

# OWASP TOP 10

## Introduction

Owasp Top 10 identify us what the vulnerabilities is, how it will happen and how you will take down the vulnerabilities. It has list that identify most important threat regarding web applications. In this room we can learn theory and put it into practical learning

## Severity 1 -> Injection

In this vulnerability it happens when user input the data or command and the server performs action or executes without sanitizing the input then it is known as injection vulnerability.

It is of types when we pass SQL queries then it is called SQL injection another one is when we pass some commands and it executes according to attacker's need.

Preventions:

- We defined some parameters of characters which is used.
- Sanitize the input.

## Severity 2 -> Broken Authentication

Broken Authentication can be defined as when attacker gains the credentials or broke the authentication mechanism with help of brute force attacks, taken advantage of weak credentials and weak session cookies.

Preventions:

- Multi factor authentication.
- Make sure of strong password and define certain number of login attempts.

### **Severity 3 -> Sensitive Data Exposure**

Sensitive Data Exposure said as when the important data like username, dob, passwords and more technical information. When data lie on main server and customer side by taking advantage of this attacker access on server and expose the data.

#### **Preventions:**

- Use best encryption methods.
- Use modern technical advancements.

### **Severity 4 -> XML External Entity**

XML External Entity attack happens when an attacker uses some features of server interact with backend or private part of server, read files etc. Taking advantage, they can perform DoS and SSRF attacks also.

#### **Preventions:**

**Disable public usage of External parses.**

### **Severity 5 -> Broken Access Control**

It can be defined as the when a visitor accesses the private or protected pages of the web server then this is known as Broken access Control vulnerability.

#### **Preventions:**

We can limit the visitor access and use tools to keep private the important pages.

## **Severity 6 -> Security Misconfiguration**

It happens when security cannot be configured properly like poor configured permissions, unnecessary features enable and default account with unchanged passwords.

### **Preventions:**

Manages security configurations perfectly don't open loop holes.

## **Severity 7 -> Cross-site Scripting**

Cross-site Scripting also known as XSS. When the web application allows to executes user input without sanitize properly, XSS can be in JavaScript, CSS etc. By result of this attacker executes the malicious scripts on victim's machine.

### **Preventions:**

We can validate the input and uses the blacklist and whitelist filtering.

## **Severity 8 -> Insecure Deserialization**

Insecure Deserialization is possible when we Deserialize a format and which is insecure and, in this process, attacker replaces the data format with malicious code by possibles attacks then this is consider as Insecure Deserialization.

### **Preventions:**

Avoid objects from untrusted source and Process need to be encrypted.

## **Severity 9 -> Components with Known Vulnerabilities**

When you are using an outdated software and this version has a known vulnerability. Then attacker easily use this or take advantage of this and easily exploit your server.

### **Preventions:**

Regularly updated your software.

## **Severity 10 -> Insufficient Logging and Monitoring**

In the setup of web application when there is not proper logging or monitoring this result as an attacker steals the information and easily attack on our server. Like user has proper location monitored but with same username anybody access from out of country then we know about this.

### **Preventions:**

Proper logging and monitoring the activities with username, IP addresses or Time stamps.


## **Conclusion**

By using and take learning from Owasp Top 10 vulnerability we can maintain a very good base and safe from any type of threats. It is useful as there are labs are also provided.



Congratulations on completing OWASP Top 10!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
 336	 31	 Walkthrough	 Easy	 1

 Leave Feedback

Close 