Vulnerabilities

What is a vulnerability?

A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application. Stakeholders include the application owner, application users, and other entities that rely on the application.

Please **do not post any actual vulnerabilities** in products, services, or web applications. Those disclosure reports should be posted to bugtraq or full-disclosure mailing lists.

Examples of vulnerabilities

- Lack of input validation on user input
- Lack of sufficient logging mechanism
- Fail-open error handling
- Not closing the database connection properly

For a great overview, check out the OWASP Top Ten Project. You can read about the top vulnerabilities and download a paper that covers them in detail. Many organizations and agencies use the Top Ten as a way of creating awareness about application security.

NOTE: Before you add a vulnerability, please search and make sure there isn't an equivalent one already. You may want to consider creating a redirect if the topic is the same. Every vulnerability article has a defined structure.

List of Vulnerabilities

- Allowing Domains or Accounts to Expire
- Buffer Overflow
- Business logic vulnerability
- CRLF Injection
- CSV Injection by Timo Goosen, Albinowax
- Catch NullPointerException
- Covert storage channel
- Deserialization of untrusted data
- Directory Restriction Error
- Doubly freeing memory
- Empty String Password
- Expression Language Injection
- Full Trust CLR Verification issue Exploiting Passing Reference Types by Reference
- Heartbleed Bug
- Improper Data Validation
- Improper pointer subtraction
- Information exposure through query strings in url by Robert Gilbert (amroot)
- Injection problem
- Insecure Compiler Optimization
- Insecure Randomness
- Insecure Temporary File
- Insecure Third Party Domain Access
- Insecure Transport
- Insufficient Entropy
- Insufficient Session-ID Length
- Least Privilege Violation
- Memory leak
- Missing Error Handling
- Missing XML Validation
- Multiple admin levels
- Null Dereference
- OWASP .NET Vulnerability Research
- Overly Permissive Regular Expression
- PHP File Inclusion
- PHP Object Injection by Egidio Romano
- PRNG Seed Error
- Password Management Hardcoded Password
- Password Plaintext Storage
- Poor Logging Practice by Weilin Zhong
- Portability Flaw
- Privacy Violation
- Process Control
- Return Inside Finally Block
- Session Variable Overloading
- String Termination Error
- Unchecked Error Condition
- Unchecked Return Value Missing Check against Null
- Undefined Behavior
- Unreleased Resource
- Unrestricted File Upload
- Unsafe JNI
- Unsafe Mobile Code

- Unsafe function call from a signal handler
- Unsafe use of Reflection
- Use of Obsolete Methods
- Use of hard-coded password
- Using a broken or risky cryptographic algorithm
- Using freed memory
- Vulnerability template
- XML External Entity (XXE) Processing
- The Follina Vulnerability - A Critical Threat to Microsoft Office by Tholkappiar

Edit on GitHub

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Important Community Links

Community
Attacks
Vulnerabilities (You are here)
Controls

Upcoming OWASP Global Events

OWASP Global AppSec Washington DC 2023
- October 30 - November 3, 2023

OWASP Global AppSec Lisbon 2024
- June 24-28, 2024

OWASP Global AppSec San Francisco 2024
- September 23-27, 2024

OWASP Global AppSec Washington DC 2025
- November 3-7, 2025

OWASP Global AppSec San Francisco 2026
- November 2-6, 2026

Spotlight: F5

SECURE AND DELIVER EXTRAORDINARY DIGITAL EXPERIENCES F5's portfolio of automation, security, performance, and insight capabilities empowers our customers to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users.

Corporate Supporters

Become a corporate supporter

PRIVACY SITEMAP CONTACT