task 4

10 web server attacks

1. **Distributed Denial of Service (DDoS) Attack**: In this attack, multiple compromised systems are used to flood a target server with a massive amount of traffic, overwhelming its resources and causing it to become inaccessible.
2. **SQL Injection Attack**: Attackers exploit vulnerabilities in web applications to inject malicious SQL queries into input fields, potentially allowing them to manipulate databases and gain unauthorized access to sensitive data.
3. **Cross-Site Scripting (XSS) Attack**: Attackers inject malicious scripts into web pages viewed by other users. These scripts can steal user information, manipulate content, or perform actions on behalf of the victim user.
4. **Cross-Site Request Forgery (CSRF) Attack**: Attackers trick users into unknowingly executing actions on a web application without their consent. This can lead to unauthorized actions being performed on the user's behalf.
5. **Remote File Inclusion (RFI) Attack**: Attackers exploit vulnerabilities to include remote files on a web server, which can lead to the execution of malicious code and unauthorized access.
6. **Local File Inclusion (LFI) Attack**: Similar to RFI, LFI involves exploiting vulnerabilities to include local files on a web server, potentially revealing sensitive information or executing malicious code.
7. **Server-Side Request Forgery (SSRF) Attack**: Attackers manipulate a web application to make it perform arbitrary requests to other internal or external systems, potentially revealing sensitive information or compromising the server's security.
8. **Brute Force Attack**: Attackers use automated tools to repeatedly guess usernames and passwords to gain unauthorized access to a web application or server.
9. **XML External Entity (XXE) Attack**: Attackers exploit vulnerable XML parsers to include external entities, which can lead to the disclosure of internal files or

potentially perform DoS attacks.

10. **Slowloris Attack**: A type of DoS attack where an attacker sends a large number of slow and incomplete HTTP requests to a web server, consuming its resources and keeping legitimate users from accessing the server.

It's important to note that these attacks can vary in complexity and impact. Web server administrators should implement strong security measures and keep their systems updated to mitigate the risks associated with these attacks.