What is OWASP MASVS?

OWASP MASVS (Mobile Application Security Verification Standard) is the checklist of what a secure mobile app should do. It groups requirements into areas like storage, encryption, login, network traffic, how the app uses the phone, code quality, and resistance to tampering. A mobile pentest usually scores findings against MASVS, so you can see exactly which requirements pass and which fail. More and more enterprise buyers and app-store rules point to it directly.

HOW IT WORKS

01 What does MASVS cover?

The current MASVS is organised into control groups. The main categories:

- Storage (MASVS-STORAGE). How the app stores sensitive data on the device. Is it encrypted, is it in the right secure-storage mechanism, does it leak into logs, backups, or caches?
- Cryptography (MASVS-CRYPTO). Does the app use cryptography correctly: strong algorithms, proper key management, no hardcoded keys?
- Authentication (MASVS-AUTH). How the app authenticates the user and handles sessions, including biometric and local authentication.
- Network (MASVS-NETWORK). Is traffic encrypted and protected against interception, including certificate validation and pinning?
- Platform (MASVS-PLATFORM). Does the app interact safely with the platform: inter-process communication, deep links, WebViews, permissions?
- Code (MASVS-CODE). Is the app built and maintained with security in mind: up-to-date dependencies, no debugging artefacts, proper error handling?
- Resilience (MASVS-RESILIENCE). Does the app resist reverse engineering and tampering, including anti-tamper, root/jailbreak detection, and obfuscation?

02 What are the MASVS verification levels?

Not every app needs every requirement. MASVS provides a way to scope the standard to the app's risk profile.

SOURCES

[1] OWASP MASVS

[2] OWASP MASTG

[3] OWASP Mobile Application Security Project

[4] PCI Mobile Payments on COTS (MPoC)

- The baseline requirements (storage, crypto, auth, network, platform, code) apply to essentially every app that handles any sensitive data. These are the requirements most engagements verify.
- The resilience requirements (MASVS-RESILIENCE) apply to apps that need to resist reverse engineering and tampering: payment apps, apps protecting valuable content, apps with anti-fraud requirements. Not every app needs them, and they are explicitly a defence-in-depth layer, not a substitute for server-side security.

The scoping conversation at the start of an engagement decides which requirements apply. A simple informational app needs the baseline; a banking app needs the baseline plus resilience.

03 How is MASVS used in a pentest?

MASVS gives the engagement a defined bar. In practice:

- Scoping. The customer and tester agree which MASVS categories and level apply to the app.
- Testing. The tester verifies each in-scope requirement using the techniques from the MASTG.
- Reporting. Each finding is tied to the specific MASVS requirement it violates. The report shows which requirements pass, which fail, and the remediation for each.

The result is a report that an auditor, a customer-security team, or an app-store-compliance reviewer can read as a coverage map: here is the standard, here is what passes, here is what does not. This is more useful than a flat list of findings with no reference to a standard.

04 Does MASVS satisfy compliance?

MASVS is not a regulation, but it is increasingly the reference that regulations and procurement point to.

- PCI Mobile Payments on COTS (MPoC) references mobile security requirements aligned with MASVS thinking.

- Enterprise procurement for mobile apps increasingly asks for a MASVS-mapped pentest report.
- App-store and platform requirements overlap with several MASVS categories (data handling, transport security).

A MASVS-mapped pentest report is the standard evidence most of these processes want. It does not replace the specific compliance audit, but it is the artefact that demonstrates the app was tested against a recognised standard.

Get a MASVS-mapped mobile pentest.
securelayer7.net/learn/mobile-security/owasp-masvs

Open online