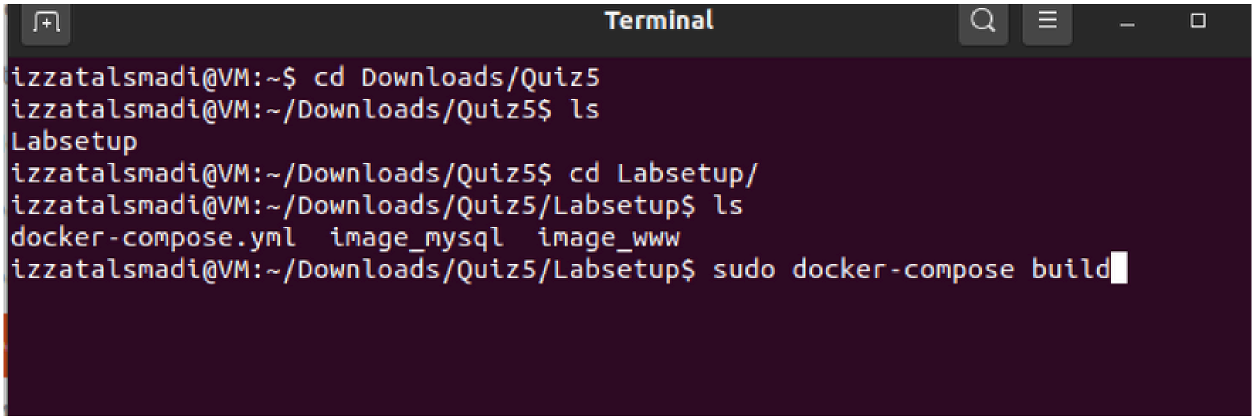
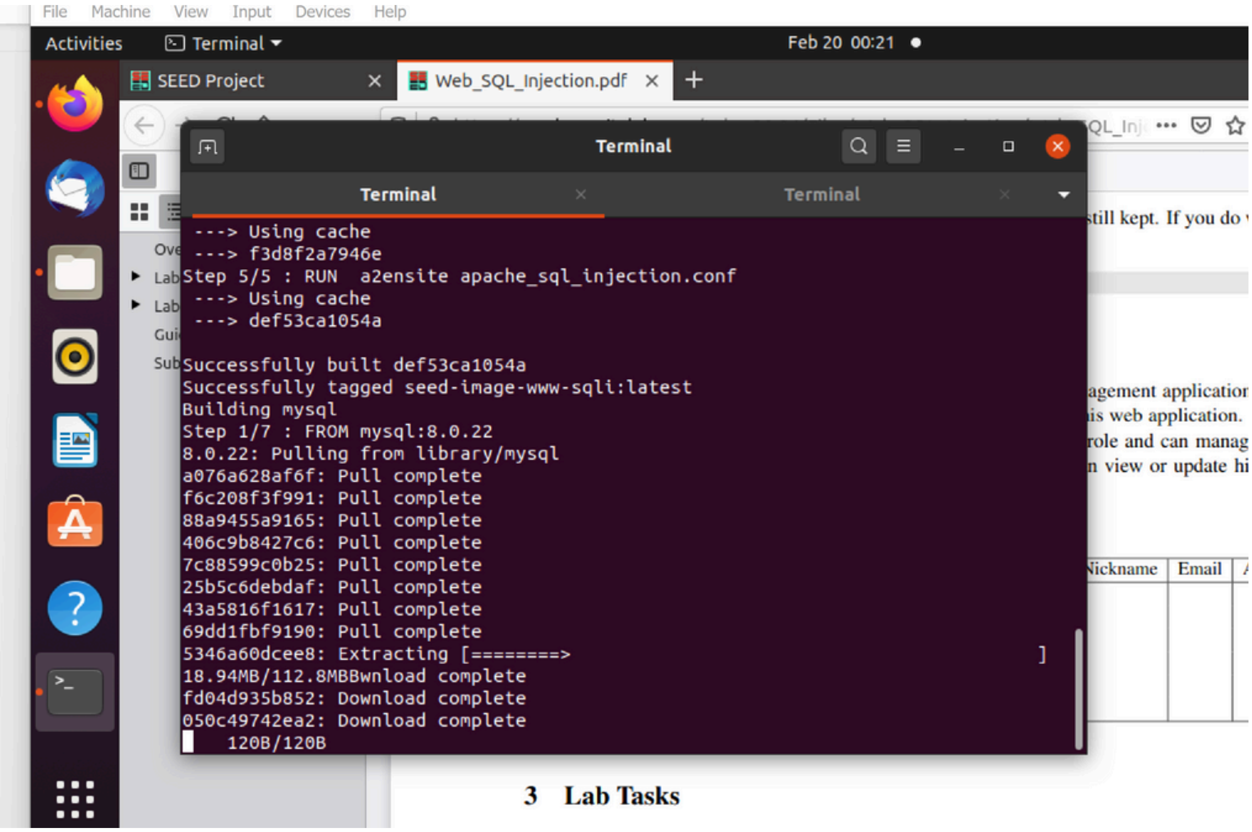
Lab10 SQL Injection

https://seedsecuritylabs.org/Labs_20.04/Web/Web_SQL_Injection/



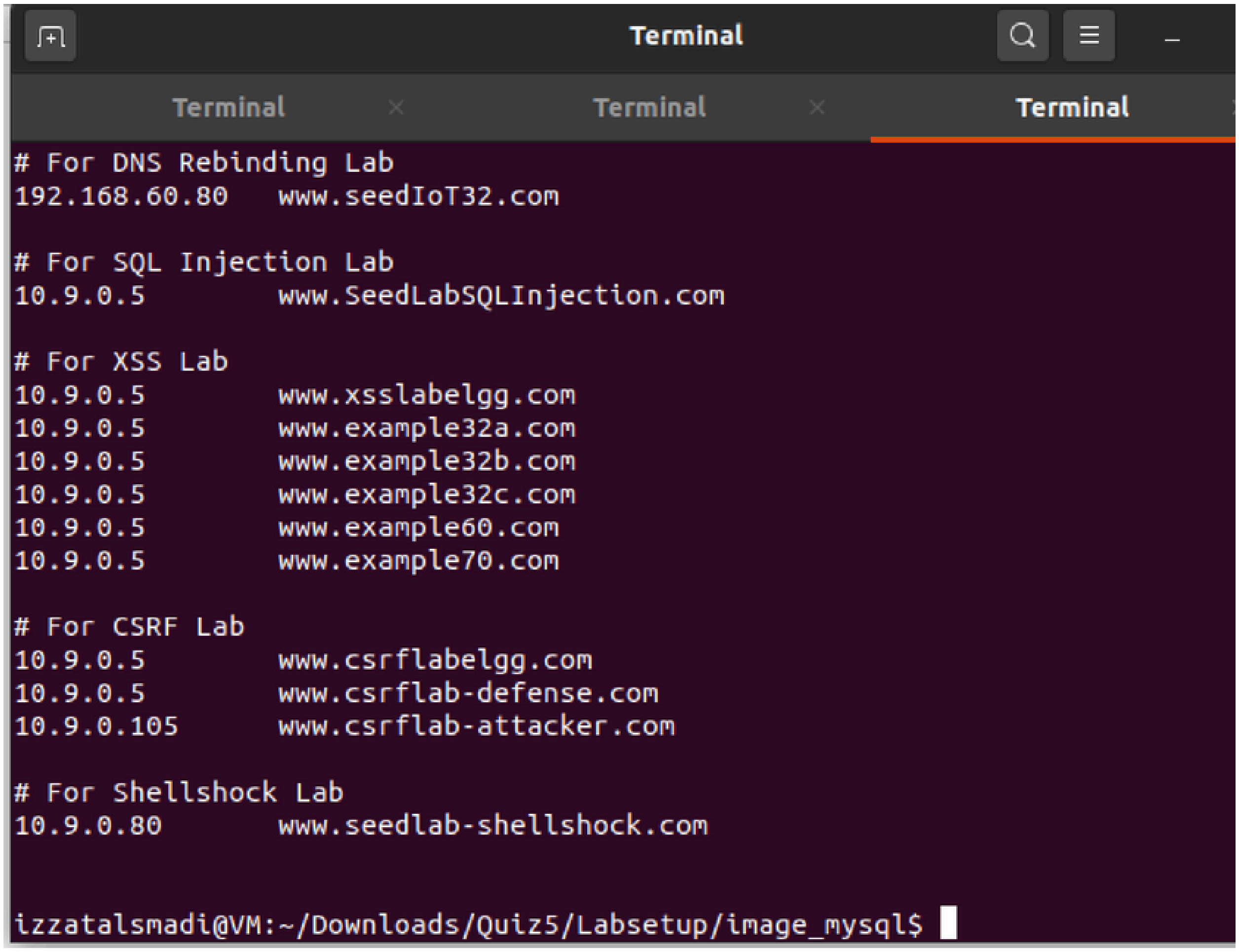
```
izzatalsmadi@VM:~$ cd Downloads/Quiz5
izzatalsmadi@VM:~/Downloads/Quiz5$ ls
Labsetup
izzatalsmadi@VM:~/Downloads/Quiz5$ cd Labsetup/
izzatalsmadi@VM:~/Downloads/Quiz5/Labsetup$ ls
docker-compose.yml  image_mysql  image_www
izzatalsmadi@VM:~/Downloads/Quiz5/Labsetup$ sudo docker-compose build
```

- You have two containers in two folders, you need to build and up each one separate



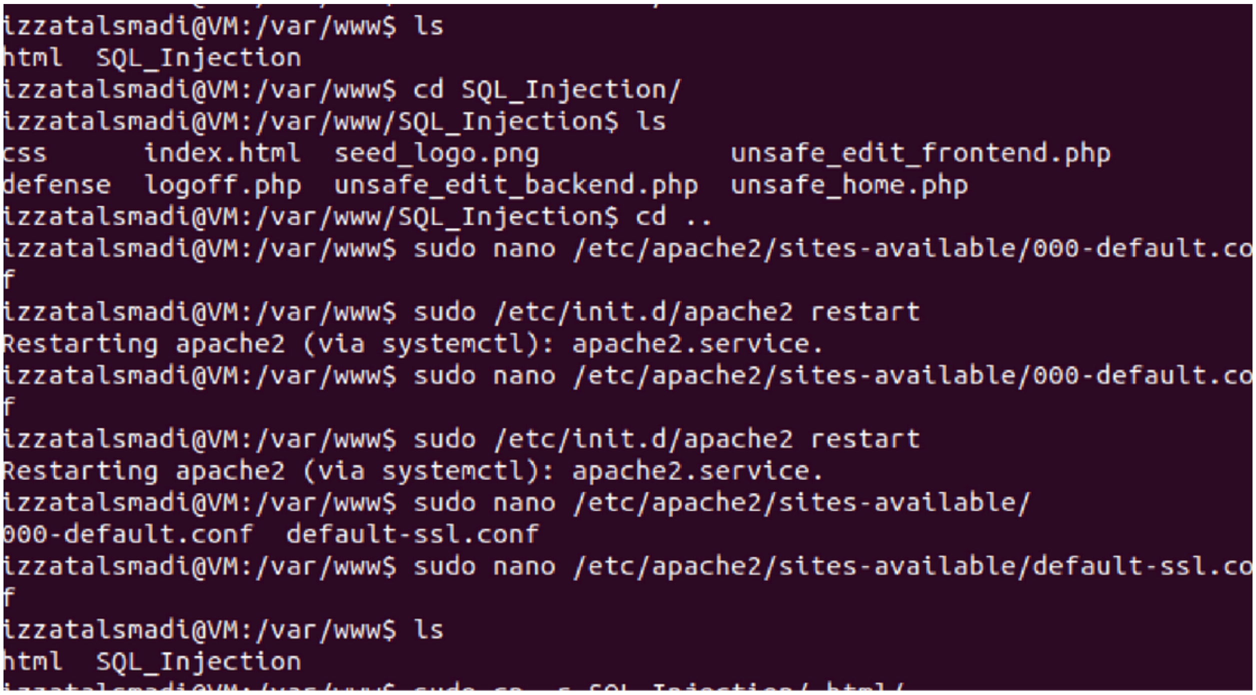
```
 ---> Using cache
 ---> f3d8f2a7946e
Step 5/5 : RUN  a2ensite apache_sql_injection.conf
 ---> Using cache
 ---> def53ca1054a

Successfully built def53ca1054a
Successfully tagged seed-image-www-sqli:latest
Building mysql
Step 1/7 : FROM mysql:8.0.22
8.0.22: Pulling from library/mysql
a076a628af6f: Pull complete
f6c208f3f991: Pull complete
88a9455a9165: Pull complete
406c9b8427c6: Pull complete
7c88599c0b25: Pull complete
25b5c6debdaf: Pull complete
43a5816f1617: Pull complete
69dd1fbf9190: Pull complete
5346a60dcee8: Extracting [========>                                          ]
18.94MB/112.8MBBwnload complete
fd04d935b852: Download complete
050c49742ea2: Download complete
    120B/120B
```

- If both containers build properly you should see this up in your Browser
  Check etc/hosts



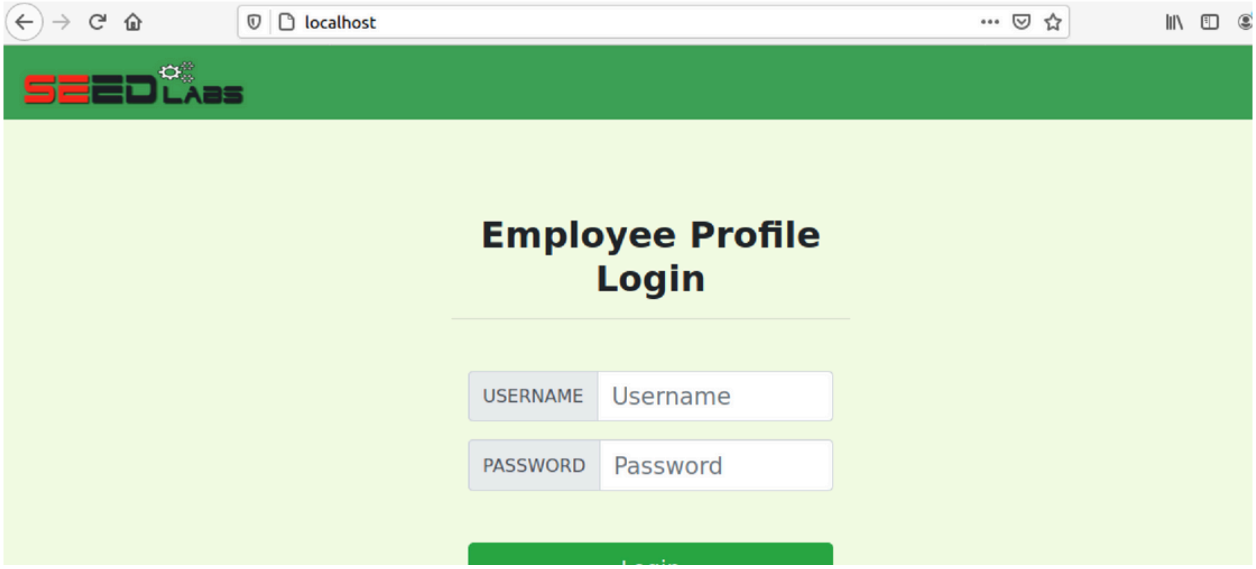
```
# For DNS Rebinding Lab
192.168.60.80   www.seedIoT32.com

# For SQL Injection Lab
10.9.0.5        www.SeedLabSQLInjection.com

# For XSS Lab
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com

# For CSRF Lab
10.9.0.5        www.csrflabelgg.com
10.9.0.5        www.csrflab-defense.com
10.9.0.105      www.csrflab-attacker.com

# For Shellshock Lab
10.9.0.80       www.seedlab-shellshock.com


izzatalsmadi@VM:~/Downloads/Quiz5/Labsetup/image_mysql$ 
```

- I have to reinstall Apache and copy code folder (rename it SQL_Injection) to /var/www/html



```
izzatalsmadi@VM:/var/www$ ls
html   SQL_Injection
izzatalsmadi@VM:/var/www$ cd SQL_Injection/
izzatalsmadi@VM:/var/www/SQL_Injection$ ls
css       index.html   seed_logo.png             unsafe_edit_frontend.php
defense   logoff.php   unsafe_edit_backend.php   unsafe_home.php
izzatalsmadi@VM:/var/www/SQL_Injection$ cd ..
izzatalsmadi@VM:/var/www$ sudo nano /etc/apache2/sites-available/000-default.co
f
izzatalsmadi@VM:/var/www$ sudo /etc/init.d/apache2 restart
Restarting apache2 (via systemctl): apache2.service.
izzatalsmadi@VM:/var/www$ sudo nano /etc/apache2/sites-available/000-default.co
f
izzatalsmadi@VM:/var/www$ sudo /etc/init.d/apache2 restart
Restarting apache2 (via systemctl): apache2.service.
izzatalsmadi@VM:/var/www$ sudo nano /etc/apache2/sites-available/
000-default.conf   default-ssl.conf
izzatalsmadi@VM:/var/www$ sudo nano /etc/apache2/sites-available/default-ssl.co
f
izzatalsmadi@VM:/var/www$ ls
html   SQL_Injection
izzatalsmadi@VM:/var/www$ sudo cp -r SQL_Injection/ html/
```

- Now if I type in the Browser localhost, I can see the web app



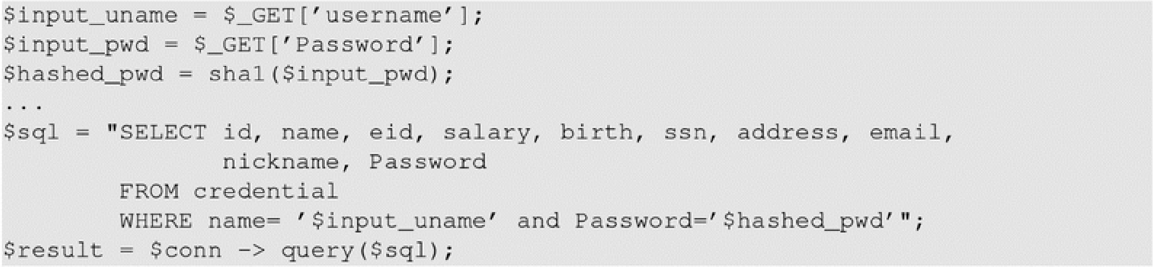
localhost

Employee Profile Login

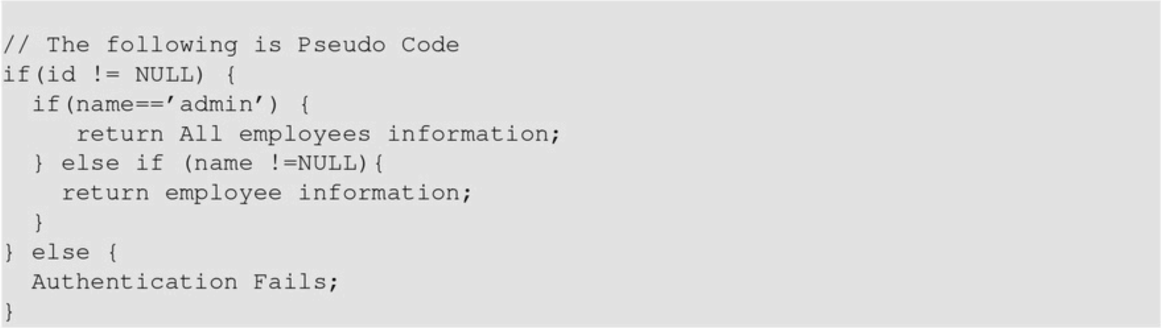
USERNAME Username

PASSWORD Password

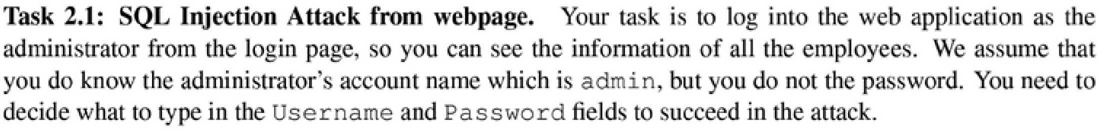
To help you started with thi stask, we explain how authentication is implemented in the web application. The PHP code unsafe home.php, located in the/var/www/SQL_Injection directory, isused to conduct user authentication. The following code snippet show how users are authenticated.



```
$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);
...
$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,
              nickname, Password
        FROM credential
        WHERE name= '$input_uname' and Password='$hashed_pwd'";
$result = $conn -> query($sql);
```

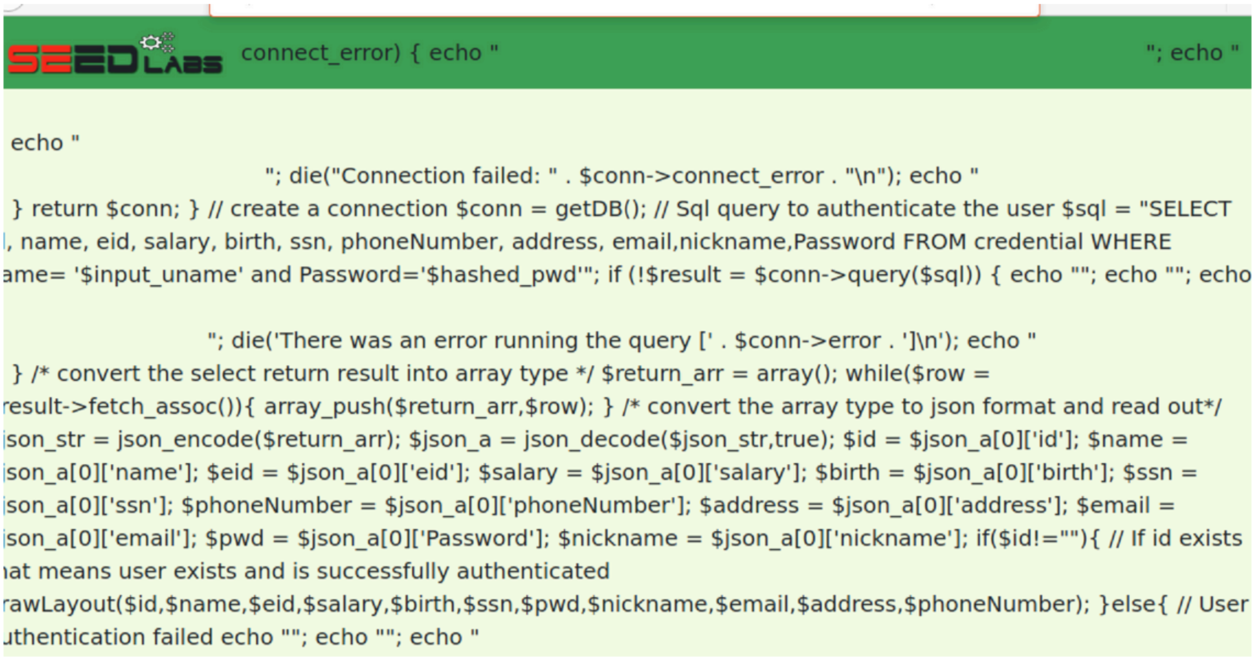


```
// The following is Pseudo Code
if(id != NULL) {
  if(name=='admin') {
     return All employees information;
  } else if (name !=NULL){
    return employee information;
  }
} else {
  Authentication Fails;
}
```



Task 2.1: SQL Injection Attack from webpage. Your task is to log into the web application as the administrator from the login page, so you can see the information of all the employees. We assume that you do know the administrator's account name which is `admin`, but you do not the password. You need to decide what to type in the `Username` and `Password` fields to succeed in the attack.

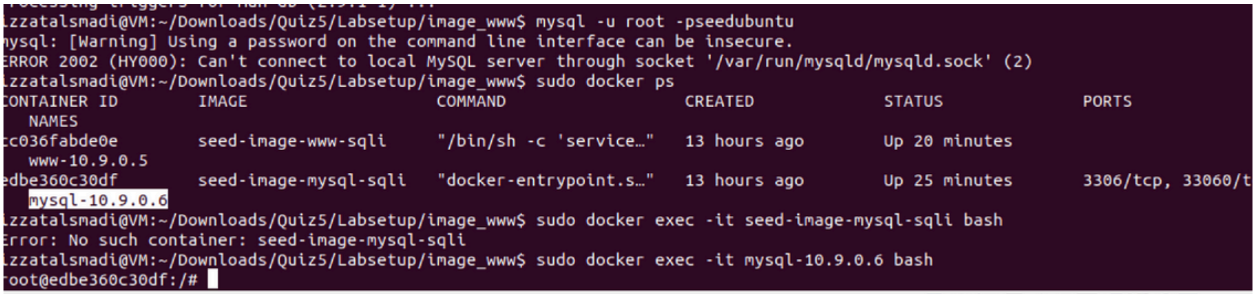
- I first tried (admin and 1=1') but didn't work



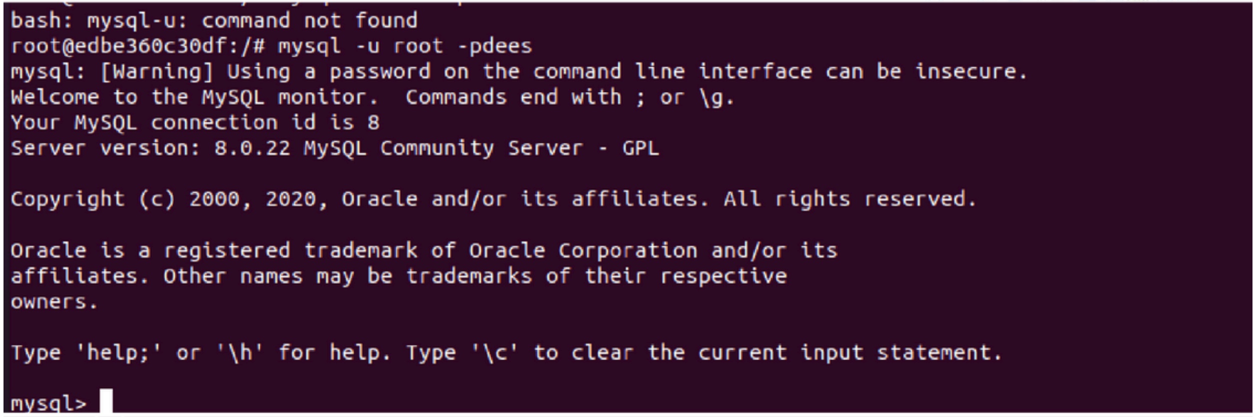
connect_error) { echo " "; echo "

echo "
"; die("Connection failed: " . $conn->connect_error . "\n"); echo "
} return $conn; } // create a connection $conn = getDB(); // Sql query to authenticate the user $sql = "SELECT
l, name, eid, salary, birth, ssn, phoneNumber, address, email,nickname,Password FROM credential WHERE
ame= '$input_uname' and Password='$hashed_pwd'"; if (!$result = $conn->query($sql)) { echo ""; echo ""; echo
"; die('There was an error running the query [' . $conn->error . ']\n'); echo "
} /* convert the select return result into array type */ $return_arr = array(); while($row =
result->fetch_assoc()){ array_push($return_arr,$row); } /* convert the array type to json format and read out*/
json_str = json_encode($return_arr); $json_a = json_decode($json_str,true); $id = $json_a[0]['id']; $name =
json_a[0]['name']; $eid = $json_a[0]['eid']; $salary = $json_a[0]['salary']; $birth = $json_a[0]['birth']; $ssn =
json_a[0]['ssn']; $phoneNumber = $json_a[0]['phoneNumber']; $address = $json_a[0]['address']; $email =
json_a[0]['email']; $pwd = $json_a[0]['Password']; $nickname = $json_a[0]['nickname']; if($id!=""){ // If id exists
nat means user exists and is successfully authenticated
rawLayout($id,$name,$eid,$salary,$birth,$ssn,$pwd,$nickname,$email,$address,$phoneNumber); }else{ // User
uthentication failed echo ""; echo ""; echo "

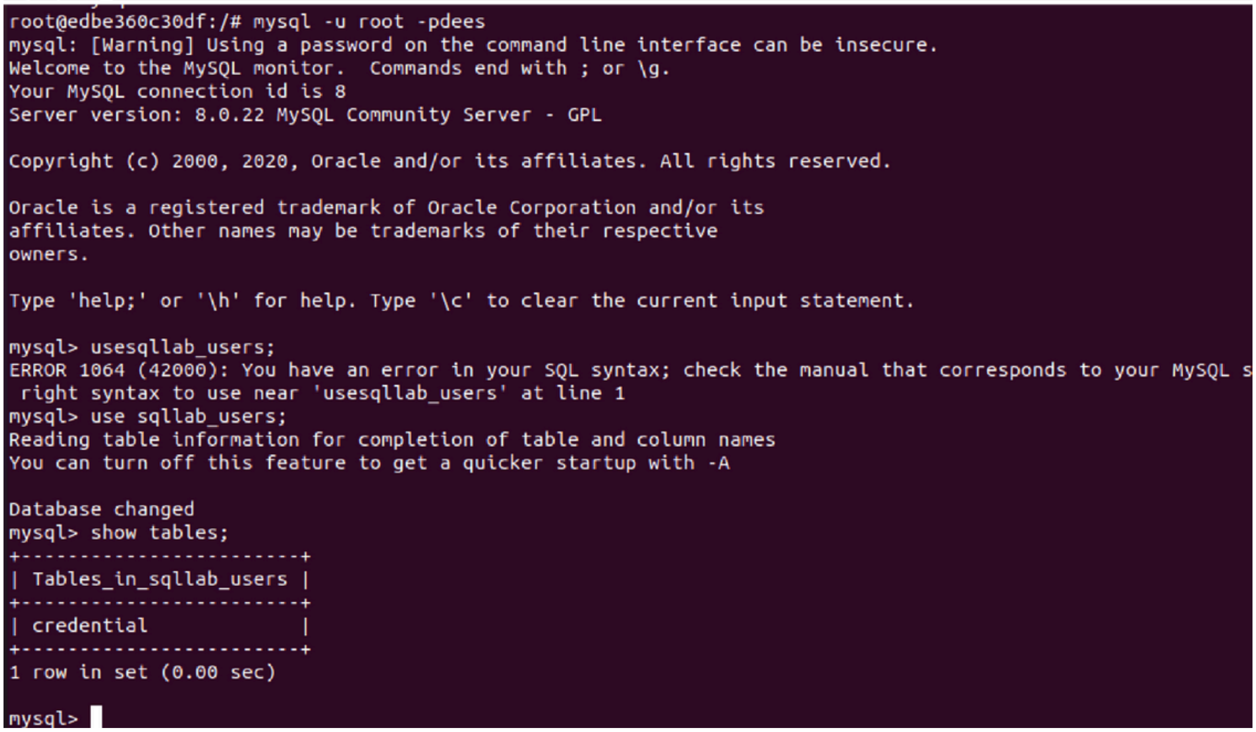
- Login to mysql container



```
izzatalsmadi@VM:~/Downloads/Quiz5/Labsetup/image_www$ mysql -u root -pseedubuntu
nysql: [Warning] Using a password on the command line interface can be insecure.
ERROR 2002 (HY000): Can't connect to local MySQL server through socket '/var/run/mysqld/mysqld.sock' (2)
izzatalsmadi@VM:~/Downloads/Quiz5/Labsetup/image_www$ sudo docker ps
CONTAINER ID        IMAGE                  COMMAND                  CREATED            STATUS             PORTS
  NAMES
cc036fabde0e        seed-image-www-sqli    "/bin/sh -c 'service…"   13 hours ago       Up 20 minutes
  www-10.9.0.5
edbe360c30df        seed-image-mysql-sqli  "docker-entrypoint.s…"   13 hours ago       Up 25 minutes      3306/tcp, 33060/t
  mysql-10.9.0.6
izzatalsmadi@VM:~/Downloads/Quiz5/Labsetup/image_www$ sudo docker exec -it seed-image-mysql-sqli bash
Error: No such container: seed-image-mysql-sqli
izzatalsmadi@VM:~/Downloads/Quiz5/Labsetup/image_www$ sudo docker exec -it mysql-10.9.0.6 bash
root@edbe360c30df:/#
```



```
bash: mysql-u: command not found
root@edbe360c30df:/# mysql -u root -pdees
mysql: [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 8
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, 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>
```



```
root@edbe360c30df:/# mysql -u root -pdees
mysql: [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 8
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, 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> usesqllab_users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL s
 right syntax to use near 'usesqllab_users' at line 1
mysql> use sqllab_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_sqllab_users |
+------------------------+
| credential             |
+------------------------+
1 row in set (0.00 sec)

mysql>
```

-