/C2732a.java l1/C2736e.java l1/C2740i.java l1/DialogInterfaceOnCancelListenerC2744m.java l1/EnumC2730U.java l1/w.java m1/AbstractC2764b.java m3/d.java m3/f.java n5/b.java n5/d.java n5/e.java o5/b.java o6/AbstractC2796A.java p/C2843r.java p/C2845t.java p/C2849x.java p/RunnableC2833h.java q4/C2905a.java r7/l.java r7/n.java s7/e.java t2/AbstractC3005b.java t4/C3011A.java t4/C3014D.java t4/s.java t4/v.java t4/z.java u3/C3040B.java u3/C3041C.java u3/C3053O.java u3/C3119z.java u3/E1.java u4/l.java u4/u.java u4/y.java v/AbstractC3131d.java v/C3128a.java v/K.java v/Q.java v2/l.java v2/m.java v3/AbstractC3157a.java v3/AsyncTaskC3158b.java v4/C3164f.java w/o.java w1/a.java w2/AbstractC3181a.java x3/C3213a.java x4/C3221a.java y/RunnableC3231e.java y3/C3233a.java y4/C3234a.java y4/C3235b.java y4/c.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	C4/b.java d2/C1872b.java diet/dietai/core/common/models/ProFeaturesContainerV2.java i7/Q.java m5/C2770c.java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	B4/AbstractC0040h.java a4/f.java
4	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	B4/I.java D/i.java D2/t.java J2/d.java J2/h.java J2/i.java J2/j.java K2/k.java K2/l.java u3/AbstractC3120z0.java u3/C3051M.java u3/C3089k.java u3/H1.java u3/x1.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	P6/a.java Q6/a.java Q6/b.java Q6/c.java R6/a.java f5/k.java i5/c.java i5/d.java j5/C2570c.java j5/C2576i.java j5/n.java n5/e.java u3/E1.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	diet/dietai/homepage/main/tabs/DietitianScreen.java
7	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	diet/dietai/homepage/main/tabs/DietitianScreen.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	r7/e.java r7/h.java r7/m.java r7/n.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	h6/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	u3/E1.java
11	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	a5/b.java i3/AbstractC2464c.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	B4/AbstractC0040h.java B4/t.java C4/g.java C4/p.java G0/h.java G4/a.java K0/k.java L0/c.java X2/i.java j1/C2563g.java w7/r.java z1/C3258a.java z1/e.java z1/g.java
00012	Read data and put it into a buffer stream	file	j1/C2563g.java
00004	Get filename and put it to JSON object	file collection	P6/a.java h5/c.java
00014	Read file into a stream and put it into a JSON object	file	C4/g.java
00022	Open a file from given absolute path of the file	file	C4/g.java coil/disk/a.java i2/e.java
00005	Get absolute path of file and put it to JSON object	file	C4/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	U5/a.java Y2/j.java Z2/f.java diet/dietai/app/publicpage/SplashActivity.java diet/dietai/core/ui/base/W.java diet/dietai/logfood/logscreen/C2320v.java diet/dietai/settings/C2339d.java diet/dietai/settings/webview/b.java f5/j.java u3/E1.java u3/x1.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	Z2/f.java diet/dietai/logfood/logscreen/C2320v.java diet/dietai/settings/C2339d.java
00036	Get resource file from res/raw directory	reflection	Z2/f.java c2/C1499a.java diet/dietai/logfood/logscreen/C2320v.java w2/AbstractC3181a.java
00147	Get the time of current location	collection location	e/r.java
00075	Get location of the device	collection location	e/r.java
00115	Get last known location of the device	collection location	e/r.java
00096	Connect to a URL and set request method	command network	J2/j.java o5/b.java
00089	Connect to a URL and receive input stream from the server	command network	J2/j.java b5/c.java diet/dietai/network/openfood/a.java o5/b.java
00109	Connect to a URL and get the response code	network command	J2/j.java P2/c.java X2/c.java b5/c.java diet/dietai/network/openfood/a.java o5/b.java
00162	Create InetSocketAddress object and connecting to it	socket	r7/c.java r7/n.java
00163	Create new Socket and connecting to it	socket	r7/c.java r7/n.java
00091	Retrieve data from broadcast	collection	N1/c.java Y2/j.java f5/j.java v/AbstractC3131d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	i2/e.java
00125	Check if the given file path exist	file	X2/i.java
00108	Read the input stream from given URL	network command	u3/C3059V.java u3/Q0.java
00009	Put data in cursor to JSON object	file	P6/a.java
00065	Get the country code of the SIM card provider	collection	diet/dietai/app/di/k.java
00132	Query The ISO country code	telephony collection	diet/dietai/app/di/k.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/531962798772/namespaces/firebase:fetch?key=AIzaSyCLEBpbQd1HCBc3JCOERr-X7vS_R9s5hXM is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'abTestCategory': '', 'appWorking': 'N', 'inAppPurchaseSkusV4': '{"monthlySub":"diet_ai_pro_week_v1","sixMonthSub":"diet_ai_pro_month_v1","yearlySub":"diet_ai_pro_12_month_v1","yearlyIntroductorySub":"diet_ai_pro_12_month_v9","yearlyIntroductorySubOffer":"introductory","extraSkus":[],"introductoryTime":300000,"showIntroductoryOnce":true,"lifeTimeSku":"diet_ai_pro_lifetime_v1","extraProductSkus":[],"winBackSku":"diet_ai_pro_12_month_v8","winBackSkuOffer":"introductory","winbackIntroductoryTime":300000,"subsCheckSku":"diet_ai_pro_12_month_v1","subsCheckOffer":"freetrial"}', 'lottieABVersion': '2', 'notificationParams': '{"zeroNotificationNonBuyerMs":86400000,"firstNotificationNonBuyerMs":172800000,"secondaryNotificationNonBuyerMs":172800000,"secondaryNotificationTimes":2}', 'open_paywall_stepresult': '0', 'paywallABVersion': '0', 'proColors': '{ "badgeColor": "FF32cd32", "paywallBadgeColor": "ff0E7832", "promoButtonColor": "FF32cd32", "paywallButtonColor": "FF32cd32", "upgradeProColor": "ffFF7300" }', 'proFeaturesV3': '{"localizedOfferTitleKey":"str_auto_seasonal","localizedOfferTitle":{"en":""},"features":[{"localTitleKey":"str_pro_feature1","localImageName":"def1","localLottiName":"","localLottiScale":1,"localizedTitle":{"en":"Achieve a healthier life with AI!"},"localizedImageUrl":{},"isForFreeTrial":0,"actions":[]},{"localTitleKey":"str_pro_feature2","localImageName":"def2","localLottiName":"","localLottiScale":1,"localizedTitle":{"en":"Unlimited AI crafted diets!"},"localizedImageUrl":{},"isForFreeTrial":0,"actions":[]},{"localTitleKey":"str_pro_feature3","localImageName":"def3","localLottiName":"","localLottiScale":1,"localizedTitle":{"en":"Access your AI dietitian anytime, anywhere!"},"localizedImageUrl":{},"isForFreeTrial":0,"actions":[]},{"localTitleKey":"str_pro_feature4","localImageName":"def4","localLottiName":"","localLottiScale":1,"localizedTitle":{"en":"Scan your food with AI!"},"localizedImageUrl":{},"isForFreeTrial":0,"actions":[]},{"localTitleKey":"str_pro_feature5","localImageName":"def5","localLottiName":"","localLottiScale":1,"localizedTitle":{"en":"Improve your life with AI-driven insights!"},"localizedImageUrl":{},"isForFreeTrial":0,"actions":[]},{"localTitleKey":"str_pro_feature6","localImageName":"def6","localLottiName":"","localLottiScale":1,"localizedTitle":{"en":"Track your weight smartly!"},"localizedImageUrl":{},"isForFreeTrial":0,"actions":[]}]}', 'promo_control': '0', 'rate_watch_step': '0', 'startStepMode': '{"mode":0,"localTexts":[],"localizedTexts":{},"images":[],"showHCButton":1}', 'stepsUxMode': '15'}, 'state': 'UPDATE', 'templateVersion': '78'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, 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
fonts.gstatic.com	ok	**IP:** 172.217.21.163 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.nhlbi.nih.gov	ok	**IP:** 13.107.246.69 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.googleadservices.com	ok	**IP:** 142.250.74.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.hsph.harvard.edu	ok	**IP:** 89.106.200.1 **Country:** Luxembourg **Region:** Luxembourg **City:** Luxembourg **Latitude:** 49.611671 **Longitude:** 6.130000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.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
world.openfoodfacts.org	ok	**IP:** 213.36.253.214 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
openai.com	ok	**IP:** 172.64.154.211 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.mayoclinic.org	ok	**IP:** 184.28.254.23 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.heart.org	ok	**IP:** 104.18.26.158 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.ncbi.nlm.nih.gov	ok	**IP:** 130.14.29.110 **Country:** United States of America **Region:** Maryland **City:** Bethesda **Latitude:** 38.999641 **Longitude:** -77.155083 **View:** Google Map
developer.android.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
www.google.com	ok	**IP:** 142.250.74.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.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
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.162 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.niddk.nih.gov	ok	**IP:** 13.107.246.69 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.webmd.com	ok	**IP:** 172.64.153.18 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 216.58.207.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
1s-2s.cloudfunctions.net	ok	**IP:** 216.239.36.54 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 209.85.233.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
socialtechcompany.com	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebaseinstallations.googleapis.com	ok	**IP:** 142.250.74.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
firebase-settings.crashlytics.com	ok	**IP:** 216.58.207.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
google.com	ok	**IP:** 216.58.207.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebasestorage.googleapis.com	ok	**IP:** 216.58.207.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	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

EMAILS

EMAIL	FILE
dietaiteam@gmail.com	o6/i.java

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	Z2/l.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com.google.firebase.crashlytics.mapping_file_id" : "d8c261a1858c4e57b3b0c19b9a082763"
"google_api_key" : "AIzaSyCLEBpbQd1HCBc3JCOERr-X7vS_R9s5hXM"
"google_crash_reporting_api_key" : "AIzaSyCLEBpbQd1HCBc3JCOERr-X7vS_R9s5hXM"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
Vn3kj4pUblROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=
axKTyNy6aDN/YTh2Uu8fXeEZsRk+a+NFtp7tOmBULXg=
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
ceeea6f024f6744e0a08d5a81cc56a40
af60eb711bd85bc1e4d3e0a462e074eea428a8
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
36864200e0eaf5284d884a0e77d31646
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
8081828384858687888 98a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
0136024004378801593602050 5
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
a0784d7a4716f3feb4f64e7f4b39bf04
f2f2d1cb3a0c77a6e28d8a7bafe0db9a
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
1157920892103562487626974469494075735299969552241357603424222590610685120443 69

PLAYSTORE INFORMATION

Title: Calorie Counter Planner DietAI

Score: 4.6220474 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** dietaiplan.calorietracker.app

Developer Details: Social Tech Inc, 5817220418198887508, None, https://socialtechcompany.com, contact@socialtechcompany.com,

Release Date: Sep 29, 2024 **Privacy Policy:** Privacy link

Description:

New Year, New You! Start tracking calories in 2025 with a 70% Discount! Kickstart your health journey with our "New Year, New You" campaign! For a limited time, enjoy 70% off DietAI Premium: our biggest discount so far! Crush your New Year's resolutions with advanced tools to help you lose weight, eat healthier, and achieve your wellness goals. Don’t wait, start transforming your health today! DietAI is your all-in-one calorie counter and nutrition tracker designed to help you achieve your health and fitness

goals. Whether you're aiming for weight loss, muscle gain, or maintaining a healthy lifestyle, DietAI provides personalized diet plans tailored to your specific needs. Track your calories, macros, and nutrients effortlessly with our AI-powered food diary and meal planner. Personalized Diet Plans and Meal Tracking Custom Diets: Choose from a variety of diets such as Keto, Intermittent Fasting, Mediterranean, High Protein, Low Carb, Anti-Inflammatory, DASH, and Diabetic diets. Tailored Recommendations: The app creates custom plans based on your fitness profile, including your height, weight, allergies, and target weight. Weight Loss Goals: Set your goals and let DietAI guide you on your weight loss journey with structured meal plans and calorie deficit strategies. AI Photo & Text Meal Logging Effortless Logging: Simplify meal tracking with AI-powered features that allow you to log your meals by taking a photo or providing a brief description. Instant Calculations: The app instantly calculates macronutrients, calories, and essential nutrients like potassium, iron, and magnesium. Food Scanner: Quickly scan food photos to automatically fetch nutritional information and add items to your food diary. Comprehensive Nutrition and Macro Tracking Macro Tracker: Monitor your intake of carbs, proteins, fats, and over 25 essential nutrients like vitamins and minerals. Nutrition Insights: Get in-depth nutrient analysis to help you stay on top of your nutritional goals, whether you're tracking high protein foods, low-calorie snacks, or high fiber foods. Custom Targets: Set personalized goals for macros, calories, and nutrients to align with your diet plan. Fitness and Activity Integration Exercise Tracking: Log workouts and daily activities to see their impact on your calorie and nutrient needs. Progress Monitoring: Track your weight over time with interactive graphs. In-Depth Nutrient Analysis Balanced Diet Support: Whether you're following a pescatarian, vegetarian, carnivore, or any other diet, DietAI ensures you maintain a balanced intake of key vitamins and minerals. Essential Nutrients: Keep track of nutrients like vitamin D, iron, magnesium, and more to support your overall health. Personal AI Dietitian and Expert Guidance Customized Advice: With a personal AI dietitian at your fingertips, get expert recommendations tailored to your goals. Weight Loss Programs: Get information about structured meal plans, calorie deficit strategies, and weight watcher techniques to accelerate your progress. Health Tips: Receive guidance on the best ways to lose belly fat, boost metabolism, and find effective fat burners with AI dietitian. Healthy Meal and Snack Suggestions Meal Planner: Discover healthy meals for dinner, high protein snacks, low-calorie snacks, and more that fit your diet plan. Diet-Friendly Foods: Find ketosis-friendly foods, anti-inflammatory foods, and high fiber options to support your health. Recipe Ideas: Explore a variety of recipes tailored to your dietary preferences and nutritional needs with Dietitian AI.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:08:14	Generating Hashes	OK
2025-09-01 13:08:14	Extracting APK	OK
2025-09-01 13:08:14	Unzipping	OK
2025-09-01 13:08:15	Parsing APK with androguard	OK
2025-09-01 13:08:15	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:08:15	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:08:16	Parsing AndroidManifest.xml	OK
2025-09-01 13:08:16	Extracting Manifest Data	OK
2025-09-01 13:08:16	Manifest Analysis Started	OK
2025-09-01 13:08:17	Reading Network Security config from network_security_config.xml	OK
2025-09-01 13:08:17	Parsing Network Security config	OK

2025-09-01 13:08:17	Performing Static Analysis on: DietAI (dietaiplan.calorietracker.app)	OK
2025-09-01 13:08:18	Fetching Details from Play Store: dietaiplan.calorietracker.app	OK
2025-09-01 13:08:20	Checking for Malware Permissions	OK
2025-09-01 13:08:20	Fetching icon path	OK
2025-09-01 13:08:20	Library Binary Analysis Started	OK
2025-09-01 13:08:20	Reading Code Signing Certificate	OK
2025-09-01 13:08:20	Running APKiD 2.1.5	OK
2025-09-01 13:08:26	Detecting Trackers	OK
2025-09-01 13:08:29	Decompiling APK to Java with JADX	OK
2025-09-01 13:08:49	Converting DEX to Smali	OK
2025-09-01 13:08:49	Code Analysis Started on - java_source	OK
2025-09-01 13:08:53	Android SBOM Analysis Completed	OK
2025-09-01 13:08:59	Android SAST Completed	OK
2025-09-01 13:08:59	Android API Analysis Started	OK
2025-09-01 13:09:05	Android API Analysis Completed	OK
2025-09-01 13:09:05	Android Permission Mapping Started	OK

2025-09-01 13:09:12	Android Permission Mapping Completed	OK
2025-09-01 13:09:13	Android Behaviour Analysis Started	OK
2025-09-01 13:09:21	Android Behaviour Analysis Completed	OK
2025-09-01 13:09:21	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:09:24	Email and URL Extraction Completed	OK
2025-09-01 13:09:24	Extracting String data from APK	OK
2025-09-01 13:09:24	Extracting String data from Code	OK
2025-09-01 13:09:24	Extracting String values and entropies from Code	OK
2025-09-01 13:09:38	Performing Malware check on extracted domains	OK
2025-09-01 13:09:42	Saving to Database	OK