What is the OWASP Top 10?

3 November 2026 · 5 min read · blogs.iictp.org/owasp-top-10-explained

The OWASP Top 10 is a widely used awareness document that ranks the most critical security risks to web applications, produced by the Open Worldwide Application Security Project. It is a starting point for developers and teams, not a complete security standard. The list below follows the 2021 edition; check owasp.org for the current one.

TL;DR The short version

- The OWASP Top 10 ranks the most critical security risks to web applications and is a starting point, not a complete standard.
- Injection happens when user input is pasted into a command; broken access control is forgetting to check permission.
- Use it as a checklist in reviews and design discussions, but go beyond it.

Read online, listen to it, or change the text size: https://blogs.iictp.org/owasp-top-10-explained

What are the ten categories?

- **Broken access control:** users can act outside their permissions.
- **Cryptographic failures:** sensitive data is not protected properly.
- **Injection:** untrusted input is run as a command or query.
- **Insecure design:** the design lacks security thinking from the start.
- **Security misconfiguration:** unsafe defaults or settings.
- **Vulnerable and outdated components:** known flaws in libraries you use.
- **Identification and authentication failures:** weak login or session handling.
- **Software and data integrity failures:** updates or pipelines are not verified.
- **Security logging and monitoring failures:** attacks go unnoticed.
- **Server-side request forgery:** the server is tricked into fetching attacker-chosen addresses.

What is injection, in plain terms?

It happens when an application builds a command, such as a database query, by pasting in user input, so the input can change the command. The standard defence is to keep data and commands separate with parameterised queries and to validate input.

What is broken access control?

It is when the application forgets to check that the person asking is allowed to see or change the thing they asked for. Changing an ID in a URL and seeing someone else's record is a classic case. Check permissions on the server for every request.

How should a junior developer use the list?

Treat it as a checklist for reviews and design discussions. When you add a form, a login or a file upload, ask which categories apply. The depth of each category comes from OWASP's cheat sheets, not from the list itself.

Is it enough to follow the Top 10?

No. It covers common, high-impact risks, not every risk. Pair it with dependency scanning, secure defaults, testing and monitoring as described in what is DevSecOps.

> Related credential: Associate Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. OWASP Foundation. OWASP Top 10:2021. owasp.org/Top10.
2. OWASP Foundation. Cheat Sheet Series. cheatsheetseries.owasp.org.

Published by IICTP, an independent technical credential body, on 3 November 2026. The current version of this post is at https://blogs.iictp.org/owasp-top-10-explained. More guides: blogs.iictp.org.