// TMG SECURITY RESEARCH — QUICK REFERENCE

OWASP Top 10:2025 for Penetration Testers — Quick Reference

A condensed, field-ready reading of the OWASP Top 10:2025 — what to look for in each category during an engagement.

TMG Security Research Team

Version 1.0

Published 07 September 2026

Category names and order verified against the official OWASP Top 10:2025 publication

What this reference is

OWASP's Top 10:2025 is an awareness document naming the ten application security risks the project currently considers most critical — not a testing standard. This is TMG Security's own condensed reading of that list, built for use during a penetration test: what each category means for a tester, what to look for, and why it matters.

> This reference is not an official OWASP publication and does not replace one. See References for the primary OWASP sources and TMG's full analysis.

What this reference is not

- Not authored, governed, or endorsed by OWASP. TMG Security is not affiliated with OWASP.
- Not a testing standard, an industry-standard certification, or a substitute for a full assessment.
- Not a source of new statistics — this reference contains no CWE counts, CVE figures, survey data, or severity/likelihood scoring.

OWASP Top 10:2025 quick reference

Category names and ordering follow the official OWASP Top 10:2025 publication exactly. The "what to look for" and "why it matters" columns are TMG's own condensed testing notes, not OWASP quotations.

Category	What to look for	Why it matters
A01 Broken Access Control	Object-level checks on every verb, not just reads. Endpoints added after the original CRUD surface. Authorization performed client-side. Internal calls that trust the network.	Cannot be centralised like authentication — every handler has to get it right.
A02 Security Misconfiguration	Defaults left in place, verbose errors, permissive CORS, reachable management interfaces, looser staging holding the same data as production.	Inherited configuration is where the findings are.
A03 Software Supply Chain Failures	Inventory existence, artefact integrity, who can modify a pipeline definition, where build secrets live, install-time code execution.	The pipeline is a production system with production credentials, often out of scope.
A04 Cryptographic Failures	Data classification, transport/cert validation incl. internal hops, key management and rotation, secrets storage, password hashing.	The question is what threat the encryption addresses, not just whether it's encrypted.
A05 Injection	Past SQL: template engines, expression languages, command construction, LDAP, XML, NoSQL. TMG extension: LLM prompt construction (see note below).	Parameterize where supported, allow-list where not, encode at output.
A06 Insecure Design	Missing rate limits, recovery flows that weaken authentication, unverified trust between services, unenforced process sequencing.	No amount of correct coding fixes an unsafe design.
A07 Authentication Failures	Session lifecycle (fixation, rotation, invalidation), MFA coverage on recovery/legacy paths, token handling (expiry, audience, signature, algorithm pinning).	See TMG's full analysis for this category's testing rationale.
A08 Software or Data Integrity Failures	Unsigned updates, deserialisation of untrusted data, unverified CI/CD artefacts, client-side dependencies without integrity checks.	Distinct from A03 — trusting content never verified, not supply-chain provenance.
A09 Security Logging & Alerting Failures	Whether events are recorded with subject/object/action, tamper-resistance, whether anything is actually alerted on. Did anyone see the testing traffic?	Determines whether the next real incident is found internally or reported by a third party.
A10 Mishandling of Exceptional Conditions	Whether failures fail closed/open, error paths skipping checks, timeout mid-transaction states, error disclosure, retry idempotency.	The error path is frequently under-tested; both A09 and A10 routinely determine how bad an incident becomes.

A05 note: the LLM/prompt-construction line is a TMG testing extension. OWASP addresses LLM prompt injection separately in the OWASP LLM Top 10 — it is not part of the official A05:2025 scope. No CWE counts, CVE figures, or other external statistics are included in this reference.

How to use this during a penetration test

Treat each category as a prompt for a line of enquiry rather than a test case. The table gives a tester's framing for each: what to look for, and what the defensive takeaway is. Refer to the official OWASP publication for the authoritative definitions and data.

TMG practical testing note: scope

The practical value of the 2025 edition is the reminder that the perimeter of an assessment is usually drawn too tightly. If the pipeline that builds the application and the error paths that run when it fails are both out of scope, two of the categories above cannot be evaluated at all. Use this list to argue for scope. Then test the application properly, which means going well past ten categories.

Attribution and limitations

- OWASP (the Open Worldwide Application Security Project) authors and maintains the OWASP Top 10. TMG Security did not create, govern, or contribute to the OWASP Top 10:2025, and is not affiliated with or endorsed by OWASP.
- This reference is TMG Security's own condensed, pentester-oriented reading of the published OWASP Top 10:2025 categories — not an official OWASP publication, and not a substitute for one.
- Official OWASP material always takes precedence over this summary. Consult the official OWASP Top 10:2025 project page and its category pages for authoritative, current definitions.
- The OWASP Top 10 is an awareness document, not a testing standard or an industry-standard certification.
- This reference does not include CWE counts, CVE statistics, survey data, or severity/likelihood scoring.

References

TMG SOURCE

- tmgsec.com/resources/owasp-top-10-2025-pentesting/ (full analysis)

OFFICIAL OWASP SOURCES

- OWASP Top 10 — owasp.org/Top10/
- OWASP Web Security Testing Guide
- OWASP Application Security Verification Standard
- OWASP Proactive Controls

> **This is TMG Security's own condensed reference, not an OWASP publication.** TMG does not create, govern, or claim authorship of the OWASP Top 10, and is not affiliated with or endorsed by OWASP. Official OWASP Top 10:2025 material takes precedence over this summary.