SQl Injection in php system

Aim – To execute SQLI in vulnerable websites!

Description –

SQL injection is a web security weakness that helps an attacker to interfere with the requests an application makes to its database. Generally, it helps an intruder to access data that they are not normally able to retrieve. This could include data belonging to other users or any other data that may be accessed by the program itself. In certain instances, the attacker can change or delete this.

Impact of the attack-

Effective SQL injection attacks can result in unauthorized access to sensitive data, such as passwords, credit card numbers, or personal user information. Many high-profile data breaches in recent years have resulted from SQL injection attacks, leading to credibility loss and regulatory penalties. In certain instances, the intruder will achieve a permanent loophole to the organization's processes, lea.

Tools Used-

Burp suite Pro, Sqlmap,

Prevention of the attack –

Parameterized queries may be used in any case where the untrusted input appears as data within the query, including the WHERE clause and values in the INSERT or UPDATE statement. They cannot be used to manage untrusted input in other aspects of the query, such as table or column names, or the ORDER BY clause. Application code that positions untrusted data in certain parts of the query would need to take a different path, such as white listing enabled input values, or using a different logic to provide the necessary actions.