Internet & Networking

By Devi Sri Charan

[OWASP Vulnerabilities 2](#_Toc1992418810)

[1. Broken Access Control 3](#_Toc990812181)

[2. Cryptographic Failures 3](#_Toc1051992819)

[3. Injection 3](#_Toc1448722922)

[4. Insecure Design 4](#_Toc1690678147)

[5. Security Misconfiguration 4](#_Toc507553467)

[6. Vulnerable and Outdated Components 4](#_Toc1220109448)

[7. Identification and Authentication Failures 5](#_Toc970422393)

[8. Software and Data Integrity Failures 5](#_Toc1886895328)

[9. Security Logging and Monitoring Failures 5](#_Toc754088557)

[10. Server-Side Request Forgery (SSRF) 5](#_Toc87254890)

# OWASP Vulnerabilities

The OWASP (Open Web Application Security Project) Top Ten is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. Below are explanations for each of the vulnerabilities listed in the OWASP Top Ten:

## Broken Access Control

* + **Explanation**: Access control ensures that users can perform only the actions they are permitted to. Broken access control occurs when restrictions on what authenticated users are allowed to do are not properly enforced, allowing users to access unauthorized functionalities or data.
  + **Example**: A user modifies the URL to access data of another user without proper authorization checks.
  + **Impact:** Unauthorized access to sensitive data or functions.
  + **Risks:** Data breaches, privilege escalation, unauthorized actions.

## Cryptographic Failures

* + **Explanation**: Previously known as "Sensitive Data Exposure," this category involves security failures related to cryptography. These failures often lead to sensitive data exposure when not protected correctly in storage or transit.
  + **Example**: Data transmitted over the network in plaintext without encryption, making it easily accessible to attackers.
  + **Impact**: Exposure of sensitive data.
  + **Risks**: Data theft, financial loss, identity theft.

## Injection

* + **Explanation**: Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
  + **Example**: SQL injection where an attacker can manipulate a SQL query to access unauthorized data or execute arbitrary commands on the database.
  + **Impact**: Execution of unintended commands or queries.
  + **Risks**: Data corruption, unauthorized data access, system compromise.

## Insecure Design

* + **Explanation**: Insecure design refers to the absence of security controls in the design phase of software development, leading to vulnerabilities that are exploitable once the software is implemented.
  + **Example**: An application designed without considering secure coding practices, such as input validation and output encoding.
  + **Impact:** Fundamental security flaws in application architecture.
  + **Risks:** Exploitable weaknesses leading to data breaches, unauthorized access, and compromised systems.

## Security Misconfiguration

* + **Explanation**: Security misconfiguration is the most common issue. It occurs when security settings are not defined, implemented, or maintained properly. This includes using default configurations, open cloud storage, and verbose error messages.
  + **Example**: An application deployed with default settings, exposing sensitive information through error messages.
  + **Impact:** Exposure of application to various attacks due to misconfigured settings.
  + **Risks:** Unauthorized access, data leaks, system compromise.

## Vulnerable and Outdated Components

* + **Explanation**: Using components with known vulnerabilities can compromise application security. This includes outdated software libraries, frameworks, or other software modules.
  + **Example**: Using an outdated version of a web framework with known security flaws that can be exploited.
  + **Impact:** Exploitation of known vulnerabilities in software components.
  + **Risks:** System breaches, data loss, unauthorized control over application.

## Identification and Authentication Failures

* + **Explanation**: This category, previously known as "Broken Authentication," involves weaknesses related to authentication mechanisms, allowing attackers to compromise passwords, keys, or session tokens, or exploit other implementation flaws to assume other users' identities.
  + **Example**: An application that allows weak passwords or does not properly protect session tokens, leading to unauthorized access.
  + **Impact:** Compromise of user identities and credentials.
  + **Risks:** Account takeovers, unauthorized access, identity theft.

## Software and Data Integrity Failures

* + **Explanation**: This category involves issues related to code and infrastructure that do not protect against integrity violations. This includes insecure CI/CD pipelines, software updates without proper verification, and data tampering.
  + **Example**: A CI/CD pipeline that deploys software without verifying the integrity of the code, allowing attackers to inject malicious code.
  + **Impact:** Unauthorized alterations of software or data.
  + **Risks:** Malicious code execution, data tampering, loss of data integrity.

## Security Logging and Monitoring Failures

* + **Explanation**: Insufficient logging and monitoring can lead to undetected security breaches. Adequate logging, monitoring, and alerting are crucial for detecting and responding to security incidents.
  + **Example**: A web application that does not log failed login attempts or unusual activities, making it difficult to detect brute force attacks or other malicious actions.
  + **Impact:** Lack of detection and response to security incidents.
  + **Risks:** Prolonged undetected breaches, increased damage from attacks.

## Server-Side Request Forgery (SSRF)

* + **Explanation**: SSRF occurs when a web application fetches a remote resource without validating the user-supplied URL. This can allow attackers to coerce the application into sending requests to an unintended destination, potentially exposing internal systems.
  + **Example**: An application that allows users to specify a URL to fetch data from, without proper validation, leading to access to internal services or sensitive data.
  + **Impact:** Coercion of server to interact with unintended locations.
  + **Risks:** Internal system exposure, data leakage, access to internal services.