CYBERSECURITY · SEC-07

OWASP Top 10 Web Risks

Use this when: you build, review or test a web app and need the ten most important risk areas, what they look like and how to fix them.

BreakFixLearn

OWASP Top 10:2025 · Security+
Sheet v1.0 · Nov 2026

Scan to visit

The 2025 list: what it looks like, how to fix it

Ranked from data plus a practitioner survey

ID	RISK	LOOKS LIKE	FIX
A01	**Broken Access Control**	Change `?id=1001` to `1002` and see another user's data. Includes SSRF.	Deny by default; check every request on the server, per object
A02	**Security Misconfiguration**	Default admin password, debug pages, open cloud storage	Hardened baseline, remove extras, same config in every environment
A03	**Software Supply Chain Failures**	Old library with a known CVE, poisoned package, tampered build	SBOM, scan dependencies, trusted and signed sources
A04	**Cryptographic Failures**	HTTP logins, MD5 passwords, keys in code	TLS everywhere; bcrypt or Argon2 for passwords; a key vault
A05	**Injection**	SQL injection `' OR 1=1--`, XSS, command injection	Parameterized queries; encode output; validate input
A06	**Insecure Design**	Password reset with guessable questions; no rate limits	Threat model early; secure design patterns; abuse cases
A07	**Authentication Failures**	Credential stuffing works, no MFA, session never expires	MFA, breached-password checks, short sessions, lockout
A08	**Software or Data Integrity Failures**	Unsigned auto-updates, unsafe deserialization	Sign and verify code and data; protect the CI/CD pipeline
A09	**Security Logging & Alerting Failures**	Breach found months later; no alert on 1,000 failed logins	Log auth and access events; alert on them; keep logs safe
A10	**Mishandling of Exceptional Conditions** NEW	Stack trace shown to users; error leaves a transaction half done	Catch errors where they happen; fail closed; roll back fully

What changed from 2021

Expanded	A03 Supply Chain (was Vulnerable Components)
New	A10 Mishandling of Exceptional Conditions
Merged	SSRF now sits inside A01
Moved up	Misconfiguration from #5 to #2

Five habits that cover most

Server-side checks	Never trust the browser
Parameterize	Every query, every time
Patch deps	Scan and update weekly
MFA	For users and admins
Log and alert	Logins, access denied, errors

Test safely

LEGAL Test only apps you own or have written permission to test. Use practice targets like OWASP Juice Shop.

CAUTION Scanners can change or delete data. Point them at a test copy, never production.

Go deeper

ASVS	Requirements to build and verify against
Cheat Sheets	OWASP Cheat Sheet Series, per topic
Juice Shop	Safe, deliberately vulnerable app

REMEMBER

- **A01** access control is #1
- Fix the class of bug, not one URL
- It's an awareness list, not a full standard

Sources: OWASP Top 10:2025 (top10.owasp.org) · OWASP ASVS · OWASP Cheat Sheet Series

CC BY-NC 4.0 · SEC-07 v1.0