National University Of Technology

Name : Ayesha Imran

Id : F24605019

Assignment : 03rd

Date : 4th-December-2025

Course : Information- Security

Submitted to : Ma'am Attiya Ashraf

OWASP TOP 10 VULNERABILITIES

1] Unvalidated Input:

- What it is: Accepting user input without checking or sanitizing it.
- Risks: Attackers can inject malicious data, leading to security breaches.
- Example: A login form that accepts any input without validation could allow SQL injection.

2] Broken Access Control:

- What it is: Failure to enforce restrictions on what users can access.
- Risks: Unauthorized users may view or modify sensitive data.
- Example: A normal user accessing admin-only pages by changing the URL.

3] Broken Account/Session Management:

- What it is: Weak handling of authentication, passwords, or session tokens.
- Risks: Attackers can hijack accounts or impersonate users.
- Example: Session IDs stored in URLs can be copied and reused by attackers.

4] Cross-Site Scripting (XSS)

- What it is: Injecting malicious scripts into webpages viewed by others.
- Risks: Theft of cookies, credentials, or user data.
- Example: A comment box that allows <script> tags lets attackers steal session cookies

5] Buffer Overflow:

- What it is: Writing more data into a memory buffer than it can hold.
- Risks: Can crash applications or allow execution of malicious code
- Example: Supplying overly long input in a form field to overwrite memory.

6] SQL Injection:

- What it is: injecting malicious SQL queries into database inputs.
- Risks: Attackers can read, modify, or delete database records.
- Example: Entering `' OR '1'='1` in a login field to bypass authentication.

7] Improper Error Handling:

- What it is: Revealing too much information in error messages.
- Risks: Attackers gain insights into system structure or database queries
- Example: A "Database connection failed at line 42" message exposes backend details.

8] Insecure Storage:

- What it is: Storing sensitive data (passwords, credit cards) without encryption.
- Risks: Data leaks if attackers gain access to storage.
- Example: Passwords stored in plain text files can be stolen easily.

9] Denial-of-Service [DOS]

- What it is: Overloading a system with excessive requests.
- Risk: website becomes unavailable to legitimate users.
- Example: Flooding a server with thousands of requests per second.

10] Insecure Configuration Management:

- What it is: Using default settings, weak permissions, or outdated software
- Risks: Attackers exploit misconfigurations to gain control.
- Example: Leaving default admin passwords unchanged on a web server.