Injection Attacks:

Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

There are different types of Injection based attacks:

1. SQL Injection Attack
2. Cross Site Scripting Attack
3. Cross Site Request Forgery

SQL injection

SQL injection is a code injection technique in which malicious SQL statements are inserted into an entry field for execution.

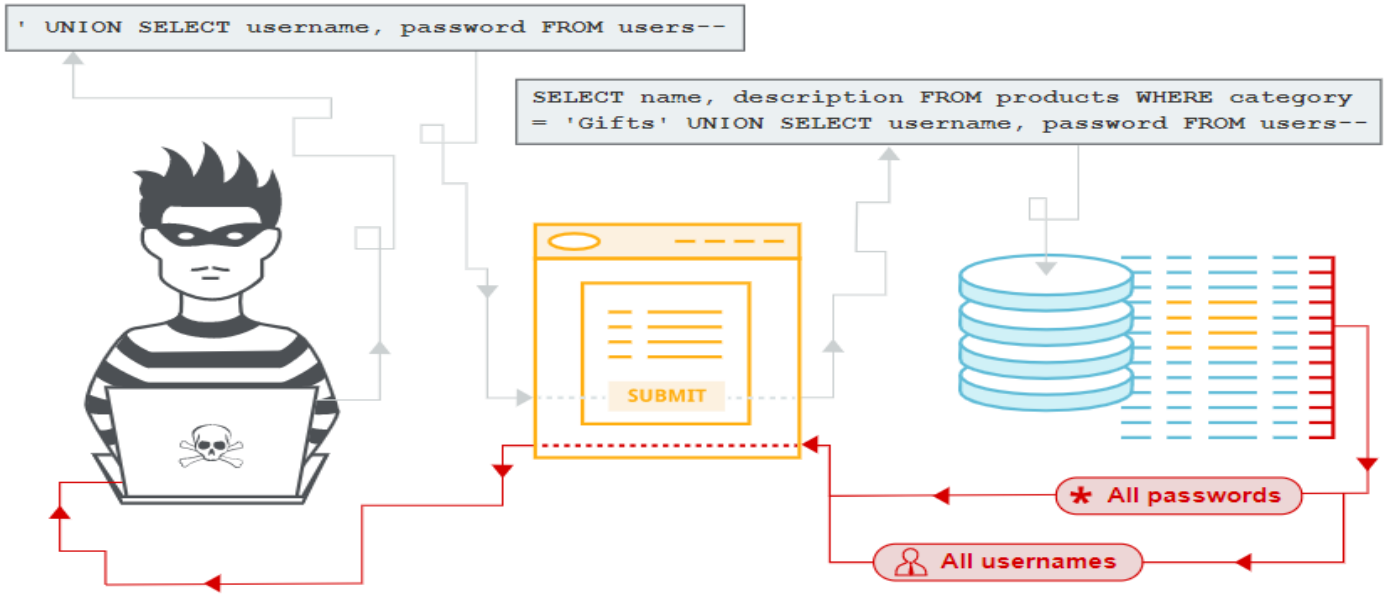
These SQL statements control a database server behind a web application. By executing malicious statements, the attacker can gain unauthorized access, copy, modify or delete the data.

Example of malicious SQL Statement:

1. * OR '1'='1'
2. SELECT * FROM Users WHERE UserId = 105 OR 1=1;

Mitigations:

1. Input validation
2. Sanitize all inputs (like remove quotes and special characters)
3. Use IPS and WAF solutions
4. Turn off visibility of Database errors on production servers



Cross-site Scripting (XSS)

- Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. Usually happens where there is a text message box in the website. Like comments for a blog
- The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.
- The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user's browser.
- Vulnerable vehicles that are commonly used for Cross-site Scripting attacks are forums, message boards, and web pages that allow comments.

How Cross-site Scripting Works…?

- There are two stages to a typical XSS attack:
- To run malicious JavaScript code in a victim's browser, an attacker must first find a way to inject malicious code (payload) into a web page that the victim visits.
- After that, the victim must visit the web page with the malicious code. If the attack is directed at particular victims, the attacker can use social engineering and/or phishing to send a malicious URL to the victim.

Mitigations:

1. Input validation
2. Sanitize all inputs (like remove quotes and special characters)
3. Encode data on output.
4. Use appropriate response headers.
5. Content Security Policy.

Click on the below Link to view more about XSS Attack:

https://www.youtube.com/watch?v=cbmBDiR6WaY

Cross Site Request Forgery

Also called as **one-click attack or session riding**

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

Example: User A is connected to a banking webs it e - www.mybank.com

Attacker tricks the user into downloading and executing a code.

This code will send request to www.mybank.com to transfer money to attackers account.

In this case the banking website performs the request because it see the request coming from User A's machine who is already authenticated with the server.

Mitigations:

1. Synchronize token pattern
2. Cookie-to-header token
3. Double Submit Cookie

How CSRF Works..?