

OWASP Top 10 Vulnerabilities 2025 – Detailed Explanation

A01:2025 – Broken Access Control

Background: Broken Access Control is the most critical risk in OWASP Top 10 2025. It occurs when applications fail to properly enforce authorization policies, allowing users to perform actions outside their intended permissions.

Score Table (Overview): High prevalence, ~40 mapped CWEs, consistently ranked #1 across OWASP testing data.

Description: These vulnerabilities allow unauthorized disclosure, modification, or destruction of data and unauthorized execution of business functions. It includes IDOR, privilege escalation, and SSRF-related authorization flaws.

How to Prevent: Enforce deny-by-default access control, validate authorization server-side, use centralized authorization mechanisms, and perform access testing on all endpoints.

Example Attack Scenarios: A user modifies a URL to access another user's account; standard users access admin APIs due to missing authorization checks.

References: OWASP Top 10:2025 Official Documentation.

Mapped CWEs: CWE-284, CWE-285, CWE-639, CWE-862, CWE-863

A02:2025 – Security Misconfiguration

Background: Security Misconfiguration affects almost all applications and arises from insecure default settings or incomplete configurations.

Score Table: 16 CWEs mapped, ~3.00% average incidence, over 700,000 observed occurrences.

Description: Includes exposed services, default credentials, verbose error messages, and misconfigured cloud resources.

How to Prevent: Harden systems using secure baselines, automate deployments, remove unused features, and regularly audit configurations.

Example Attack Scenarios: Public access to cloud storage; exposed admin panels in production.

References: OWASP Top 10:2025 Security Misconfiguration.

Mapped CWEs: CWE-16, CWE-611, CWE-1004

A03:2025 – Software Supply Chain Failures

Background: New in 2025, this category expands component risks to include CI/CD pipelines and third-party services.

Score Table: Few CWEs mapped, but very high impact and exploit potential.

Description: Occurs when applications rely on compromised libraries, malicious updates, or insecure build pipelines.

How to Prevent: Maintain SBOMs, scan dependencies, verify update sources, and secure CI/CD systems.

Example Attack Scenarios: Malicious code injected into a popular open-source library; compromised build server inserting backdoors.

References: OWASP Top 10:2025 Introduction.

Mapped CWEs: CWE-829, CWE-494

A04:2025 – Cryptographic Failures

Background: Cryptographic Failures expose sensitive data due to weak or misused cryptography.

Score Table: ~32 CWEs mapped, ~3.8% average incidence.

Description: Includes weak encryption algorithms, improper key management, and failure to encrypt data in transit or at rest.

How to Prevent: Use strong cryptographic standards, protect keys, and avoid custom crypto implementations.

Example Attack Scenarios: MITM attacks exploiting weak TLS; decrypted sensitive data from stolen databases.

References: OWASP Top 10:2025 Cryptographic Failures.

Mapped CWEs: CWE-326, CWE-327, CWE-522

A05:2025 – Injection

Background: Injection attacks remain among the most common and dangerous vulnerabilities.

Score Table: 37 CWEs mapped, over 1.4 million occurrences observed.

Description: Occurs when untrusted input is executed as commands or queries (SQL, OS, XSS).

How to Prevent: Use parameterized queries, validate input, and encode output.

Example Attack Scenarios: SQL Injection dumping databases; XSS hijacking user sessions.

References: OWASP Top 10:2025 Injection.

Mapped CWEs: CWE-79, CWE-89, CWE-78

A06:2025 – Insecure Design

Background: Focuses on architectural and business logic flaws introduced during application design.

Description: Includes missing threat modeling, insecure workflows, and poor trust boundaries.

How to Prevent: Apply secure design principles, conduct threat modeling, and review business logic.

Example Attack Scenarios: Approval workflow bypass; unlimited resource consumption.

References: OWASP Top 10:2025 Insecure Design.

Mapped CWEs: CWE-840

A07:2025 – Authentication Failures

Background: Authentication failures occur when identity verification mechanisms are weak or misused.

Description: Includes weak passwords, missing MFA, and poor session handling.

How to Prevent: Enforce MFA, strong password policies, and secure session management.

Example Attack Scenarios: Credential stuffing; session fixation attacks.

References: OWASP Top 10:2025 Authentication Failures.

Mapped CWEs: CWE-287, CWE-384

A08:2025 – Software or Data Integrity Failures

Background: Arises when systems fail to verify the integrity of software or data.

Description: Includes untrusted updates and tampered critical data.

How to Prevent: Use digital signatures, checksums, and secure update mechanisms.

Example Attack Scenarios: Trojanized updates installing malware.

References: OWASP Top 10:2025 Integrity Failures.

Mapped CWEs: CWE-353

A09:2025 – Security Logging and Alerting Failures

Background: Insufficient logging prevents timely detection of attacks.

Description: Missing logs, ineffective monitoring, or no alerting mechanisms.

How to Prevent: Centralized logging, SIEM integration, and real-time alerts.

Example Attack Scenarios: Breaches remain undetected for months.

References: OWASP Top 10:2025 Logging Failures.

Mapped CWEs: CWE-778

A10:2025 – Mishandling of Exceptional Conditions

Background: New in 2025, focuses on insecure handling of errors and unexpected conditions.

Score Table: 24 CWEs mapped, ~2.95% average incidence.

Description: Applications fail open or leak sensitive information during errors.

How to Prevent: Implement secure error handling and fail-safe mechanisms.

Example Attack Scenarios: Stack traces exposing database structure.

References: OWASP Top 10:2025 Exceptional Conditions.

Mapped CWEs: CWE-209, CWE-636