Group no: - 8

Group Member:- **Shrut Shah – 19BCP125**

Shubham Kathiriya – 19BCP127

Vedant Patel – 19BCP138

Subject: - Cyber Security Lab

Division:-2

Lab 8:- SQL Injection

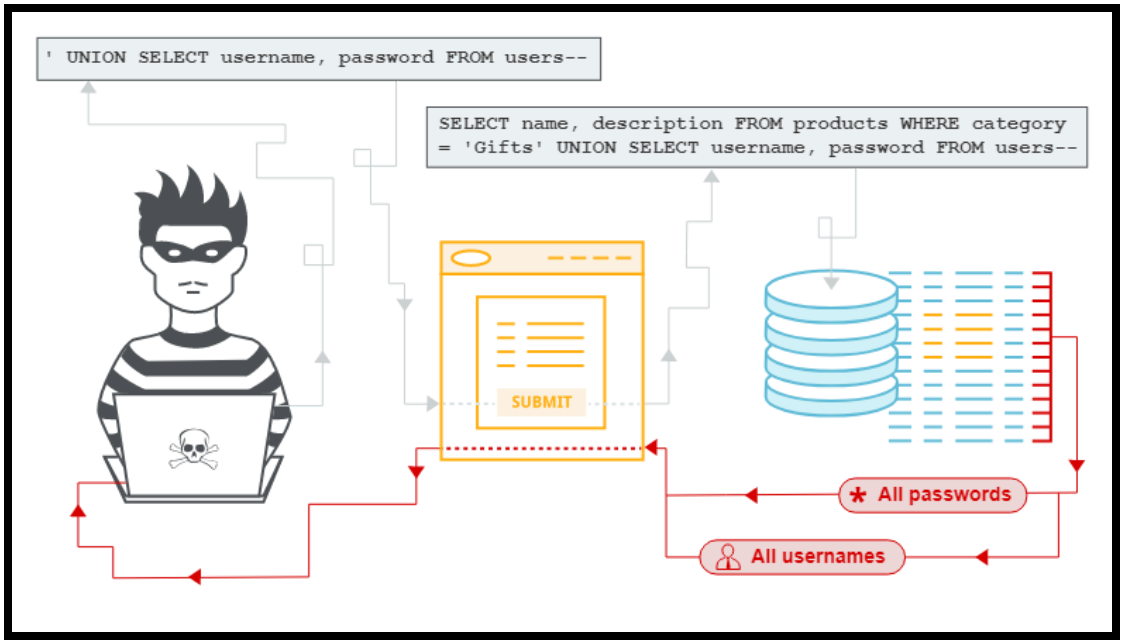
SQL Injection Attack

SQL Injection can be defined as a technique where hacker executes malicious SQL queries on the database server through web application to either gain access over the sensitive information or on the database.

This is the web-based vulnerability which allows attacker to spoof the identity, destroys the data present on the system and changes the record present on the database.

The main consequences of SQL injection include loss of confidentiality, authentication as the attacker without providing the authentic username and password could successfully obtain access over the network by manipulating the logic of SQL commands.

❖ ***Threats of SQL Injection***



A. Identity Spoofing
B. Modifying the records resent in the database
C. Gaining access over administrative privileges
D. Denial of Service
E. Attacking machine's performance

❖ ***Types of SQL Injection***

1. In-band SQLi (classic SQLi)
    a.) Error-based SQLi
    b.) Union-based SQLi
2. Blind SQLi (inferential SQLi)

❖ ***Step by step methods used by the attacker to implement SQL injection are as following:***

- ✔ Information Gathering
- ✔ SQL injection Vulnerability Detection
- ✔ Launch SQL injection attack
- ✔ Extract the data

❖ ***SQL Injection Queries***

1. Malicious SQL query:

   Input- a' OR 1=1#

   Query-SELECT userid , name FROM users WHERE id = 'a' OR 1=1#'

   Output-This query is always true.If website is vulnerable to SQL injection then attacker without providing the authentic username and password could successfully obtain the access over the network.

2. Query for Updating Table:
   Input- a';UPDATE users SET name='pqr' WHERE id=1 #

   Query- SELECT userid,name FROM users WHERE userid='a';UPDATE users SET name='pqr' WHERE id=1 #'

   Output- This query modifies the name of the user with id 1 to 'pqr'

3. Query for deleting Table:
   Input- a' ; DROP TABLE users ;#

   Query- SELECT userid,name FROM users WHERE userid='a'; DROP TABLE users ;#'

   Output – Through this query the table 'users' is dropped

❖ ***Code:-***

★ ***SQL Scripts:-***

➔Sql code for creating tables:-

```
CREATE TABLE users(

ID                      integer,
name            varchar(30),
password        varchar(30),
description     varchar(30)
);


CREATE TABLE PC(

ID                      integer,
code            varchar(30),
name            varchar(30),
price           integer
);
```

➔Sql code for Inserting the values:-

```
INSERT INTO USERS VALUES(1,'Admin', 'P?a?w@d', 'root');
INSERT INTO USERS VALUES(2, 'user1', 'pass1word', 'usuario1');
INSERT INTO USERS VALUES(3, 'user2', 'pass2word', 'usuario2');
INSERT INTO PC VALUES(1,'BC1212', 'PC1', 300);
```

```
INSERT INTO PC VALUES(2, 'BC1222', 'PC2', 350);
INSERT INTO PC VALUES(3, 'BC9122', 'PC3', 540);
```

It provides a vulnerable webserver (Apache) with html and php related scripts to configure the server. Also, some possible solutions are given to break the system. The DB for this project is PostgreSQL. Other DB can be used, just change the conexion file and PostgreSQL functions.

❖ ***Output Screenshot:-***

```
test=# select * from users;
 id | name  | password | description
----+-------+----------+-------------
  1 | Admin | 1212     | root
  2 | user1 | pwd4     | user1
  3 | user2 | pwd?@    | user2
(3 rows)
```

```
test=# select * from pc;
 id |  code  | name | price
----+--------+------+-------
  1 | BCA123 | pc2  |   350
  2 | BCA123 | pc2  |   350
  3 | BCA777 | pc3  |   633
(3 rows)
```

SQL Scripts:-

SQL Injection Prevention:

- ✔ Minimizing the Privileges

- ✔ SQL Server Firewalling
- ✔ We use the following functions which is already defined in PHP -

  mysqli_real_esape_string(database connection,query);
  stripslashes();

- ❖ **example:**

  When user types his/her username and password in this form ("" or ""="“); access should not be granted.
  as it may lead to false negative query result from the database and grant access to intruder or illegitimate user.

- ❖ ***Conclusion:***

SQL injection attacks are the major problem for the database, which in turn applied to the web application, which includes the database as a background data controller. Severity levels of attacks are increasing day-by-day with the huge usage of data. SQLi attack is one of the sophisticated methods resulting in great financial loss to an organization when it attacks the sensitive data in the database. It also destroy the data or make it otherwise unavailable, and intruder become administrators of the database server and cause change up to large extent which may be very dangerous for any organization and can cause heavy loss to that organization .