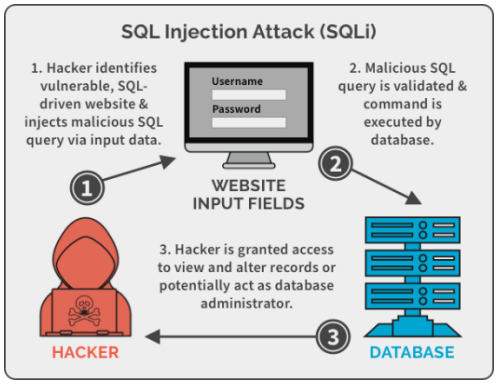
Saumyaa Prajapat
21BCI0265

Task5:

10 most common web server attacks

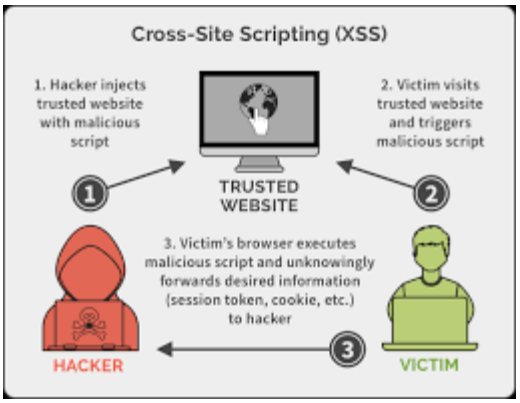
1. **SQL Injection (SQLi):**

This attack involves injecting malicious SQL queries into input fields or URLs, exploiting vulnerabilities in the application's database layer to gain unauthorized access to the database or manipulate data.



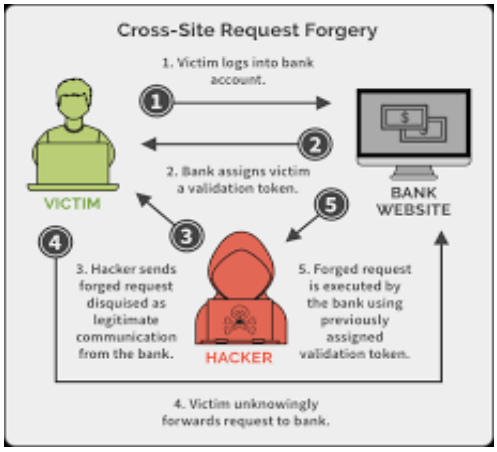
2. **Cross-Site Scripting (XSS):**

Attackers inject malicious scripts into web applications, which are then executed by users' browsers. This can lead to theft of sensitive information or session hijacking.



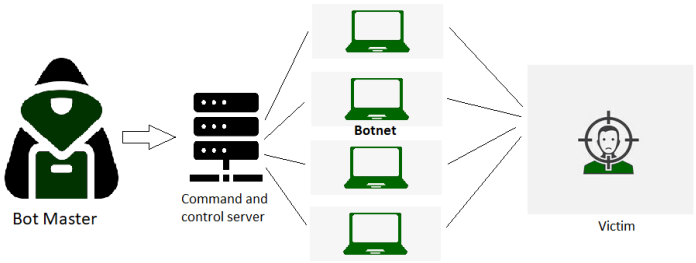
3. **Cross-Site Request Forgery (CSRF):**

In a CSRF attack, a user is tricked into unknowingly making unwanted requests to a web application, usually resulting in actions performed on behalf of the user without their consent.



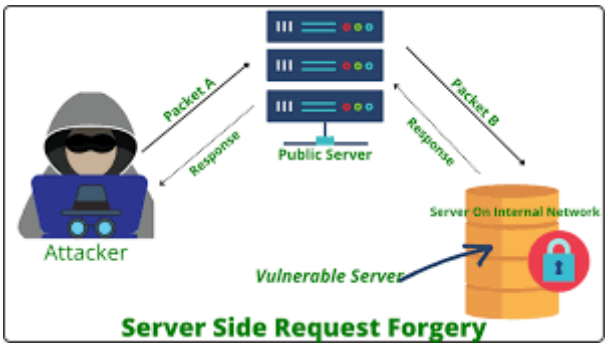
4. **Distributed Denial of Service (DDoS):**

In a DDoS attack, multiple compromised computers are used to flood a target server with traffic, overwhelming its resources and making it inaccessible to legitimate users.



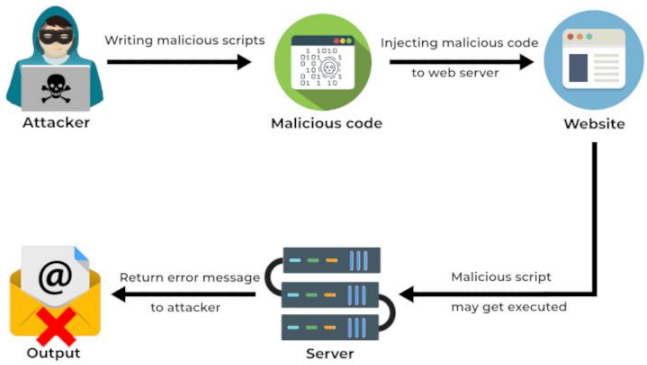
5. **Server-Side Request Forgery (SSRF):**

Attackers exploit a vulnerability to make a server perform requests to other internal resources or external servers, which can lead to unauthorized data access or further attacks.



6. **Remote Code Execution (RCE):**

This attack allows an attacker to execute arbitrary code on a target server, gaining complete control over the system and potentially leading to data breaches or server compromise.



7. File Inclusion Exploits:

Attackers exploit insecure file inclusion methods to execute malicious code stored in external files, potentially gaining unauthorized access to the server.

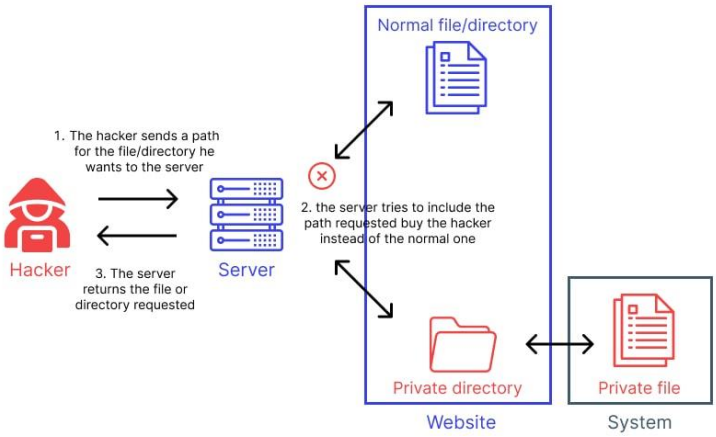
8. Brute Force Attacks:

In a brute force attack, attackers repeatedly try different username and password combinations to gain unauthorized access to a web server, exploiting weak or easily guessable credentials.

9. Path Traversal Attacks:

By manipulating input, attackers attempt to navigate to directories outside the web server's root directory, potentially gaining access to sensitive files or directories.

Saumyaa Prajapat
21BCI0265



10. Zero-Day Exploits:

Attackers target previously unknown vulnerabilities in web server software before the vendor releases a patch. These attacks can be particularly dangerous, as there are no available fixes.