AICS-TASK : 5

TITTLE : Explain any 10 Web Server Attacks determine them using images if

available

Name : Rohitha Koganti

1. SQL Injection (SQLi):

   - Attackers inject malicious SQL queries into input fields, exploiting vulnerabilities in poorly sanitized user inputs to access or manipulate a web application's database.

2. Cross-Site Scripting (XSS):

   - Attackers inject malicious scripts (usually JavaScript) into web pages, which are then executed in the context of other users' browsers, potentially stealing data or performing actions on their behalf.

3. Cross-Site Request Forgery (CSRF) :

   - Attackers trick users into performing unwanted actions on a different site, often by embedding malicious requests in innocent-looking links or images, leading to actions like changing account passwords.

4. Distributed Denial of Service (DDoS):

   - In a DDoS attack, multiple compromised systems are used to flood a target server with traffic, overwhelming its resources and causing it to become unavailable to legitimate users.

5. Brute Force Attack:

   - Attackers repeatedly try different username and password combinations to gain unauthorized access to a web application. This can be used to crack weak passwords.

6. Directory Traversal (Path Traversal):

- Attackers manipulate input to access files and directories outside the web application's intended directory structure, potentially exposing sensitive information or executing unauthorized actions.

7. Server-Side Request Forgery (SSRF):

- Attackers trick the server into making requests to internal or external resources on their behalf, potentially revealing sensitive information or launching further attacks.

8. XML External Entity (XXE) Attack:

- Attackers exploit weakly configured XML parsers to include malicious external entities in XML input, leading to information disclosure or denial of service.

9. Remote File Inclusion (RFI) and Local File Inclusion (LFI):

- RFI allows attackers to include remote files, often scripts, into a web application. LFI allows them to include local files, potentially revealing sensitive information or executing code.

10. Buffer Overflow:

- Attackers send excessive data to an application's buffer, overflowing it and potentially executing malicious code or crashing the server.

To prevent these attacks, web administrators should regularly update software, employ strong authentication mechanisms, sanitize user inputs, use web application firewalls (WAFs), and follow security best practices.