


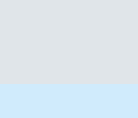
# 10 BUGS & VULNERABILITIES THAT THREATEN YOUR WEB APPLICATIONS

The top 10 bugs and vulnerabilities listed are extracted from a standard developer and web application security awareness document - known as the OWASP Top 10. Companies should ensure that their web applications minimize these risks.

Using the OWASP Top 10 is the most effective first step in your organization to produce more secure code. The traffic lights indicate which of these bugs and vulnerabilities Code Intelligence can automatically detect with the CI Fuzz solution.

 Detected automatically

 Detected with manual effort

 Not detected

## INJECTION

Injection flaws, such as SQL injections, occur when an attacker sends untrusted data to an interpreter as part of a command or query. The hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

## BROKEN AUTHENTICATION

When authentication functions are not implemented correctly, attackers have the opportunity to compromise passwords, keys, or session IDs, or to exploit other flaws using stolen user credentials.

## 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 conduct credit card fraud, identity theft, or other crimes.

## XML EXTERNAL ENTITIES

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

## BROKEN ACCESS CONTROL

Attackers can exploit improperly configured restrictions to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

## SECURITY MISCONFIGURATION

This risk is a result of improper implementation of controls such as misconfigured HTTP headers, error messages containing sensitive information and not patching or upgrading systems, frameworks, and components.

## CROSS-SITE SCRIPTING XSS

XSS flaws allow attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

## INSECURE DESERIALIZATION

Insecure deserialization often leads to remote code execution or they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

## USING COMPONENTS WITH KNOWN VULNERABILITIES

Developers use open source and third-party components without testing them in advance. If a vulnerability in these components is exploited, such an attack can facilitate serious data loss or server takeover.

## 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.

## WOULD YOU LIKE TO DISCOVER MORE?

Get in-depth guidance that will lead you into the world of application security!

[Download Resources](#)



code intelligence

**CODE INTELLIGENCE**

Rheinwerkallee 6

D-53227 Bonn

**CONTACT US**

+49 228 2869 5830

sales@code-intelligence.com

