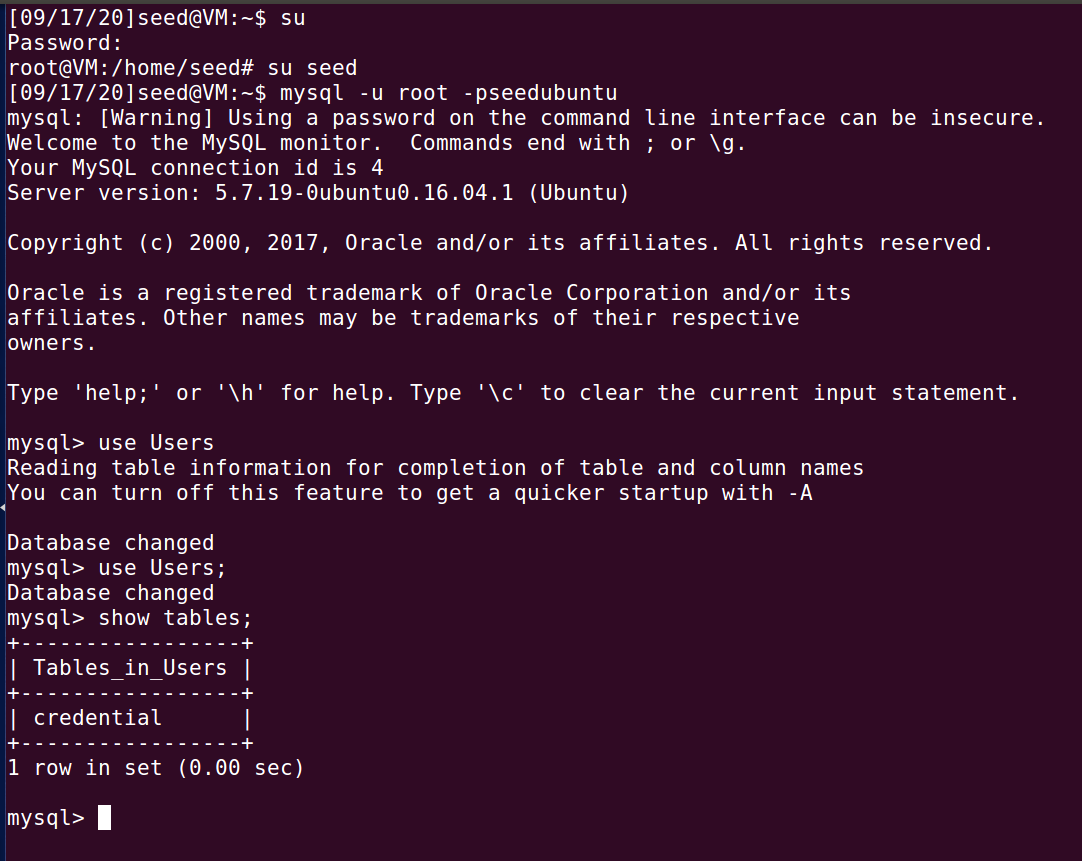
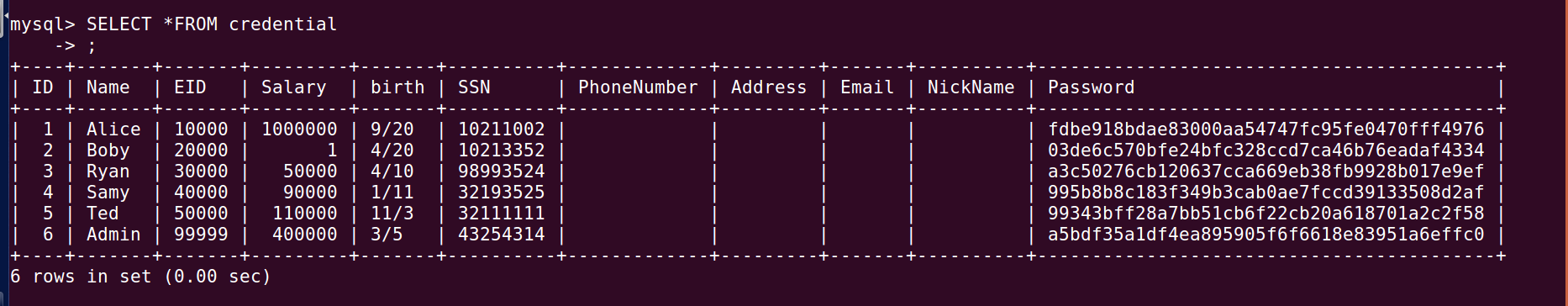
Lab 6 SQL Injection Attack Lab

57118115 陈烨

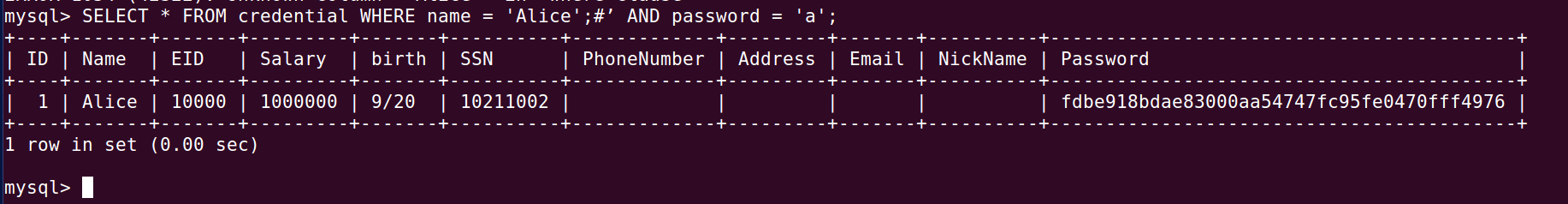
**Task 1: Get Familiar with SQL Statements**



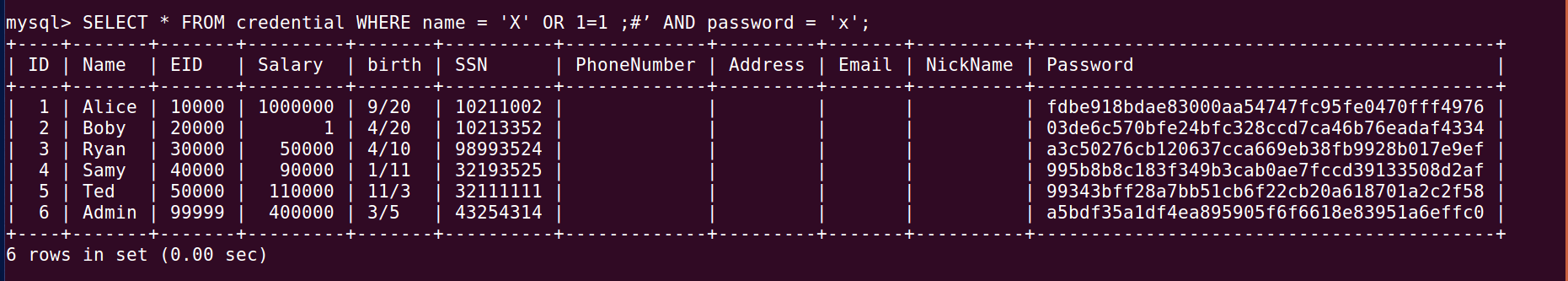
use a SQL command to print all the profile information of the employee Alice



利用命令SELECT \* FROM credential WHERE name = ‘Alice’;#’ AND password = ‘a’;使数据库返回Alice的记录



利用命令SELECT \* FROM credential WHERE name = ‘X’ OR 1=1 ;#’ AND password = ‘x’;使数据库返回一些人的记录。



SQL注入，就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。当应用程序使用输入内容来构造动态sql语句以访问数据库时，会发生SQL注入攻击。

**Task 2: SQL Injection Attack on SELECT Statement**

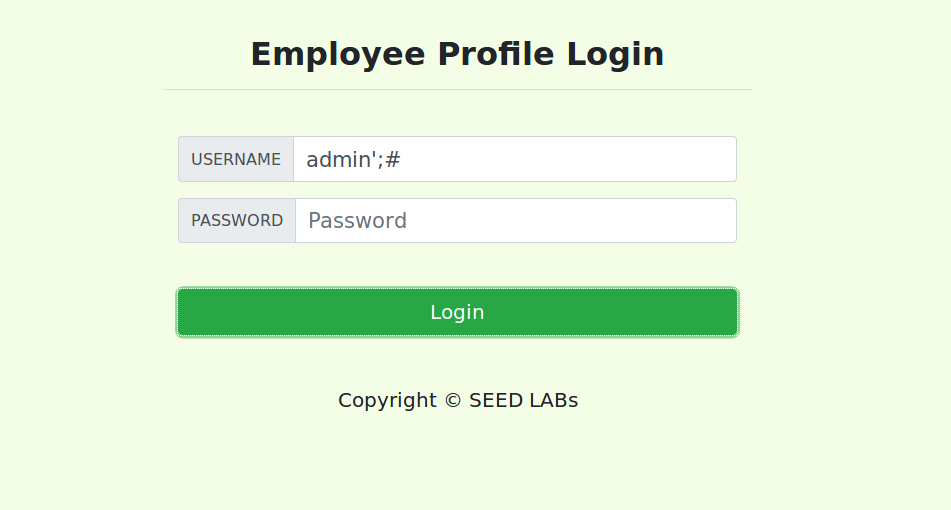
Task 2.1: SQL Injection Attack from webpage.

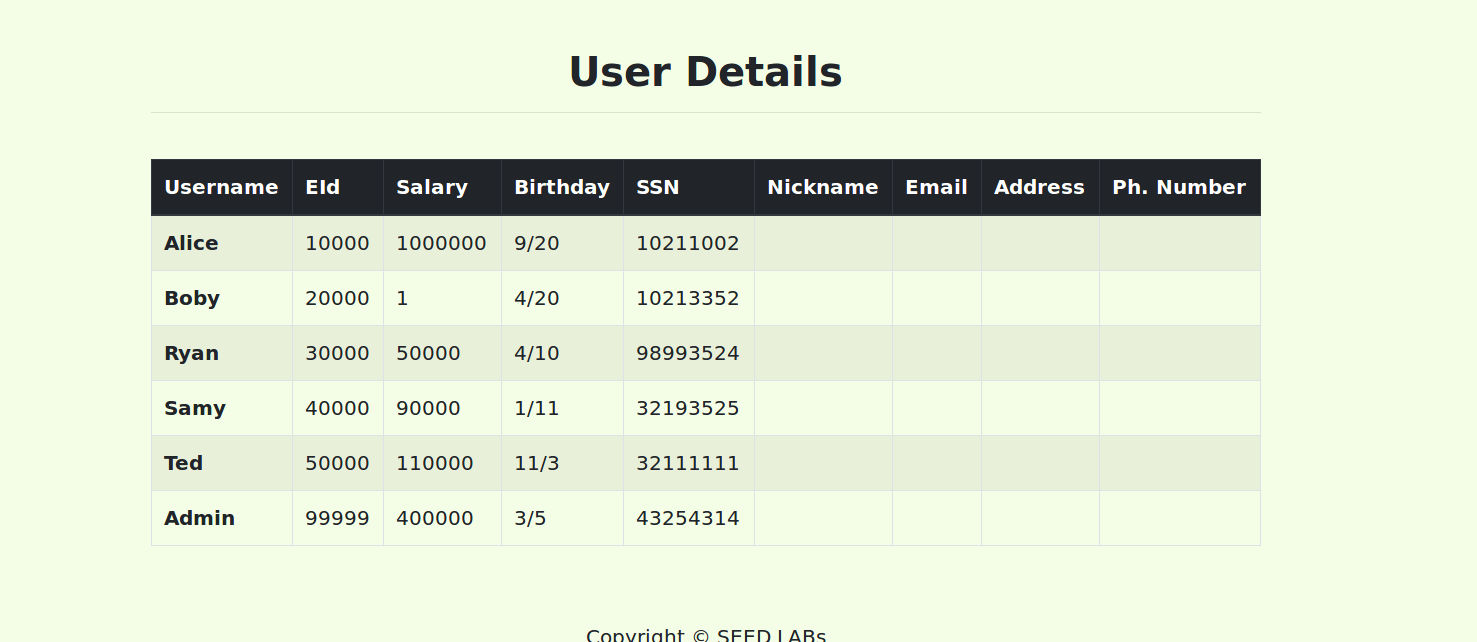
Your task is to log into the web application as the administrator from the login page

You need to decide what to type in the Username and Password fields to succeed in the attack

在终端的mysql中键入SELECT \*FROM credential WHERE='Admin':#' AND password ='';

打开sql网页，用户名如下，密码随意





**Task 2.2: SQL Injection Attack from command line.**

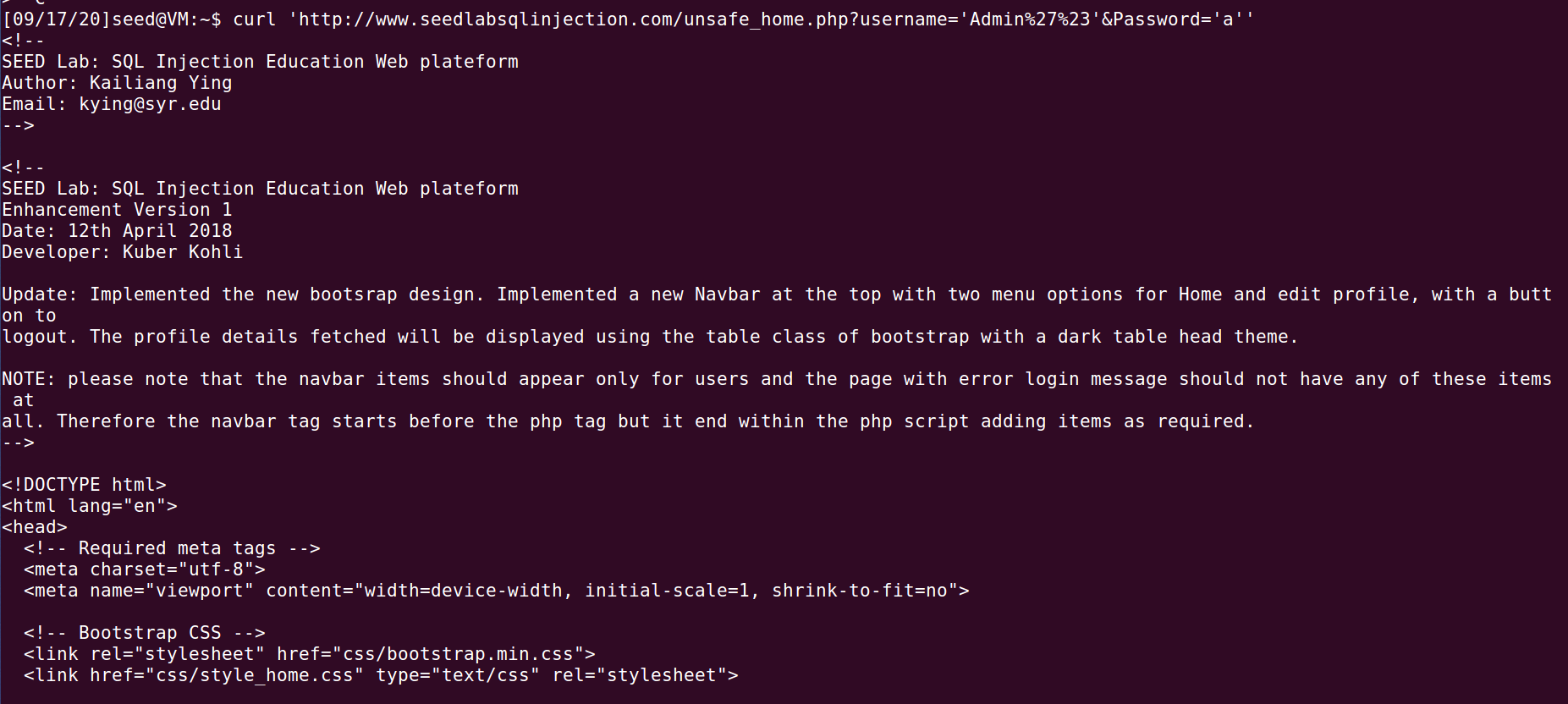
repeat Task 2.1, but you need to do it without using the webpage

If you want to include single quote in those fields, you should use %27 instead; if you want to include white space, you should use %20.

Handle HTTP encoding while sending requests using curl

在终端使用命令行登录到Admin账户

curl 'http://www.seedlabsqlinjection.com/unsafe\_home.php?username="Admin%27%23'&Password='a''

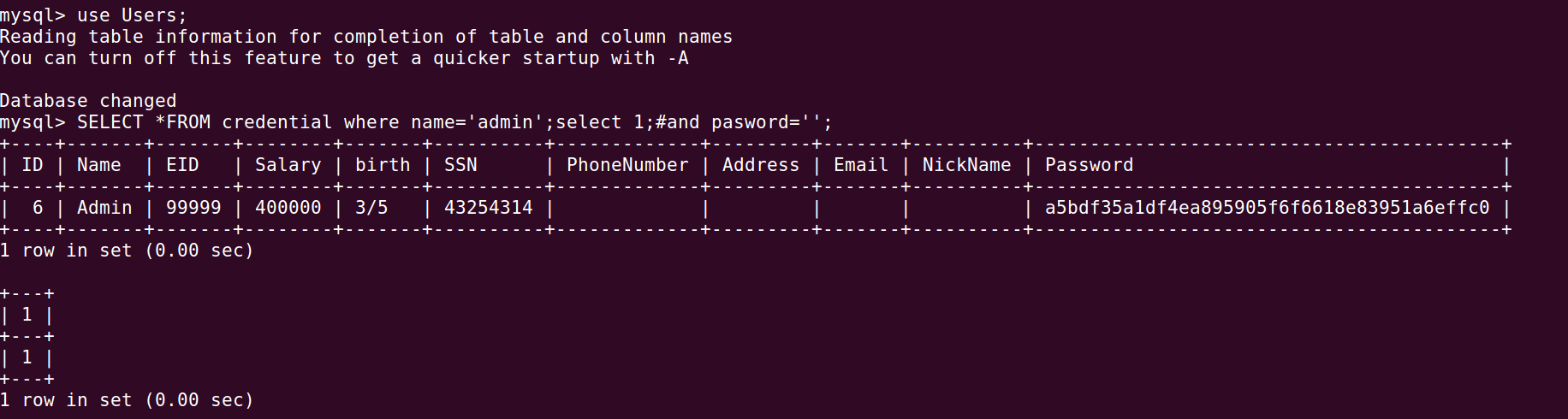


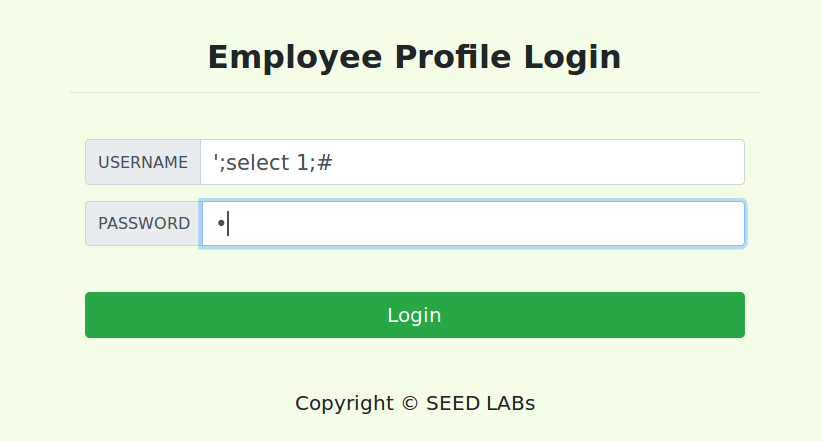


**Task 2.3: Append a new SQL statement.**

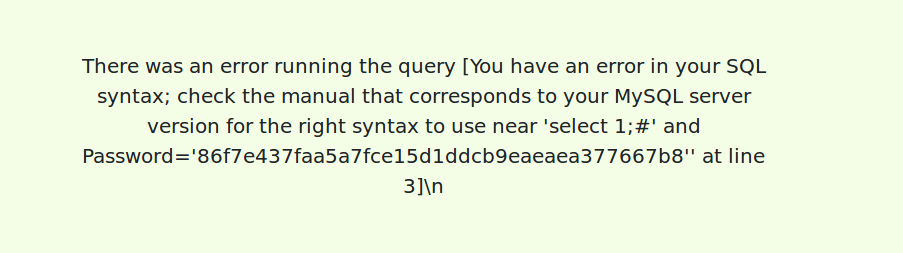
modify the database using the same vulnerability in the login page.

describe how you can use the login page to get the server run two SQL statements.





不成功，因为两条语句会被数据库识别，导致攻击失败。

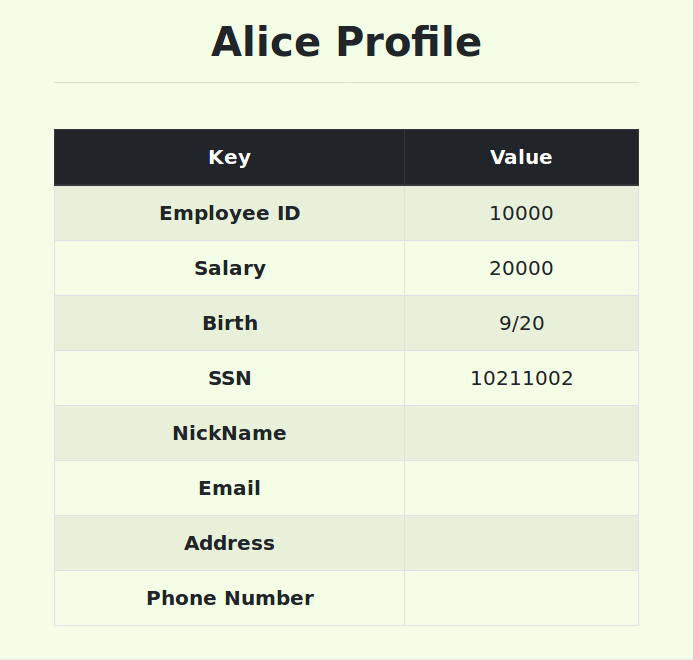


SQL注入漏洞的本质是数据和代码混编，攻击者在输入框中输入一定的内容，利用select命令可能会导致数据库数据泄露

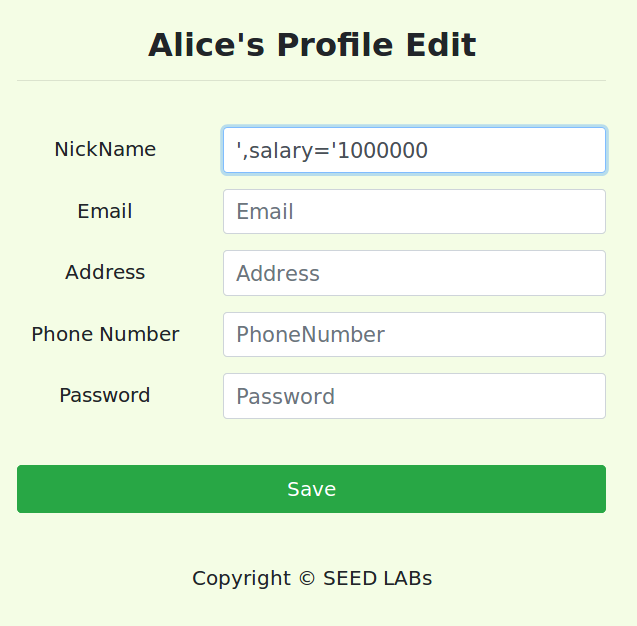
**Task 3: SQL Injection Attack on UPDATE Statement**

**Task 3.1: Modify your own salary.**

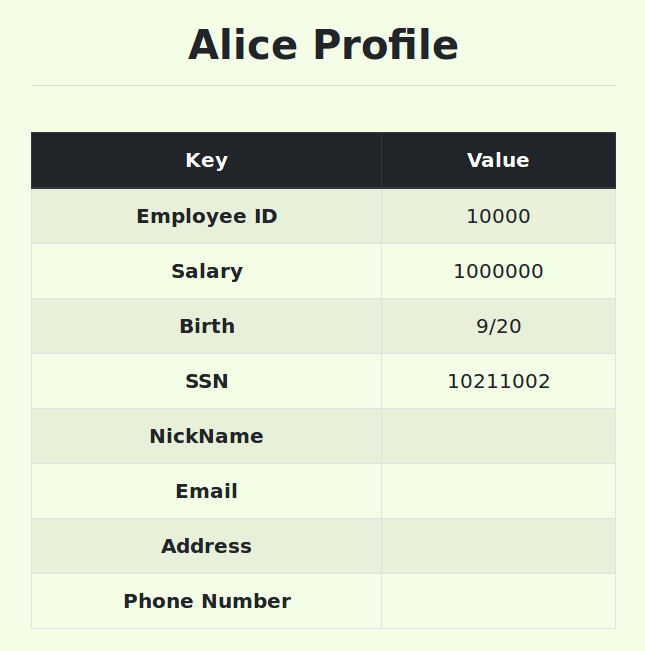
登录Alice账号，查看修改前工资：



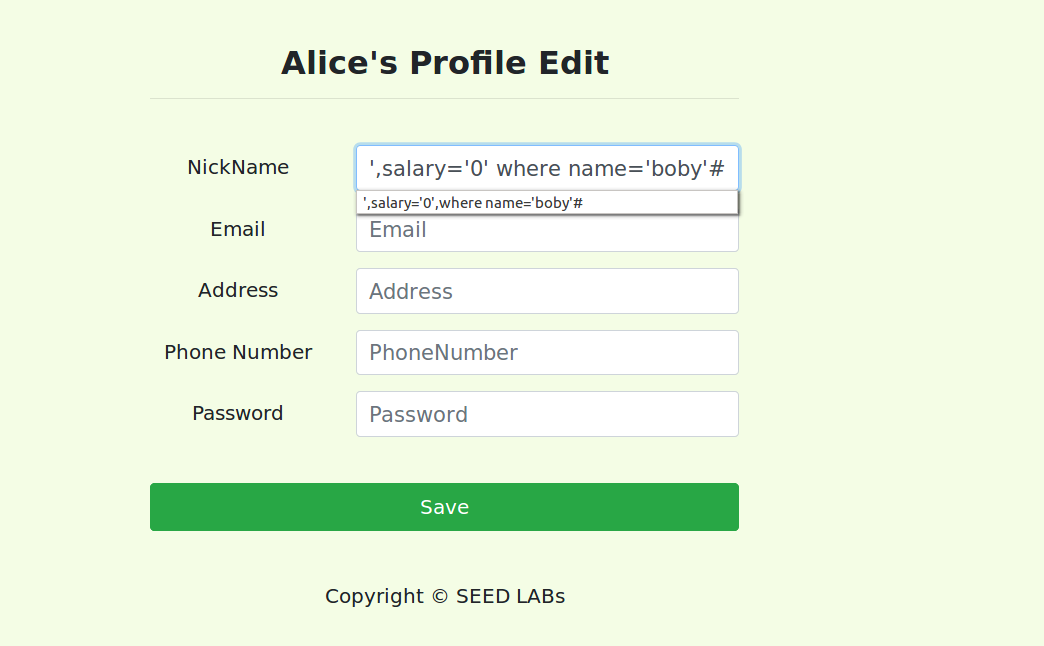
SQL注入攻击



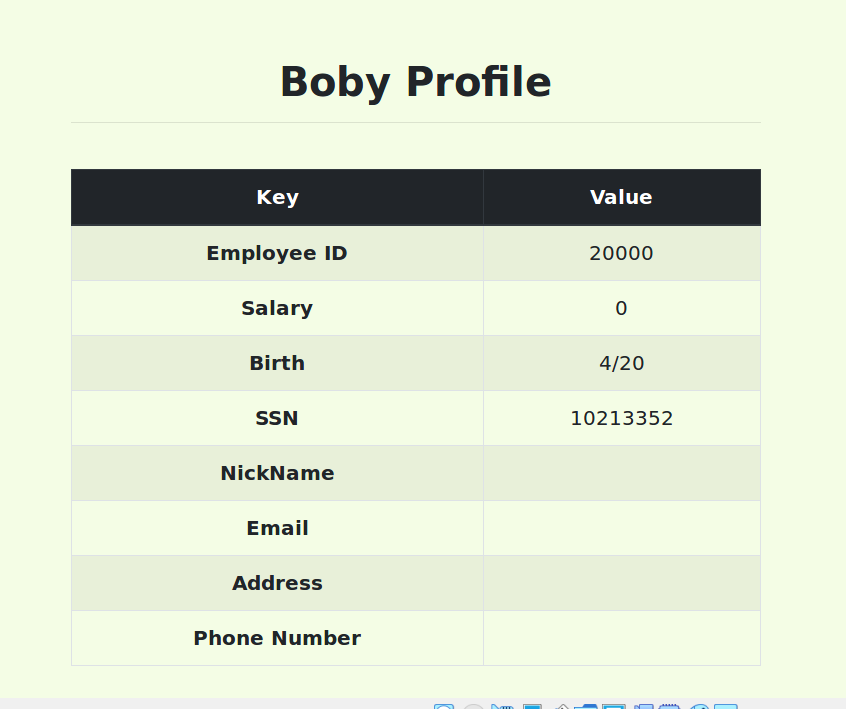
查看修改后Alice的工资：



**Task 3.2: Modify other people’ salary.**



登录Bboy账号



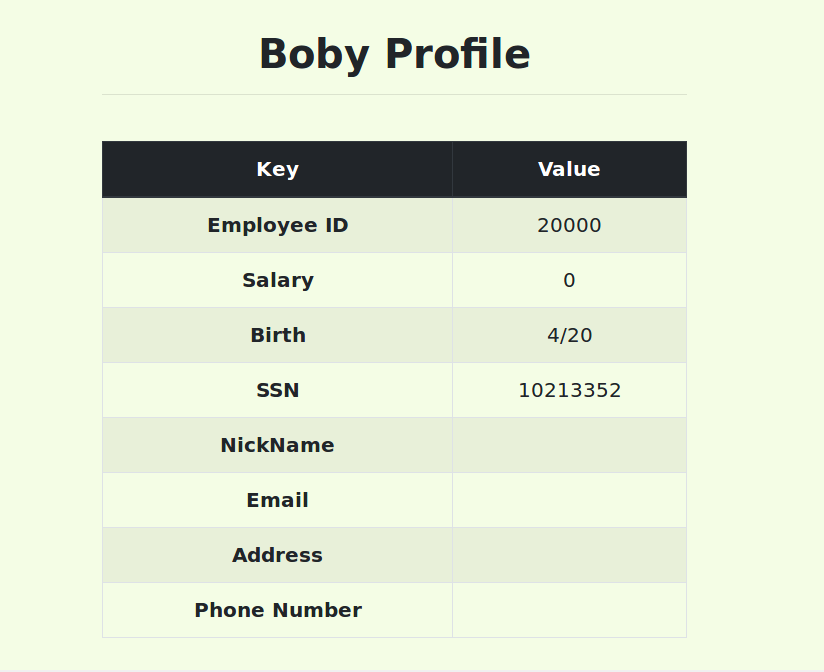
**Task 3.3: Modify other people’ password.**

change Boby’s password to something that you know, and then you can log into his

account and do further damage.

Alice在自己账户edit profile处修改为

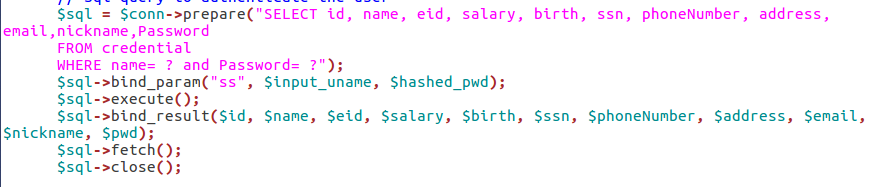
',password=sha1('abcdef') where name='boby'#



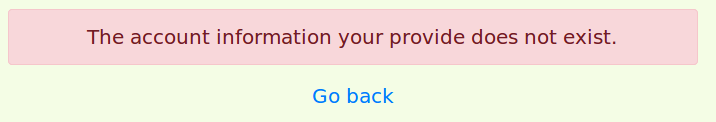
修改后Alice可以使用boby的账户名以及密码进行登录

**Task4:** **Countermeasure—Prepared Statement**

Unsafe\_home.php代码更改后如下

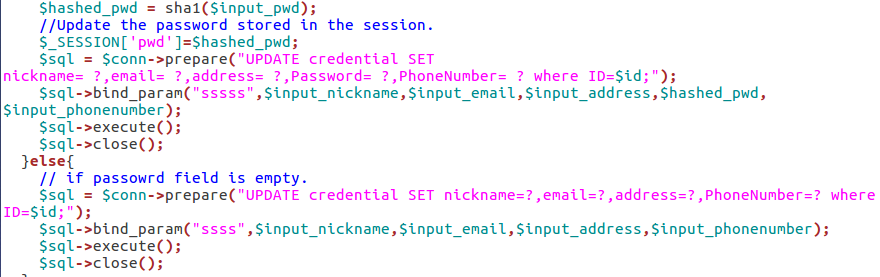


修改后再次攻击，发现攻击失败：



使用命令行进行攻击，同样失败

Unsafe\_edit\_backend.php代码更改后如下：



修改后再次攻击，发现攻击失败：

