# The OWASP Top 10, and What a List Like This Is Actually For

Mon, Sep 21, 6:00 PM EDT · https://scottslab.io/posts/owasp-top-10-overview

**TL;DR**

The OWASP Top 10 is a data-driven ranking of web application risk categories, not a checklist and not a certification. The 2021 edition ranked broken access control, cryptographic failures, injection, insecure design, security misconfiguration, vulnerable and outdated components, identification and authentication failures, software and data integrity failures, security logging and monitoring failures, and server-side request forgery. OWASP has since released a 2025 edition that reshuffles and merges several of those categories, which is itself the best argument for treating the list as a snapshot rather than scripture.

## What the list actually measures

OWASP stands for the Open Worldwide Application Security Project, a nonprofit that runs this and a lot of other application security work through volunteer contributors. The Top 10 is their flagship document: a ranked set of risk categories built from a mix of contributed vulnerability data and a community survey of practitioners. It answers one narrow question: given everything found in real applications recently, where does risk concentrate.

That framing matters more than the ten names people memorize. The list is not "the ten vulnerabilities that exist." It is a prioritization tool built on a sample of what got found and reported. A category with fewer entries this cycle did not stop mattering. It just moved down a ranking built from a specific dataset over a specific window.

## The 2021 list, and what each line actually bundles

The 2021 edition, still the version most training material and compliance checklists reference, ranked the categories like this: broken access control, cryptographic failures, injection, insecure design, security misconfiguration, vulnerable and outdated components, identification and authentication failures, software and data integrity failures, security logging and monitoring failures, and server-side request forgery.

Each of those ten lines is a bucket, not a bug. "Injection" alone covers SQL injection, command injection, and LDAP injection, distinct attacks that share a mechanism but not a fix. "Broken access control" covers everything from a missing role check to an object reference anyone can walk by changing a number in a URL. Treat the list as ten headings you build a test plan under, not ten boxes you tick.

## The list changes, on purpose

OWASP shipped a 2025 edition, and it is not the same shape as 2021. Broken access control stays at the top. Security misconfiguration jumps to second. Vulnerable and outdated components disappears as its own line and gets absorbed into a new, broader "software supply chain failures" category. Server-side request forgery, which had its own line in 2021, is gone as a standalone entry; a new category called "mishandling of exceptional conditions" takes its place instead. Authentication failures drops "identification" from its name.

This is not OWASP being sloppy. It is the dataset moving. Supply chain risk earned its own category because that is where incidents concentrated in the years since 2021, not because SQL injection stopped happening. If your SDLC checklist hard-codes the 2021 category names as a permanent contract, the checklist has quietly become wrong, and nobody updated it.

## What it's for, and what it isn't

Use the Top 10 as shared vocabulary and as a floor, not a ceiling. When a pentest or a scanner reports a finding, mapping it to a category tells you whether your program has coverage for that class of risk. It does not tell you your application is secure once all ten are addressed. It tells you which ten large categories account for a lot of the damage in the data OWASP had.

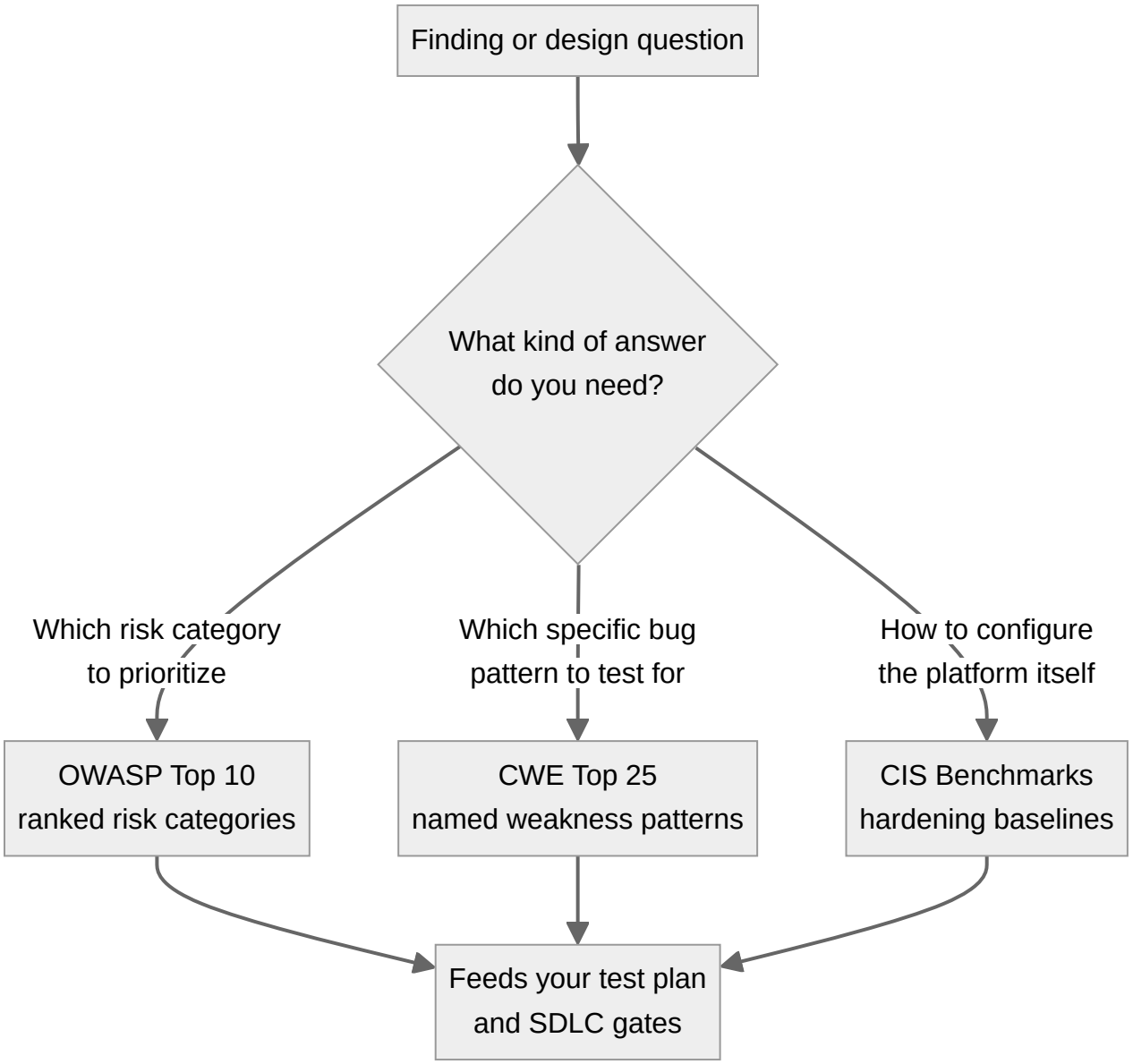
It is also not a certification. There is no "OWASP Top 10 compliant" badge OWASP issues, and a vendor claiming one is telling you they haven't read the document closely. It's an awareness document aimed at developers and architects, meant to shape where a limited testing budget goes.

## Where the other lists fit

Two other lists get invoked in the same breath, and they answer different questions. The CWE Top 25 Most Dangerous Software Weaknesses, still often called the SANS Top 25 from when SANS co-published early editions, operates at a finer grain: specific, named weakness patterns like CWE-89 for SQL injection, ranked by frequency and severity pulled from real vulnerability data. Where the OWASP Top 10 tells you which risk category to build a testing program around, the CWE Top 25 tells you which exact bug pattern to grep your code for.

CIS Benchmarks are a different animal entirely: consensus-built configuration standards for hardening a specific operating system, cloud platform, or piece of software to an agreed baseline. They don't rank risk at all. They tell you how to configure the box correctly once you've decided what to defend.

Put together, the OWASP Top 10 says where to point your program, the CWE Top 25 says which specific patterns to test for, and CIS Benchmarks say how to configure what you're running underneath. None of them is complete on its own, and none of them was ever meant to be.




Where the other lists fit

## The actual discipline

Reading a Top 10 list well means asking what it's measuring, who's in the sample, and what changed since the last edition, before you build a control around it. The 2021 to 2025 shift is a good teaching case precisely because it shows the list doing its job: reacting to where risk actually moved, at the cost of every "OWASP-aligned" slide deck built assuming ten fixed names would stay fixed. Rebuild the mapping when the list moves. Don't rebuild your whole program around a document meant to be read again next cycle.

---