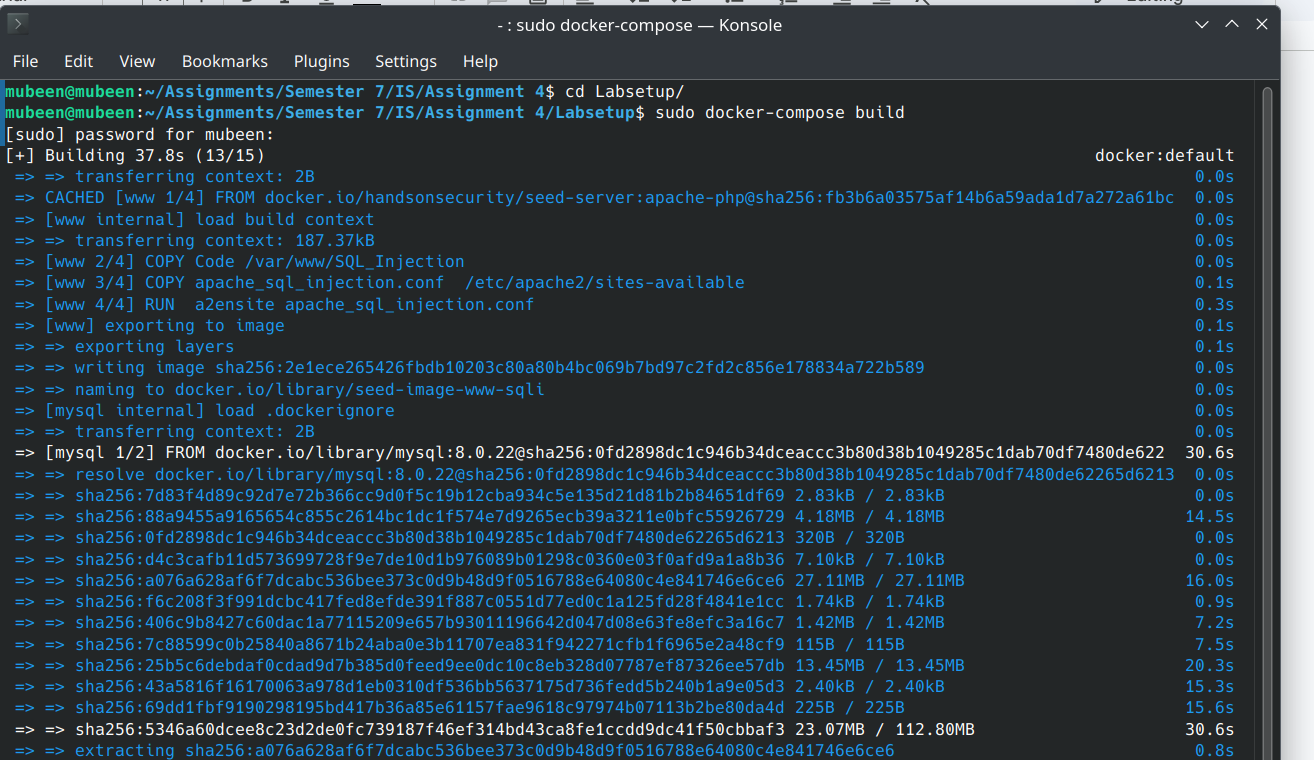
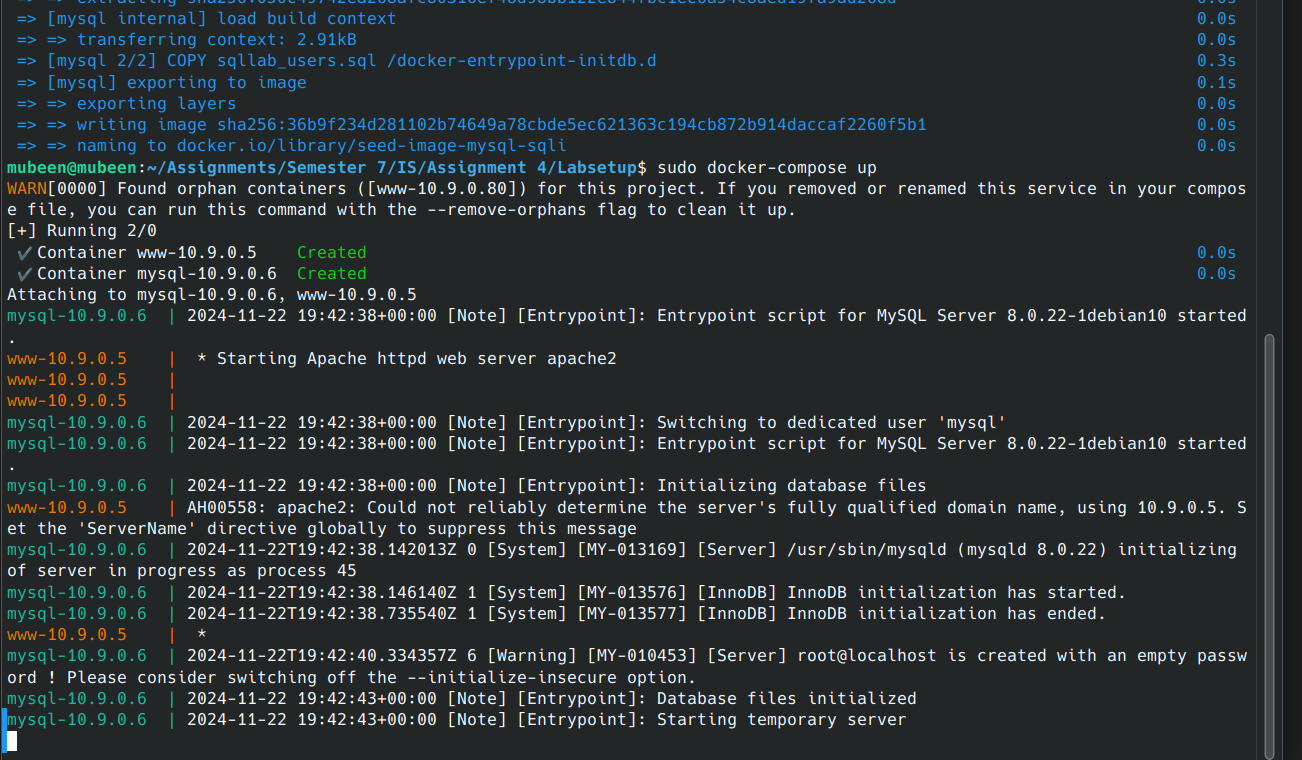
**Assignment # 4:**

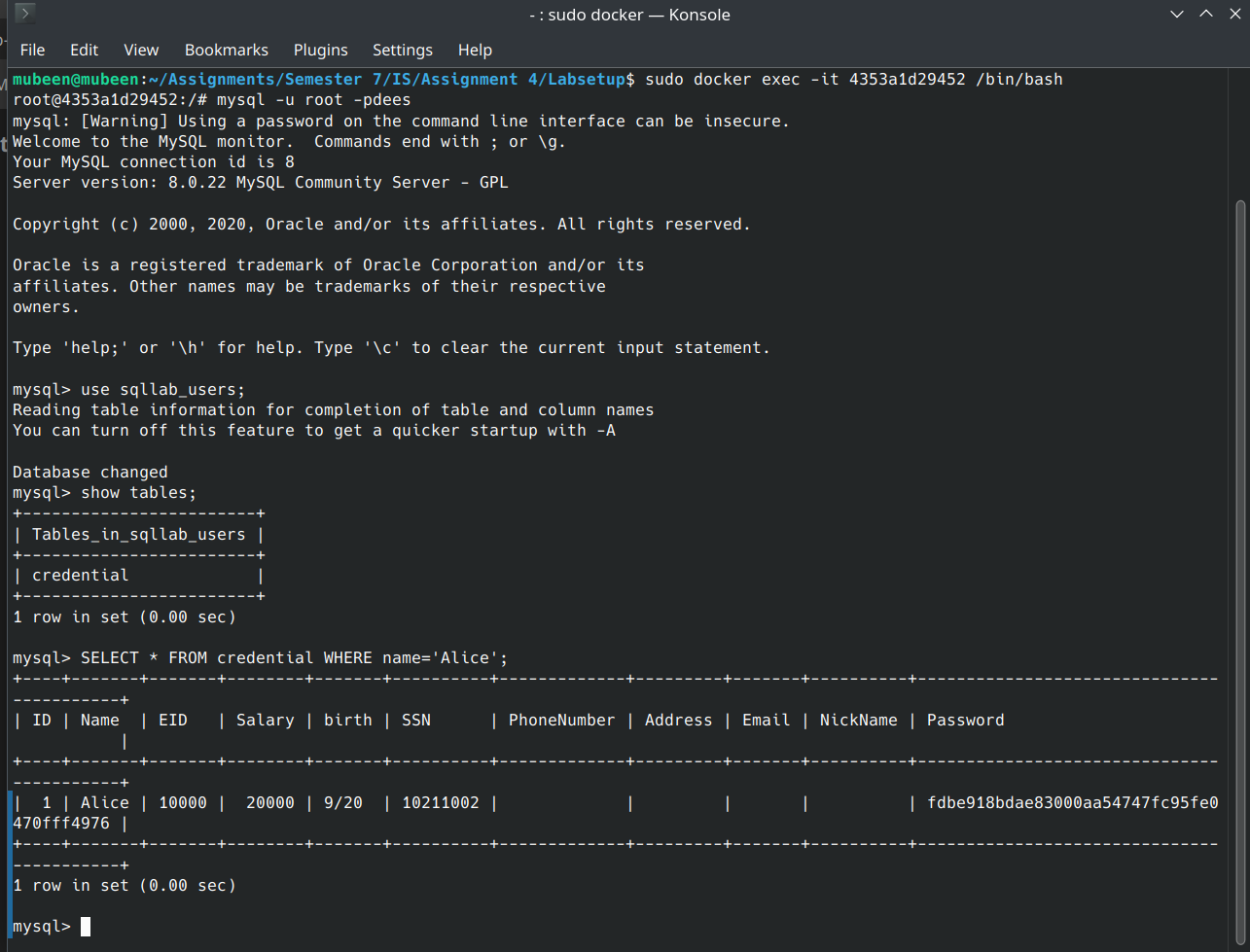
K21-3292 Mubeen Palh

K21-4557 Abdul Aziz

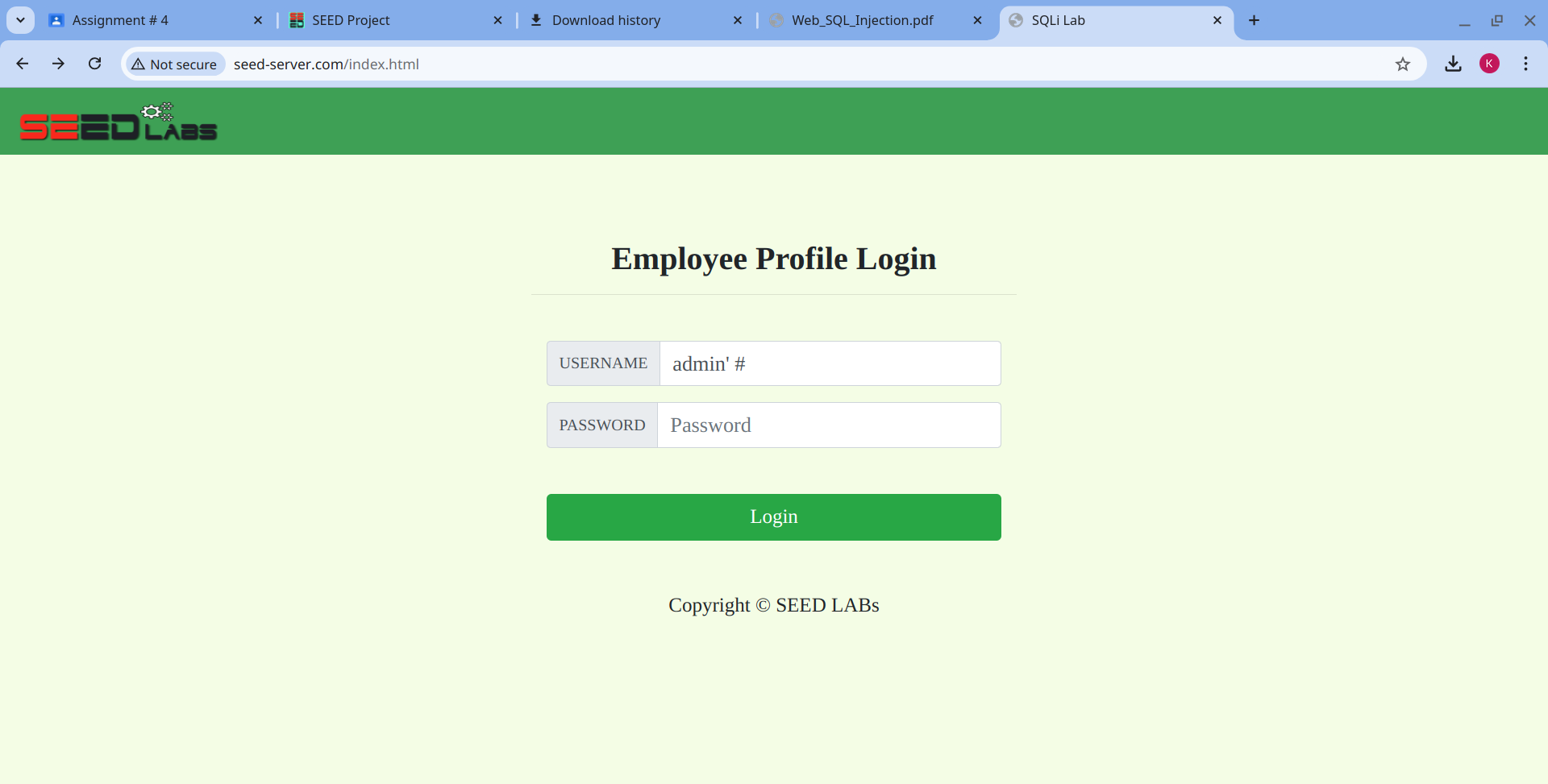
**Lab Setup:**  


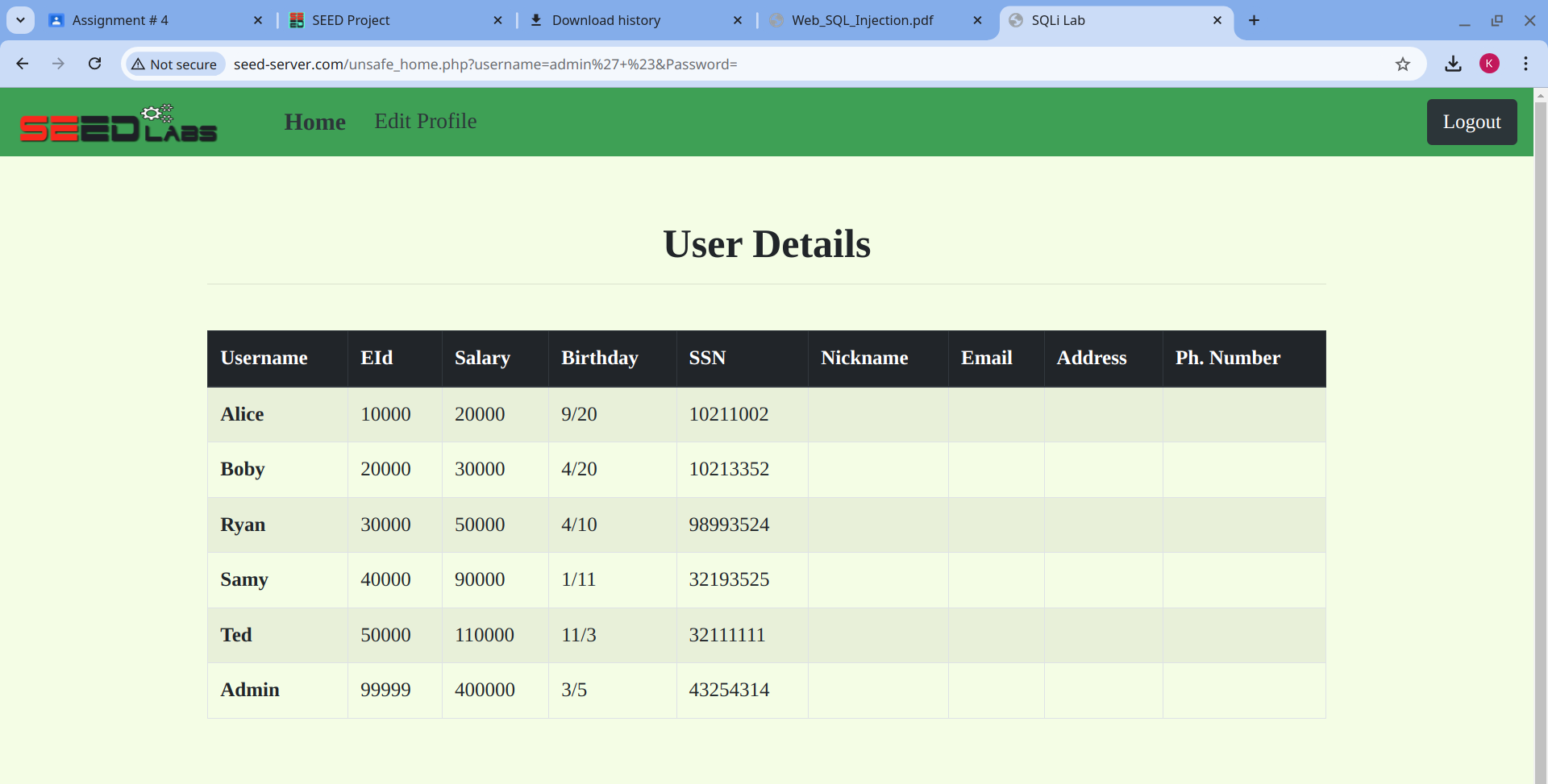


**Task 1:**

****

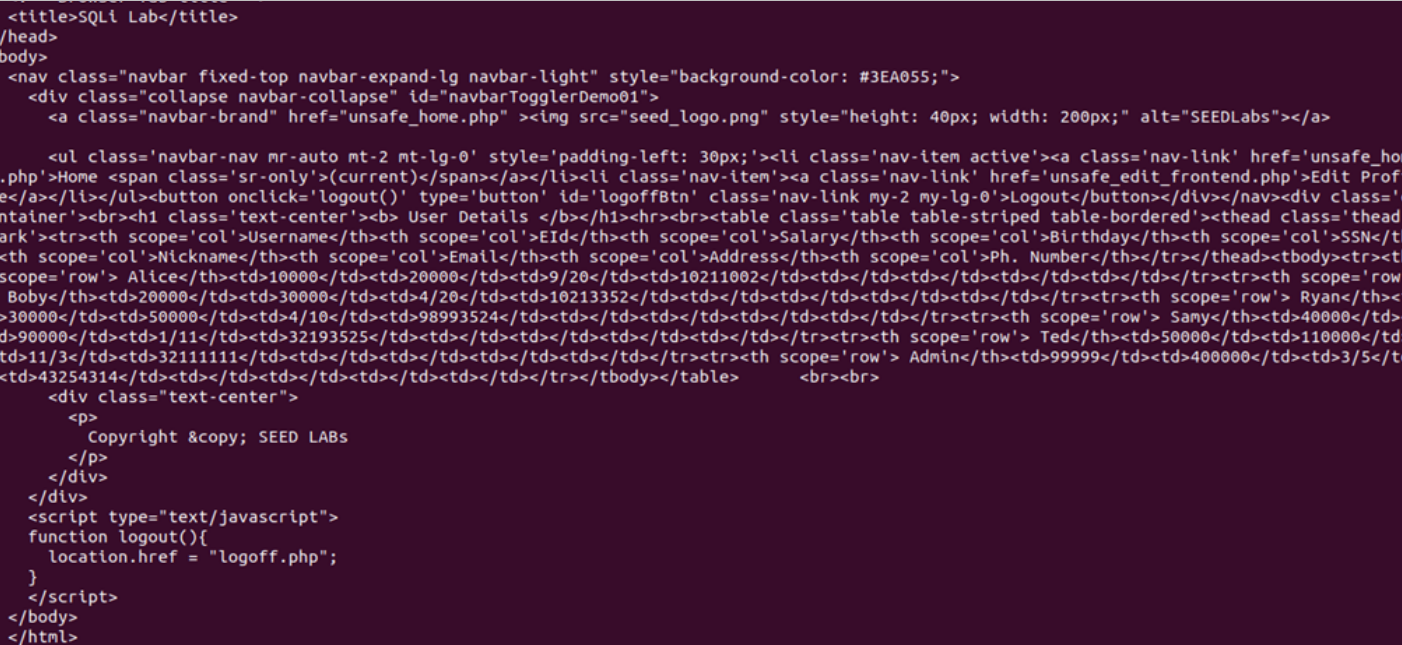
**Task 2.1 :**

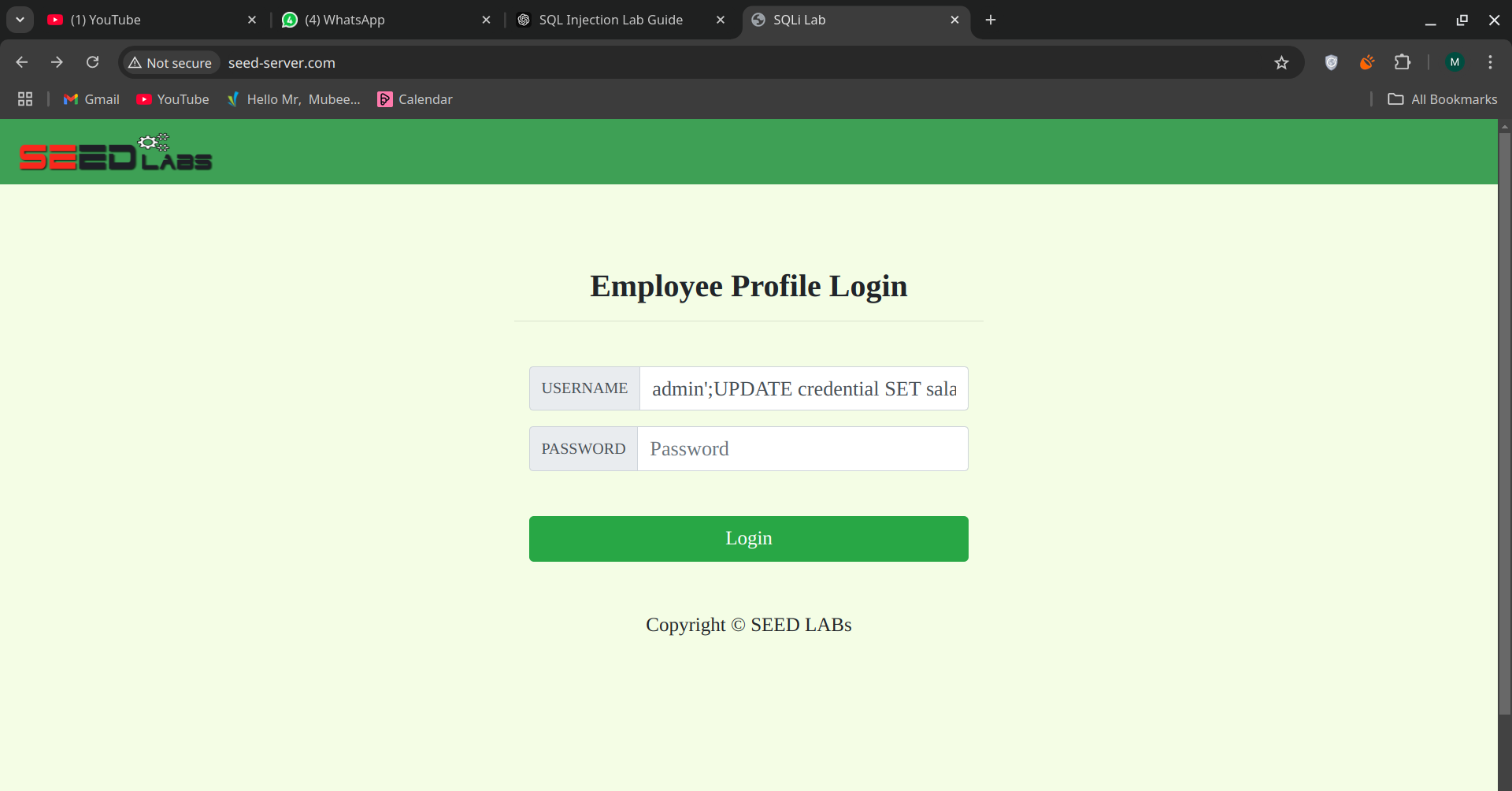
****

**Login successfully:  
**

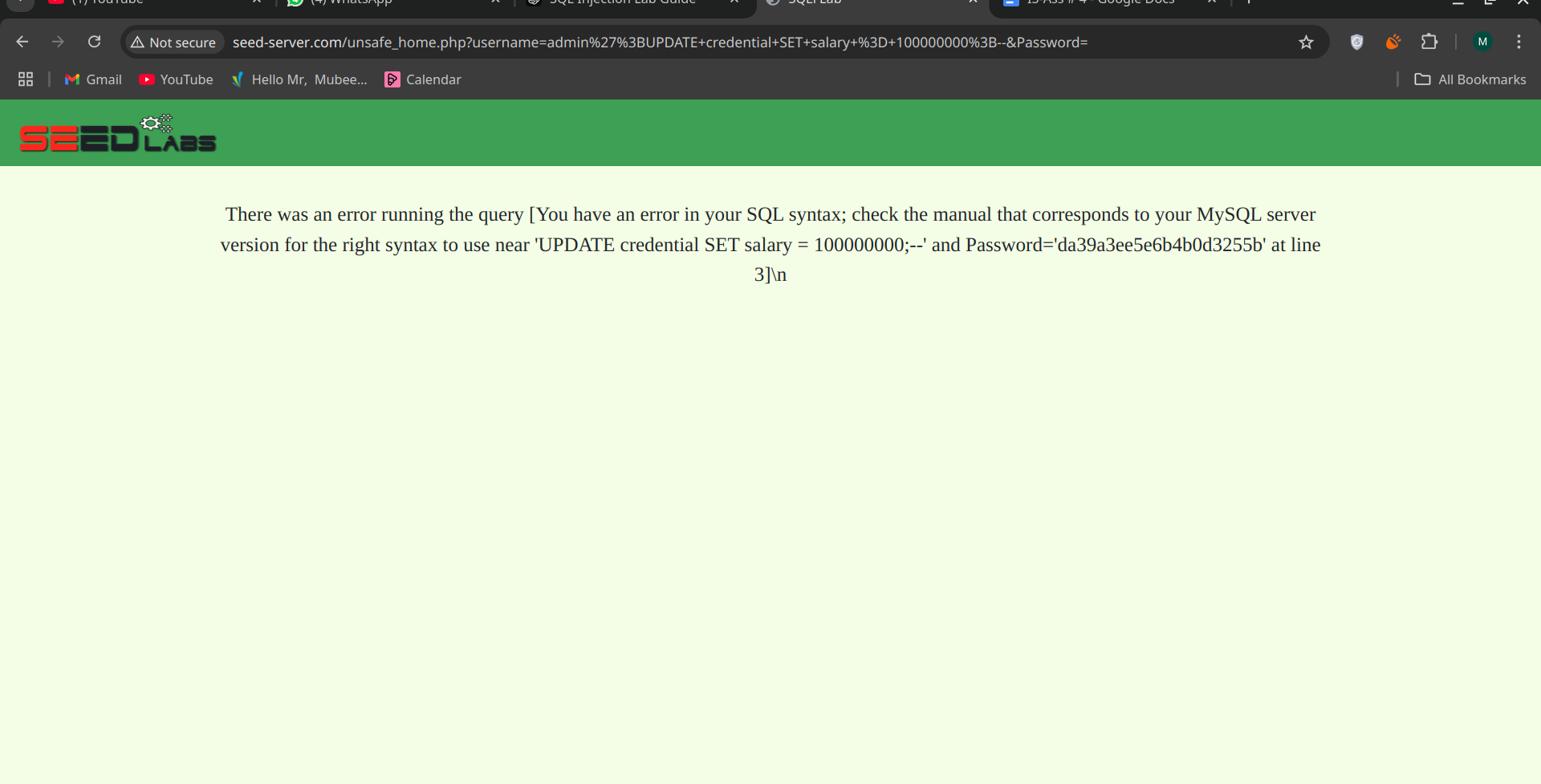
**Task 2.2:**

**Curl response:**

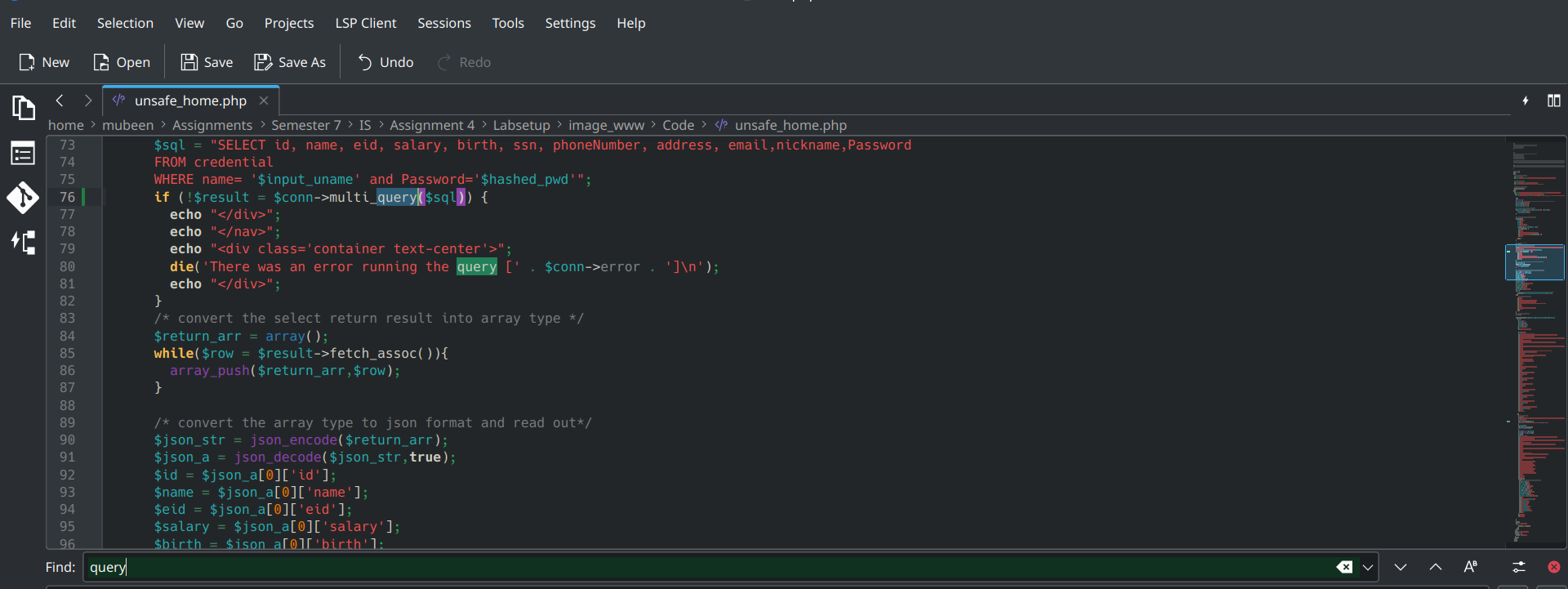
****

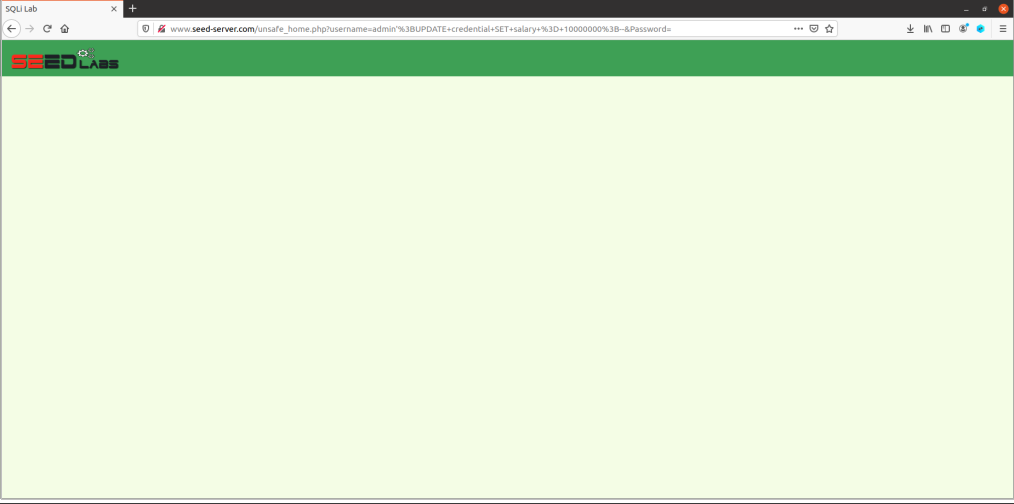
**Task 2.3:  
**

Sql Injection failed due to mysql::query( ) API

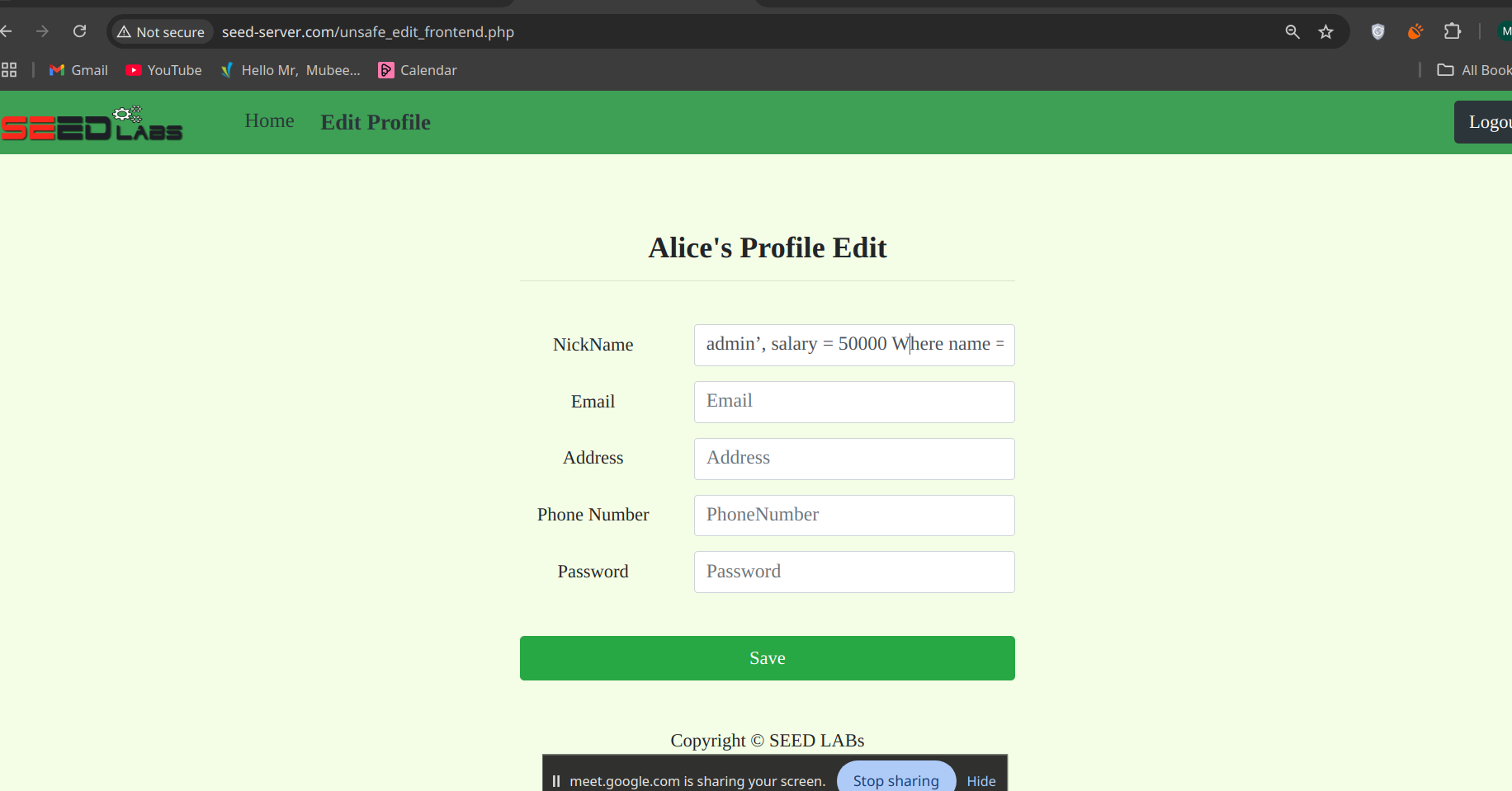


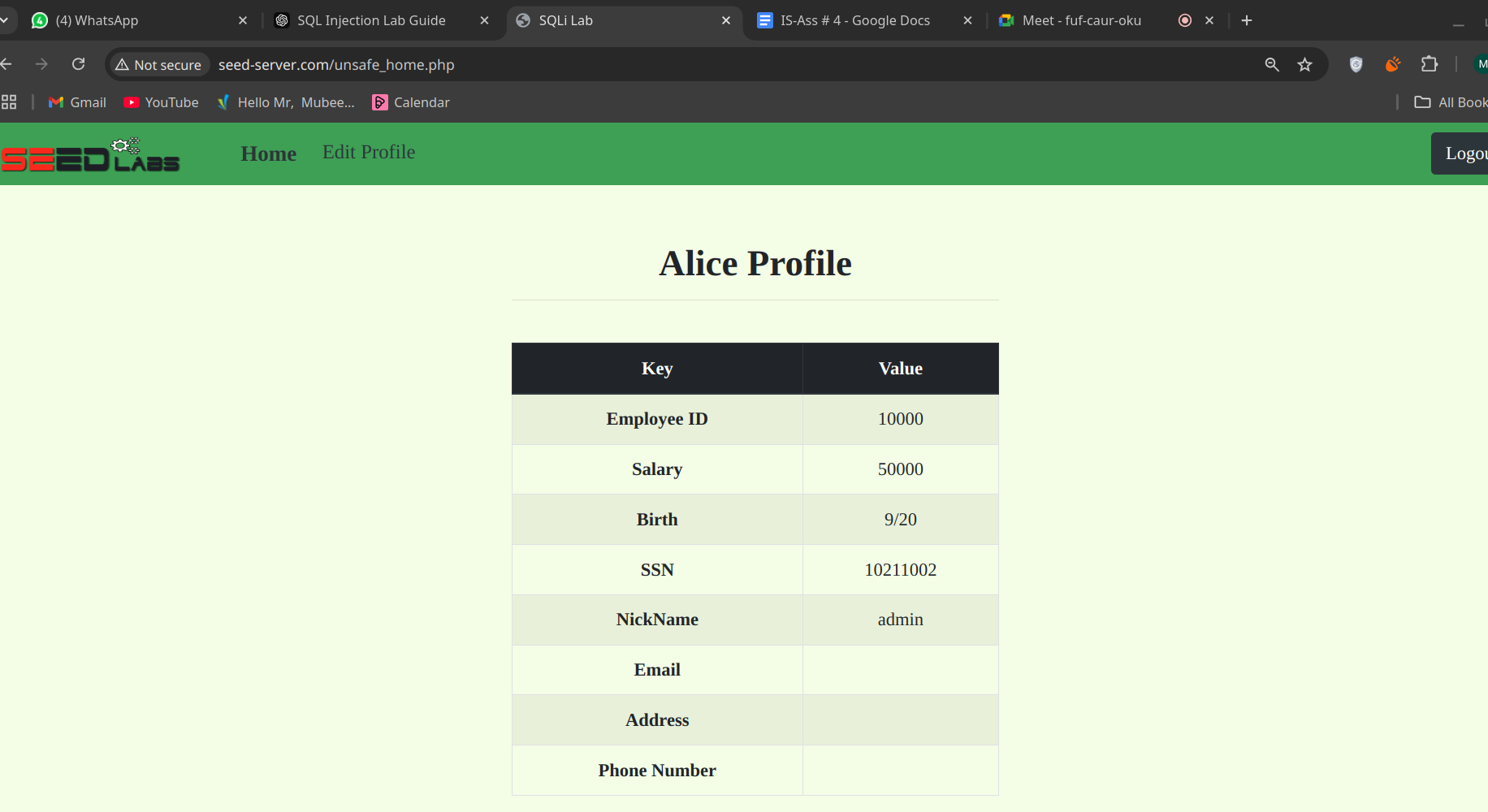
**Using** multi\_query( ):

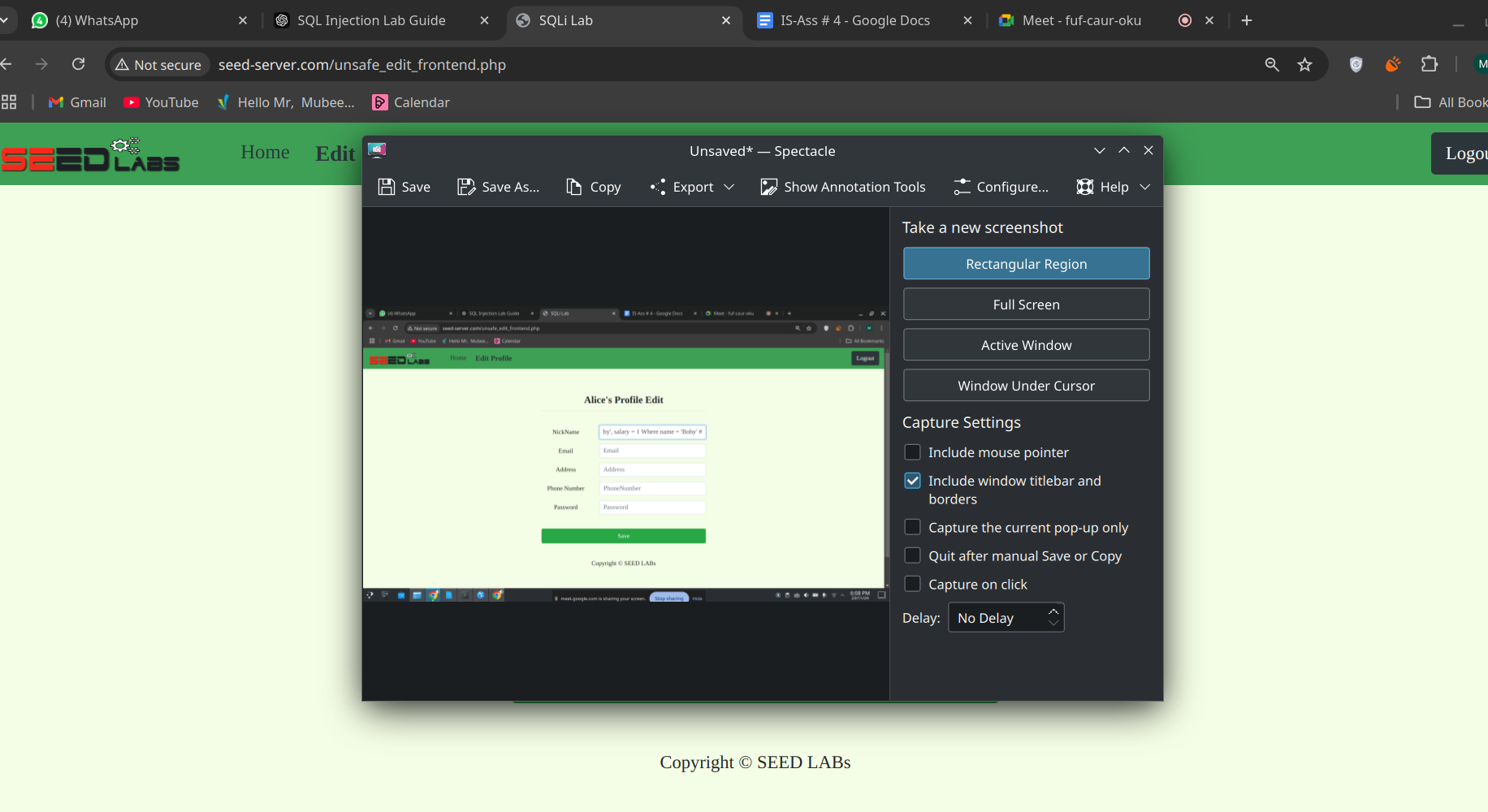


Result:  


**Task 3.1:**



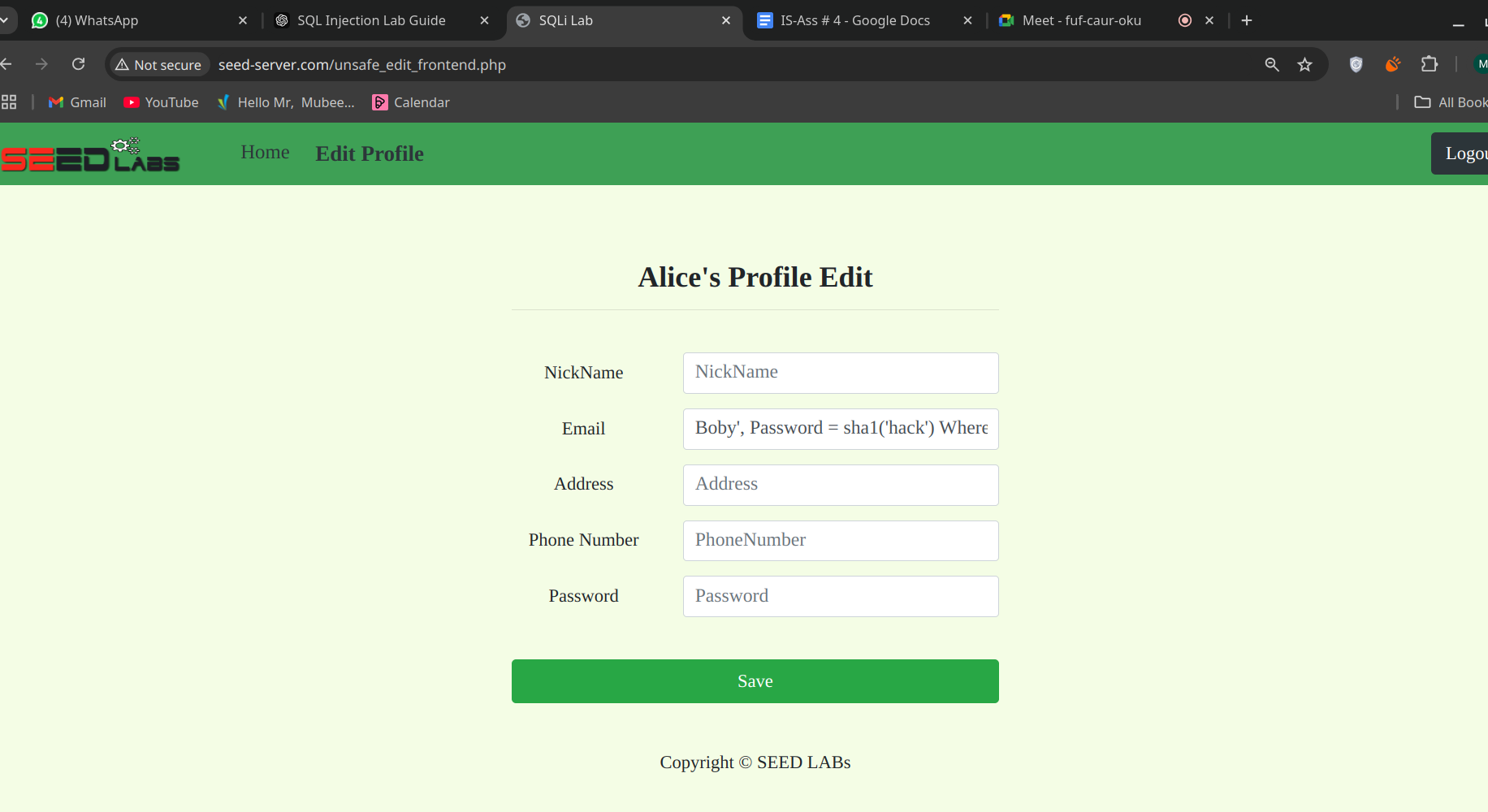


**Task 3.2:**  


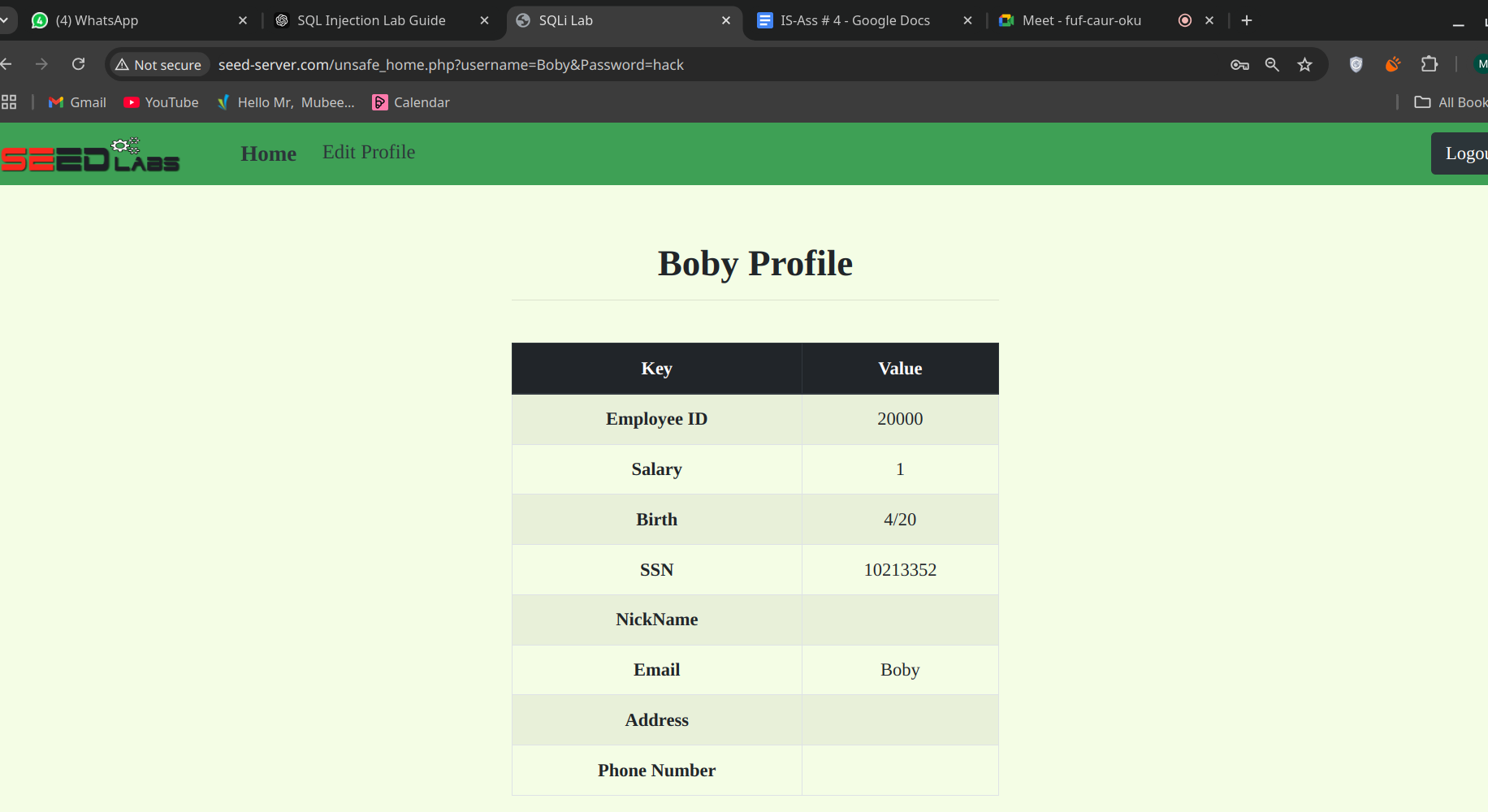
**Command :**

Boby', salary = 1 Where name = 'Boby' #

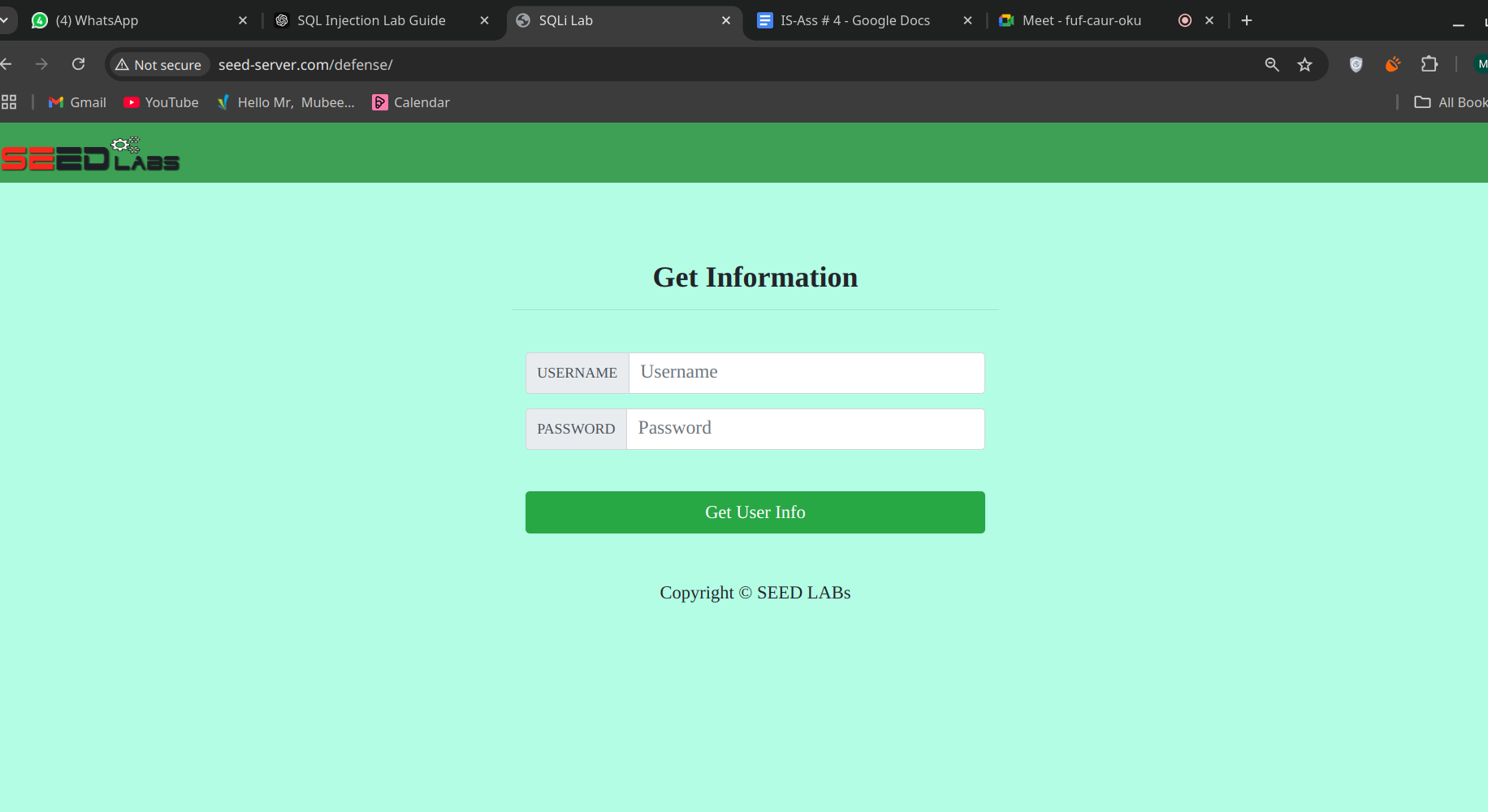
**Task 3.3:**

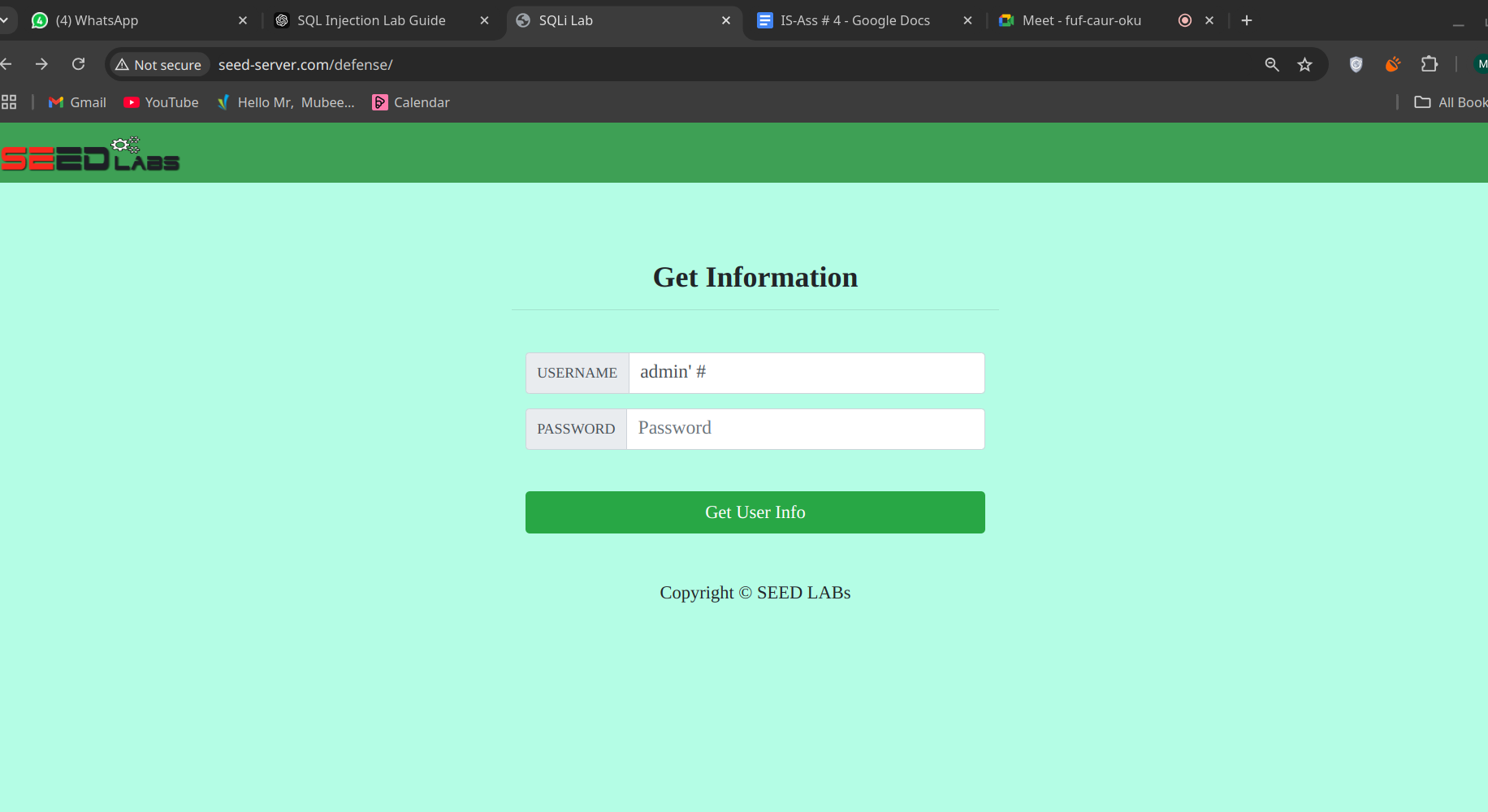


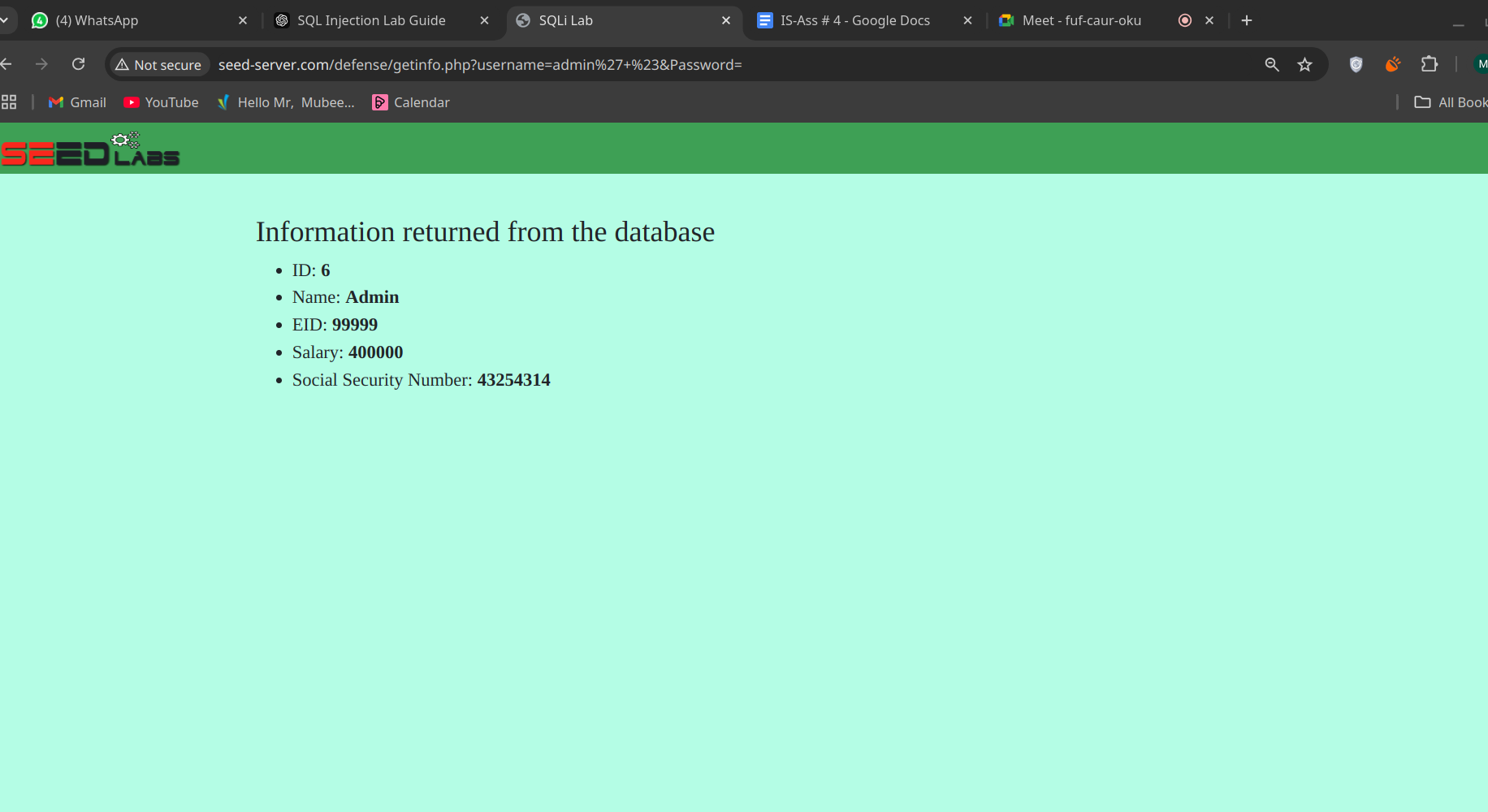
**Command** : Boby', Password = sha1('hack') Where name = 'Boby' #

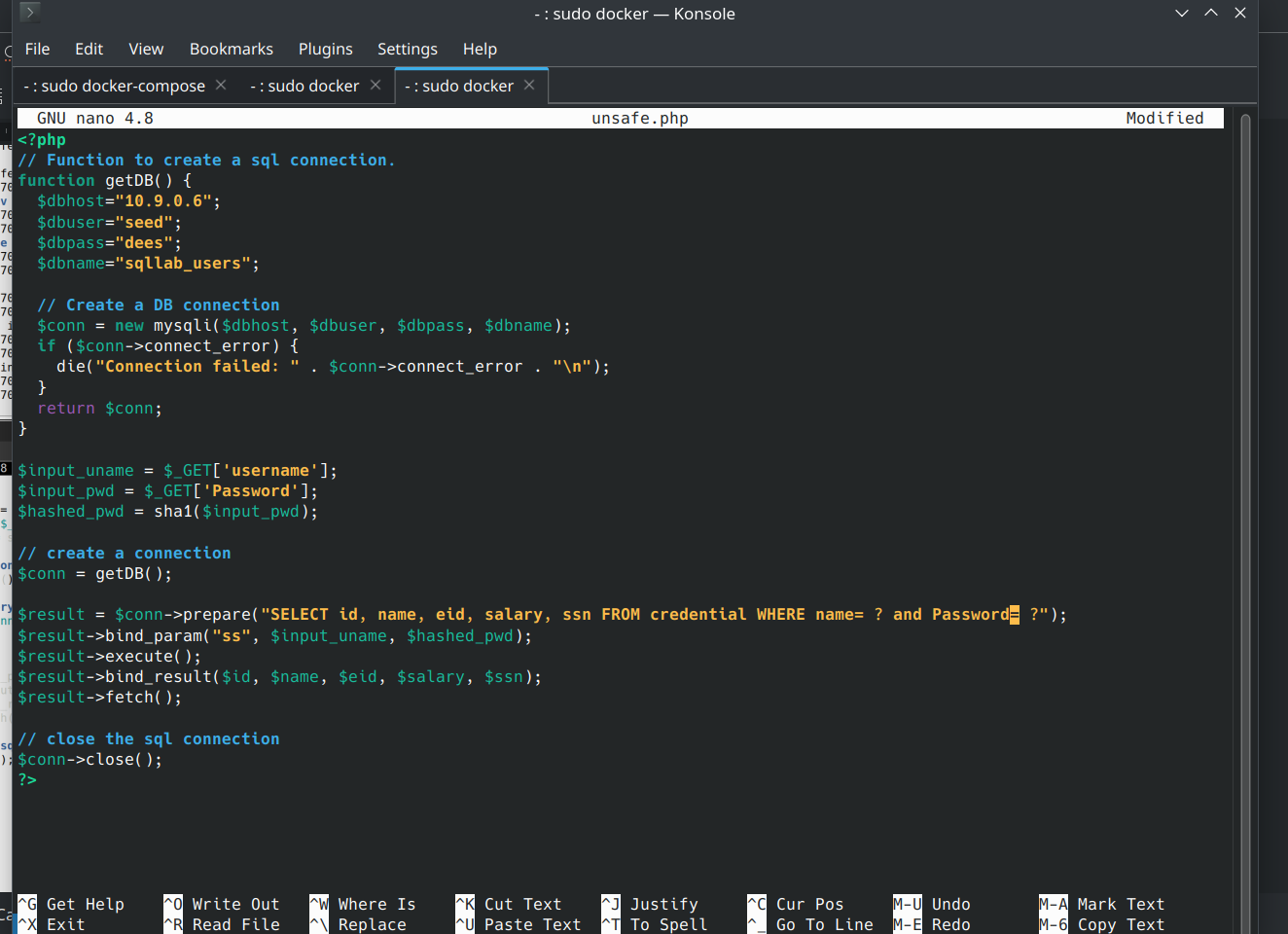


**Task 4:**

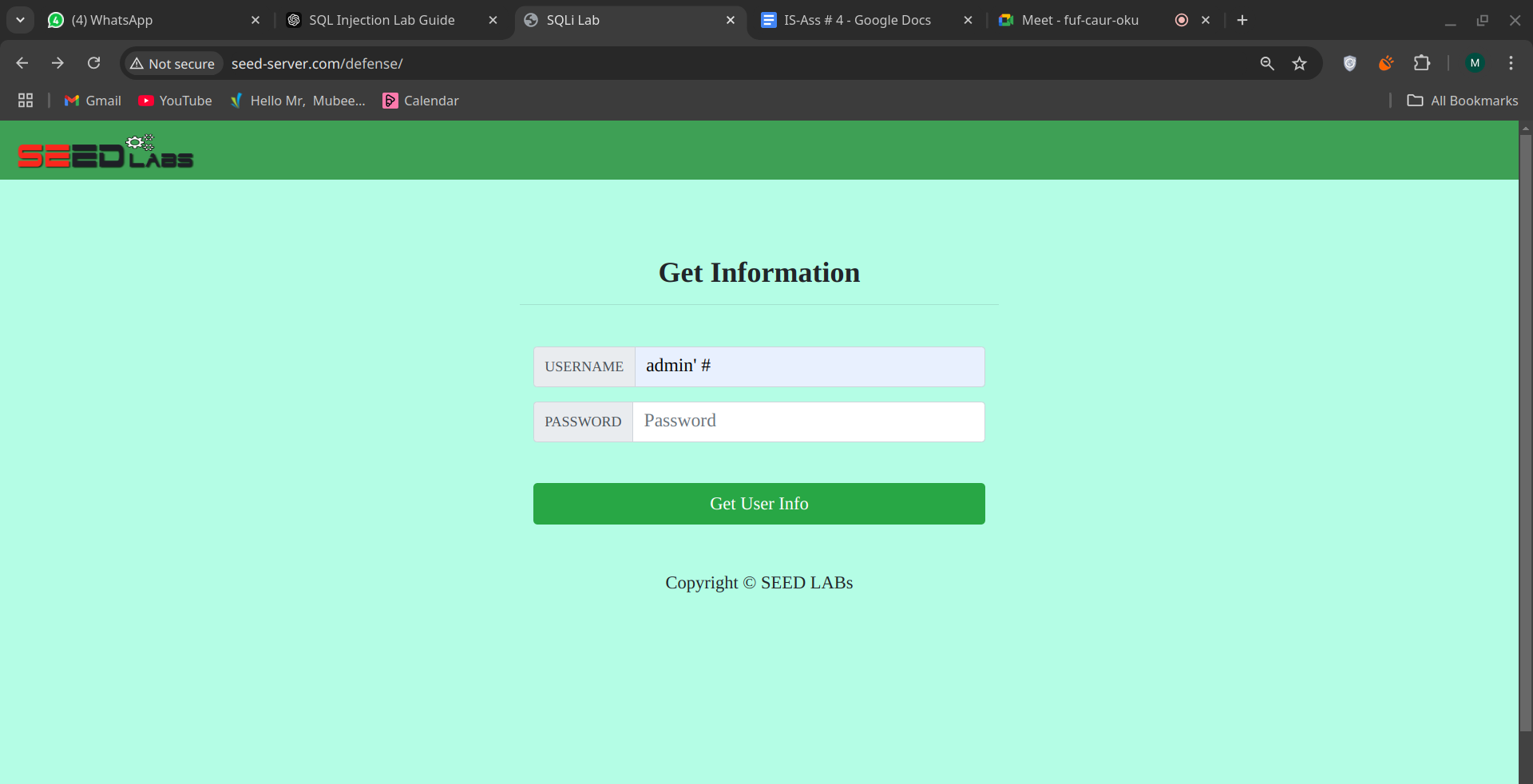








Now we will check the endpoint again



Result not fetched after sanitization:

