TASK 1:


```
good practice to stop labs before transitioning to
new labs or to instructor instances, otherwise there
may be networking name conflicts.

If you wish to restart a lab from scratch, wiping out
all previous data and work in the lab, use:

    labtainer <labname> -r
student@LabtainersVM:~/labtainer/labtainer-student$ labtainer sql-inject
non-network local connections being added to access control list
[2023-09-30 18:59:13,350 - ERROR : labutils.py:813 - CreateSubnets() ] Already
exists! Not creating some_network subnet at 172.25.0.0/24!

Starting the lab, this may take a moment...
Started 2 containers, 2 completed initialization. Done.




The lab manual is at
    file:///home/student/labtainer/trunk/labs/sql-inject/docs/sql-inject.pdf

You may open the manual by right clicking
and select "Open Link".


Press <enter> to start the lab

student@LabtainersVM:~/labtainer/labtainer-student$
```

Activities   ▣ Terminal ▾   Sat 19:14 ●   🔗 🔊 ⏻ ▾

student@web-server:~   ⊖ ▢ ✕

File Edit View Search Terminal Help

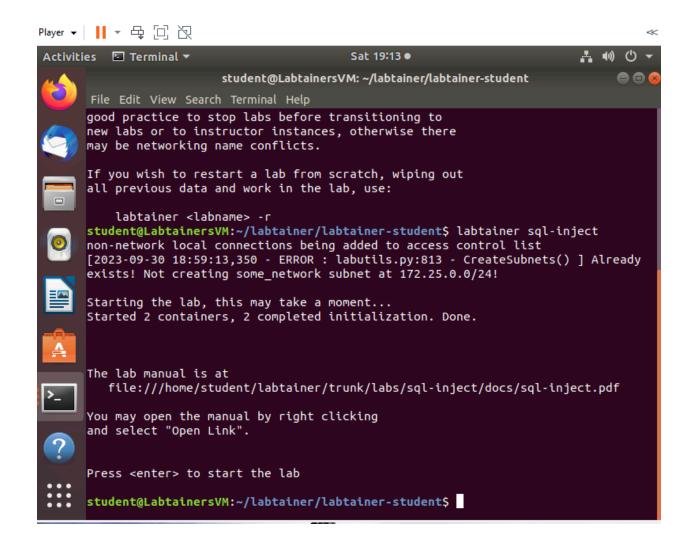Last login: Sat Sep 30 21:44:16 UTC 2023 on pts/1
[student@web-server ~]$
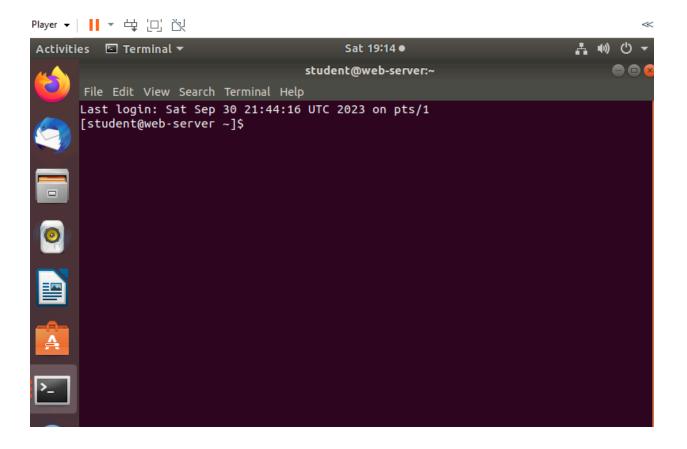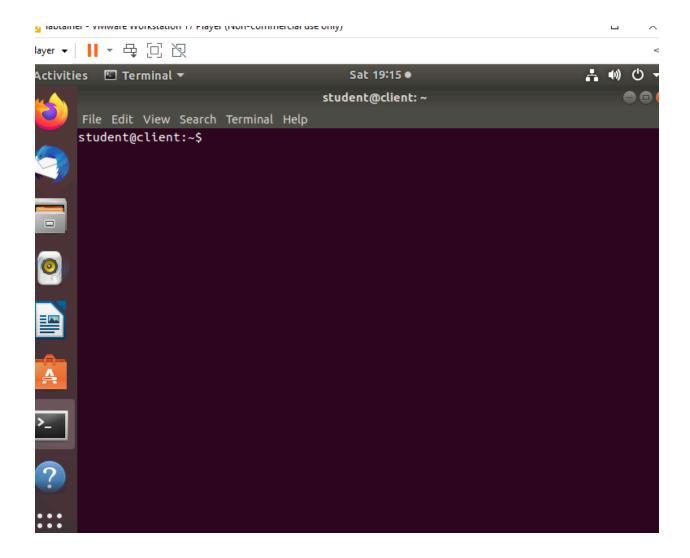
Description of Task 1

We run the command on labtainer sql-inject -r

This will create 2 more terminal which is student client and student web server

Also have firefox instance from client

Task 2

student@web-server:~

File Edit View Search Terminal Help

```
Last login: Sat Sep 30 21:44:16 UTC 2023 on pts/1
[student@web-server ~]$ mysql -u root -pseedubuntu
Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.6.39 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> select * from credential;
```

```
1 row in set (0.00 sec)

mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+------
--+----------+-------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Emai
l | NickName | Password                                  |
+----+-------+-------+--------+-------+----------+-------------+---------+------
--+----------+-------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |
  |          | fdbe918bdae83000aa54747fc95fe0470fff4976  |
|  2 | Boby  | 20000 |  30000 | 4/20  | 10213352 |             |         |
  |          | b78ed97677c161c1c82c142906674ad15242b2d4  |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |         |
  |          | a3c50276cb120637cca669eb38fb9928b017e9ef  |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |         |
  |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af  |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |         |
  |          | 99343bff28a7bb51cb6f22cb20a618701a2c2f58  |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |         |
  |          | a5bdf35a1df4ea895905f6f6618e83951a6effc0  |
+----+-------+-------+--------+-------+----------+-------------+---------+------
--+----------+-------------------------------------------+
6 rows in set (0.01 sec)

mysql>
```

Select statement shows information on the table that created on the database

```
6 rows in set (0.01 sec)

mysql> select * from credential where eid = 10000 and Password = 'fdbe918bdae83
000aa54747fc95fe0470fff4976';
+----+-------+-------+--------+-------+----------+-------------+---------+------
--+----------+-------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Emai
l | NickName | Password                                  |
+----+-------+-------+--------+-------+----------+-------------+---------+------
--+----------+-------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |
  |          | fdbe918bdae83000aa54747fc95fe0470fff4976  |
+----+-------+-------+--------+-------+----------+-------------+---------+------
--+----------+-------------------------------------------+
1 row in set (0.02 sec)

mysql>
```

seedlabsqlinjection.com ╳   +

← → C ⌂   ⓘ seedlabsqlinjection.com/unsafe_credential   ⋯ ▽ ☆   ↓ » ≡

Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Ryan Profile

Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number:

Samy Profile

Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

Ted Profile

Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile

Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:

```
<br><h4> Alice Profile</h4>Employee ID: 10000      salary: 20000      birth: 9/20
    ssn: 10211002    nickname: email: address: phone number: <br><h4> Boby Prof
ile</h4>Employee ID: 20000      salary: 30000      birth: 4/20    ssn: 10213352
    nickname: email: address: phone number: <br><h4> Ryan Profile</h4>Employee ID
: 30000      salary: 50000      birth: 4/10     ssn: 98993524    nickname: email:
address: phone number: <br><h4> Samy Profile</h4>Employee ID: 40000      salary:
 90000      birth: 1/11     ssn: 32193525    nickname: email: address: phone numb
er: <br><h4> Ted Profile</h4>Employee ID: 50000      salary: 110000      birth: 1
1/3    ssn: 32111111    nickname: email: address: phone number: <br><h4> Admin
Profile</h4>Employee ID: 99999      salary: 400000      birth: 3/5    ssn: 432543
14    nickname: email: address: phone number:
<div class=wrapperL>
<p>
<button onclick="location.href = 'edit.php';" id="editBtn" >Edit Profile</butto
n>
</p>
</div>


<div id="page_footer" class="green">
<p>
Copyright &copy; SEED LABs
</p>
</div>
</body>
</html>
student@client:~$
```