**DAY 23**

**6. Security misconfiguration**

Default passwords and settings

**7.Cross-site scripting**

-This vulnerability exists in web application which take user input and generates a dynamic page with user’s given input and if the server isn’t validating the user input.

-The hacker injects malicious JavaScript/HTML code into the web application

EX. E-commerce websites

LMS

Comment pages

FAQ pages

Search pages

If there is an input field: <script>alert(“Test XSS”)</script>

It gives a popup.

**3 types of XSS vulnerability:**

1. Reflected XSS

2. Stored XSS

3. DOM based XSS (Document Object Model)

The webpages for client and server side:

Client-side languages:

1. HTML (Hypertext markup language)

2. CSS (Cascading Style Sheets)

3. JS (JavaScript)

Server-Side languages:

1. PHP (Hypertext pre-processor)

2. JAVA (JSP-Java Server Pages)

3. C#

4. .NET