Infographic created by
TARAS SAHAIDACHNYI

OWASP

TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

OWASP TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

1. Injection

Occurs 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.

Use safe APIs, parameterized queries, or ORM frameworks.
Validate and sanitize all input data.

OWASP TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

2. Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

Implement multi-factor authentication, do not deploy with default credentials, and ensure session management is secure.

OWASP TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

3. Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Encrypt sensitive data at rest and in transit. Disable caching for responses that contain sensitive data.

OWASP

TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

4. XML External Entities (XXE)

Poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

Use less complex data formats such as JSON, and avoid serialization of sensitive data.

OWASP TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

5. Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

Employ the principle of least privilege. Ensure that users can only access the data and resources necessary for their role.

OWASP TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

6. Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is usually a result of insecure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.

Regularly update and patch systems, remove unused features and frameworks, and configure error handling to prevent information leakage.

OWASP

TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

7. Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript.

Use frameworks that automatically escape XSS, implement Content Security Policy, validate and sanitize all input data.

OWASP

TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

8. Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

Implement integrity checks, such as digital signatures on any serialized objects, and enforce strict type constraints during deserialization before object reuse.

OWASP

TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

9. Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

Keep all components and dependencies up to date, and remove unused dependencies and features.

OWASP TOP 10 IN 2024

ISSUES & SOLUTIONS

IN SIMPLE WORDS

Infographic created by
TARAS SAHAIDACHNYI

10. Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.

Ensure proper logging and monitoring is in place and integrated with incident response mechanisms.

Infographic created by
TARAS SAHAIDACHNYI

DON’T FORGET TO LIKE & SAVE THIS POST