MASTODON GENERATED: 2026-07-07

com.facebook.lite

com.facebook.lite@518.0.0.8.104.apk

Application Overview

File name	com.facebook.lite@518.0.0.8.104.apk
Package name	com.facebook.lite
Version	518.0.0.8.104 (515401105)
SHA-256	`07545cafce707b64596f82d07ea5c30a8caed784d81edfdcc5f0454d86d39ef3`
Analysis duration	8 min 19 s

About MASTodon

This is an early-stage **MAST**odon demo report. It runs a selected suite of 7 MASTG tests focused on sensitive-data exposure and resilience signals, chosen to show how **MAST**odon can automatically drive mobile app security testing. Our roadmap extends this toward fully automated, standards-compliant coverage of the entire MASTG catalog that is ready to drop into your CI/CD pipeline, steadily raising coverage and evidence confidence while keeping every finding clear and reproducible.

This MASTG report is grounded in the OWASP Mobile Application Security (MAS) project and the OWASP Mobile Application Security Testing Guide (MASTG). The MASTG tests presented here are based on that open-source body of work: https://mas.owasp.org/. vulnit collaborates with the OWASP MAS project and actively supports its continued development as advocates.

What you get. **MAST**odon builds on vulnit's core strengths in automated mobile security testing. For each test, a clear verdict backed by reproducible, evidence-linked observations: **MAST**odon pairs static analysis and reverse engineering, which surface code references, SDK usage and behaviors worth testing, with dynamic exploration in which an AI agent drives the app autonomously, with no human tester in the loop. The agent runs the application inside orchestrated virtual mobile sandboxes capable of handling hundreds of isolated devices at the same time, injecting tagged test values and tracking them across runtime logs, network traffic (plain and encrypted), API references and syscalls.

How to read it. Results apply only to the selected scope above and to the app flows our AI agent actually reached. The agent grows more capable every day and, for this demo, necessarily runs under a deliberately limited exploration budget (we're a bootstrapped startup, baby!). Contact us to learn more about the present and planned capabilities of our mobile security testing tools!

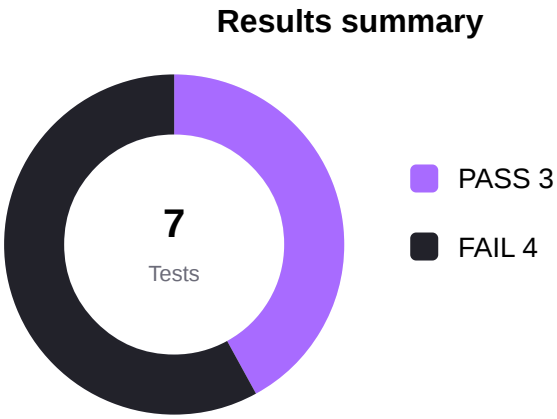
You Ship. We Hack. Repeat.

Executive Summary

com.facebook.lite was assessed against a focused mobile security scope centered on storage, network, and resilience behaviors, alongside the exercised login-and-post user flow. The review produced four failed outcomes and no review items. The failed outcomes were associated with logging references, cleartext network traffic, and runtime root-detection and hook-detection techniques. No verified pass outcomes were recorded, and no inconclusive outcomes were recorded. The combination of these results points to specific behaviors that merit customer attention, while the remaining checked areas were observed during the run without producing additional recorded issues.

The recorded failures indicate behaviors that can expose operational or privacy-relevant risk in specific conditions. Logging references can point to paths where sensitive data may be written to logs if those code paths are reached. Cleartext traffic observed on the network shows data leaving the app without transport protection in at least one exercised path. The runtime detection of root and hook techniques shows the app actively probes the device or runtime environment for those conditions, which is relevant to resilience assessment. These outcomes do not by themselves establish impact across all usage, but they do identify concrete areas that warrant follow-up review and validation.

Exploration covered the sign-in path with the provided credentials, confirmation of the logged-in identity, return to the home feed, creation of a post using the requested text, and confirmation that the post appeared in the feed after submission. The run reached the intended end state without blockers. One limitation is that there was no direct in-app success dialog after posting; confirmation relied on the feed update immediately after submission. The summary therefore reflects the observed application path and the evidence gathered during that execution, not broader behavior beyond the exercised screens.

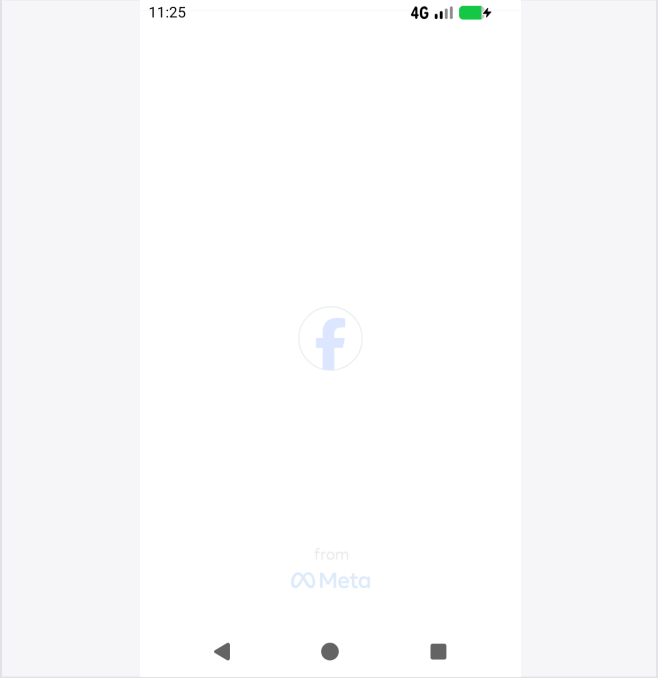


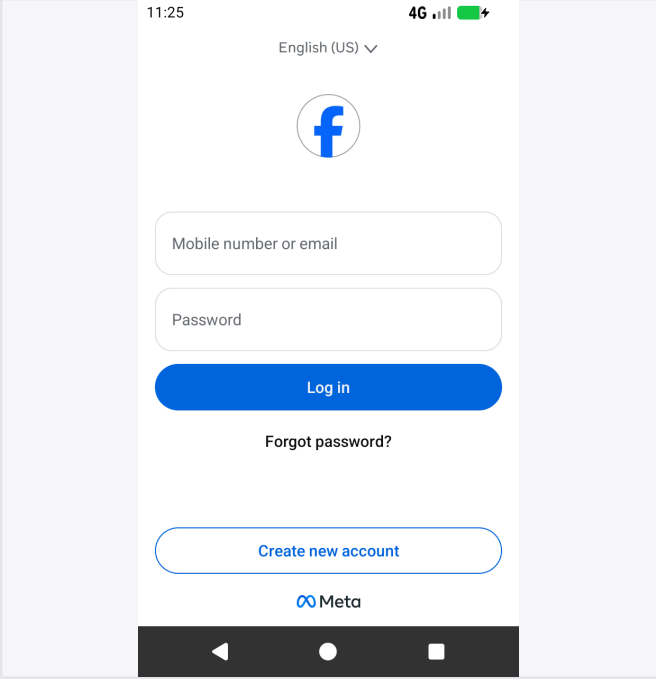
App Exploration

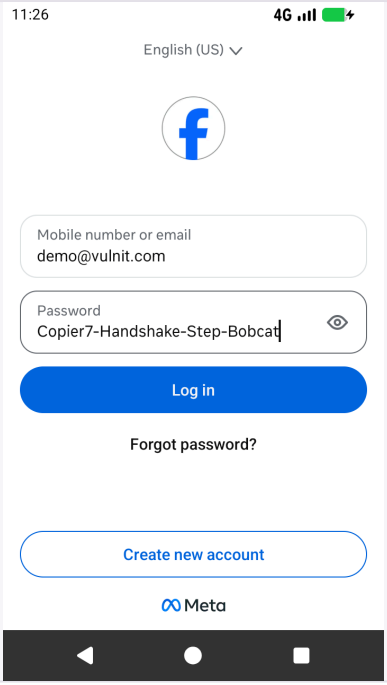
During the analysis, our agent exercised the available app screens and flows trying to reach as much functionality as possible. The observations below summarize the behavior captured during that exploration.

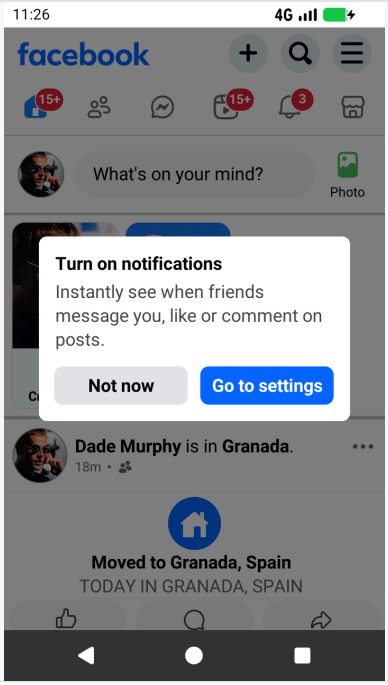
- The Facebook Lite login screen shows the email field filled with demo@vulnit.com and the password field filled with the provided password before login is tapped.
- A post-login prompt appears, indicating the account has successfully signed in and reached the logged-in app flow.
- The home feed is visible in com.facebook.lite, and the user profile/page area shows the name Dade Murphy.
- The profile/post view header reads Your post and shows the author name Dade Murphy, confirming the logged-in user's own profile identity.
- The create post screen contains the exact text MASTodon is so cool! and the POST button is tapped to submit it.
- Back on the home feed, a new feed item by Dade Murphy marked Just now displays the exact post text MASTodon is so cool!, which is strong evidence that the post was successfully submitted.

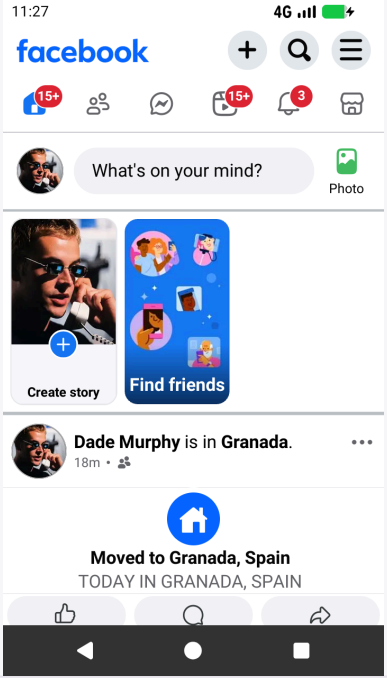
Relevant exploration screenshots

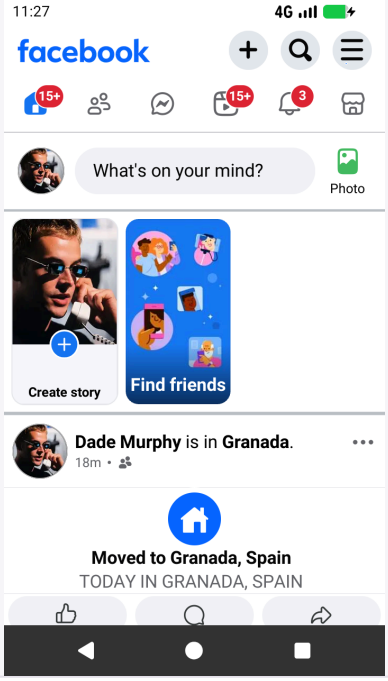


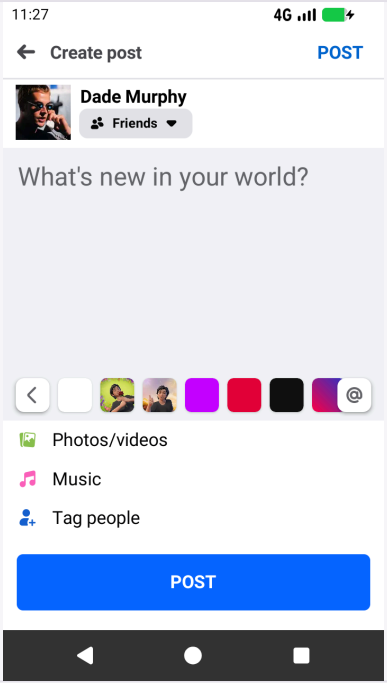


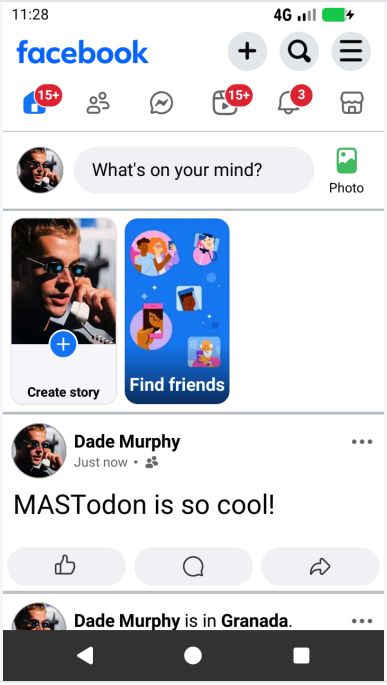

11:26
4G
English (US)
Mobile number or email
demo@vulnit.com
Password
Copier7-Handshake-Step-Bobcat
Log in
Forgot password?
Create new account
Meta


11:26
4G
facebook
What's on your mind?
Photo
Turn on notifications
Instantly see when friends message you, like or comment on posts.
Not now
Go to settings
Dade Murphy is in Granada.
18m
Moved to Granada, Spain
TODAY IN GRANADA, SPAIN


11:27
4G
facebook
What's on your mind?
Photo
Create story
Find friends
Dade Murphy is in Granada.
18m
Moved to Granada, Spain
TODAY IN GRANADA, SPAIN


11:27
4G
facebook
What's on your mind?
Photo
Create story
Find friends
Dade Murphy is in Granada.
18m
Moved to Granada, Spain
TODAY IN GRANADA, SPAIN


11:27
4G
Create post
POST
Dade Murphy
Friends
What's new in your world?
Photos/videos
Music
Tag people
POST


11:28
4G
facebook
What's on your mind?
Photo
Create story
Find friends
Dade Murphy
Just now
MASTodon is so cool!
Dade Murphy is in Granada.

Test Summary

MASTG test verdicts

TEST ID	TITLE	VERDICT
MASTG-TEST-0203	Runtime Use of Logging APIs	PASS
MASTG-TEST-0206	Undeclared PII in Network Traffic Capture	PASS
MASTG-TEST-0231	References to Logging APIs	FAIL
MASTG-TEST-0236	Cleartext Traffic Observed on the Network	FAIL
MASTG-TEST-0318	References to SDK APIs Known to Handle Sensitive User Data	PASS
MASTG-TEST-0325	Runtime Use of Root Detection Techniques	FAIL
MASTG-TEST-0341	Runtime Use of Hook Detection Techniques	FAIL

Detailed Test Results

MASTG-TEST-0203 — Runtime Use of Logging APIs

MASVS	STORAGE
LEVEL	L1
REFERENCE	https://mas.owasp.org/MASTG/tests/android/MASVS-STORAGE/MASTG-TEST-0203/
VERDICT	PASS

During the run, the app is exercised with synthetic values for email, password, name, phone number, and other sensitive values. This test looks for those values in runtime logs, where sensitive app input can be exposed through Logcat, crash reports, or support diagnostics.

No evidence of non-compliance was identified within the scope of this analysis.

MASTG-TEST-0206 — Undeclared PII in Network Traffic Capture

MASVS	PRIVACY
LEVEL	L1
REFERENCE	https://mas.owasp.org/MASTG/tests/android/MASVS-PRIVACY/MASTG-TEST-0206/
VERDICT	PASS

During the run, synthetic personal-data values are submitted through app workflows. This test checks captured network traffic for those values to identify transmitted credentials, contact details, phone numbers, or location-like data for privacy and data-disclosure review.

No evidence of non-compliance was identified within the scope of this analysis.

MASTG-TEST-0231 — References to Logging APIs

MASVS	STORAGE
LEVEL	L1
REFERENCE	https://mas.owasp.org/MASTG/tests/android/MASVS-STORAGE/MASTG-TEST-0231/
VERDICT	FAIL

This test performs taint analysis to trace data from sensitive sources such as text fields, account data, location APIs, cookies, shared preferences, and cryptographic material into Android, Java, or standard-output logging calls. It highlights code paths where secrets or personal data can be written to logs.

Log flow

DATA SOURCE	LOG SINK
android.content.SharedPreferences.getString	android.util.Log.e
android.content.SharedPreferences.getString	android.util.Log.w

MASTG-TEST-0236 — Cleartext Traffic Observed on the Network

MASVS	NETWORK
LEVEL	L1
REFERENCE	https://mas.owasp.org/MASTG/tests/android/MASVS-NETWORK/MASTG-TEST-0236/
VERDICT	FAIL

This test identifies unencrypted HTTP requests or responses generated by the app. Cleartext communication can expose content and metadata to local networks or intermediaries and allows traffic to be read or modified in transit.

Network

TRANSPORT	APPLICATION	DESTINATION ENDPOINT	DESTINATION PORT
TCP	HTTP	57.144.238.141 (edge-star-shv-01-lhr6.facebook.com)	80
TCP	HTTP	57.144.238.1 (edge-star-mini-shv-01-lhr6.facebook.com)	80

MASTG-TEST-0318 — References to SDK APIs Known to Handle Sensitive User Data

MASVS	PRIVACY
LEVEL	N/A
REFERENCE	https://mas.owasp.org/MASTG/tests/android/MASVS-PRIVACY/MASTG-TEST-0318/
VERDICT	PASS

This test finds calls to analytics and tracking SDK APIs that commonly receive user identifiers, user properties, behavioral events, and other privacy-relevant telemetry. It highlights places where app activity or user attributes can be shared with third-party services.

No evidence of non-compliance was identified within the scope of this analysis.

MASTG-TEST-0325 — Runtime Use of Root Detection Techniques

MASVS	RESILIENCE
LEVEL	N/A
REFERENCE	https://mas.owasp.org/MASTG/tests/android/MASVS-RESILIENCE/MASTG-TEST-0325/
VERDICT	FAIL

This test looks for runtime probes of rooted-device indicators such as su binaries, Magisk paths, and superuser packages. These probes show that the app checks whether it is running in a modified or privileged Android environment.

The analysis did not identify evidence that the expected behavior was implemented within the exercised scope.

MASTG-TEST-0341 — Runtime Use of Hook Detection Techniques

MASVS	RESILIENCE
LEVEL	N/A
REFERENCE	https://mas.owasp.org/MASTG/tests/android/MASVS-RESILIENCE/MASTG-TEST-0341/
VERDICT	FAIL

This test looks for runtime probes of high-confidence hook and instrumentation artifacts, including Frida, Frida Gadget, Xposed-family frameworks, and Cydia Substrate. These probes show that the app checks for tools commonly used to hook, inspect, or alter application behavior at runtime.

The analysis did not identify evidence that the expected behavior was implemented within the exercised scope.

Runtime Telemetry

During automated exploration, MASTodon continuously records runtime telemetry that supports security analysis beyond individual test cases. The metrics below summarize artifacts collected while the application was exercised, including network activity, system calls, logs, and the most active communication channels. These observations provide additional context for understanding application behavior during the analysis run.

Runtime Summary

METRIC	VALUE
Incoming network traffic	6.9 MB (11.6 MB decrypted)*
Outgoing network traffic	143.0 KB (94.8 KB decrypted)*
Syscalls analyzed	287151
Log entries analyzed	7705

*Traffic successfully decrypted during analysis

Top 10 Communication Endpoints By Data Volume

ENDPOINT	TRAFFIC
57.144.238.128 (xx-fbcdn-shv-01-lhr6.fbcdn.net)	In: 2.4 MB Out: 22.2 KB
57.144.238.6 (edge-z-m-mini-shv-01-lhr6.facebook.com)	In: 1.3 MB Out: 7.3 KB
57.144.238.129 (edge-video-shv-01-lhr6.fbcdn.net)	In: 1015.1 KB Out: 19.4 KB
57.144.238.2 (edge-fblite-tcp-mini-shv-01-lhr6.facebook.com)	In: 645.7 KB Out: 49.8 KB
157.240.214.36 (edge-z-m-mini-shv-02-lhr8.facebook.com)	In: 558.3 KB Out: 1.7 KB
163.70.151.33 (edge-z-m-mini-shv-02-lhr6.facebook.com)	In: 467.2 KB Out: 1.7 KB
57.144.62.6 (edge-z-m-mini-shv-01-lhr11.facebook.com)	In: 411.8 KB Out: 2.1 KB
57.144.238.141 (edge-star-shv-01-lhr6.facebook.com)	In: 170.7 KB Out: 9.0 KB
57.144.238.3 (edge-dgw-mini-shv-01-lhr6.facebook.com)	In: 22.9 KB Out: 8.5 KB
157.240.214.11 (xx-fbcdn-shv-02-lhr8.fbcdn.net)	In: 17.5 KB Out: 3.7 KB