OWASP Top 10 2025 vs. Top Web Vulnerabilities in Pentests

Comparing Critical Risks vs. Frequent Real-World Findings

Strong Overlap | Categorical Overlap | OWASP-Only Risk | Cobalt-Only Finding

OWASP Top 10 2025

01 **Broken Access Control**

02 **Security Misconfiguration**

03 **Software Supply Chain Failures** (New)

04 **Cryptographic Failures**

05 **Injection**

06 **Insecure Design**

07 **Authentication Failures**

08 **Software or Data Integrity Failures**

09 **Logging & Alerting Failures**

10 **Mishandling of Exceptional Conditions** (New)

Cobalt Top 10 2025

01 **Cross-Site Scripting (XSS)**
18.4%

02 **Information Exposure / Sensitive Data Leak**
13.9%

03 **Improper Access Control**
11.8%

04 **SQL Injection**
10.6%

05 **Weak Encryption / TLS Misconfiguration**
8.7%

06 **Unrestricted File Upload**
7.5%

07 **Cross-Site Request Forgery (CSRF)**
6.3%

08 **Server-Side Request Forgery (SSRF)**
5.5%

09 **Improper Input Validation**
4.4%

10 **Clickjacking / Frame Injection**
3.0%

Key Similarities & Differences

Key Similarities

- **Access Control is King:** Both lists identify this is a top-tier threat. It's OWASP's #1 critical risk and the #3 most frequent pentest finding. (Cobalt pentests put SSRF at #8, which also rolls into this category).
- **Data Protection:** OWASP's A04: Cryptographic Failures is the strategic risk that maps to frequent Cobalt pentest findings of Information Exposure (#2) and Weak Encryption (#5).

Key Differences

- **The Injection Disconnect:** This is the biggest difference. OWASP demoted the broad A05: Injection category to #5, while Cobalt data shows it's the #1 real-world threat. XSS (Cobalt #1) and SQL Injection (Cobalt #4) alone make up 29% of all web pentest findings.
- **OWASP's New Strategic Risks:** The 2025 list adds two new categories driven by community survey: A03: Software Supply Chain Failures and A10: Mishandling of Exceptional Conditions. These are broad, systemic risks, not specific pentest findings.
- **Cobalt Tactical Findings:** The Cobalt list features high-frequency flaws like CSRF (#7) and Improper Input Validation (#9) that are no longer on the OWASP Top 10 but are still found by pentesters.

The Main Takeaway

The **OWASP Top 10** is a **what to plan for** list,
guiding long-term security programs.

The **Cobalt Top 10** is a **what to fix now** list,
showing the real-world flaws found most often in pentests.

See how to build an offensive security strategy at Cobalt.io

Source: OWASP Top 10 2025 and Cobalt data from web penetration tests Jan–Sep 2025.

Cobalt