What is OWASP MASTG?

OWASP MASTG (Mobile Application Security Testing Guide) is the how-to manual for testing mobile-app security. It pairs with the MASVS checklist: MASVS says what a secure app should do, MASTG shows the exact steps to check each item on Android and iOS. It used to be called the MSTG and was renamed to fit the wider MAS (Mobile Application Security) project. It is the manual nearly every mobile tester works from.

HOW IT WORKS

01 Why is it sometimes called the MSTG?

It was first published as the MSTG (Mobile Security Testing Guide). OWASP renamed it to MASTG (Mobile Application Security Testing Guide) when the wider project was reorganised under the MAS (Mobile Application Security) name, alongside MASVS and the Mobile Top 10.

Both names mean the same document. Older articles and job posts still say MSTG; current OWASP material says MASTG. Either way, it is the same guide.

02 What does the MASTG cover?

The guide follows the MASVS categories, with separate chapters for Android and iOS. It covers:

- How to set up a test environment on each platform: devices, emulators, instrumentation, traffic interception.
- Static analysis: decompiling the app, reading the code, finding embedded secrets.
- Dynamic analysis: hooking the running app, checking storage, testing deep links and how the app talks to other apps.
- Network testing: intercepting traffic and getting past certificate pinning where it is used.
- Resilience testing: checking anti-tamper, root and jailbreak detection, and obfuscation, and showing how each is bypassed.
- Reverse-engineering notes for both platforms.

Each technique points back to the MASVS requirement it checks, so a tester can go straight from a requirement to the right test.

SOURCES

[1] OWASP MASTG

[2] OWASP MASVS

[3] OWASP Mobile Application Security Project

03 How do testers use the MASTG?

On a real job, the MASTG is the manual the tester works from, not a script they read line by line. An experienced tester uses it to:

- Pick the right technique for a given MASVS requirement on a given platform.
- Look up platform details (the exact storage spots to check, the app-to-app channels to test).
- Ground the report's method section in a known standard.

The MASTG keeps jobs consistent and complete. Working from it, a tester covers the categories in order instead of only testing what comes to mind. For you, a MASTG-based job means the testing followed a known, repeatable method, not random poking.

04 Is the MASTG useful for developers, not just testers?

Yes. Dev teams use the MASTG (and MASVS) to see what testers will check, and to build the app to pass before the pentest.

The storage chapter tells an Android developer exactly which storage spots a tester will inspect and what 'secure storage' means in practice. The network chapter tells them what transport security and certificate checks the tester will verify. Building to the MASTG before testing cuts the number of findings and shortens the fix cycle.

The most mature mobile teams use MASVS as the requirement list during design and the MASTG as the check during development, then bring in a pentest to confirm it from the outside.