NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

Web server attacks target vulnerabilities in web servers and web applications to compromise data, disrupt services, or gain unauthorized access. Here are ten common web server attacks, along with brief explanations:

1. SQL Injection (SQLi):
   - Description: Attackers inject malicious SQL code into input fields, exploiting poor input validation and manipulating database queries.
   - Impact: SQLi can allow unauthorized access to databases, data theft, and data manipulation.

2. Cross-Site Scripting (XSS):
   - Description: Attackers inject malicious scripts into web pages viewed by other users, typically through input fields.
   - Impact: XSS can steal session cookies, deface websites, and lead to unauthorized actions on behalf of users.

3. Cross-Site Request Forgery (CSRF):
   - Description: Attackers trick users into executing malicious actions without their consent, leveraging the user's authentication credentials.
   - Impact: CSRF attacks can modify settings, initiate financial transactions, and cause data loss.

4. Brute Force Attacks:
   - Description: Attackers attempt to gain access to a web application by repeatedly trying different combinations of usernames and passwords.
   - Impact: Successful brute force attacks lead to unauthorized access and potential data breaches.

5. Distributed Denial of Service (DDoS):
   - Description: Attackers flood a web server with an overwhelming volume of traffic, rendering it inaccessible to legitimate users.
   - Impact: DDoS attacks disrupt services, cause downtime, and impact business continuity.

6. Remote File Inclusion (RFI):
   - Description: Attackers exploit vulnerabilities to include malicious files from remote servers into web applications.
   - Impact: RFI can lead to the execution of arbitrary code, unauthorized access, and data breaches.

7. Server-Side Request Forgery (SSRF):
   - Description: Attackers trick the server into making unintended requests to internal resources, often by manipulating URLs.
   - Impact: SSRF can lead to unauthorized access to internal resources, data leakage, or remote code execution.

NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

---

8. Path Traversal (Directory Traversal):
   - Description: Attackers manipulate input to access files or directories outside the web server's root directory.
   - Impact: Path traversal can lead to unauthorized access to sensitive files, including configuration files.

9. XML External Entity (XXE) Attack:
   - Description: Attackers exploit XML parsing vulnerabilities to load malicious XML files or entities, leading to data disclosure or remote code execution.
   - Impact: XXE attacks can expose sensitive information, compromise system integrity, and execute arbitrary code.

10. HTTP Response Splitting:
    - Description: Attackers inject malicious characters into HTTP responses, causing the browser to interpret multiple responses as separate HTTP headers.
    - Impact: HTTP response splitting can lead to various attacks, including cache poisoning, session fixation, and cookie theft.

Preventing these web server attacks involves implementing security best practices, conducting regular security assessments, patching vulnerabilities, and staying informed about emerging threats. Additionally, using web application firewalls (WAFs) and intrusion detection systems (IDS) can help mitigate the risks associated with these attacks.