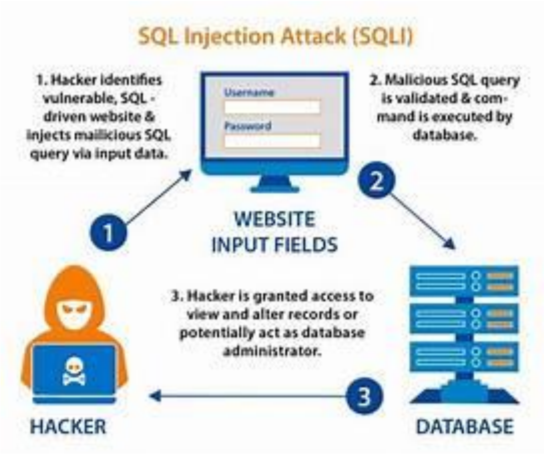
Task – 5

10 Web Server Attacks

Web Server Attacks:

Web server attacks are malicious activities designed to exploit vulnerabilities in web servers and compromise their security.

1.**SQL Injection (SQLi):** SQL Injection (SQLi) is a web attack where malicious SQL code is inserted into input fields, exploiting poor validation. This can manipulate databases, granting unauthorized access and potentially compromising data or the entire server.


SQL Injection Attack (SQLI)
1. Hacker identifies vulnerable, SQL - driven website & injects mailicious SQL query via input data.
Username
Password
2. Malicious SQL query is validated & command is executed by database.
2
1
WEBSITE INPUT FIELDS
3. Hacker is granted access to view and alter records or potentially act as database administrator.
3
HACKER
DATABASE

2. **Cross-Site Scripting (XSS):** Attackers inject malicious scripts into web pages viewed by other users. These scripts can steal user data, session cookies, or redirect users to phishing sites.

3. **Cross-Site Request Forgery (CSRF):** Attackers trick users into performing actions they didn't intend, often by embedding malicious requests in seemingly harmless links or forms.

4. **Denial of Service (DoS)**: Attackers flood the web server with excessive traffic or resource requests, causing it to become overwhelmed and unable to respond to legitimate requests.

5. **Distributed Denial of Service (DDoS):** Similar to DoS, but involves multiple compromised systems (a botnet) attacking the server simultaneously, making it even harder to mitigate.

6**. Remote File Inclusion (RFI):** Attackers exploit insecure file inclusion mechanisms to execute arbitrary code from a remote file, potentially gaining unauthorized access to the server.

7. **Local File Inclusion (LFI):** Similar to RFI, but the attacker includes files that are already present on the server, often exposing sensitive information or gaining unauthorized access.

8. **Server-Side Request Forgery (SSRF):** Attackers manipulate a web application into making requests on behalf of the server, potentially exposing internal resources or services.

9. **Path Traversal**: Attackers manipulate input to traverse directories and access files outside of the intended directory structure, potentially exposing sensitive information.

10. **Buffer Overflow**: Attackers exploit vulnerabilities in a web application's code to overwrite parts of memory, potentially leading to unauthorized code execution.