MOBSF

ANDROID STATIC ANALYSIS REPORT

Moodee (3.2.1)

File Name:	com.bluesignum.little_lighthouse_3020102.apk
Package Name:	com.bluesignum.little_lighthouse
Scan Date:	Aug. 29, 2025, 8:25 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	18	2	3	1

FILE INFORMATION

File Name: com.bluesignum.little_lighthouse_3020102.apk
Size: 127.89MB
MD5: c8ba38087a5cb08f61638850ceb108cb
SHA1: d7f24ace1717f2feee09a3eba55f4d5f7600ffdc
SHA256: d502fa1062acc7aa52fbfde83b27b2bd8389dd3a6c07141e5f25202db9bb30e4

APP INFORMATION

App Name: Moodee
Package Name: com.bluesignum.little_lighthouse
Main Activity: com.bluesignum.little_lighthouse.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 3.2.1

Android Version Code: 3020102

APP COMPONENTS

Activities: 14
Services: 16
Receivers: 19
Providers: 6
Exported Activities: 0
Exported Services: 2
Exported Receivers: 6
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: 2023-03-01 12:37:16+00:00
Valid To: 2053-03-01 12:37:16+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x131627c9cf37f81e8f39553da2ef179345fc24b1
Hash Algorithm: sha256
md5: 6955d9e2babf80cfbe129608cf2aa6b9
sha1: 8b25e948e5299460d2a326c256a52b359d92317f
sha256: 0a951f5a223ac4a671796a513886cda84aa5b8567dd3e38c43b7ebba6a42e29b
sha512: c8f463094fbe6aaa564f50a7eae785c73c9b574b03ad7a26faf7ecf09107f63f2982f49c1674b21ac856e8bb13d17c95c3e3ec6ccd5d72594acb90c51ce31ebb
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 929d198f5c00183d26caf66eca6f1ddf3fa721f9cdb4dd1c5d20e30a9e0008ff
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.bluesignum.little_lighthouse.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

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

<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-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD 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>dx</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>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

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

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: 9 | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (com.bluesignum.little_lighthouse.RecordWidgetProvider) 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.
4	Broadcast Receiver (com.bluesignum.little_lighthouse.QuestWidgetProvider) 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 (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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.
8	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
9	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
10	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: **2** | WARNING: **7** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/d.java a1/j.java b1/d.java b2/a.java ba/g.java bh/a.java c1/a.java c2/d.java c2/e.java c3/a.java cd/a.java cd/e.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/manager/f.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/q.java com/bumptech/glide/manager/s.java com/bumptech/glide/manager/t.java com/bumptech/glide/manager/u.java com/dexterous/flutterlocalnotifications/ActionBroadcastReceiver.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/ScheduledNotificationReceiver.java com/pichillilorenzo/flutter_inappwebview/JavaScriptBridgeInterface.java com/pichillilorenzo/flutter_inappwebview/ServiceWorkerManager.java com/pichillilorenzo/flutter_inappwebview/Util.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview/content_blocker/ContentBlockerHandler.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserActivity.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserManager.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/DisplayListenerProxy.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/FlutterWebView.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/InAppWebView.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/InAppWebViewChromeClient.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/InAppWebViewClient.java com/pichillilorenzo/flutter_inappwebview/in_app_webview/InAppWebViewRenderProcessClient.java com/pichillilorenzo/flutter_inappwebview/in

NO	ISSUE	SEVERITY	STANDARDS	FILES
				_app_webview/InputAwareWebView.java d7/g.java dd/h.java dev/fluttercommunity/workmanager/BackgroundWorker.java e2/c.java e2/e.java e9/a.java e9/b.java e9/c.java ea/r.java f1/b.java f2/h.java f2/i.java f2/k.java f2/q.java f2/z.java f3/b.java f7/b.java f7/b0.java f7/c0.java f7/d.java f7/k.java f7/u.java f7/w.java f7/y.java f8/a.java g2/i.java g2/j.java g6/a.java g6/d.java g7/b0.java g7/e.java g7/g0.java g7/j.java g7/k.java g7/l0.java g7/o.java g7/x.java g8/a.java h2/e.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	h2/i.java hd/b0.java hd/d0.java hd/i.java i2/a.java i7/d0.java io/flutter/plugins/firebase/crashlytics/n.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/b.java io/flutter/plugins/firebase/messaging/i.java io/flutter/plugins/googlemobileads/b.java io/flutter/plugins/googlemobileads/d.java io/flutter/plugins/googlemobileads/e0.java io/flutter/plugins/googlemobileads/f0.java io/flutter/plugins/googlemobileads/i0.java io/flutter/plugins/googlemobileads/k.java io/flutter/plugins/googlemobileads/p.java io/flutter/plugins/googlemobileads/u.java io/flutter/plugins/googlemobileads/w.java io/flutter/plugins/googlemobileads/x.java io/flutter/plugins/imagepicker/o.java io/flutter/plugins/webviewflutter/f.java io/flutter/plugins/webviewflutter/o3.java j2/c.java j2/d.java j2/g.java j2/t.java j2/u.java j2/v.java j3/a.java j3/d.java j7/a.java j7/c.java j7/c0.java j7/c1.java j7/d1.java j7/e1.java j7/f0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j7/g1.java j7/m1.java j7/q1.java j7/z0.java j8/s.java jc/a.java jc/e.java k1/a.java kg/c.java l0/d.java l2/a.java ld/f.java m1/k.java m2/c.java m2/c0.java m2/d.java m2/j.java m2/l.java m2/m.java m2/p.java m7/a.java mc/d0.java mc/g.java mc/g0.java mc/i0.java mc/k.java mc/y.java md/d.java n0/a.java n3/a.java n6/t1.java n7/b.java n9/f.java nc/a.java o7/h.java o7/s.java o7/t.java oa/o.java oc/c.java oc/f.java oc/d0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				oc/d0.java pe/w.java p8/i.java pc/a.java pc/b.java pc/c.java pc/i.java pe/a.java q/d.java q0/c.java q2/a.java q2/d.java q2/j.java qb/b.java qc/e.java rb/c.java s2/d.java s3/k.java s7/b.java t/f.java t9/a.java te/a.java te/d.java u2/k.java u7/l.java u9/b.java ud/b.java ue/f.java v/a.java v0/c.java v3/a.java va/m.java ve/e.java w0/k0.java w0/o.java w0/o0.java w0/r.java wb/e.java we/f0.java x2/b.java xe/i.java y0/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y6/a.java y1/a.java y1/p.java y1/r.java y1/t.java y9/f.java y9/n.java ye/k.java z2/a.java z5/r.java z6/i.java z7/b3.java z7/d1.java z7/m3.java z7/o.java z7/p0.java z7/q.java z7/r1.java z7/v0.java z7/w2.java z7/y2.java za/a.java zb/c.java ze/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	bb/i.java dev/fluttercommunity/workmanager/BackgroundWorker.java e4/q1.java ec/d.java f5/r0.java gd/d.java i5/b.java j$/util/concurrent/ThreadLocalRandom.java k6/v.java pc/c.java ra/a.java sf/a.java sf/b.java tf/a.java va/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/pichillilorenzo/flutter_inappwebview/credential_database/URLCredentialContract.java com/pichillilorenzo/flutter_inappwebview/types/URLCredential.java d2/g.java f2/d.java f2/p.java f2/x.java fa/b.java ga/e.java ga/w.java i3/f.java lc/b.java r1/d.java rd/q.java
4	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	pd/b.java qb/b.java va/m.java
5	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	b1/c.java com/pichillilorenzo/flutter_inappwebview/credential_database/CredentialDatabaseHelper.java hd/i.java oa/p.java z3/m0.java z3/t0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	dd/h.java k5/a.java
7	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/d.java io/flutter/plugin/platform/g.java
8	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	qb/c.java w0/o0.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	ea/i.java j8/c.java p8/w.java
10	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	c3/a.java j3/e.java xe/a.java xe/i.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	qg/e.java
12	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	z7/o1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	bb/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/TrustedWebActivity.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserManager.java g7/f.java io/flutter/plugins/imagepicker/l.java j6/s.java m6/a.java md/d.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java w1/a.java y1/a.java y1/p.java y1/t.java z7/d1.java ze/h.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserManager.java g7/f.java j6/s.java m6/a.java w1/a.java y1/a.java y1/p.java y1/t.java ze/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/bluesignum/little_lighthouse/QuestWidgetProvider.java com/bluesignum/little_lighthouse/RecordWidgetProvider.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java g7/f.java lg/b.java lg/c.java md/d.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java me/leolin/shortcutbadger/impl/a.java y1/a.java y1/p.java y5/h0.java
00022	Open a file from given absolute path of the file	file	b1/d.java c1/a.java c3/a.java e0/m.java fa/f.java g3/a.java j3/a.java j3/d.java j3/e.java sa/g.java w0/o0.java xe/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	b2/a.java c3/a.java com/bumptech/glide/load/a.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview/Util.java e0/m.java ea/a0.java fa/f.java j2/g.java j3/d.java j3/e.java ja/e.java la/a.java nf/i.java nf/k.java qb/c.java w0/o0.java y0/b.java y5/g.java y5/h0.java
00003	Put the compressed bitmap data into JSON object	camera	com/pichillilorenzo/flutter_inappwebview/in_app_webview/InAppWebView.java z7/d1.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/d.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00092	Send broadcast	command	sd/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	y5/c.java
00014	Read file into a stream and put it into a JSON object	file	com/pichillilorenzo/flutter_inappwebview/Util.java fa/f.java la/a.java qb/c.java
00005	Get absolute path of file and put it to JSON object	file	fa/f.java
00189	Get the content of a SMS message	sms	f3/f.java j3/e.java me/leolin/shortcutbadger/impl/a.java
00188	Get the address of a SMS message	sms	f3/f.java j3/e.java me/leolin/shortcutbadger/impl/a.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	f3/f.java me/leolin/shortcutbadger/impl/a.java
00191	Get messages in the SMS inbox	sms	f3/f.java me/leolin/shortcutbadger/impl/a.java
00200	Query data from the contact list	collection contact	f3/f.java j3/e.java me/leolin/shortcutbadger/impl/a.java
00187	Query a URI and check the result	collection sms calllog calendar	f3/f.java j3/e.java me/leolin/shortcutbadger/impl/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00201	Query data from the call log	collection calllog	f3/f.java j3/e.java me/leolin/shortcutbadger/impl/a.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	e2/c.java f3/f.java j3/e.java me/leolin/shortcutbadger/impl/a.java
00091	Retrieve data from broadcast	collection	com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/ActionBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserActivity.java n6/i2.java
00096	Connect to a URL and set request method	command network	rb/c.java y5/s.java z7/m3.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/j.java rb/c.java y5/s.java z7/m3.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java y5/s.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/j.java d7/f.java g6/d.java rb/c.java y5/s.java z7/m3.java
00094	Connect to a URL and read data from it	command network	ia/a.java y5/s.java
00108	Read the input stream from given URL	network command	y5/s.java
00034	Query the current data network type	collection network	n6/c.java
00162	Create InetSocketAddress object and connecting to it	socket	wg/d.java wg/h.java
00163	Create new Socket and connecting to it	socket	wg/d.java wg/h.java
00004	Get filename and put it to JSON object	file collection	com/pichillilorenzo/flutter_inappwebview/Util.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	f3/f.java
00102	Set the phone speaker on	command	fd/l.java
00056	Modify voice volume	control	fd/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00132	Query The ISO country code	telephony collection	z5/p0.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	c3/a.java
00202	Make a phone call	control	y1/t.java
00203	Put a phone number into an intent	control	y1/t.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/l.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/l.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/978616305658/namespaces/firebase:fetch?key=AIzaSyBsNc_EVCtkcKADqh_hbui0mh_pHOc5pE8. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK
Other Common Permissions	5/44	com.google.android.gms.permission.AD_ID, android.permission.ACCESS_NOTIFICATION_POLICY, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
www.firebase.com	ok	**IP:** 151.101.65.195 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
support.google.com	ok	**IP:** 64.233.177.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
fundingchoicesmessages.google.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
default.url	ok	No Geolocation information available.
googlemobileadssdk.page.link	ok	**IP:** 74.125.21.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 74.125.136.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.15.103 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.9.154 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
accounts.google.com	ok	**IP:** 74.125.137.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 142.250.9.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebasestorage.googleapis.com	ok	**IP:** 142.250.105.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dashif.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
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
console.firebase.google.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	g7/w.java

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
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
"facebook_client_token" : "5792764d8e3f4e8186992978331e6edf"
"google_api_key" : "AIzaSyBsNc_EVCtkcKADqh_hbui0mh_pHOc5pE8"
"google_crash_reporting_api_key" : "AIzaSyBsNc_EVCtkcKADqh_hbui0mh_pHOc5pE8"
TOlHmdp8XsKJiprHSu957VTnJJL2Dj58ytcwt3QLHDQ=
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
wsk3Vojf7RmX+WtFiGWOJo7xhFKFeiDn9iUtTCe0eNY=
FdxRYG9/HOndmgVdj1eVgDulreHUGSjsWl31nKn2TzY=
6diiPm6leEU3dn6Yh3093iP+CyZAN47Ila9hmZbBOygAlbw7IfYBD8oUvevGhzQp
470fa2b4ae81cd56ecbcda9735803434cec591fa
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
ki2ip3Sp4zD5u1iHxdI5CQP+nQytWboRZ8YxUMq1u4GDs7rHoXiw6vz07EKttNE7
0BurIdBwA1Yjcso9P1TmQgVgvpSOR3INLha4uP5JdYXgWQEacWBPKA8E9hy+9dAe
t0k+Q4WGODPCHlTh1fiMgaVG6LJXWEyq2lqorD4gMCo=
zuOSwgzLq/YXiyJNPWGjICL0KrcqY8eXUxyiBgiihdg=

POSSIBLE SECRETS
5BsC37pqFx3Fp5Qtv0y+RSU8LVttAMXjX8aFccLrzxg=
8UEA9TmdE+sqV3zcsNgnFI5Sf8uIsQHU61W37Ddl8zaNqY23x/FpuoK+mm9MWruA
XE2927Ta6gTWmjrPmk4in7GLLwsXJnqTbhVN3N+/b3M=
m4BHDSYRnsEEIrYlgM0yy1C5NfyYnIIeJvwgjuCY5HY=
af60eb711bd85bc1e4d3e0a462e074eea428a8
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
8lD2ezwwsI93agi51tjtw1sdZVRU2vHPSc7HynOlFDE=
tk45mDotIpTZidmNYxxiIBsjVftw/e0h3Unlwpf2Me4=
ae2044fb577e65ee8bb576ca48a2f06e
GZJYAQ87uqT/39Vw1xO4VkKaUA+BZKFiVkKasBC0VSw=
ZzhYXgKMhken/ic2sDR8A53WLOTMzsBN7DfnMjKoyhk=
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
nKZwK8oioxkTwDfG9V2sR2xNb9GbO72JaQ9OaUpmWGl7ZX+EiCwiESnhzEGly7cm
U5Ngb8pPuPEbyAEAeNCt0wgGFK4YAtkNGCrOQKfD/ONzQcV8GTtSZ6EoO3NY8V1s
a1Na7bntM+sktGxZBhUnqailj8ITQ7piLQZ5OyqVU2HU4R0rOCZ63N/fUHG081A+
tJ+SvALjKnpAv9FF8u56pKKRS55/vzUDe+m9ct97Lx4=
36864200e0eaf5284d884a0e77d31646
eISRjanjhAfdgJ9+lE3tGViJFRMvsuX1oVbmo+9k2XU=
ChMYhePBDqkXl5DeRTg9cgSXXNPVEcIqgEVciYHEVlkZyx/HkVQXSnen8aw33G2s
9a04f079-9840-4286-ab92-e65be0885f95

POSSIBLE SECRETS
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
gziBDgIPHk3UnbqAN9Ta9zRxJ8KBrTfiKBXyCZDQ588=
J3qHQsXE9gxUWY3EQze3pD9LpRQkp3i0z4IBb3xvxMfPfsFZNBOU+l2pHi8zC3DO
Q0EftCh9LNoL/97bVNRGH4YGKN2mjVuI8Ruidx0q8xs=
f+0D9BT8zkFXnX9yG742KHeQy11nhCJFb6PFndn+zMk=
W1peSRrFFzj+W6DyflucA6CQWTsphM4X4AkhjKjRy/o=
eEgPK4FD9N/fpMPwsM6h+Wvbqi3j4L5DBTwMY2KteC4=
e2719d58-a985-b3c9-781a-b030af78d30e
hIbo0WHjc5N2XBD7HI+Mwh9BXu/nIzOhdTaHZ1DPjeizuR48SZNCpBdtOxY4cHlb
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
69psxaRqrIVZzPpt4pN0wGmA/kc6O8gjOJlblyEzW1E=
mLbfRIQxtPVbZphUgAhWqMeuqa25Ale/5rz8vv9YVkc=
qIbJd0rViXaFpU2SvrkcezPlE/VtgXulMFWFUXmIBBg=
CbnHJiUmcb7bV3nHtVfkQJESWUzuF9spYS2HkpVPEQ4sOQCQUFomcsL6vpMTm+JY
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE

POSSIBLE SECRETS
WIPKXsZv2l0NBmLvWdV3TkucPJ5dkfbRYYrTASAxFfQ=
B3EEABB8EE11C2BE770B684D95219ECB
JHENilgoa32pdW2+FQZfbiKa1To+b6hAFc5hyxP6u/LWvHbIhkfTDC3kQMR4mpq3
m4uJd6hJYeAUgFAUB1OT370Awen8YINd4hKC7XM/6ec=
IWYMNwupvIr4nCzhi63Y96rPhOxZK2U2oV0yQU5ISOuxDdywn/U6CBTwu78HOm4H
IcH9chIM8pdQBP/eeaIVQOxIkEFtHwPKwBzAXjYRdyw5KOKrZsfN3FYxHItVH2IL
JQeYWB/Ar5LqSSZ5i6IhxYZ+uXn8SEDYL9xPjgGTx2M=
CYcH4LBpiH+KaEScKuk48/IbmIORuaeHTHx2iwUA0vRWrbIkTWIgIbVYJ8eozDwX
somG6HzRa3YZJrwwnfL6K8d6jP9Npv493BtTLjfx2vaqxDUDPiPCNzpi42Jpggs8
d4INySQwKXrFgcw/Yp0O6t4YGx7HF+F75DncE44LSIy22mr4UP50R657OPRB1jqZ
AemuwIJaLmYE+nU5fadET3FINkdby4LnWDkawsC9pWk=
5181942b9ebc31ce68dacb56c16fd79f
Q2oRzQFBrNQ6PISKRcfuekSxxMHiBiKCGVgSnsIVkCh9YR7J4L17zMBZU0VVyUEU

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030e060355040a1307416e64726f69643110300e060355040b1307 416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333 3635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550 408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030e060355040a1307416e64726f69643110300e060355040b1307 416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d 01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb 6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a 92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051 196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86 d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61 dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce1 44ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03 f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa4 8197308194310b300906035504061302555331133011060355040813 0a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030e060355040a1307416e64726f69643110300e060355040b1307 416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c06 03551d13040530030101ff300d06092a864886f70d01010405000382010100 19d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913 d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3 be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759 733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94 eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46 eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
PyZj3I+LGZvAhJ9n3OQrlENydgM2JwW0T6dRxf3as8iTDiIpqvAE/3692CSblz+3
F0+pSvx9GtXcjR12oFzzp5apK08MRky74lYez805WxvZBZTjFs672zxMax8w5kp9
2ZUgS25mCfmBpvNAAnoop42ZvK9H4E17vIqHMHWBgDSruAgpJ0/PRWhyN3sqcUbC
AtCF0F/Ugi3KOt6zYtgfLSsd+8KzXVTsnhwfj9NoYBY=
WQCGmUFTrgSOZ83nswxrNh39wVE6t1Ouq3E0zMLvIMA=
pY1LPqV65osROa0AkcabhXHjwpz5nP0HOapDW2QtdtU=

POSSIBLE SECRETS
bae8e37fc83441b16034566b
ZqqofhkB4+yK9ARzF+IbcECpWBtuTXlqWFDkC/AVdcM=
nK4MIXXv/sY+coqtAjalB6f9NiJ1zVnlRnfsJ++LIaOoNJXY+cpXhUK9rjjc0N2G
hvOzu3pRF2dcNdvDy8db1rttL97bOQyvLLd+NabZhD5sRaprNsAQL2vdtDd+eY16
Srq4/7DDafVhhxKPQvFzGwPCcbAxjsRhBUoTZMyZ8i1elMwCHCPiECib9I+dpg+U

PLAYSTORE INFORMATION

Title: Moodee: To-dos for your mood

Score: 4.7712765 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.bluesignum.little_lighthouse

Developer Details: □□□□□(BlueSignum Corp.), 8164671131301990059, None, None, moodee@bluesignum.com,

Release Date: Mar 2, 2023 **Privacy Policy:** Privacy link

Description:

Meet Moodee, your own little mood guide! Everyone has bad days. Find out how to manage your mood with Moodee. ■ Look back on your emotions Sometimes it’s hard to put a name to what you’re feeling. Research shows that simply labeling your emotion can be an immense help in dealing with it. In Moodee, you have access to a large variety of emotion tags that will help you identify exactly what you’re feeling in this moment. Make it a routine to reflect on your emotions and put time into understanding yourself better. ■ AI-recommended quests for your mood When you’re feeling overwhelmed by an emotion, it’s hard to think about what you should do to make it better. Whether you're feeling upbeat or low, Moodee will give you curated quest recommendations for how you can make your day better. Discover small to-dos and routines that you can try out right away. ■ In-depth analysis of your emotional records Check out detailed stats about you, from frequently recorded emotions to your to-do preferences. Get monthly and annual reports to gain deeper insights about yourself - and understand what you feel, what you like, and what you need. ■ Rewire your brain to think different with Training Do you have any thinking habits that make you feel bad? Neuroplasticity theory says that our brains can be rewired with repeated practice. With Moodee’s Training, you can go through various fictional scenarios and practice thinking in a different way - whether it be to be more optimistic, or feel less guilty on a daily basis. ■ Talk with animal friends in interactive Stories Various animal friends who are trapped in their stories have come to you for help! Listen to what they have to say, help them figure out what they need, and guide them to their happy ending. In the process, perhaps you’ll discover a piece of yourself in them. ■ Your most private emotion journal Build your own private and honest emotion journal, just by using Moodee daily. You can lock your Moodee app with a secure

passcode, so that no one but you will have access to your honest feelings. Feel free to say anything you want, anytime you want.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:25:31	Generating Hashes	OK
2025-08-29 20:25:32	Extracting APK	OK
2025-08-29 20:25:32	Unzipping	OK
2025-08-29 20:25:32	Parsing APK with androguard	OK
2025-08-29 20:25:33	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:25:33	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:25:35	Parsing AndroidManifest.xml	OK
2025-08-29 20:25:35	Extracting Manifest Data	OK

2025-08-29 20:25:35	Manifest Analysis Started	OK
2025-08-29 20:25:35	Reading Network Security config from network_security_config.xml	OK
2025-08-29 20:25:35	Parsing Network Security config	OK
2025-08-29 20:25:35	Performing Static Analysis on: Moodee (com.bluesignum.little_lighthouse)	OK
2025-08-29 20:25:35	Fetching Details from Play Store: com.bluesignum.little_lighthouse	OK
2025-08-29 20:25:35	Checking for Malware Permissions	OK
2025-08-29 20:25:35	Fetching icon path	OK
2025-08-29 20:25:35	Library Binary Analysis Started	OK
2025-08-29 20:25:35	Reading Code Signing Certificate	OK
2025-08-29 20:25:36	Running APKiD 2.1.5	OK
2025-08-29 20:25:41	Detecting Trackers	OK

2025-08-29 20:25:44	Decompiling APK to Java with JADX	OK
2025-08-29 20:25:56	Converting DEX to Smali	OK
2025-08-29 20:25:56	Code Analysis Started on - java_source	OK
2025-08-29 20:25:59	Android SBOM Analysis Completed	OK
2025-08-29 20:26:06	Android SAST Completed	OK
2025-08-29 20:26:06	Android API Analysis Started	OK
2025-08-29 20:26:11	Android API Analysis Completed	OK
2025-08-29 20:26:12	Android Permission Mapping Started	OK
2025-08-29 20:26:17	Android Permission Mapping Completed	OK
2025-08-29 20:26:18	Android Behaviour Analysis Started	OK

2025-08-29 20:26:25	Android Behaviour Analysis Completed	OK
2025-08-29 20:26:25	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:26:27	Email and URL Extraction Completed	OK
2025-08-29 20:26:27	Extracting String data from APK	OK
2025-08-29 20:26:27	Extracting String data from Code	OK
2025-08-29 20:26:27	Extracting String values and entropies from Code	OK
2025-08-29 20:26:30	Performing Malware check on extracted domains	OK
2025-08-29 20:26:35	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.