HACKER COMBAT
COMMUNITY

# OWASP Top 10 Security Risks

Hackercombat.com

# OWASP Vulnerabilities

**This list represents the most relevant threats to software security today.**

1

## Vulnerability 1

Injection

2

## Vulnerability 2

Broken Authentication

3

## Vulnerability 3

Sensitive Data Exposure

4

## Vulnerability 4

XML External Entities (XXE)

# OWASP Vulnerabilities

**This list represents the most relevant threats to software security today.**

5

## Vulnerability 5

Broken Access control

6

## Vulnerability 6

Security Misconfigurations

7

## Vulnerability 7

Cross-Site Scripting (XSS)

8

## Vulnerability 8

Insecure Deserialization

# OWASP Vulnerabilities

**This list represents the most relevant threats to software security today.**

## Vulnerability 9

9

Using Components with known vulnerabilities

## Vulnerability 10

10

Insufficient logging and monitoring

**Follow us**

**Visit**

**Hackercombat.com**

- **Injection**

Injection flaws, such as SQL injection, LDAP injection, and CRLF injection, occur when an attacker sends untrusted data to an interpreter that is executed as a command without proper authorization.

- **Broken Authentication**

Incorrectly configured user and session authentication could allow attackers to compromise passwords, keys, or session tokens, or take control of users' accounts to assume their identities.

- **Sensitive Data Exposure**

Applications and APIs that don't properly protect sensitive data such as financial data, usernames and passwords, or health information, could enable attackers to access such information to commit fraud or steal identities.

Source: Veracode

---

## • XML External Entities (XXE)

Poorly configured XML processors evaluate external entity references within XML documents. Attackers can use external entities for attacks including remote code execution, and to disclose internal files and SMB file shares.

## • Broken Access control

Improperly configured or missing restrictions on authenticated users allow them to access unauthorized functionality or data, such as accessing other users' accounts, viewing sensitive documents, and modifying data and access rights.

## • Security Misconfigurations

This risk refers to improper implementation of controls intended to keep application data safe, such as misconfiguration of security headers, error messages containing sensitive information (information leakage), and not patching or upgrading systems, frameworks, and components.

Source: Veracode

- **Cross-Site Scripting (XSS)**

Cross-site scripting (XSS) flaws give attackers the capability to inject client-side scripts into the application, for example, to redirect users to malicious websites.

- **Insecure Deserialization**

Insecure deserialization flaws can enable an attacker to execute code in the application remotely, tamper or delete serialized (written to disk) objects, conduct injection attacks, and elevate privileges.

Source: Veracode

- **Using Components with known vulnerabilities**

Developers frequently don't know which open source and third-party components are in their applications, making it difficult to update components when new vulnerabilities are discovered. Attackers can exploit an insecure component to take over the server or steal sensitive data.

- **Insufficient logging and monitoring**

The time to detect a breach is frequently measured in weeks or months. Insufficient logging and ineffective integration with security incident response systems allow attackers to pivot to other systems and maintain persistent threats.

Source: Veracode


HACKER COMBAT
COMMUNITY
LIKE
COMMENT
SHARE
HACKERCOMBAT.COM
FOLLOW HACKER COMBAT LINKEDIN PAGE