FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING
Department of Computer Engineering

Course , Subject & Experiment Details

Academic Year	**2019-20**	**Estimated Time**	**02 - Hours**
Course & Semester	**T.E. (CMPN)- Sem VI**	**Subject Name & Code**	**CSS - (CSL604)**
Module No.	**06– Mapped to CO- 3**	**Chapter Title**	**System Security**

Practical No:	**10**
Title:	To study and implement SQL Injection.
Date of Performance:	
Date of Submission:	
Roll No:	
Name of the Student:	

Evaluation:

Sr. No	**Rubric**	**Grade**
1	**On time submission Or completion (2)**	
2	**Preparedness(2)**	
3	**Skill (4)**	
4	**Output (2)**	

Signature of the Teacher:

Date:

Prepared By MNS

Title: : To study and implement SQL Injection.

Lab Objective :

This lab provides insight into:

- What is SQL injection attack .

Reference : “Information security Principles and Practice” by Mark Stamp, Wiley publication

Prerequisite : Java, Database .

Theory:

SQL injection is one of the web attack mechanism used by attackers to insert malicious SQL statements directly to the database.

It is the most common application layer attack technique that allows an attacker to alter the SQL statements in order to exploit vulnerability in software.

The vulnerability is present when user input is either incorrectly filtered for string literal,escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is in fact an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.

Following vulnerabilities may be used by an attacker to perform SQL injection

i) Insufficient input validation

ii) Improper construction of SQL statement

iii) Incorrectly filtered escape characters

iv) Incorrect type handling.

e. g. Consider following SQL query which extracts the record of given username from the table LoginData.

```
 Var statement = select * from LoginData

      where name = ‘ “ +username+”’;”
```

Here an attacker may set the username maliciously as,

```
username : a100' OR 1=1- -
```

password : anything

then the query in DB is executed as

select * from LoginData

where username='a100' OR 1=1- -'

and password='anything'

becomes true as 1=1 is true and - - marks the start of SQL comment

Here, the second clause ‘1’ = ‘1’ is always evaluated to True , So an attacker is easily granted an access to the database.

Defenses against SQL injection attack

i) Using web application firewall : The set of rules should be used by firewall to filter dangerous web requests.

ii) Limit database privileges by context : Minimum level of privileges should be assigned to multiple user accounts.

iii) Comprehensive data sanitization : Web sites must perform validation by filtering all user inputs. The user input should be filtered for content i.e for email-id, phone number etc.

iv) Avoid constructing SQL queries with user input : Instead of constructing full queries, SQL variable binding with prepared statements should be used.

ALGORITHM:

1. Start
2. Create a GUI for entering username and password
3. Establish database connection using JDBC
4. Perform SQL injection attack
5. End

Conclusion:

The program was tested for different sets of inputs.
Program is working SATISFACTORY NOT SATISFACTORY
(Tick appropriate outcome)

Post Lab Assignment:

1. **Give different types of malicious attacks possible on web server.**

2. An SQL injection attack may be used to
   a) delete a table
   b) read a row in a table
   c) change column names in a table
   d) change number of columns in a table

3. The most effective remedy for SQL injection attacks is
   a) to filter HTML form input at the client side
   b) to employ stored procedures on the database server
   c)to employ prepared SQL statements on the web server
   d)to perform input validation on the server via regular expression