MOBSF

ANDROID STATIC ANALYSIS REPORT

How We Feel (0.0.347)

File Name:	org.howwefeel.moodmeter_347.apk
Package Name:	org.howwefeel.moodmeter
Scan Date:	Sept. 1, 2025, 3:10 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	29	4	2	1

FILE INFORMATION

File Name: org.howwefeel.moodmeter_347.apk
Size: 89.25MB
MD5: b0ac105373a41501fb70656e3fce0a16
SHA1: 36f567da71cf41086f133b5a76938cc13bb7b414
SHA256: 9b7dbf939d990a52bc0b22db699a45376eda7254542bde667c802091a6ebe83d

APP INFORMATION

App Name: How We Feel
Package Name: org.howwefeel.moodmeter
Main Activity: org.howwefeel.moodmeter.screens.main.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 0.0.347

Android Version Code: 347

APP COMPONENTS

Activities: 11
Services: 20
Receivers: 22
Providers: 3
Exported Activities: 4
Exported Services: 4
Exported Receivers: 8
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-11-21 20:27:07+00:00
Valid To: 2052-11-21 20:27:07+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe47db482cafd2fab622fcea7b75e42206d32b26f
Hash Algorithm: sha256
md5: d89a2451712d54e4e49a97db4f7bfc42
sha1: ff733f6d1f027af3bc8061c5ebdcc49622dad5a3
sha256: aa5de3e7c44109c488249e969b3f623e918ecbee89719360fbaaa31159d8747b
sha512: cbb7350f7082d82302f4ecb8b88979363b72e58ae9f8110a69e783e80309c1b66c93d86b481bf269e182ff2ad8761e0b599170891132229f6b2e36035b7a8c3d
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 2b03615d15ebf320547ba73ea962f1b9d562808e8f7d1855e69067a538fb818a
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.STORAGE	unknown	Unknown permission	Unknown permission from android reference
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.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.health.READ_EXERCISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_SLEEP	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_STEPS	unknown	Unknown permission	Unknown permission from android reference
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.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.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
org.howwefeel.moodmeter.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>b0ac105373a41501fb70656e3fce0a16.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</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.howwefeel.moodmeter.screens.main.MainActivity	Schemes: https://, app://, Hosts: howwefeel.org, howwefeel, Path Prefixes: /checkin, /demographic, Path Patterns: /strategies/.*, /friends/.*,
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

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **19** | 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	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (org.howwefeel.moodmeter.screens.privacypolicy.PrivacyPolicyActivity) 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	Broadcast Receiver (org.howwefeel.moodmeter.util.notifications.RescheduleAlarmsBroadcastReceiver) 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 (org.howwefeel.moodmeter.widgets.checkins.small.CheckInSmallReceiver) 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 (org.howwefeel.moodmeter.widgets.checkins.medium.CheckInMediumReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (org.howwefeel.moodmeter.widgets.friends.small.FriendsSmallWidgetReceiver) 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.
8	Broadcast Receiver (org.howwefeel.moodmeter.widgets.friends.medium.FriendsMediumWidgetReceiver) 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.
9	TaskAffinity is set for activity (androidx.glance.appwidget.action.InvisibleActionTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
10	Service (androidx.glance.appwidget.GlanceRemoteViewsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_REMOTEVIEWS [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
11	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.
12	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.
13	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) 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.
14	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.

NO	ISSUE	SEVERITY	DESCRIPTION
15	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.
16	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.
17	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.
18	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
19	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: 1 | WARNING: 7 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/z.java a5/o.java a7/f0.java a7/i1.java a7/j1.java a7/k1.java a7/q.java a7/q0.java a7/x.java a7/x1.java a9/j.java ab/b2.java ab/d1.java ab/g0.java ab/i0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ab/j0.java ab/m1.java ab/r.java ab/r0.java ab/s.java ab/s1.java ab/u1.java ab/w0.java ab/z0.java aj/b.java b0/j.java b0/u1.java b6/a.java b7/b.java b9/j.java bj/b.java bj/d.java c/k.java c0/f.java c6/p.java c6/u.java cb/p.java cb/t.java cb/u.java cc/f.java cf/a.java ch/a.java d/b.java d0/b.java d0/g.java d2/u.java d5/f.java df/d.java eg/b.java ej/a0.java ej/b0.java ej/e.java ej/e0.java ej/g0.java ej/h.java ej/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ej/p.java ej/u.java ej/v.java ej/w.java ej/z.java ek/d.java f/c.java f0/g.java f4/z.java f5/b.java f5/d.java f5/f.java f5/g.java f5/i.java f5/m.java f6/c.java f8/c.java f8/e.java f8/f.java f9/f.java fc/e.java fc/g.java fe/c.java fe/g.java g/a.java g1/t2.java gc/b.java gc/c.java gc/h.java gc/j.java gf/d.java gf/f.java gg/c.java gk/i.java gl/f0.java h2/h2.java hc/f.java hc/l.java hc/m.java hg/a.java hh/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				hj/a.java hj/b.java hl/a.java hl/b.java hw/f.java hz/a.java hz/s.java i/b0.java i/c.java i/c0.java i/f.java i/g0.java i/m.java i/r.java i/r0.java i6/d.java i7/x.java ij/b.java ij/c.java ij/e.java ij/m.java ij/o.java il/k.java iz/q.java iz/r.java j0/d.java j0/l.java j0/s.java j5/f.java j5/i0.java j5/o0.java j5/t.java jg/g.java k/i.java k/j.java k5/f.java k5/h.java kb/k0.java kb/t0.java kb/w.java kb/z0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				kb/z0.java ke/a.java kh/a0.java kh/e0.java kh/f0.java kh/i0.java kh/x.java ko/b.java l/i.java l/o.java l0/i.java lb/d.java lb/d0.java lb/j0.java lb/t.java lb/w.java lb/x.java lb/y.java lh/b0.java lh/h0.java lh/l.java lh/m.java lh/t.java lh/u.java m5/n.java m9/r.java ma/f.java md/a.java mh/d.java mh/h.java mj/c0.java mj/i0.java mj/k0.java mj/n.java mj/o.java mj/o0.java mj/p0.java mj/r0.java mk/c.java ml/c.java ms/d.java n0/d.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	n6/d.java n5/f.java n5/h.java n5/i.java n6/a.java ng/e.java ng/k.java ni/e.java nm/h0.java np/l.java o5/c.java o6/a.java oh/a.java oh/c.java oh/d.java oh/e.java oj/d.java oj/e.java oj/f.java ok/b.java org/howwefeel/moodmeter/App.java p/h0.java p/i.java p/p.java p/t.java p0/x.java p9/d.java pb/c.java pd/b.java pf/h0.java pf/i2.java pf/v3.java ph/b.java ph/c.java ph/d.java pj/b.java pj/d.java pj/e.java pz/b.java q6/r.java qh/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				qb/e.java qf/a.java qf/b.java qj/c.java qk/b.java qk/c.java qk/d.java r1/f0.java r4/e.java r4/n.java r4/q.java r4/r.java r4/u.java r4/x.java r5/n.java r9/o.java rb/a.java rg/d.java rg/u.java rh/b.java ri/b.java ri/c.java rk/h.java rk/j.java rk/n.java s3/m0.java s3/r.java s4/d.java s5/a.java s8/b.java s8/d.java s9/g.java s9/j.java sf/a.java sh/g.java sh/l.java sh/m.java sh/o.java sh/p.java sh/r.java sh/s.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sh/t.java sh/u.java sh/v.java sh/x.java sh/z.java t/f0.java t/g.java t/h.java t/h0.java t/i2.java t/x1.java t/z1.java t7/a0.java t7/c0.java t7/e.java t7/g.java t7/g0.java t7/h0.java t7/i.java t7/u.java t7/z.java t8/a.java tf/a.java th/d.java th/g.java th/l.java ti/a.java u2/e.java u5/f.java u6/b.java u6/c.java u6/g.java v0/d.java ve/b.java ve/d.java ve/e.java ve/i.java ve/j.java ve/k.java ve/m.java ve/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				vf/b.java vf/i.java vy/j.java w5/b.java w5/i1.java w5/j0.java w5/o.java w5/q1.java w5/r1.java w5/u0.java w5/v1.java w6/a.java w6/d.java w6/e0.java w6/f.java w6/f1.java w6/g.java w6/h0.java w6/h1.java w6/i1.java w6/k.java w6/n.java w6/o0.java w6/p.java w6/r0.java w6/u0.java w6/v.java we/e.java we/f.java we/j.java we/k.java we/m.java we/p.java we/t.java we/w.java wh/b.java wh/c.java wi/h.java wi/j.java wi/k.java wi/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				wp/d.java x4/e.java x6/a.java x6/d.java xb/h.java xb/s.java xh/b.java y0/e.java y4/a.java y8/n.java yh/b.java z/d.java z/f1.java z/v0.java z1/g0.java z4/f.java za/a1.java za/c0.java za/j2.java za/n2.java za/v.java za/v1.java za/z1.java ze/a.java zg/f.java zg/h.java zi/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	d9/g.java fe/c.java fe/g.java ge/l.java j0/d.java ni/h0.java ni/n0.java ni/o0.java ni/p0.java p9/d.java pf/d0.java pf/j.java pf/q3.java pf/z3.java qb/b.java qk/a.java rk/l.java rk/m.java t/b2.java t/j.java t/y2.java t7/k.java uh/f0.java za/a1.java za/l1.java
3	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	g9/a.java nm/h0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	c0/e.java c9/m0.java c9/t0.java d00/e.java d9/a0.java gk/j.java hj/i.java hj/j.java ij/c.java ij/h.java ij/o.java il/e4.java il/f1.java il/h1.java il/w2.java jl/n.java jl/p.java km/a.java km/b.java lm/a.java m9/g1.java mh/g.java pf/v3.java pj/e.java pl/u.java x6/a.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	ng/k.java rg/d.java sh/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	e4/p0.java fk/c.java fr/a.java h2/l1.java ji/i.java jl/k.java mi/a.java mq/n.java oi/m.java pi/h.java ri/f0.java uc/b.java z8/a.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	c0/f.java gl/v1.java jg/e.java nc/e0.java ni/b0.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	vp/d.java vp/g.java vp/k.java vp/l.java
9	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	aj/b.java sh/g.java t7/d.java wh/c.java
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	f/g.java pf/v3.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	ft/e0.java hz/a.java k5/k.java
12	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	s3/k.java
13	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	c6/p.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a9/e.java a9/e0.java aq/t.java c0/f.java hc/g.java ib/a.java ib/h.java il/k.java jg/e.java k5/h.java k6/s0.java k6/t0.java mk/c.java ni/b0.java nm/h0.java o5/c.java sh/g.java sh/p.java t7/a0.java t7/c0.java th/g.java u6/g.java wh/b.java yh/b.java
00022	Open a file from given absolute path of the file	file	c0/f.java cd/d.java ft/e0.java jg/e.java k6/u0.java k6/x0.java lc/e.java qk/c.java th/g.java x2/d.java z3/b0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	cd/d.java
00108	Read the input stream from given URL	network command	a9/t.java lh/s.java pf/j2.java pf/k0.java
00199	Stop recording and release recording resources	record	iz/r.java
00012	Read data and put it into a buffer stream	file	c0/f.java u6/g.java
00109	Connect to a URL and get the response code	network command	a9/t.java b9/j.java bj/d.java d00/e.java lh/s.java p9/d.java qj/c.java ue/d.java
00026	Method reflection	reflection	cn/b0.java in/i.java
00078	Get the network operator name	collection telephony	mk/c.java rk/f.java
00132	Query The ISO country code	telephony collection	mk/c.java q9/f.java
00198	Initialize the recorder and start recording	record	iz/q.java

RULE ID	BEHAVIOUR	LABEL	FILES
00194	Set the audio source (MIC) and recorded file format	record	iz/q.java
00197	Set the audio encoder and initialize the recorder	record	iz/q.java
00196	Set the recorded file format and output path	record file	iz/q.java
00091	Retrieve data from broadcast	collection	ac/c.java b7/b.java pf/i2.java t7/u.java w6/g.java
00075	Get location of the device	collection location	i/c.java
00137	Get last known location of the device	location collection	i/c.java
00096	Connect to a URL and set request method	command network	a9/t.java d00/e.java lh/s.java linc/com/amplituda/FileManager.java p9/d.java qj/c.java
00030	Connect to the remote server through the given URL	network	a9/t.java d00/e.java linc/com/amplituda/FileManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	a9/t.java gk/b.java lh/s.java linc/com/amplituda/FileManager.java za/a1.java
00114	Create a secure socket connection to the proxy address	network command	rp/j.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a7/o1.java bj/b.java cb/u.java hz/a.java nz/e.java org/howwefeel/moodmeter/util/notifications/ExactAlarmBroadcastReceiver.java pf/i2.java pf/v3.java s3/h1.java t7/c0.java w6/g.java we/f.java xv/t.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a7/o1.java bj/b.java hz/a.java t7/c0.java we/f.java xv/t.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	a9/e0.java bj/b.java hz/a.java lc/b.java sj/u.java t7/c0.java we/f.java
00112	Get the date of the calendar event	collection calendar	bp/k.java
00089	Connect to a URL and receive input stream from the server	command network	a9/t.java bj/d.java d00/e.java lh/s.java p9/d.java qj/c.java
00121	Create a directory	file command	wh/c.java
00125	Check if the given file path exist	file	t7/w.java wh/c.java
00104	Check if the given path is directory	file	wh/c.java
00009	Put data in cursor to JSON object	file	rk/l.java rk/m.java za/a1.java
00014	Read file into a stream and put it into a JSON object	file	ni/b0.java th/g.java yh/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	ni/b0.java ri/c.java
00005	Get absolute path of file and put it to JSON object	file	th/g.java
00162	Create InetSocketAddress object and connecting to it	socket	vp/c.java vp/l.java
00163	Create new Socket and connecting to it	socket	vp/c.java vp/l.java
00028	Read file from assets directory	file	a9/b.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://howwefeel.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/666825112376/namespaces/firebase:fetch?key=AIzaSyBtTmIzqH5IvVTpdHibzP_bXwMYSR7kciM is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'actionTilesVariant': '', 'aiEarlyAccessCohortId': 'default cohort', 'aiPrivacyUpdatedAt': '2024-01-02', 'allowDailyRemindersDynamicCopy': 'false', 'allowDemographicSurvey': 'true', 'allowDonateFromHomepage': 'true', 'allowInAppUpdate': 'true', 'allowToolsTabHeroSection': 'false', 'appShareLink': 'https://howwefeel.org/get', 'attachmentsCheckInFormatEnabled': 'false', 'bestSelfToolsEnabled': 'false', 'betaShareLink': 'https://apps.apple.com/us/app/how-we-feel/id1562706384', 'beta_share_link': 'https://apps.apple.com/us/app/how-we-feel/id1562706384', 'bodyMapEnabled': 'false', 'checkInNoteOnMainPage': 'true', 'checkInPhotoOnMainPage': 'false', 'checkInVoiceOnMainPage': 'false', 'compactJournalOnEditor': 'false', 'disableAIKillSwitch': 'false', 'dynamicNotificationsAvailable': 'false', 'enhancedCardPrototypeEnabled': 'true', 'experimentalMoodMeterEnabled': 'true', 'extendedCheckInCardEnabled': 'false', 'forceAppUpdateModal': 'false', 'friendAutosharePolicyEnabled': 'true', 'friendRepliesEnabled': 'true', 'isAIAccessEnabled': 'false', 'isEligibleForAIEarlyAccess': 'false', 'newCheckInFlowEnabled': 'true', 'onboardingVariant': '', 'privacyUpdatedAt': '2024-07-28', 'secondCheckInTooltipVariant': 'none', 'showQuickActions': 'true', 'strategyButtonOrder': 'video_first', 'substackLink': 'https://howwefeel.substack.com', 'surveyLink': 'https://docs.google.com/forms/d/e/1FAIpQLSeIi3w9nv7PUS90FeregHKkiP8oWHMgh-Bpc1E0veAzxujrhA/viewform', 'swipeCheckInsEnabled': 'false', 'termsUpdatedAt': '2024-07-28', 'toolSuggestionsEnabled': 'true', 'toolsTabEnabled': 'false', 'wellBeingSurveyEnabled': 'false'}, 'state': 'UPDATE', 'templateVersion': '147'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, 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
health.clevelandclinic.org	ok	**IP:** 172.64.155.40 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
howwefeel.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

DOMAIN	STATUS	GEOLOCATION
howwefeel.substack.com	ok	**IP:** 104.18.37.200 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.googleadservices.com	ok	**IP:** 142.250.74.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
mobile.events.data.microsoft.com	ok	**IP:** 20.42.73.24 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebaseremoteconfig.googleapis.com	ok	**IP:** 142.250.74.106 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
www.inc.com	ok	**IP:** 151.101.1.54 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
default.url	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
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

DOMAIN	STATUS	GEOLOCATION
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
api.openweathermap.org	ok	**IP:** 38.89.70.175 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.901566 **Longitude:** -77.050781 **View:** Google Map
jsoup.org	ok	**IP:** 104.21.48.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.google.com	ok	**IP:** 216.58.207.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.mixpanel.com	ok	**IP:** 130.211.34.183 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **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:** 216.58.207.226 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.nytimes.com	ok	**IP:** 151.101.129.164 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
g.co	ok	**IP:** 172.217.21.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
storage.googleapis.com	ok	**IP:** 142.250.74.187 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.cnn.com	ok	**IP:** 151.101.67.5 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 216.58.211.10 **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
howwefeel.org	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
developer.apple.com	ok	**IP:** 17.253.83.145 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
in.appcenter.ms	ok	**IP:** 132.196.225.214 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
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
us1.locationiq.com	ok	**IP:** 172.67.99.217 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebasestorage.googleapis.com	ok	**IP:** 216.58.211.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.health.harvard.edu	ok	**IP:** 54.165.240.143 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **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
support@howwefeel.org	hz/a.java
support@howwefeel.org tools@howwefeel.org	ov/d.java
u0013android@android.com0 u0013android@android.com	we/r.java
support@howwefeel.org tools@howwefeel.org	Android String Resource

EMAIL	FILE

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" : "67c23f84353e4d429e9c6374ee2306e7"
"firebase_database_url" : "https://howwefeel.firebaseio.com"
"google_api_key" : "AIzaSyBtTmIzqH5IvVTpdHibzP_bXwMYSR7kciM"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyBtTmIzqH5IvVTpdHibzP_bXwMYSR7kciM"
"share_invite_code_and_token" : "https://howwefeel.org/friends/%s?invite=%s"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
c483d491-72d0-49f1-8383-de4845fccb49
607bb0de-a4a7-43b6-ac56-4cd7a4088ab2
9e391d44-1064-4e6c-b077-7b0b91264217
544aef1a-3aa0-48f3-8feb-cfff6c233816
4e335d05-fd57-4839-9cfa-2229f874658d
8c5e87b7-074a-4254-b0f1-e562eb75c068
582d7dbf-6a7e-4716-93f8-ff3185d7d5b0
502f0851-61ca-4e52-892a-77ceda875034
eb87e3d5-ef66-4229-a960-d8bdddbefd7a
ed441966-8f01-4674-b8b7-7333e4ce93f0
36864200e0eaf5284d884a0e77d31646
2392de02-35ce-43db-bfe7-122068c63a00

POSSIBLE SECRETS
86494f9e-2a35-4808-846f-e93575a52519
c9b70a78-b10f-470c-942b-28d53c711f48
8491e949-99e4-43b7-9237-cce591d3e4df
5d532fff-bd95-4326-9bb1-54452fde3789
449f8e89-b012-41ff-b2f2-f4d336a1af5e
2ea4a6fa-fb6b-42dd-861c-643ab154e162
31af2bfb-22b5-428d-abd9-de6ebf1fe2e3
f7c2d602-0a4e-48b1-9e6a-ca305bcb54d9
a1c941c8-ebba-4224-af51-9eeebe406bab
31332cd0-a776-4272-be15-118fee0c8e1c
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
a0c406f8-7d1d-443e-8a47-8b45d34b5b81
7d73d21f1bd82c9e5268b6dcf9fde2cb
4a36d732-5a4f-4c31-ab3f-8b72dc6eecb8

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
c05e33f6d93b6dc59379f310df3f0bb3
a0784d7a4716f3feb4f64e7f4b39bf04
e2a15d5f-4461-4fbe-8dc8-176bd8696f55
7f2a57db-32a4-4f32-baf1-c07d98c4741e
1896ee8f-c9e9-4edf-be6c-b8a3f759d8a2
f0f9d079-d00c-4a09-ba1f-766210dacaa8
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
e5a2b42d-49e3-4530-ad18-969bbc7943b6
f447ecd0-bba0-48a4-a1fb-d4c150376b83
0b4a0c76-39fc-412d-bfcf-b315bcf0b794
1361e19b-75af-4a9b-9c09-31825a71afaf
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
af60eb711bd85bc1e4d3e0a462e074eea428a8
18a283b0-0011-45de-9f44-e1a09e807f9f

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
59a06977-dffe-4a4a-9201-096958f15b0b
d028194c-8e3b-4e26-8a8f-90482a9a31f9
d88c9316-19e5-4d5f-a3b7-94a6a3372ec6
7be5cce3-c7a2-4680-83d5-8965dd8ede7e
7a81c0a1-50f5-417a-b406-e55b9dd111d8
57befcda-357a-417f-a7a4-c41e39803d9f
064929d6-117b-4b51-a45c-f7556db9ab98
954080ad-ff70-433b-af05-0de5a285a407
85053bf24bba75239b16a601d9387e17
93e1743e-b3b2-48a6-88c4-79c14c29f328
dfefddbf-2795-493a-ba58-d550de339ebf
e9cdd0f2-e42c-42c9-9df5-4e6790bc8751
52f091f2-d831-4ce3-ab9f-caf3a8519156
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

POSSIBLE SECRETS
586a9345-ce0e-4e13-9831-1bbaf6bf60f6
d6387ad7-bb07-416a-84b9-1b0da9651d24
5bced106-e4ad-40c0-a633-f15070468e14
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
f0cbc56f-c2fc-4df9-b7b7-6ef92ec0ef67
d5fdd33a-c0a6-4a8d-a6f2-62f94975a70b
cda8bd23-4659-4b5b-91de-24e4a0443ac2
ba005a4d-f523-41fc-b6c7-683e297125a8
e0e69c35c55010e98699c4dde2956b04
723c062d-6c35-4a62-91f5-f1f40b1f0713
470fa2b4ae81cd56ecbcda9735803434cec591fa
084eb227-1bba-4592-af5c-6b8fd2a17b2e
1e718ba4-3f48-4368-be23-19f2086cc2ae
f40cbf4c-75f9-4bff-a2af-e939c4fd9dee

POSSIBLE SECRETS
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
f9fa25e4-68a4-434e-9894-faba219e849f
3a172f7b-a23c-4079-9938-7b904596da3d
ade4141c-6377-4530-bb88-4ad77c69d293
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
48b39de4-91b3-4a4c-821b-972f41312778
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
c7f90dad-2068-4359-90ec-61024c39d756
98954970-f94b-4d43-be19-09a934392307
55357b8c-30a5-41c0-bba9-2ef166283a9a
9b387031-1427-48bf-a573-941e24bee5e9
19c8159b-5a71-47da-9941-c56afcaeb536
3c37fc64-40d6-44e9-b458-8c43775c2429
681a07ea-a1ba-44b9-906a-feda2b5007f7
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
626d5e8a9c575d9442a4bb46b9640184
598a2257-434e-4342-b2c5-b27412ac4d5b
3071c8717539de5d5353f4c8cd59a032
da98b7e4-e97a-48d1-948a-80aabc15f7f8
ec1b8b51-dcd4-4021-a531-9b728265e040
8015f491-fc90-4240-862a-3f4524bffaeb
3cadfa6d-ed33-495a-bc26-c087b5a2eb60
013dd0d0-9429-48af-87fc-ebfdf2a85558
9188dc63-b11e-4252-ab0b-f6b992d5bd49
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
ec8a273f-f30f-4c1e-91df-43b09860b0df
24f19851-7b4d-4011-bf22-36df389a5917
fdd18731-be9a-488e-a9fb-e33daab2b27d

POSSIBLE SECRETS
03fc8978-15e8-4b5b-8ca3-14658ca5d975
c38b4238-00ef-4fae-9b73-7bac6599baad
9bf83ea08bec871a20c8158d3bc1bd56
cba013e9-a42e-49b5-bc06-4e68e5bc4aab
fbdadf29-16e1-4de1-a03f-7ef3d5d6a3fe
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
7ff08a9e-24ae-4f66-aadd-b270f21ab505
2db600b6-8aa8-47f6-b38f-563cc6857f6b
c7ffed92-d4ba-40a1-b53e-0222c0380151
9d1cc13d-8f9b-4645-8912-74fc56ba2e40
10985f61-fda7-4968-a77a-d71020356946
692a2d0d-68f4-4e18-ad64-8cb62e4a72f7
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
92fea3d8-d793-4171-8c05-61f2d78d2450
a6ac6219-9702-4ff7-bb7c-1327c8aec9ef

POSSIBLE SECRETS
c480165d-0009-4913-87c0-36440392fe7e
c2c56acf-12f1-4867-bc7d-fa8457d8b9d0
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
46be7a5e-6d03-4552-a6ca-560614c9e946
298eec17-7c90-41cf-b125-62c89d47016b
c640dc73-f6c8-4294-88f5-91c14886a282
f5247c40-ffb8-4b74-ad77-61f1b916004d
f532aab4-f566-43e7-bea3-6872b4a55098
359cf206-019d-4b54-bf8e-98c25da5966f
93f96040-35c7-4058-a798-f0b35ba116e7
0a90ab3b-93af-4638-bf84-23e35707a46d
5e0b7f8d-197b-47b2-8c9d-18601acb4420
8df94bfa-fb9e-4f4d-b56c-acf6460a910e
f383cfd5-fa2a-4013-93c6-7cee8b65fe8c
36b7508d-668e-45c2-a435-668a5cbce4e1

POSSIBLE SECRETS
d1ed81e93d74d121077cba1cb2d875ed
c1038408-c1c4-4d0d-a98d-3b36243d9ebf
dfed733e-229c-443a-a355-0d3409cab04e
3296c187-9840-4e2d-9553-dd038d0912fe

PLAYSTORE INFORMATION

Title: How We Feel

Score: 4.514563 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** org.howwefeel.moodmeter

Developer Details: The How We Feel Project, Inc., The+How+We+Feel+Project,+Inc., None, https://howwefeel.org, support@howwefeel.org,

Release Date: Nov 21, 2022 **Privacy Policy:** Privacy link

Description:

How We Feel is a free app created by scientists, designers, engineers, and therapists to help people better understand their emotions and find strategies to help them navigate their emotions in the moment. Conceived in conjunction with Yale University's Center for Emotional Intelligence and based on the work of Dr Marc Brackett, How We Feel helps people find the right word to describe how they feel while tracking their sleep, exercise, and health trends in order to spot patterns over time. Founded as a science-based nonprofit, How We Feel is made possible by donations from people who are passionate about bringing mental wellbeing to the widest possible audience. Our data privacy policy puts you in control of how your data is stored and shared. Data is stored on your device unless you choose to send your data to an alternative storage solution. Data is only accessible by you unless you choose to share it with others. Data is not used for research unless you opt-in to contribute an anonymized version of your data for research studies designed to help more people. Whether you are downloading this app in order to build better relationships, make your emotions to work for you, not against you, improve how you handle stress and anxiety or simply to feel better, How We Feel will help you identify patterns and find emotional regulation strategies that will work for you. The How We Feel friends feature allows you to share how you feel with the people you trust most in real time, strengthening your most important relationships. Filled with step-by-step video strategies you can do in as little as one minute on themes like "Change Your Thinking" to help you address negative thought patterns with cognitive strategies; "Move Your Body" to express and release emotions through movement strategies; "Be Mindful" to gain perspective and minimize the negative impact of misunderstood emotions with mindfulness strategies; "Reach Out" to build intimacy and trust, two important tools for emotional wellbeing, with social strategies.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 15:10:36	Generating Hashes	OK
2025-09-01 15:10:36	Extracting APK	OK
2025-09-01 15:10:36	Unzipping	OK
2025-09-01 15:10:37	Parsing APK with androguard	OK
2025-09-01 15:10:37	Extracting APK features using aapt/aapt2	OK
2025-09-01 15:10:37	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 15:10:40	Parsing AndroidManifest.xml	OK
2025-09-01 15:10:40	Extracting Manifest Data	OK
2025-09-01 15:10:40	Manifest Analysis Started	OK

2025-09-01 15:10:40	Performing Static Analysis on: How We Feel (org.howwefeel.moodmeter)	OK
2025-09-01 15:10:42	Fetching Details from Play Store: org.howwefeel.moodmeter	OK
2025-09-01 15:10:44	Checking for Malware Permissions	OK
2025-09-01 15:10:44	Fetching icon path	OK
2025-09-01 15:10:44	Library Binary Analysis Started	OK
2025-09-01 15:10:44	Reading Code Signing Certificate	OK
2025-09-01 15:10:44	Running APKiD 2.1.5	OK
2025-09-01 15:10:49	Detecting Trackers	OK
2025-09-01 15:10:51	Decompiling APK to Java with JADX	OK
2025-09-01 15:11:06	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 15:11:06	Decompiling classes2.dex with JADX	OK

2025-09-01 15:11:14	Decompiling classes.dex with JADX	OK
2025-09-01 15:11:25	Decompiling classes3.dex with JADX	OK
2025-09-01 15:11:26	Decompiling classes2.dex with JADX	OK
2025-09-01 15:11:34	Decompiling classes.dex with JADX	OK
2025-09-01 15:12:03	Decompiling with JADX failed for classes.dex	OK
2025-09-01 15:12:03	Decompiling classes3.dex with JADX	OK
2025-09-01 15:12:04	Some DEX files failed to decompile	OK
2025-09-01 15:12:04	Converting DEX to Smali	OK
2025-09-01 15:12:04	Code Analysis Started on - java_source	OK
2025-09-01 15:12:10	Android SBOM Analysis Completed	OK
2025-09-01 15:12:24	Android SAST Completed	OK

2025-09-01 15:12:24	Android API Analysis Started	OK
2025-09-01 15:12:36	Android API Analysis Completed	OK
2025-09-01 15:12:36	Android Permission Mapping Started	OK
2025-09-01 15:12:45	Android Permission Mapping Completed	OK
2025-09-01 15:12:45	Android Behaviour Analysis Started	OK
2025-09-01 15:13:02	Android Behaviour Analysis Completed	OK
2025-09-01 15:13:02	Extracting Emails and URLs from Source Code	OK
2025-09-01 15:13:07	Email and URL Extraction Completed	OK
2025-09-01 15:13:07	Extracting String data from APK	OK
2025-09-01 15:13:07	Extracting String data from Code	OK
2025-09-01 15:13:07	Extracting String values and entropies from Code	OK

2025-09-01 15:13:11	Performing Malware check on extracted domains	OK
2025-09-01 15:13:15	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.