NAME : Veekshitha
REG NO : 21BCE8943

TASK - 4

Top 10 Web server attacks

1.SQL Injection (SQLi): Attackers inject malicious SQL queries through input fields to manipulate databases and gain unauthorized access or retrieve sensitive data.

2.Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users, which can lead to data theft or manipulation.

3.Cross-Site Request Forgery (CSRF): Attackers trick users into unknowingly performing actions on a different site, potentially leading to unauthorized actions on their behalf.

4.Denial of Service (DoS): Attackers overwhelm a server by flooding it with excessive requests, rendering it unavailable to legitimate users.

5.Distributed Denial of Service (DDoS): Similar to DoS, but attackers use a network of compromised computers to amplify the attack's impact.

6.Remote File Inclusion (RFI): Attackers exploit vulnerabilities in server-side scripts to include malicious files from a remote location, potentially leading to code execution.

7.Local File Inclusion (LFI): Attackers exploit vulnerabilities to include local files, often leading to exposure of sensitive information or code execution.

8.Server-Side Request Forgery (SSRF): Attackers trick a server into making requests to internal resources or external servers, potentially leading to data exposure or remote code execution.

9.XML External Entity (XXE): Attackers exploit weak XML parsers to read internal files, execute remote requests, or manipulate data.

10.**Brute Force Attacks:** Attackers attempt to gain unauthorized access by repeatedly trying different usernames and passwords until they succeed.

____