Indian Institute of Technology Jodhpur

Computer Science and Engineering Department

Lab 9

CSL6010 - Cyber Security

Date: 13-04-2023 **Marks: 10**

Aim: Understanding SQL Injection attack.

Part-1 How SQL Injection Works

Visit http://sqlfiddle.com/ and perform the following:

Step1) Enter this code in left pane

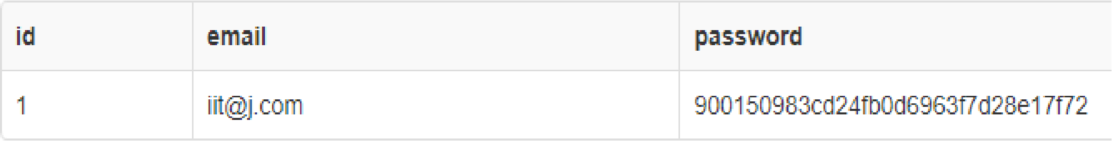
```
CREATE TABLE `users` (
  `id` INT NOT NULL AUTO_INCREMENT,
  `email` VARCHAR(45) NULL,
  `password` VARCHAR(45) NULL,
  PRIMARY KEY (`id`));
insert into users (email,password) values ('iit@j.com',md5('abc'));
```

Step 2) Click Build Schema

Step 3) Enter this code in right pane

```
select * from users;
```

Step 4) Click Run SQL. You will see the following result



id	email	password
1	iit@j.com	900150983cd24fb0d6963f7d28e17f72

Suppose the user supplies cybersecurity@iitj.ac.in and CSL6010 as the password. The SQL statement to be executed against the database would be as follows:

SELECT * FROM users WHERE email = ‘cybersecurity@iitj.ac.in’ AND password = md5(‘CSL6010’);

Q1. How can the above SQL query be exploited by the attacker using SQL Injection?

Part-2 SQL Inject a Web Application

Visit the following url: http://www.techpanda.org/index.php and try to login with some random guessed Id and password.

Let’s suppose an attacker provides the following example input:

Step 1: Enter **xxx@xxx.xxx** as the email address

Password 1: **xxx’) OR 1 = 1 —]**

Password 2: **1234**

Password 3: **xxxx**

Q2. What will be the generated SQL statement for your above guessed/example password login.