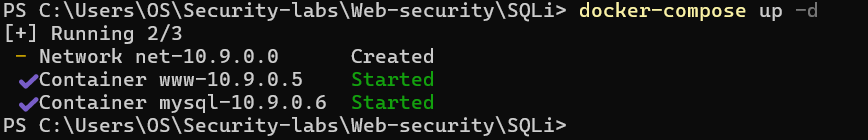
**Lab 05: Web security – SQL Injection**

**TASKS**

**1. Setup**

****

**2. About web application**

The web application is a simple employee management application. Employees can view and update

their personal information in the database through this web app. There are mainly two roles in this web

app: Admin is a privileged role and can manage each individual employees’ profile information;

Employee is a normal role and can view or update his/her own profile information. All employee

credentials are given:

Admin, seedadmin

Alice, seedalice

Boby, seedboby

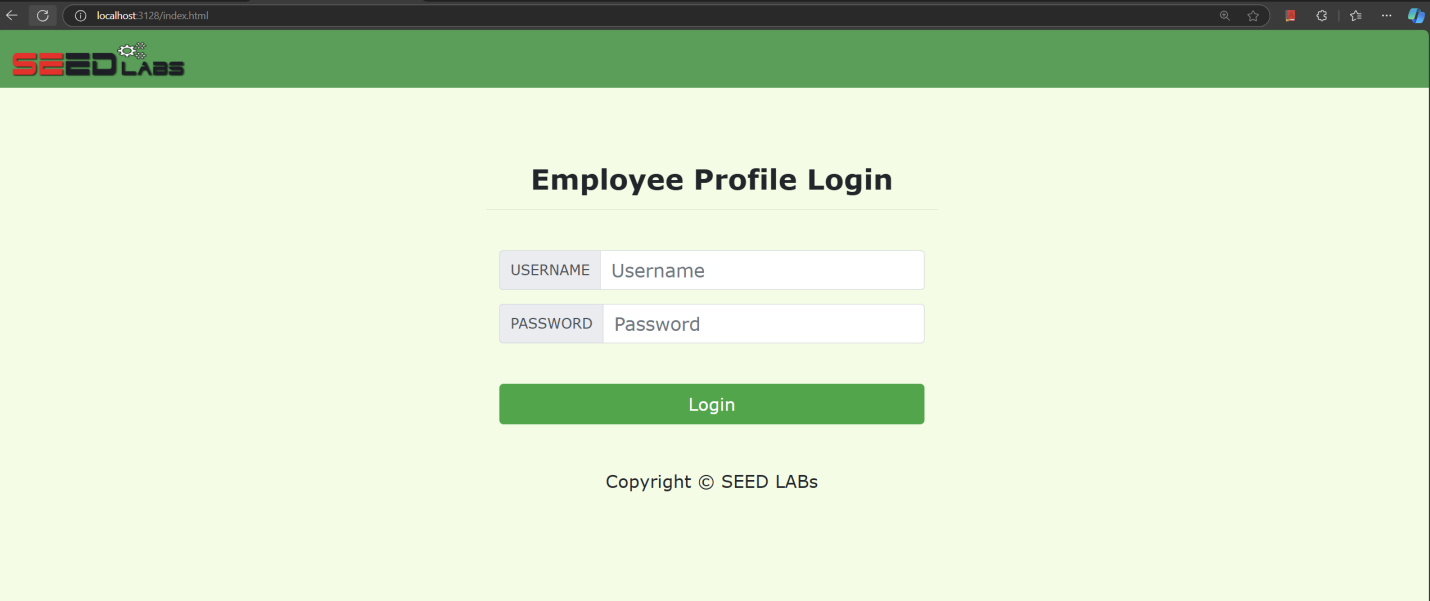
Ryan, seedryan

Ted, seed ted

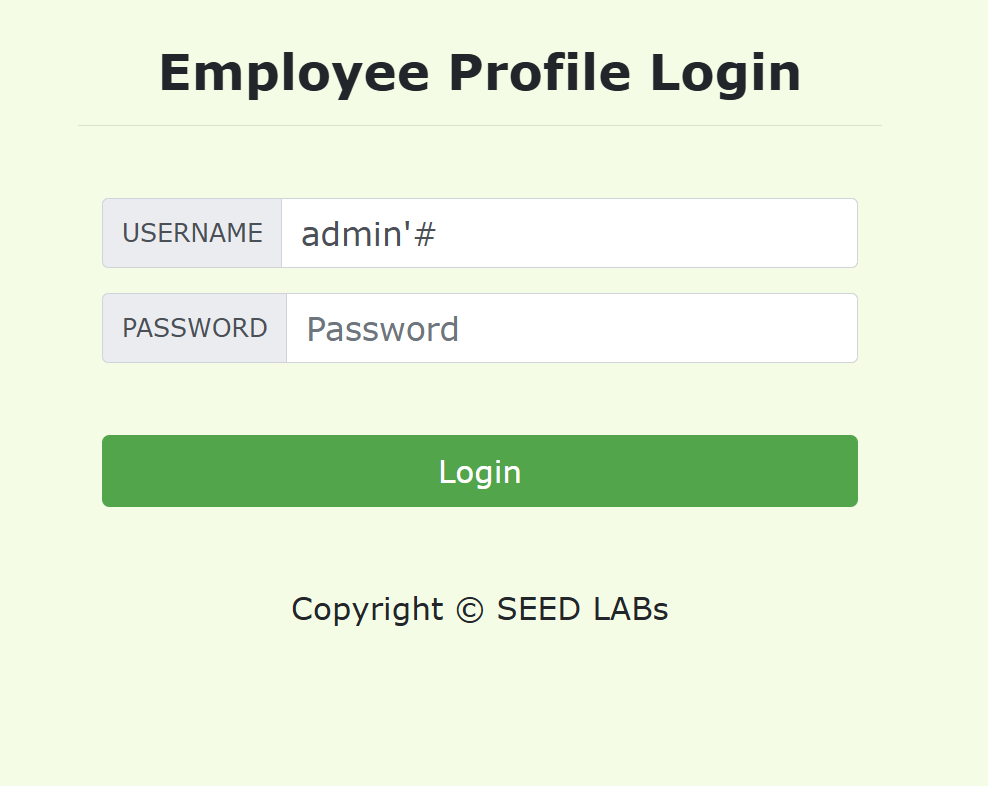
Samy, seedsamy

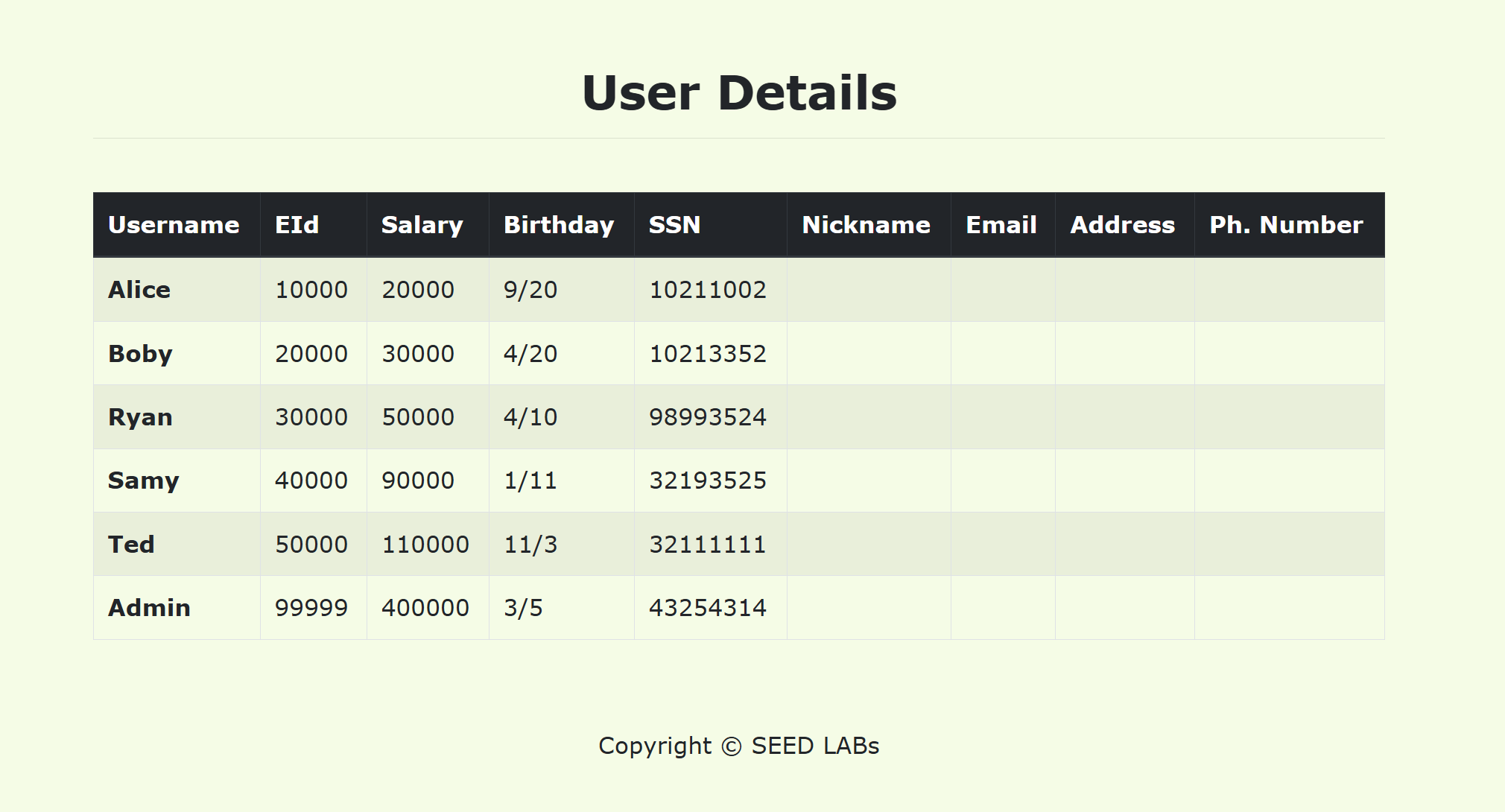
**3 SQL Injection Attack on SELECT Statement**

**3.1 SQL Injection attack from webpage**

****

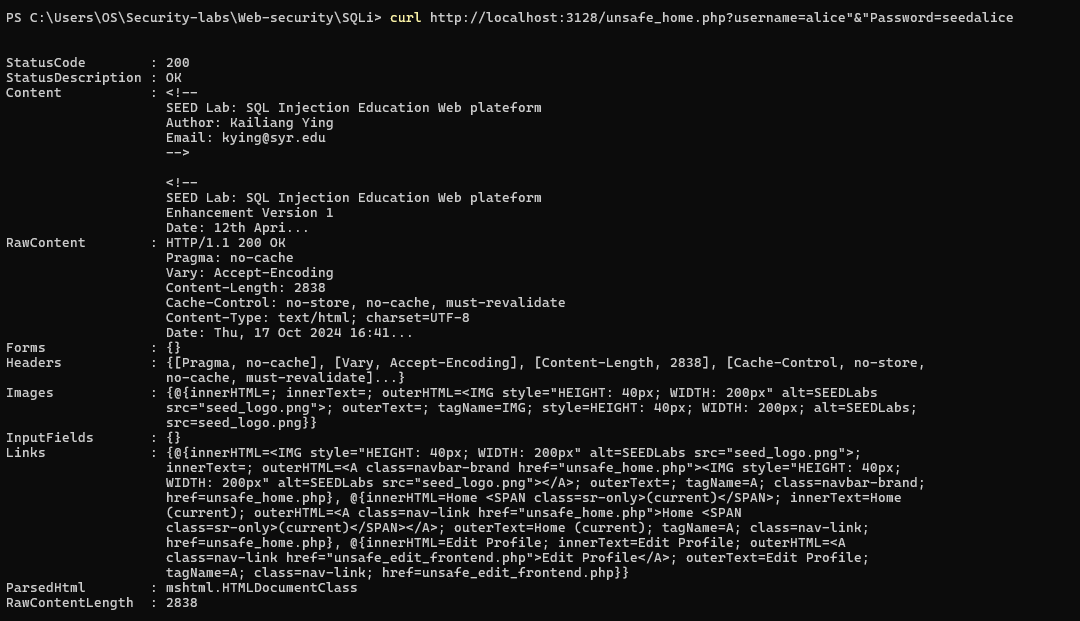
Access admin account without a password





**3.2 SQL Injection attack from command line**

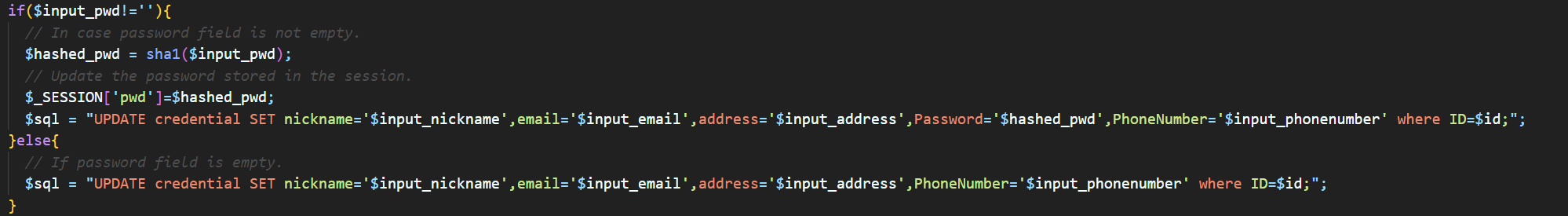
Using curl [http://localhost:3128/unsafe\_home.php?username=alice"&"Password=seedalice](http://localhost:3128/unsafe_home.php?username=alice%22&%22Password=seedalice) I can see the raw html given back to me in the command line

****

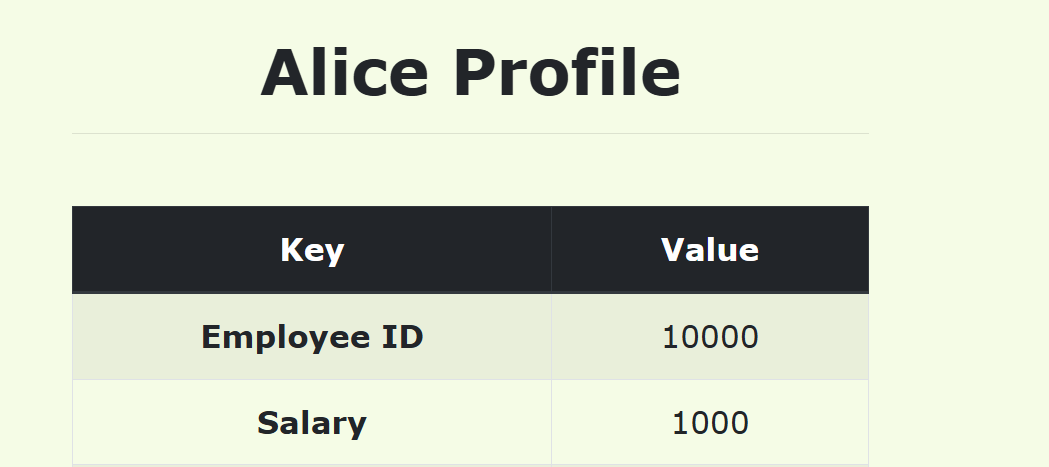
**4 SQL INJECTION ATTACK ON UPDATE STATEMENT**

**4.1 Modify your own salary**

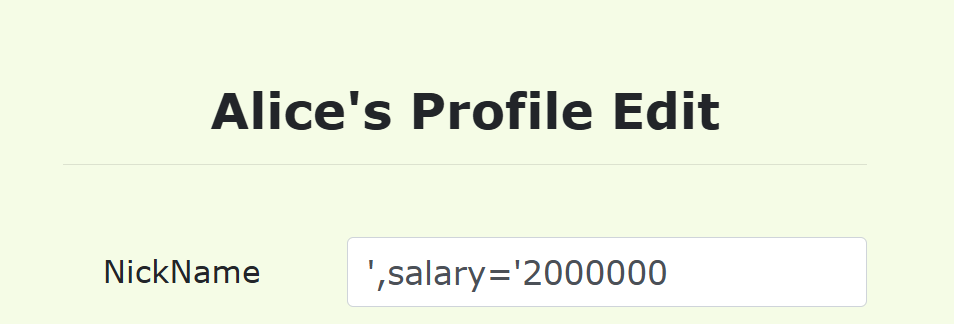
The vulnerable code

****

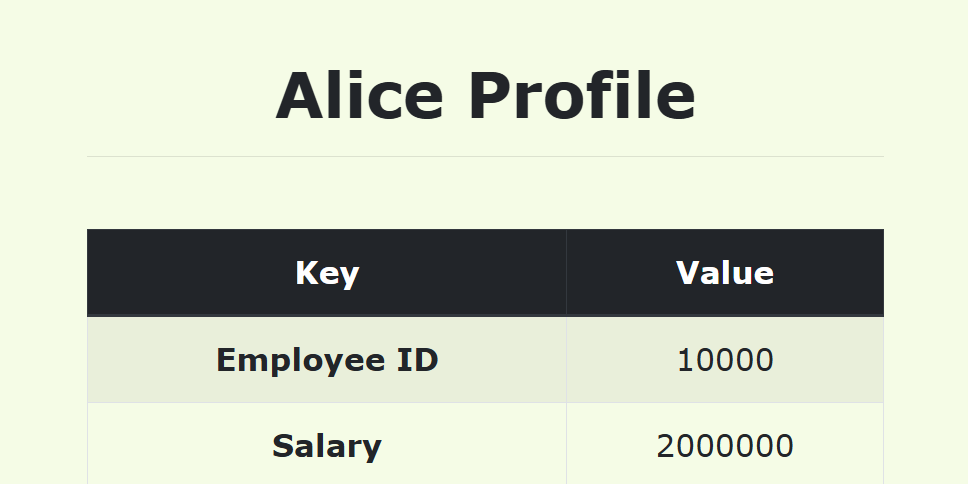
Before



The input:



result

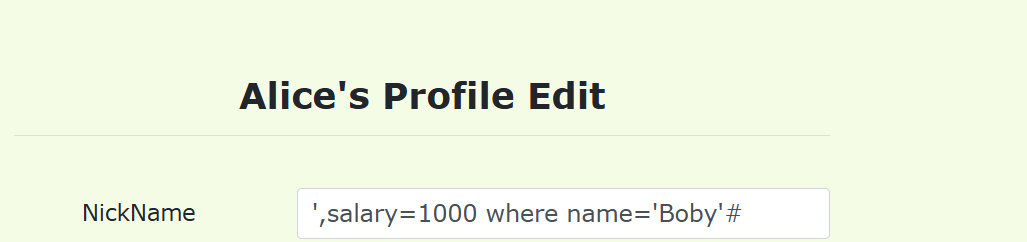


**4.2 Modify other people’s salary**

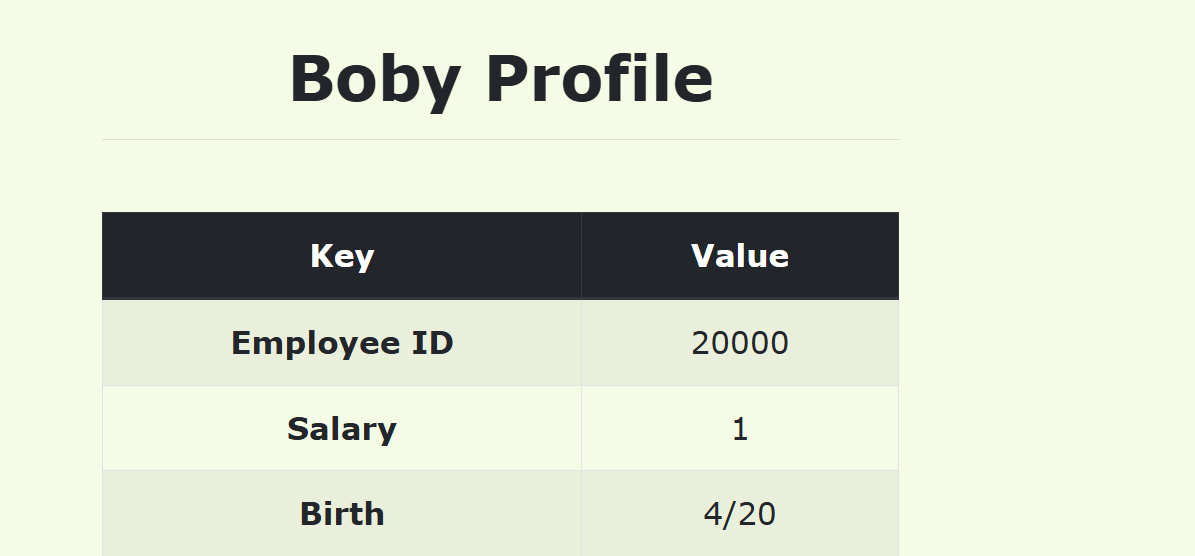
I can make use of field nicname and have input like this

',salary=1 where Name='Boby'#

Input



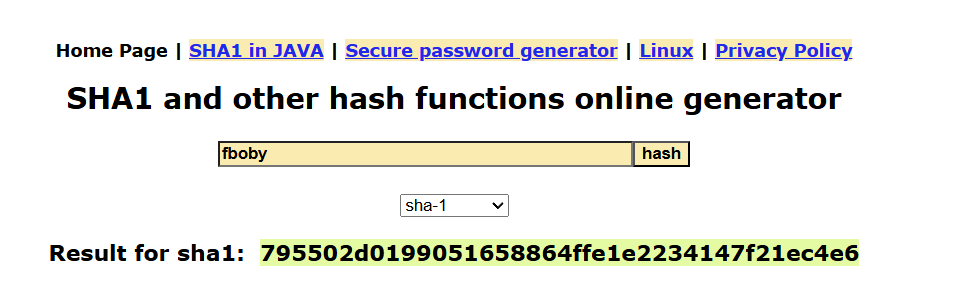
result



**4.3 Modify other people’s password**

This time I will use filed nickname again, I want to change his password to fboby

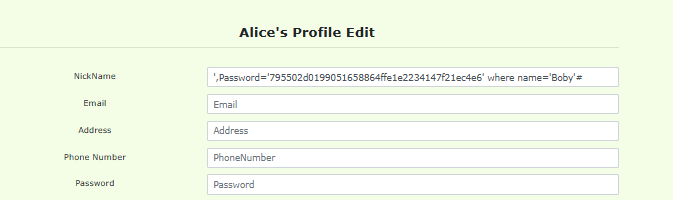
I wil use the sha1 online web to convert fboby to sha1 hash



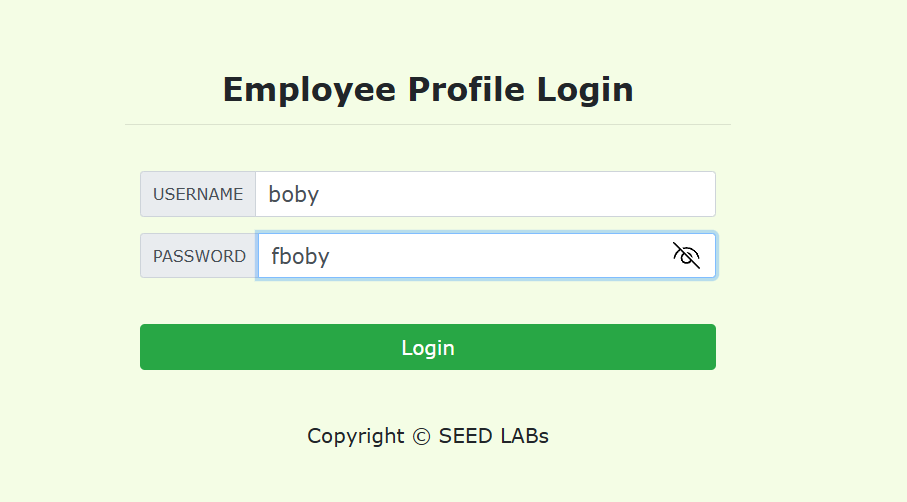
Value : 795502d0199051658864ffe1e2234147f21ec4e6

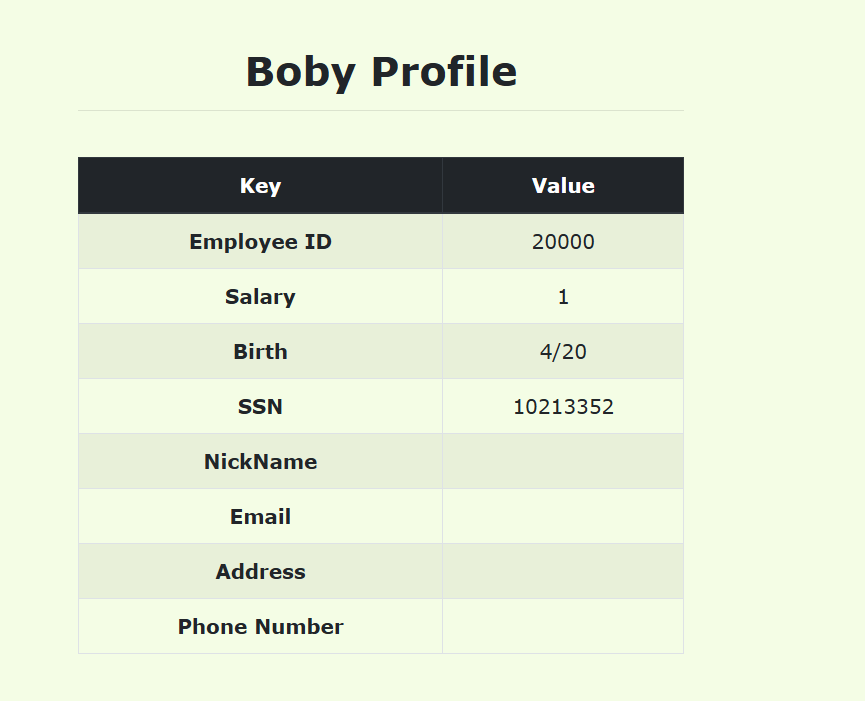
So the input will be like this:

',Password='795502d0199051658864ffe1e2234147f21ec4e6' where name='Boby'#



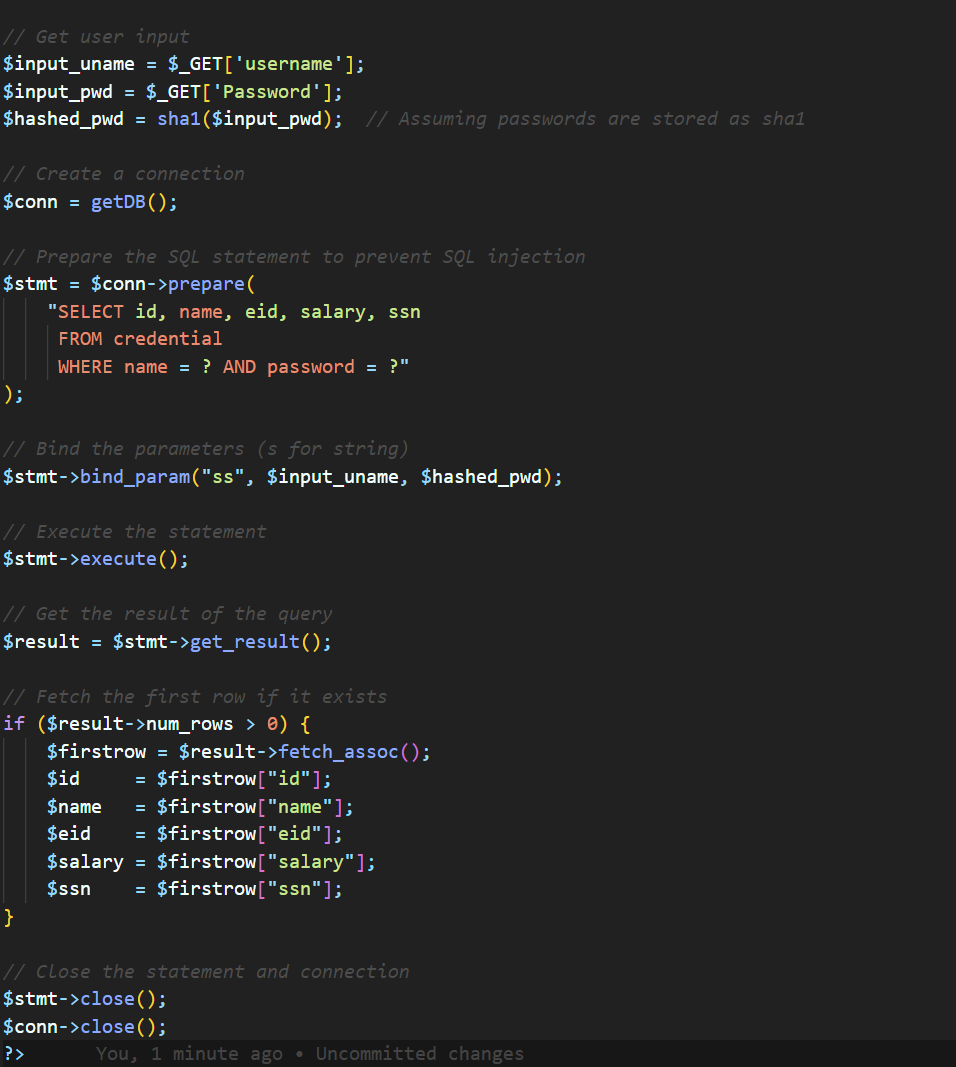
After that





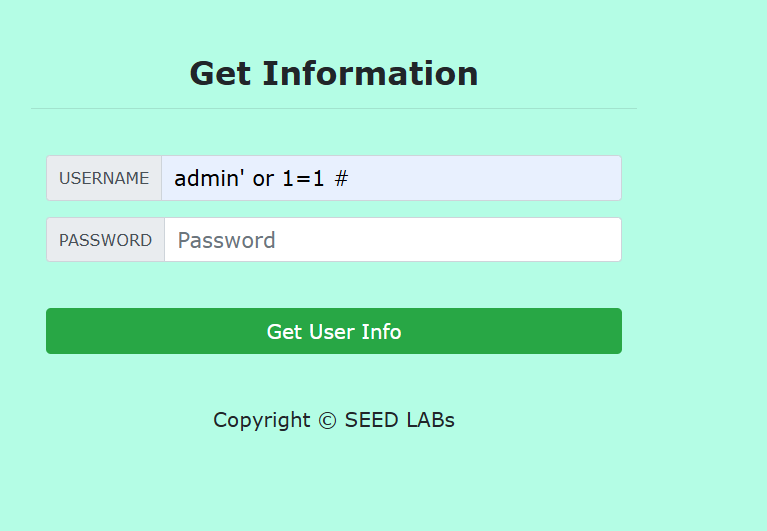
**4.5 Countermeasures**

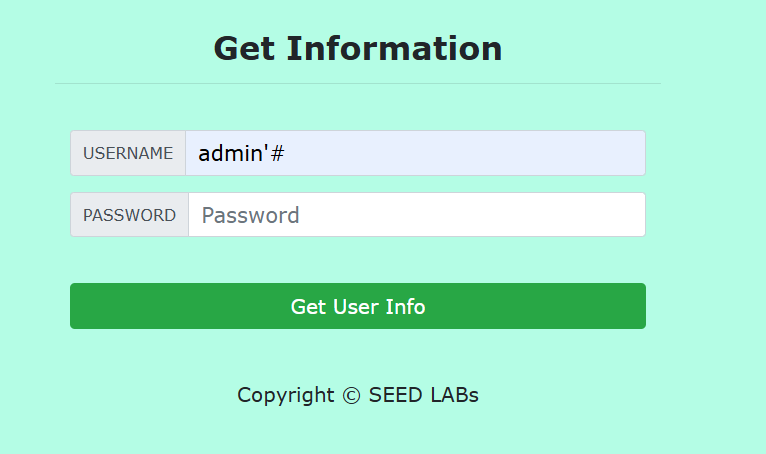
We can use raw SQL to avoid SQL Injection

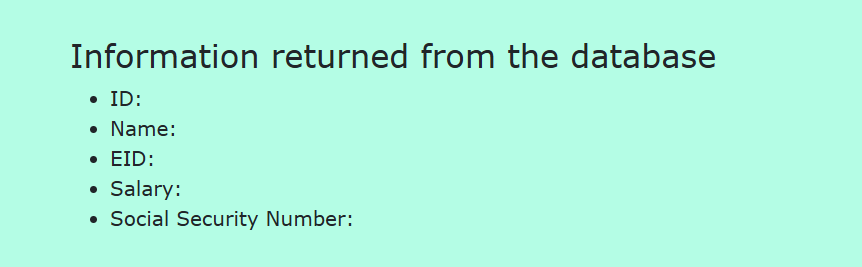


Test case:

I want to test to see if I can enter in admin account without password yet







Or we can use

