**网络空间安全实训Lab[6]**

**实验报告**

**57118117 谌雨阳**

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

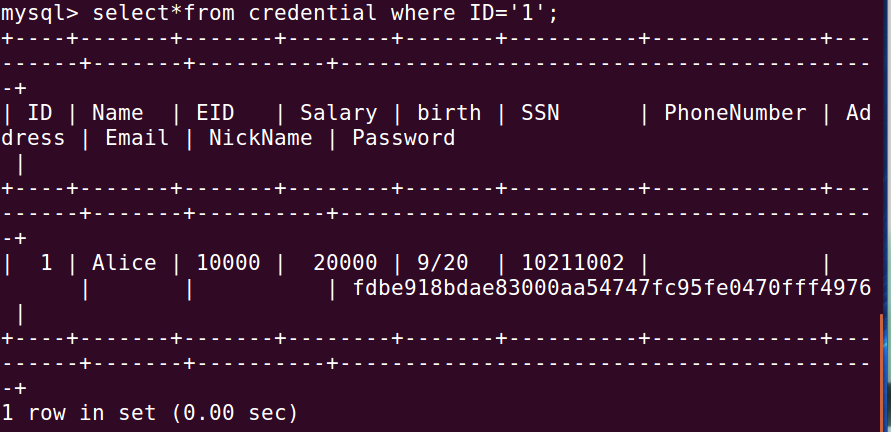
1、在终端中输入以下三行语句：

$ mysql -u root -pseedubuntu

mysql> use Users;

mysql> show tables;

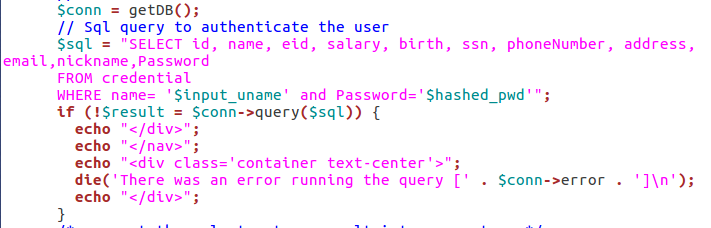
得到以下输出：



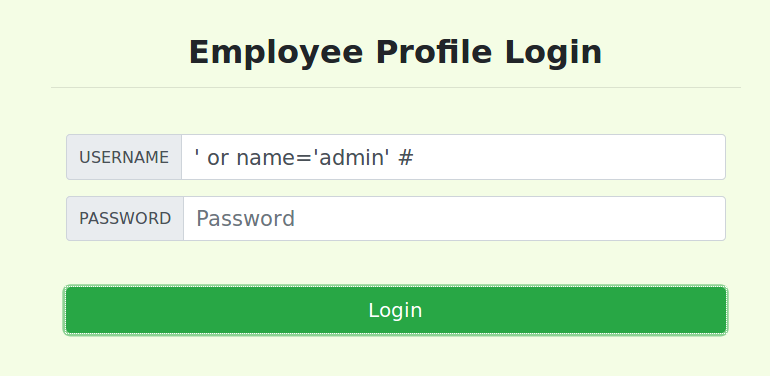
**Task 2: SQL Injection Attack on SELECT Statement**

**Task 2.1: SQL Injection Attack from webpage**

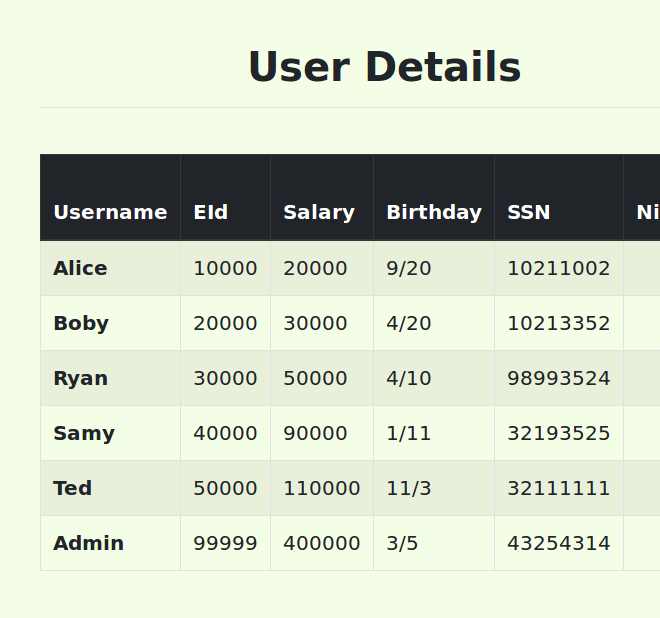
1、为了实现SQL注入攻击，先研究php文件中输入框周围代码内容:



2、用单引号进行分隔语句，输入如下语句：（后发现Admin‘#就可以做到）

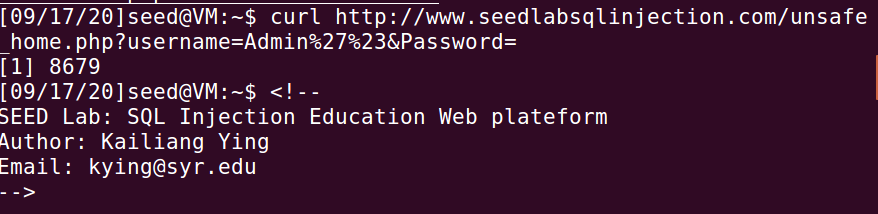


3、成功以无密码状态登录，查看到所有人的数据：



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

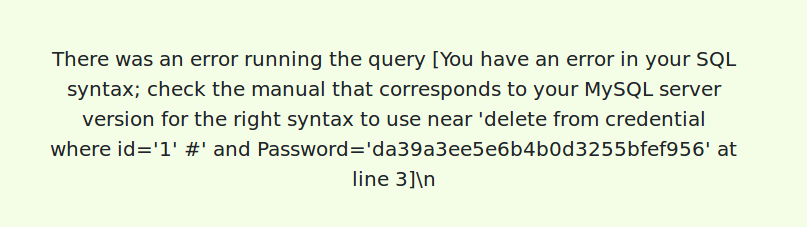
1、通过HTTP Live Header工具抓取登录操作url后，在命令行中键入如下命令；



同样可以达成Task2.1的效果。

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

1、尝试使用分号进行双语句注入被报错：

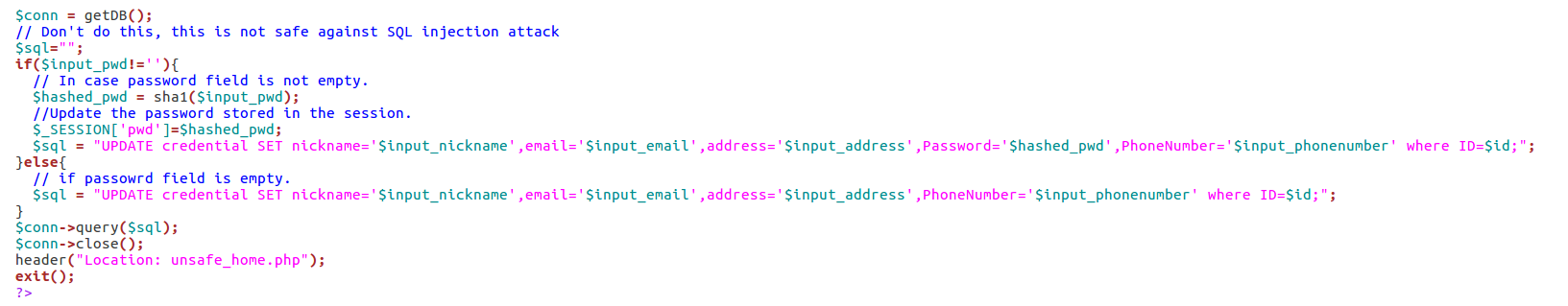


查阅资料后得知：在MySQL中实现了一种特殊的保护机制，mysq\_query不允许提交多个请求，导致我们两个连续的请求就会报错。

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

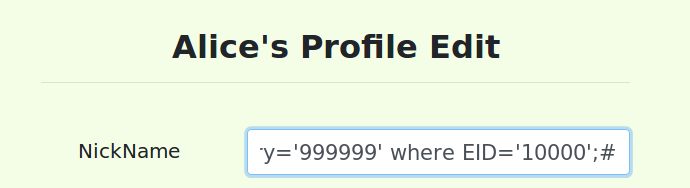
**Task 3.1: Modify your own salary**

1、同样先研究页面的phph源码，找到输入框附近的相关代码：

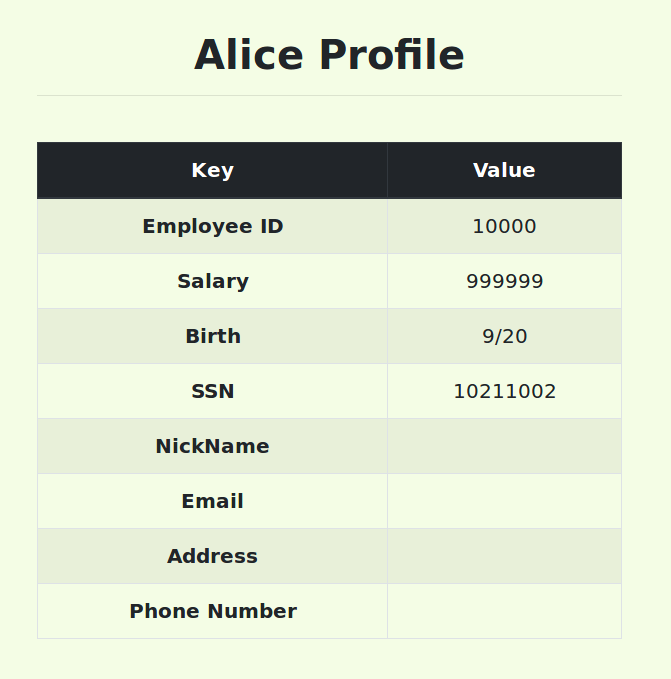


2、合理利用单引号的断句作用，输入如下内容：

', salary='999999' where EID='10000';#

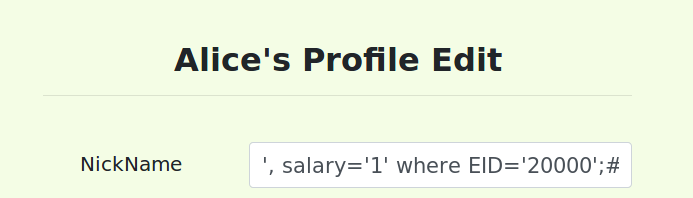


3、Alice的工资被改为999999：



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

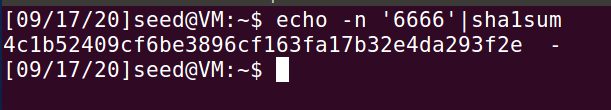
1、语句基本同上，将工资改为1，把EID改为20000：

2、发现老板Boby的工资被更改为1，复仇成功：



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

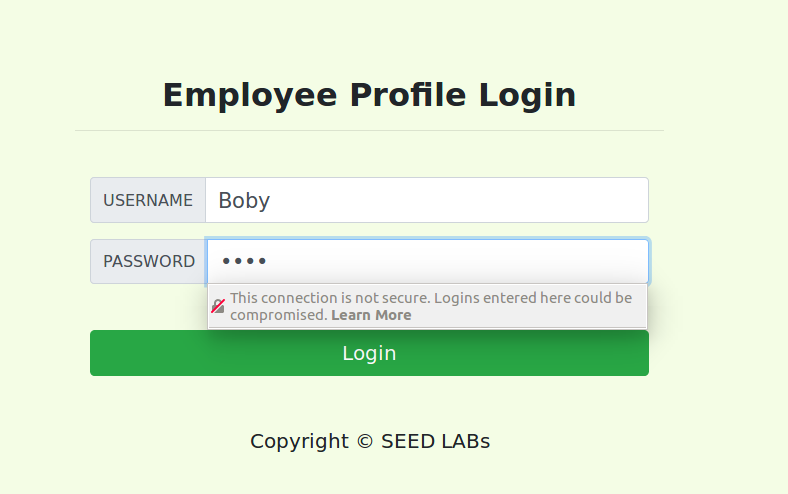
1、在linux终端中用如下命令检索6666的哈希值，6666为我们想要更改的密码：



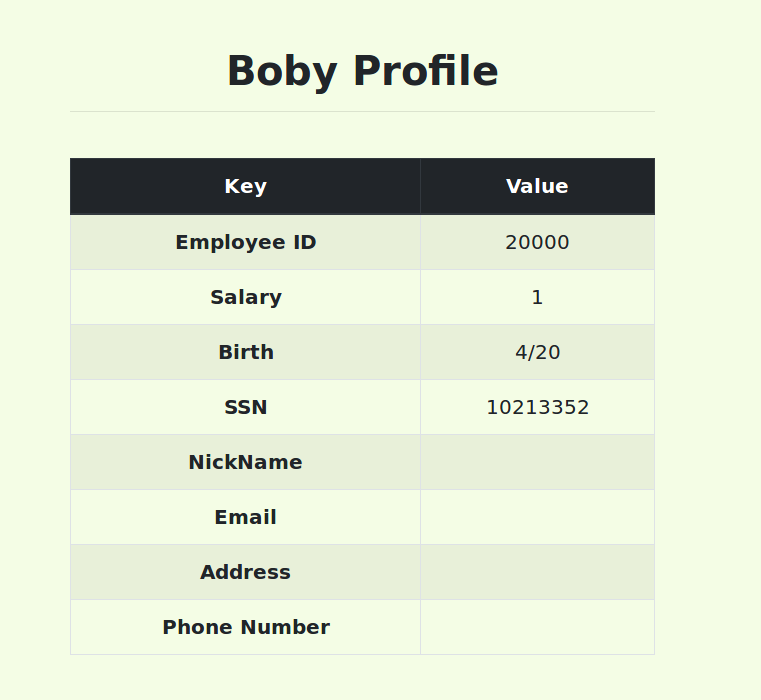
2、在nickname栏输入以下语句：

', Password=/4c1b52409cf6be3896cf163fa17b32e4da293f2e' where Name='Boby';#

3、修改完毕后可以使用新密码6666登录：

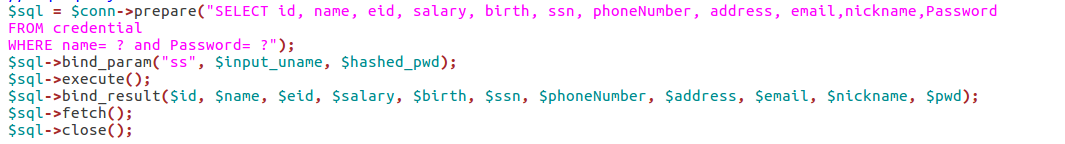


登录成功：



**Task 4: Countermeasure — Prepared Statement**

1、进入unsafe\_home.php文件，照实验手册中的代码格式修改如下：



2、再次尝试task2.1中的攻击方法发现没有响应，攻击失败。

