MOBSF

ANDROID STATIC ANALYSIS REPORT

Instagram Lite (475.0.0.15.104)

File Name:	instagramlite.apk

Package Name:	com.instagram.lite
Scan Date:	Sept. 6, 2025, 4:11 a.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	34	2	5	1

FILE INFORMATION

File Name: instagramlite.apk
Size: 3.11MB
MD5: 296e623e1ab7aea092d5bc9eeec7f841
SHA1: 916466795b124e7d878cc34f429a98275e91cfdd
SHA256: aeba7972e8c33c73821d5edc6d606bcf09ed842acc1a5264a184c49b68dde015

APP INFORMATION

App Name: Instagram Lite
Package Name: com.instagram.lite
Main Activity: com.facebook.lite.MainActivity
Target SDK: 35
Min SDK: 26
Max SDK:
Android Version Name: 475.0.0.15.104
Android Version Code: 787434609

APP COMPONENTS

Activities: 13
Services: 39
Receivers: 38
Providers: 11
Exported Activities: 6

Exported Services: 2
Exported Receivers: 11
Exported Providers: 6

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=California, L=San Francisco, O=Instagram Inc, CN=Kevin Systrom
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-02-08 01:41:31+00:00
Valid To: 2112-01-15 01:41:31+00:00
Issuer: C=US, ST=California, L=San Francisco, O=Instagram Inc, CN=Kevin Systrom
Serial Number: 0x4f31d2cb
Hash Algorithm: sha1
md5: f9cf2124dfaaccc45e7e3f739eca55ae
sha1: c56fb7d591ba6704df047fd98f535372fea00211
sha256: 5f3e50f435583c9ae626302a71f7340044087a7e2c60adacfc254205a993e305
sha512: a9b31009987e094fd2067d385056adfdb2cc4a272814a5982343335e639d064943e6025cbc7e36903f065c0e65bd99adab538dd0377c1404fa48b508970354a8
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: db2a9e7d36fb6915a995ee367d8971aca6f268c7b67e910b8431eeb636061c72
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.facebook.lite.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.facebook.katana.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.facebook.orca.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.facebook.mlite.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.facebook.wakizashi.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.
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.
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.
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	signature	required by NotificationListenerServices for system binding.	Must be required by an NotificationListenerService, to ensure that only the system can bind to it.
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	normal	allows foreground services for media projection.	Allows a regular application to use Service.startForeground with the type "mediaProjection".
android.permission.CREDENTIAL_MANAGER_SET_ALLOWED_PROVIDERS	normal	allows specifying candidate credential providers.	Allows specifying candidate credential providers to be queried in Credential Manager get flows, or to be preferred as a default in the Credential Manager create flows.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RUN_USER_INITIATED_JOBS	normal	allows using the user-initiated jobs API.	Allows applications to use the user-initiated jobs API. For more details see JobInfo.Builder.setUserInitiated(boolean) .
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.instagram.lite.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from 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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.lite.MainActivity	Schemes: http://, https://, iglite://, Hosts: instagram.com, www.instagram.com, applink.instagram.com, familycenter.instagram.com, ig.me, Mime Types: text/plain,
com.facebook.lite.loginWithFacebook.wrapper.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.instagram.lite,
com.instagram.lite.deeplinking.activities.E2EActivityAlias	Schemes: http://, https://, e2e://, instagram://,

NETWORK SECURITY

HIGH: 4 | WARNING: 1 | INFO: 1 | SECURE: 2

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

NO	SCOPE	SEVERITY	DESCRIPTION
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.
4	*	high	Base config is configured to bypass certificate pinning.
5	facebook.com fbcdn.net fbsbx.com facebookcorewwwi.onion fbcdn23dssr3jqnq.onion fbsbx2q4mvcl63pw.onion instagram.com cdninstagram.com workplace.com oculus.com facebookvirtualassistant.com discoverapp.com freebasics.com internet.org viewpointsfromfacebook.com meta.com h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

NO	SCOPE	SEVERITY	DESCRIPTION
6	facebook.com fbcdn.net fbsbx.com facebookcorewwwi.onion fbcdn23dssr3jqnq.onion fbsbx2q4mvcl63pw.onion instagram.com cdninstagram.com workplace.com oculus.com facebookvirtualassistant.com discoverapp.com freebasics.com internet.org viewpointsfromfacebook.com meta.com h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	info	Certificate pinning expires on 2026-08-27. After this date pinning will be disabled. [Pin: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= Digest: SHA-256,Pin: ICGRfpgmOUXIWcQ/HXPLQTkFPEFPoDyjvH7ohhQpjzs= Digest: SHA-256,Pin: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME= Digest: SHA-256,Pin: 58qRu/uxh4gFezqAcERupSkRYBlBAvfcw7mEjGPLnNU= Digest: SHA-256,Pin: r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E= Digest: SHA-256,Pin: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY= Digest: SHA-256,Pin: uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc= Digest: SHA-256,Pin: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18= Digest: SHA-256,Pin: Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw= Digest: SHA-256,Pin: ape1HIIZ6T5d7GS61YBs3rD4NVvkfnVwELcCRW4Bqv0= Digest: SHA-256,Pin: oC+voZLly4HLE0FVT5wFtxzKKokLDRKY1oNkfJYe+98= Digest: SHA-256,Pin: K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q= Digest: SHA-256,Pin: cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A= Digest: SHA-256,Pin: aCdH+LpiG4fN07wpXtXKvOciocDANj0daLOJKNJ4fx4= Digest: SHA-256,Pin: rn+WLLnmp9v3uDP7GPqbcaiRdd+UnCMrap73yz3yu/w= Digest: SHA-256,Pin: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= Digest: SHA-256,Pin: diGVwiVYbubAI3RW4hB9xU8e/CH2GnkuvVFZE8zmgzI= Digest: SHA-256,Pin: q4PO2G2cbkZhZ82+JgmRUyGMoAeozA+BSXVXQWB8XWQ= Digest: SHA-256]
7	h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.
8	h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. []

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **27** | 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/fb_network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Broadcast Receiver (com.facebook.lite.pretos.LiteAppComponentReceiver) 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.facebook.lite.rtc.IncomingCallReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.facebook.lite.campaign.CampaignReceiver) 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
6	Broadcast Receiver (com.facebook.lite.appManager.AppManagerReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.facebook.lite.deviceid.FbLitePhoneIdRequestReceiver) 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 (com.facebook.appupdate.DownloadCompleteReceiver) 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	Content Provider (com.facebook.lite.deviceid.FbLitePhoneIdProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Broadcast Receiver (com.facebook.lite.FbnsIntentService$CallbackReceiver) 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.
11	Broadcast Receiver (com.facebook.rti.push.service.MqttSystemBroadcastReceiver) 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.
12	Content Provider (com.facebook.lite.photo.MediaContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Content Provider (com.facebook.lite.diode.UserValuesProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Content Provider (com.facebook.lite.diode.LiteUserValuesProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Content Provider (com.facebook.lite.metainstallreferrer.InstallReferrerProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	Content Provider (com.facebook.lite.partneranalytics.LastUsedTimestampProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Broadcast Receiver (com.facebook.lite.waotp.WAOtpCodeReceiver) 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.
18	Broadcast Receiver (com.facebook.oxygen.preloads.sdk.firstparty.managedappcache.IsManagedAppReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.facebook.appmanager.ACCESS [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.
19	Service (com.facebook.secure.packagefinder.PackageFinderService) 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.
20	Activity (com.facebook.lite.loginWithFacebook.wrapper.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
21	Activity-Alias (com.instagram.lite.stories.activities.ShareToIgStoriesAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias 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
22	Activity-Alias (com.instagram.lite.stories.activities.ShareToIgFeedAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
23	Activity-Alias (com.instagram.lite.deeplinking.activities.E2EActivityAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
24	Activity-Alias (com.instagram.lite.stories.activities.ShareToIgChatsAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
25	Activity-Alias (com.instagram.lite.stories.activities.ShareTextToIgChatsAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
26	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.
27	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
28	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **4** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	X/AnonymousClass043.java X/AnonymousClass044.java X/C015606r.java X/C0BF.java X/C0BQ.java X/C0CN.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	X/AbstractC004101r.java X/AbstractC02330Ao.java X/AnonymousClass000.java X/AnonymousClass008.java X/AnonymousClass022.java X/AnonymousClass086.java X/AnonymousClass094.java X/C008503p.java X/C02230Ad.java X/C02320An.java X/C02350Aw.java X/C02590By.java X/C02600Bz.java X/C02Y.java X/C05A.java X/C06N.java X/C07R.java X/C08S.java X/C09R.java X/C0AM.java X/C0AX.java X/C0AY.java X/C0AZ.java X/C0B3.java X/C0BH.java X/C0C0.java X/C0C6.java X/C0CF.java X/JobServiceEngineC005002a.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	X/AnonymousClass079.java X/C02C.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	X/AnonymousClass054.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	X/C00S.java X/C020309b.java
6	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	X/C004701x.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libsuperpack-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__strncpy_chk', '__strchr_chk', '__fgets_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libbreakpad_cpp_helper.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libsuperpack-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__strncpy_chk', '__strchr_chk', '__fgets_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libbreakpad_cpp_helper.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	X/AnonymousClass061.java X/C02M.java
00013	Read file and put it into a stream	file	X/AnonymousClass040.java X/C007103a.java X/C02430Bh.java X/C02570Bw.java X/C05C.java X/C0BH.java X/C0C2.java X/C0CO.java X/C0CY.java
00028	Read file from assets directory	file	X/C0AM.java
00079	Hide the current app's icon	evasion	X/C07R.java
00121	Create a directory	file command	X/C07R.java
00004	Get filename and put it to JSON object	file collection	X/C0BJ.java
00162	Create InetSocketAddress object and connecting to it	socket	X/C09K.java
00163	Create new Socket and connecting to it	socket	X/C09K.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	X/C004701x.java X/C015606r.java X/C08P.java X/C0CO.java
00108	Read the input stream from given URL	network command	X/C04C.java
00012	Read data and put it into a buffer stream	file	X/C0CO.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/622912139302/namespaces/firebase:fetch?key=AIzaSyBWJZPw7wVi-NQEViQV9ZnadO-xbX4S8o0. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	16/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.GET_TASKS, android.permission.INTERNET, android.permission.READ_CONTACTS, android.permission.GET_ACCOUNTS, android.permission.READ_PHONE_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	15/44	android.permission.BATTERY_STATS, android.permission.BROADCAST_STICKY, android.permission.CALL_PHONE, android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.READ_CALENDAR, android.permission.AUTHENTICATE_ACCOUNTS, android.permission.WRITE_CONTACTS, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.BLUETOOTH, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.c2dm.permission.RECEIVE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID

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
www.facebook.com	ok	**IP:** 57.144.210.1 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.android.com	ok	**IP:** 142.250.192.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.instagram.com	ok	**IP:** 57.144.210.34 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
www.instagram.com	ok	**IP:** 57.144.210.34 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
instagram.com	ok	**IP:** 57.144.210.34 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBWJZPw7wVi-NQEViQV9ZnadO-xbX4S8o0"
RdBiQjfrXe1WnMMVVkuOoFfs8ri2eE
grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME=
aCdH+LpiG4fN07wpXtXKvOciocDANj0daLOJKNJ4fx4=
uSEJtZCVlVzKr17Lzw8VPslkCkZYwQFmetlrfkmaQJI
OaxNl9DzmpbAu1HcjBRq8oUlJBWeTEWmnftIpuLE0dY
sXPIxiZ1lvokCdbRCr64p0GHvtNvywjWNQmqJtqWw8Q
q4PO2G2cbkZhZ82+JgmRUyGMoAeozA+BSXVXQWB8XWQ=
rAusqYUIziLdH2vjRhJ9iPN8Axi1QIsEeksvpaPpywQ
zOWEMoPwpWBrD6z29z73mJHEioIOhPgR4ARENbOXnqI
rn+WLLnmp9v3uDP7GPqbcaiRdd+UnCMrap73yz3yu/w=
TuZz0WoA2PmrHxH826GLPqgB5xYhKwTR5X17cEgDRQI
diGVwiVYbubAI3RW4hB9xU8e/CH2GnkuvVFZE8zmgzI=
pA2oClnRcMqpUM8VwYxFTUejmyaYnYtkDs10W6cb9dw
i1R0ZwdXk2ev6WLsW1iXdNyytsuVi570wNd9O6D5wkA
k8zj7LE9R9iJ9bvvO2LLaoRUGkvMadXC5EX8RBVKE8w
RKhpUi1Kl9bHcO1rS0FHy3ICrjOO2X6k5yEm

POSSIBLE SECRETS
F5OoLdx6B8GGOezxJY0QifKgn3FjXCyp54J8bPv3yfI
jriiCfLl5AQq3PaWv3Uemavb2hMrZhZ
he7AWhFEJyHnLDw6N74RdhwQXHsJRDBZvQMCNgOUEgQ
ykG4fdbRb6a4ItrViJAx0l43fmUg0SW4BmU
ICGRfpgmOUXIWcQ/HXPLQTkFPEFPoDyjvH7ohhQpjzs=
oC+voZLIy4HLE0FVT5wFtxzKKokLDRKY1oNkfJYe+98=
jYWbZ4GQZ28iGykpgUFoIDlGPXHb2sIWpDljhlYw
3Occv5K3fs6f4TMEZqQMaEPOi26G1HRcRTaiMhLfbVg
uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc=
VSIRoP8NGnYBLRTCCPi6M3OQd3ZJc
UiFEC5uxJuxVHjWkQvUXlGYGiGgpCQd79NeuopUpcNU
gyMW5OL1dZSW0Hc2scNB9rSHSjgMRWYEf7gkZrysotY
1RBv0Am3VA2bLMifS4uOCNDeaKSVc7CU
AuYCk4ZRoWy5MJTr4GmbZSKv7vsGVtVR2oLiOKKp3qs
K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q=
vybElaK24hv56tyQiWFXmLmGbCmgTEF57lU
azGZDq3U2OPfsFdCgajvtrlaIKOQ8GSkAr92TLKbcjs

POSSIBLE SECRETS
9lujZx6JrDrZ5oYGBEroEyiA2x7wdavEUslqzXHMBoc
7oVvh3Fck1xX0J5u42DHceCqMyIqewU2TWaJlChTsZA
czD7n7zbifyJ6snZ1K5ViS5Gks5u2c9zL7OHrb0w
Xz5Q9DVYPJrmJjAqcfc0AEQIen4sYK2s
W1BzWTPVNZBtrA45RvTcbkVphwqyUdZwQEL7X
ztXcjgEmmxMKYWXyXR1OtAW6codwAh6kiOzYzpxMCM4
rbPBrH2K54ycBnaWuvI8pTxd7CIb
QNc4oAwpdTOEIfpXWujgRZDGvKl0dunabP0fAVcI
HC4rwCH0AxqzQcvYDrHg5ikHBl2GnUuRnJLwuJJyt8o
ZWkE4zW88gcERR0YSGDghDZDer3EdbcpWmloH7l3
WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=
62Yjx8iYhpF3VA6BQQvyUObpLzjXx0Gs5PEm1cLJaf4
Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw=
cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A=
5T7TTXxkmQH5fdzat3ewWNAAuwHC9eF2
4dJKibgNvwschNsyH9YBK3Hwl5zTIkQlBgZu10E
Jm4bl26QMphvIVgzVUeQb6f37Ys3IKRmCw0LBgLJBzs

POSSIBLE SECRETS
58qRu/uxh4gFezqAcERupSkRYBlBAvfcw7mEjGPLnNU=
2eC54WVokOBCMfraLI5w5AkPzV4OhG2rUnfhWHKBM0M
jNOc7mDzYOmJnDzPufesFxNPsjV4IeXH4tjnjOCHkUA
ZjFWitD4QhI3DDX7jC4kAdDOffGgtI0Kqf0Mg71Nkzs
ui1sfL4sZoq87KETlWIIg1GPbvD5YRhwq73X28NIPXA
MCluzmTgXDuTHyG9AnpK6nb1ffPe
XdkQEeiVeIyDkvBEAHtGJKKHfdsrOFf9te68UpyJVhA
ape1HIIZ6T5d7GS61YBs3rD4NVvkfnVwELcCRW4Bqv0=
jJXMpyOWBPAVUW5TdC0UOQCtSXS0dPbHY00jE7I1oqg
DBauJfiBkYkRdrNvtqHVxpa5W1kE4QhelLDRkQ7Syv8
BHW1qv5BLCwc378Tf0pJ6g2Mrz6xkMRE
BhbXF71VGdruXI2K92clfscrAA8xTQxV0mTVQSyTzJM
j7DW1GBqpKusFNd9HZfVNAhgyfgQRaoVc
ovbQAw7LTrM4PSNadgRBwp4vfR5ma3mkb1x
QH5XpDABqOLMQmPoU1yYkDqj4encoo
b2sRSFyeAdgq4NbTDsF6EuDfHreyS9x2Pp7oKe8QcII
6PDrONEnh3P7htSccijrhAA8B9sXJeGvGHy

POSSIBLE SECRETS
oSjSY8pqhXpum64U6nRyis9rV9XfVU3BgyBK6ru6RS8
Y5Hqye7Bbux7I1qFFmbE6EqILj2ssTFQB9Ss6LwpmGE
5MCO54QyiJ31mua72pgMV7lET8XxQmxVGsxMmN3dAkA
ilevJuB7FM2hbqbNvEalC0sSLlEcDgidA6sgzc
3zm83GueFdZc03peMLTszjjIs7veieqaGSvqMt6075s
tLXzXE27lXmkgnQiBquXXJL69T1ZBOt8Uk2MjhDs
uMnSimFvgxSFwj8TbauRsJHJmqA9ylcIGiXRTzvBn6E
YdNexVtjCN6dzf64Ix6i9ToxImvIA8AL7NhSaND5tpE
2v68LjdrY5QoGvulTHKywirmgTy2Oe
sFuP1YxKZhUvSVD07qxH67dGzFAoeykLoFN3PHnQbsc
C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
j6dyXYfIkddeJxE4pzmilaZ2S4qYC9CwaCMxfzg1zTY
ZiIZ7fdUdXcbGMNL6M656x4mTCC9kdSoSNBOifLrBAA
TMinTbXc5WFYgsXN8isdVqC2EACEZpcdz5s7I1bO
oXiTMLDip81kTvgXrtXtypfecxU3vmuNPlCfkOM
qadsRSPy8q2oOtZucRAyNlbBCyrbDQYWnD6ZESwR0vs

PLAYSTORE INFORMATION

Title: Instagram Lite

Score: 4.3693547 **Installs:** 500,000,000+ **Price:** 0 **Android Version Support:** **Category:** Social **Play Store URL:** com.instagram.lite

Developer Details: Instagram, Instagram, None, http://help.instagram.com/, android-lite-support@instagram.com,

Release Date: None **Privacy Policy:** Privacy link

Description:

Instagram Lite from Meta is a fast and smaller version of Instagram. Built to perform well on slower networks, use less mobile data and take up less storage space on your phone, Instagram Lite makes it easier to bring yourself closer to the people and things you love. Express yourself and connect with people over creative moments. See pictures, videos, and stories from friends and creators you love *Follow your friends, favorite artists, brands and creators on Instagram to see what they're sharing in your Feed. Join the conversation and see more of what you love when you like, comment and share the content you discover. Unlock creativity and endless entertainment with Reels *Watch and easily create fun, entertaining videos to share with friends or anyone on Instagram. Create multi-clip videos up to 90 seconds, and get creative with easy-to-use text, templates and music. Upload videos from your gallery, too. Share your everyday moments with Stories *Add photos and videos to your story that disappear after 24 hours, and bring them to life with fun creative tools. Use text, music, stickers and GIFs to bring your story to life. Make your story interactive for friends and followers by adding the Questions or Poll stickers. Message your friends in Direct *Start conversations about what you see on Reels, Feed and Stories. Send messages to your friends, share posts privately, and receive chat notifications. Connect with friends no matter where you are with video and audio calls. Search and Explore Instagram to find more things you love *See more of what interests you in the Search tab. Find interesting photos, reels, accounts, and more. Search by keywords to explore topics and find content and creators related to your interests. By clicking Install, you agree to the Terms of Use (https://help.instagram.com/581066165581870/) and Privacy Policy (https://help.instagram.com/519522125107875/).

SCAN LOGS

Timestamp	Event	Error
2025-09-06 04:11:32	Generating Hashes	OK
2025-09-06 04:11:32	Extracting APK	OK
2025-09-06 04:11:32	Unzipping	OK

2025-09-06 04:11:32	Parsing APK with androguard	OK
2025-09-06 04:11:32	Extracting APK features using aapt/aapt2	OK
2025-09-06 04:11:32	Getting Hardcoded Certificates/Keystores	OK
2025-09-06 04:11:35	Parsing AndroidManifest.xml	OK
2025-09-06 04:11:35	Extracting Manifest Data	OK
2025-09-06 04:11:35	Manifest Analysis Started	OK
2025-09-06 04:11:35	Reading Network Security config from fb_network_security_config.xml	OK
2025-09-06 04:11:35	Parsing Network Security config	OK
2025-09-06 04:11:35	Performing Static Analysis on: Instagram Lite (com.instagram.lite)	OK
2025-09-06 04:11:36	Fetching Details from Play Store: com.instagram.lite	OK
2025-09-06 04:11:36	Checking for Malware Permissions	OK
2025-09-06 04:11:36	Fetching icon path	OK

2025-09-06 04:11:36	Library Binary Analysis Started	OK
2025-09-06 04:11:36	Analyzing apktool_out/lib/arm64-v8a/libsuperpack-jni.so	OK
2025-09-06 04:11:36	Analyzing apktool_out/lib/arm64-v8a/libbreakpad_cpp_helper.so	OK
2025-09-06 04:11:36	Analyzing lib/arm64-v8a/libsuperpack-jni.so	OK
2025-09-06 04:11:36	Analyzing lib/arm64-v8a/libbreakpad_cpp_helper.so	OK
2025-09-06 04:11:36	Reading Code Signing Certificate	OK
2025-09-06 04:11:36	Running APKiD 3.0.0	OK
2025-09-06 04:11:38	Detecting Trackers	OK
2025-09-06 04:11:39	Decompiling APK to Java with JADX	OK
2025-09-06 04:11:49	Converting DEX to Smali	OK
2025-09-06 04:11:49	Code Analysis Started on - java_source	OK
2025-09-06 04:11:50	Android SBOM Analysis Completed	OK

2025-09-06 04:11:52	Android SAST Completed	OK
2025-09-06 04:11:52	Android API Analysis Started	OK
2025-09-06 04:11:53	Android API Analysis Completed	OK
2025-09-06 04:11:53	Android Permission Mapping Started	OK
2025-09-06 04:12:05	Android Permission Mapping Completed	OK
2025-09-06 04:12:05	Android Behaviour Analysis Started	OK
2025-09-06 04:12:07	Android Behaviour Analysis Completed	OK
2025-09-06 04:12:07	Extracting Emails and URLs from Source Code	OK
2025-09-06 04:12:08	Email and URL Extraction Completed	OK
2025-09-06 04:12:08	Extracting String data from APK	OK
2025-09-06 04:12:08	Extracting String data from SO	OK
2025-09-06 04:12:08	Extracting String data from Code	OK

2025-09-06 04:12:08	Extracting String values and entropies from Code	OK
2025-09-06 04:12:08	Performing Malware check on extracted domains	OK
2025-09-06 04:12:10	Saving to Database	OK

Report Generated by - MobSF v4.4.2

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.