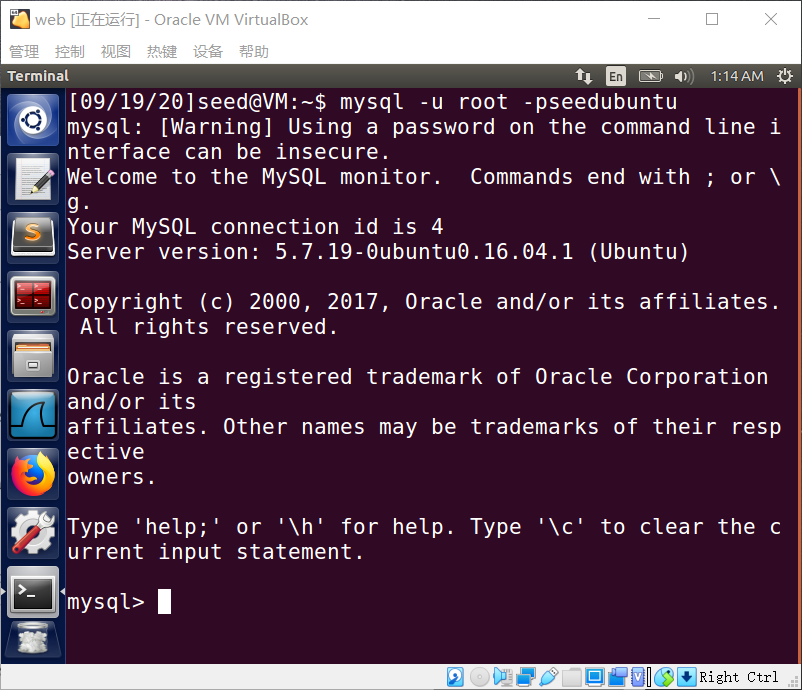
**Lab6**

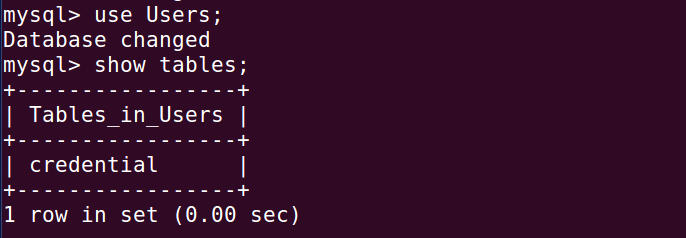
57118213 陈洪杰

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

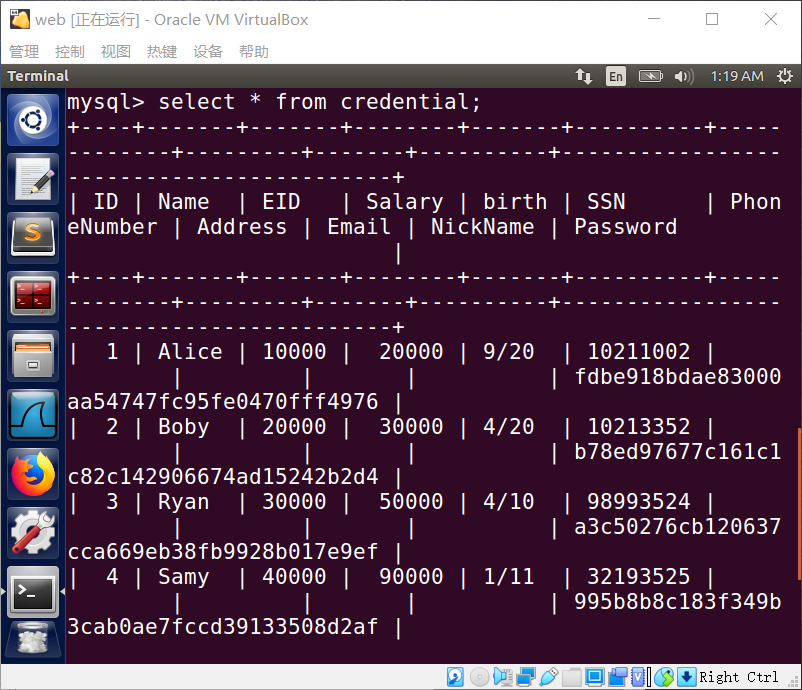
用以下命令打开mysql：



使用use Users; 进入到Users的数据库，再使用show tables; 查看Users数据库下的表格：



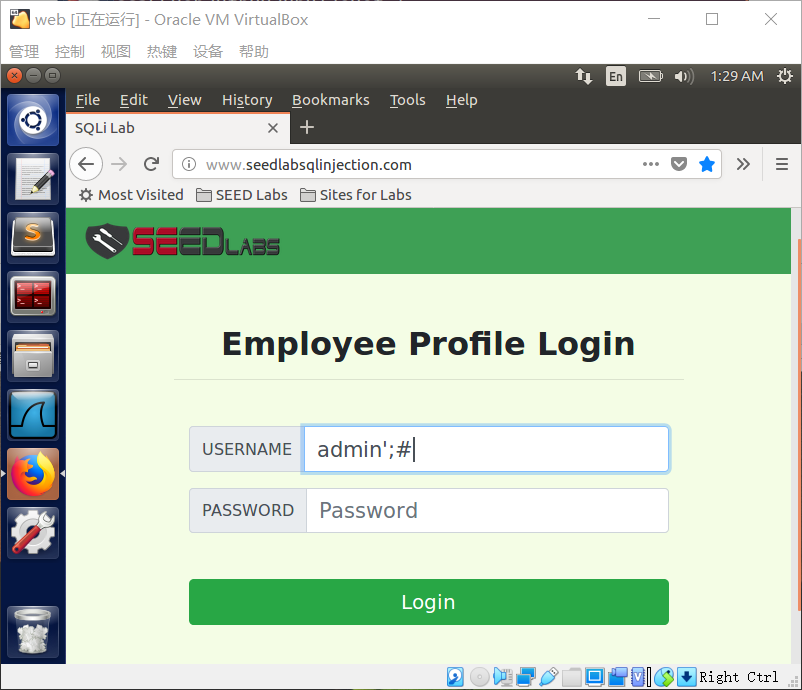
就输入“select \* from credential”，展示出每个用户的信息。从中可以找到Alice的信息：

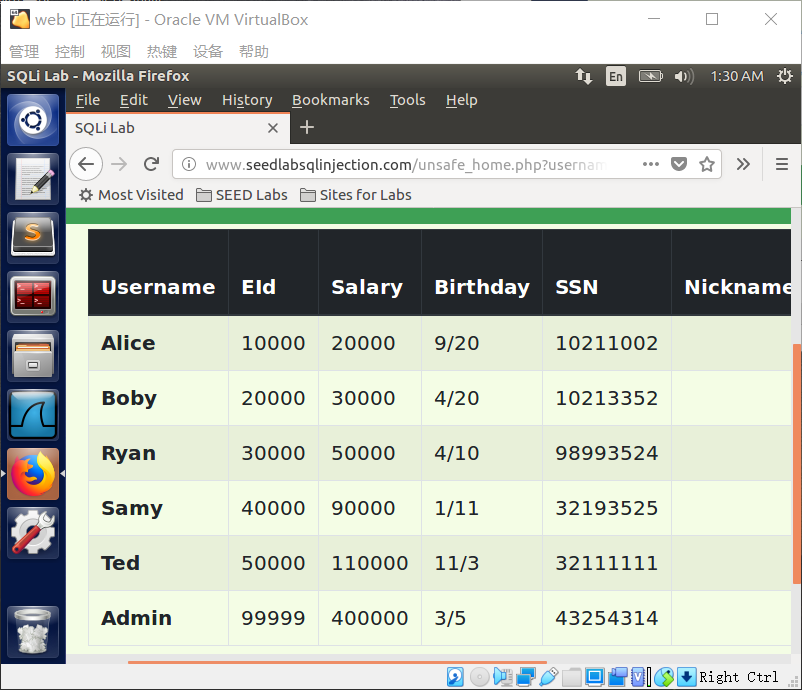


**Task 2: SQL Injection Attack on SELECT Statement**

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

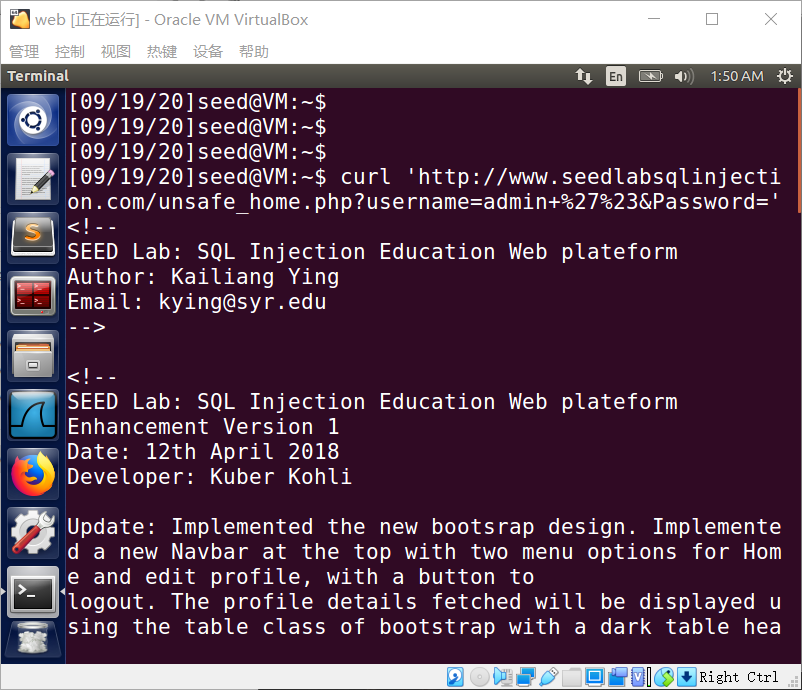
首先输入网址打开页面，输入如图账号不用密码登录可以看到所有用户：



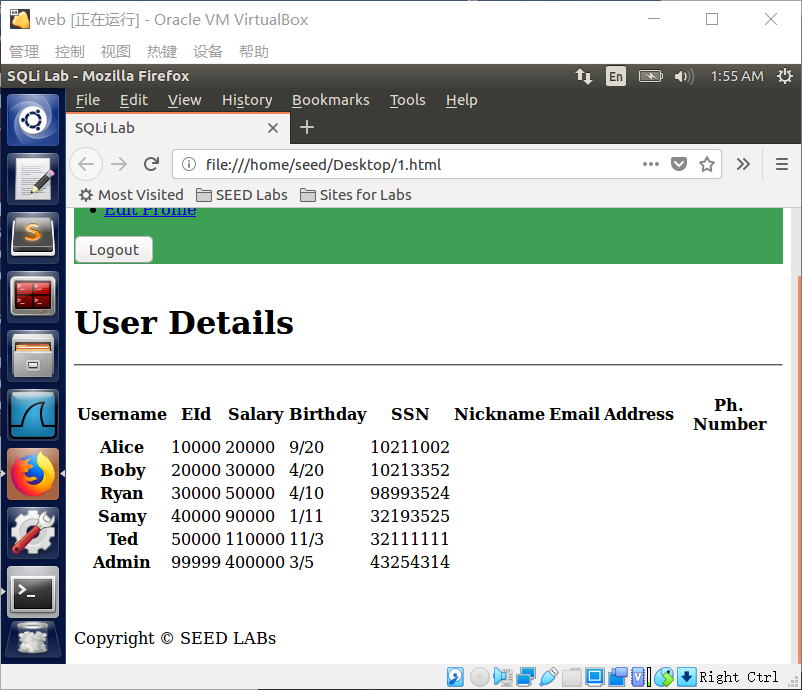


**Task 2.2: SQL Injection Attack from command line.**

用如图所示命令可以出现admin的网页代码



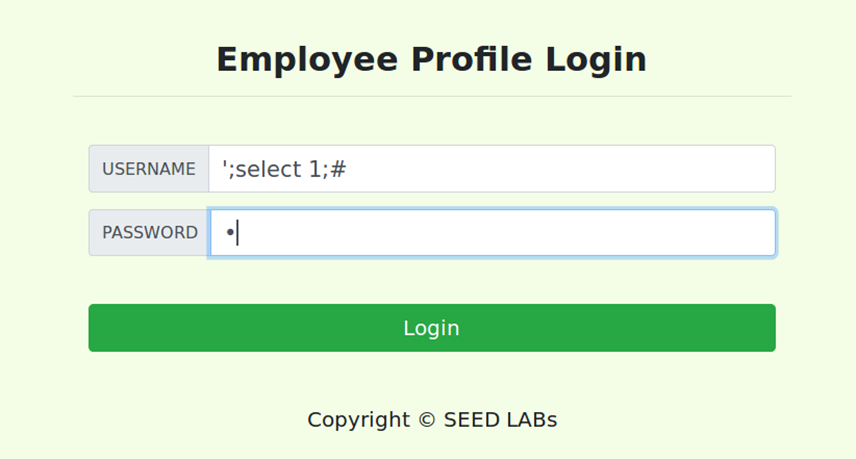
可以复制到一个html文件中用浏览器打开得到好的排版

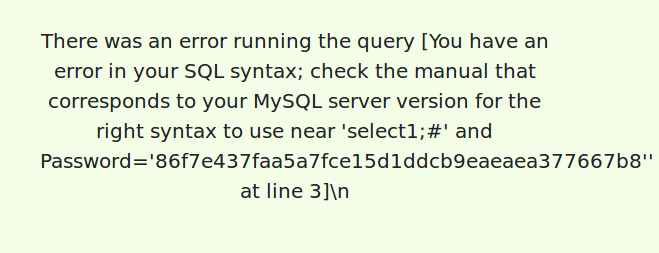


可以看到成功的打印出了admin的所有信息。

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

在登录页面进行攻击时，发现并未成功。

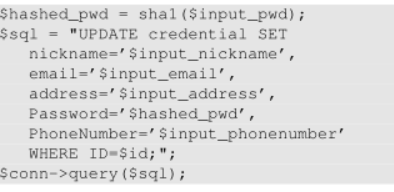




**Task 3: SQL Injection Attack on UPDATE Statement**

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

根据说明我们知道在修改个人信息时，我们会进入下面这一段代码



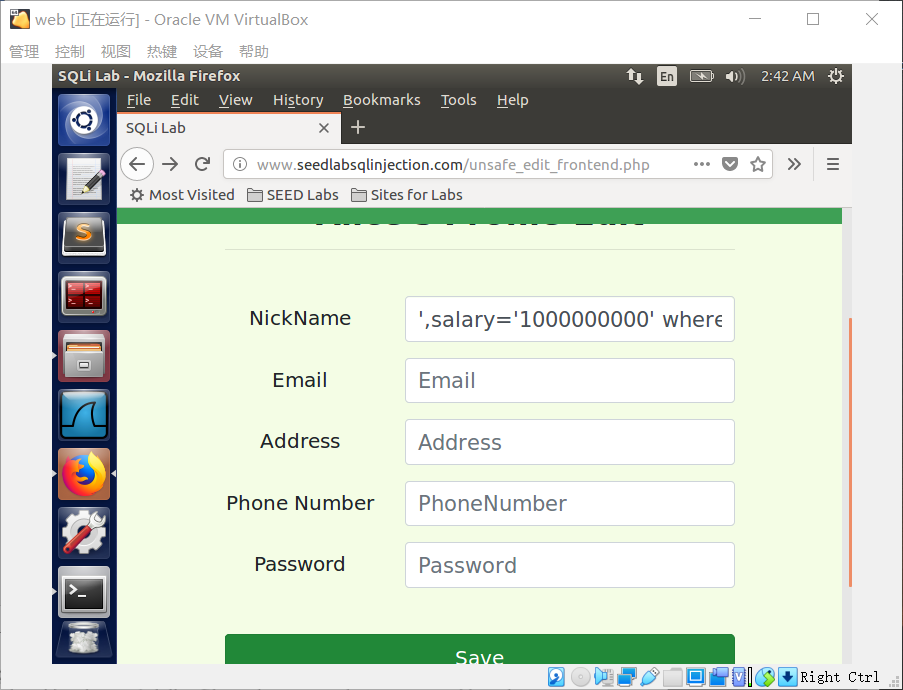
这里面并没有salary的选项，所以我们运用sql注入攻击。

用以下网址进入进入profile edit页面

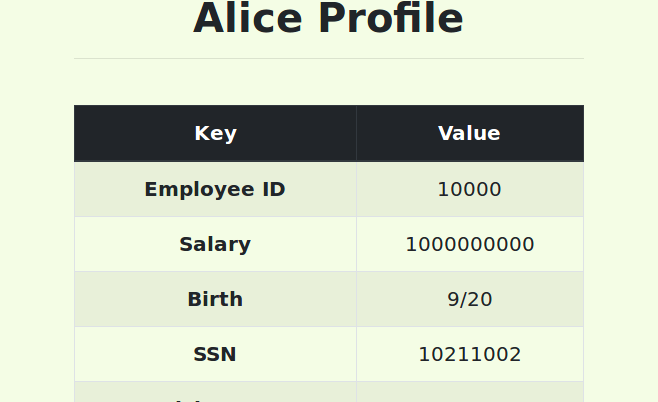


在nickname一行输入以下代码',salary='1000000000' where EID='10000';#：

这里的#相当于注释符，就是说我们进入到上面的代码中，加上了salary这一行而把后面的几项都注释掉了，所以这里改了薪水：

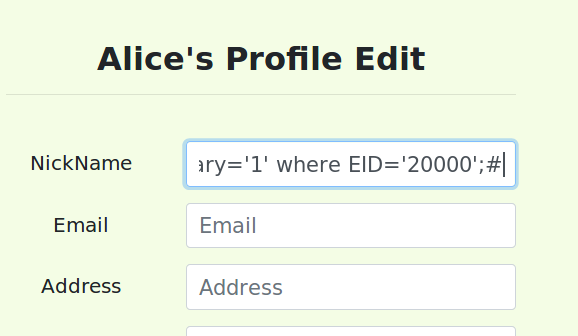


保存后跳回到Alice的Profile界面，发现工资已经被修改

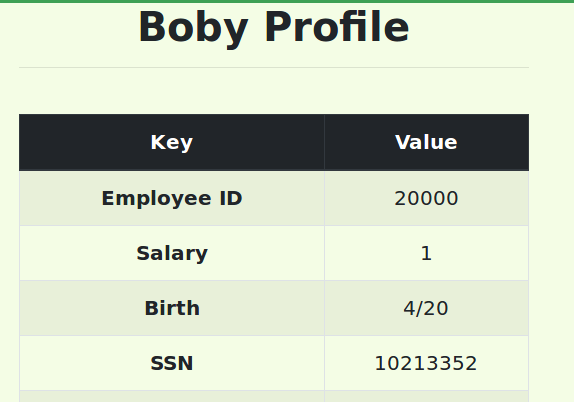


**Task 3.2: Modify other people’ salary.**

同理，我们在nickname里加入', salary='1' where EID='20000';#

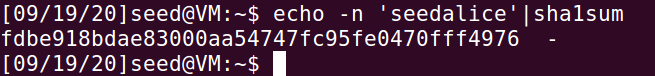


登录boby的账号查看一下，发现信息修改成功。

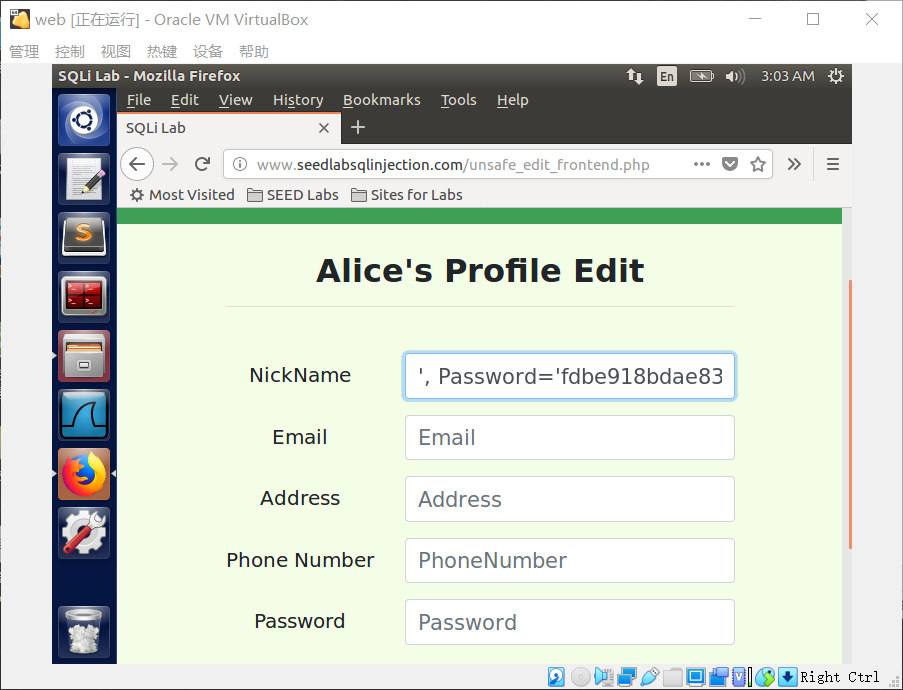


**Task 3.3: Modify other people’ password.**

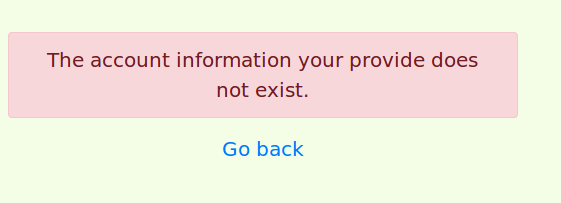
根据任务描述我们知道密码是以sha1 hash存储的，所以我们要改密码的时候，首先要知道我们修改密码的sha1 hash值，比如我们要把boby的密码改成Alice自己的密码，所以我们去终端输入以下命令：



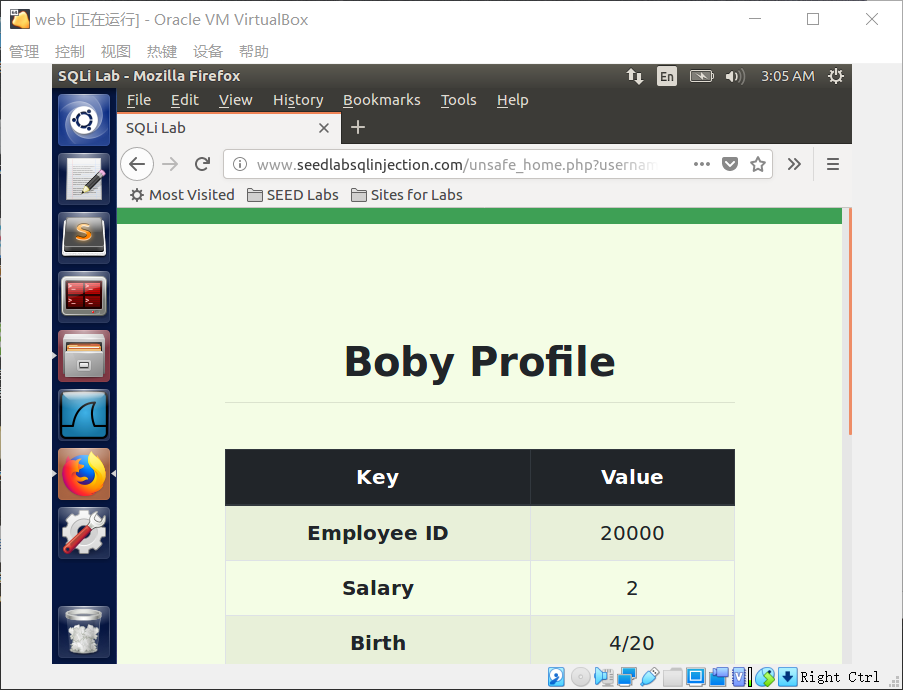
得到密码是fdbe918bdae83000aa54747fc95fe0470fff4976，接着我们去nickname里面修改boby的密码，输入以下命令：', Password=' fdbe918bdae83000aa54747fc95fe0470fff4976' where EID='20000';#



这下我们用boby输入自己原来的密码登录，出现

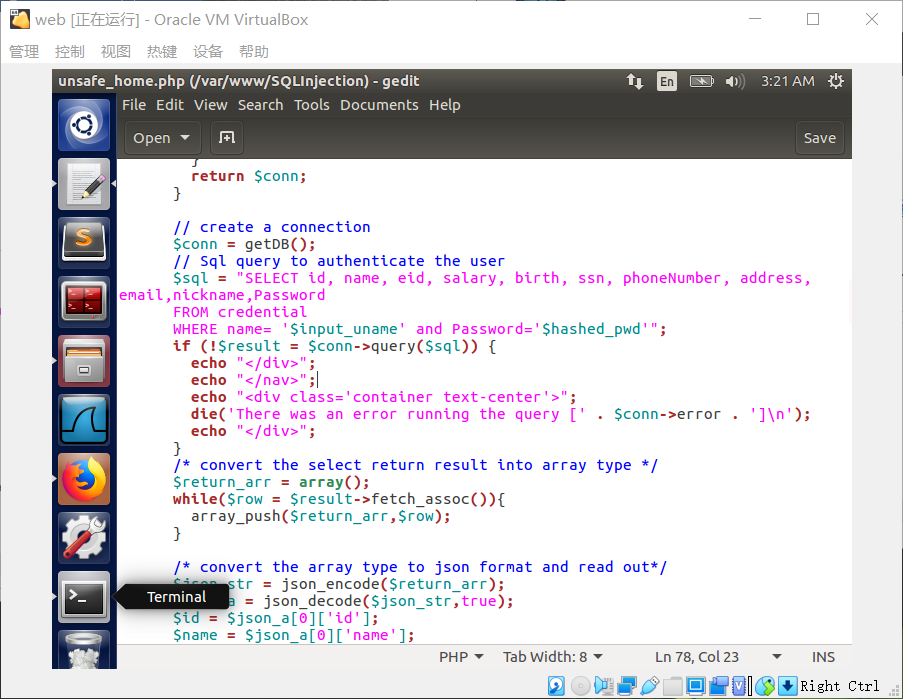


而用seedalice登录时，会发现可以正常登录，可知攻击成功。

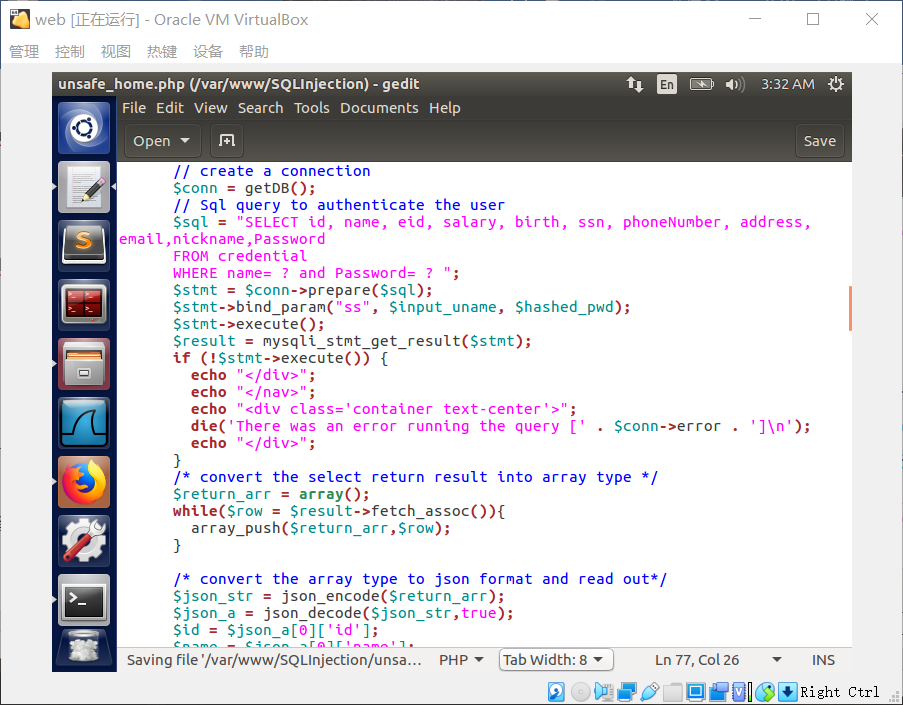


**Task 4: Countermeasure — Prepared Statement**

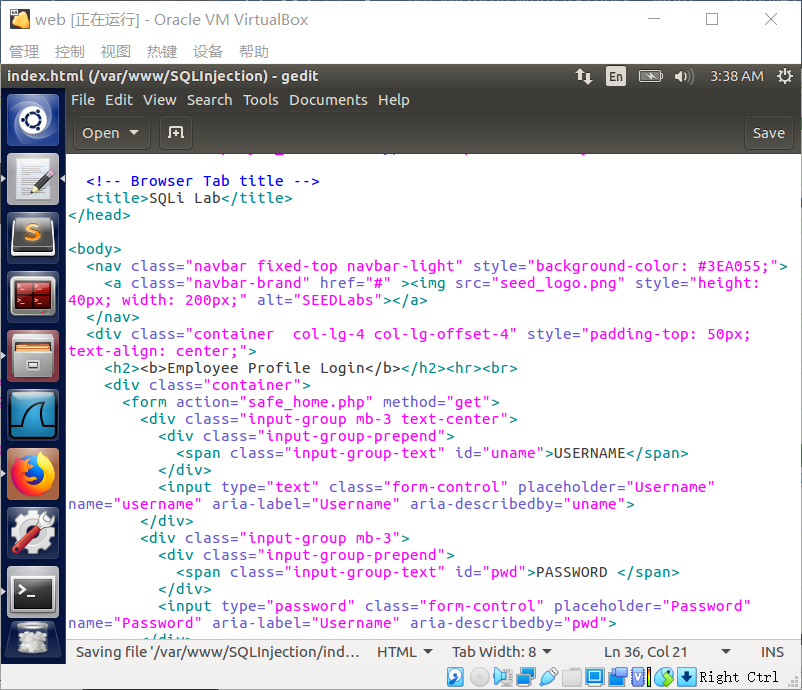
在/var/www/SQLInjection目录下找到unsafe\_home.php文件，打开修改



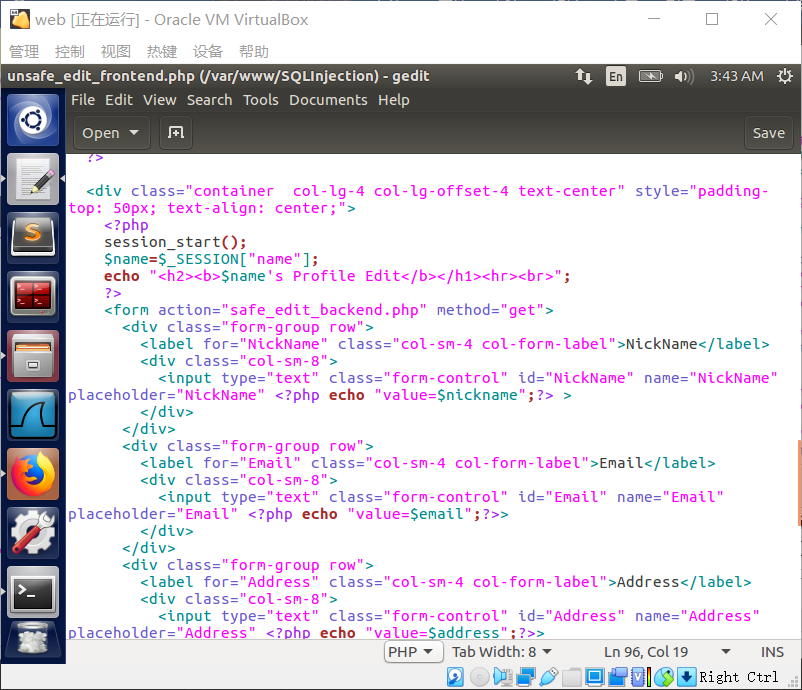
上下框中为修改前后的内容：



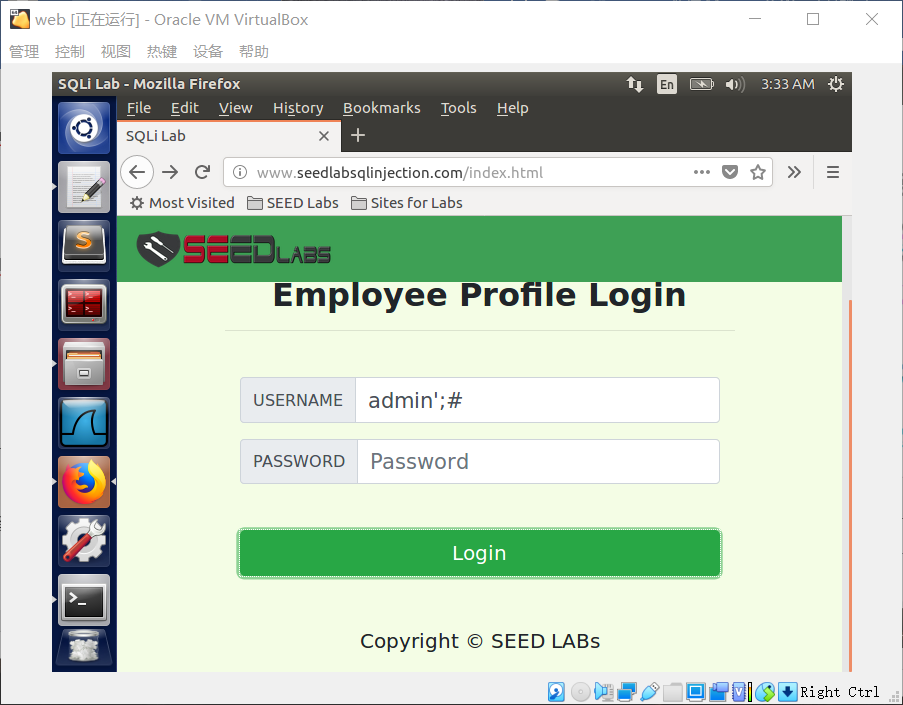
再修改index.html里的代码，将所示处的unsafe改成safe：



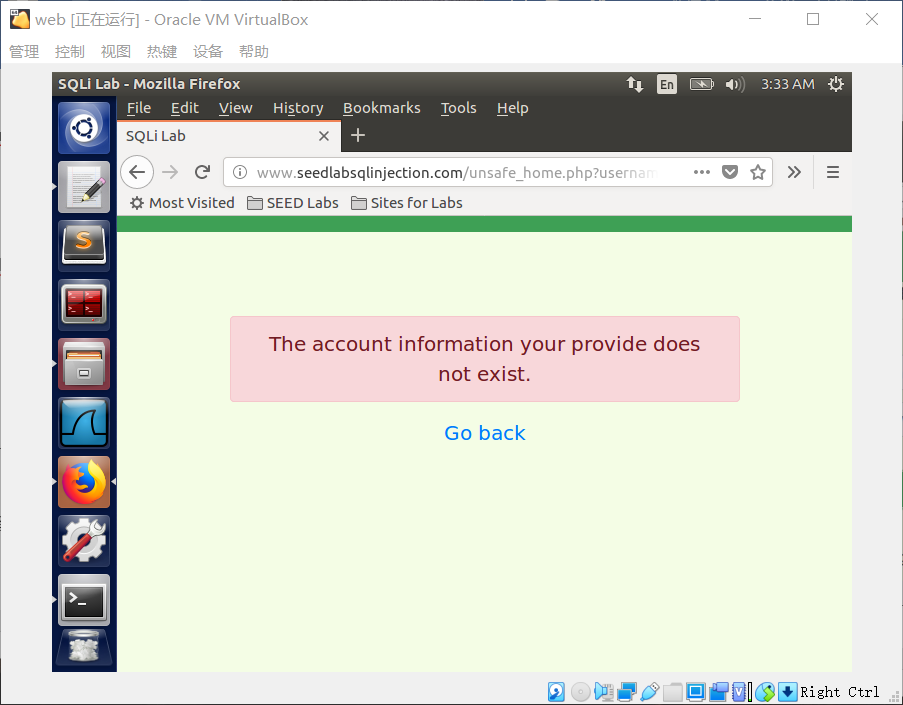
修改unsafe\_edit\_frontend.php，同样将所示处的unsafe改成safe：



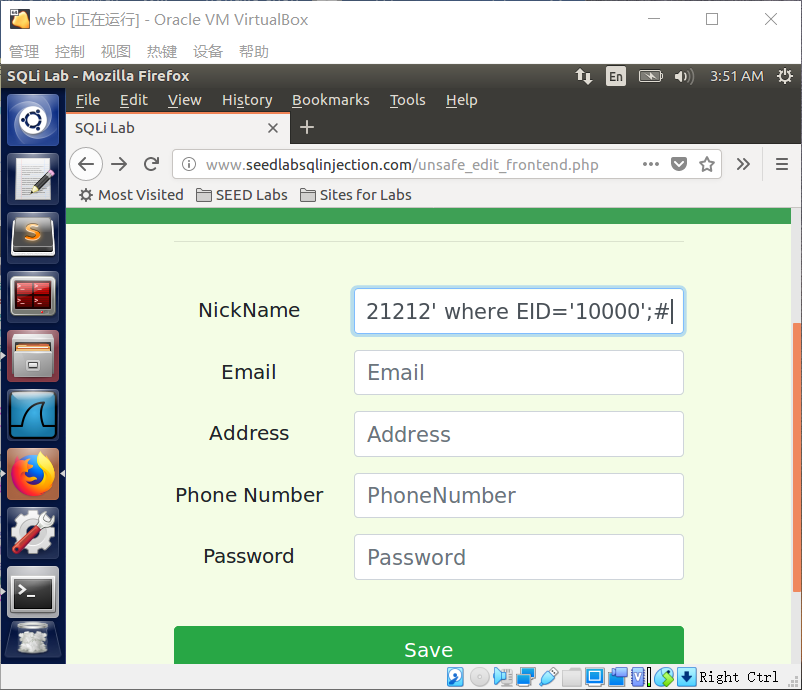
然后我们随便选择上述任意一个攻击，这里我们选择task2的攻击：



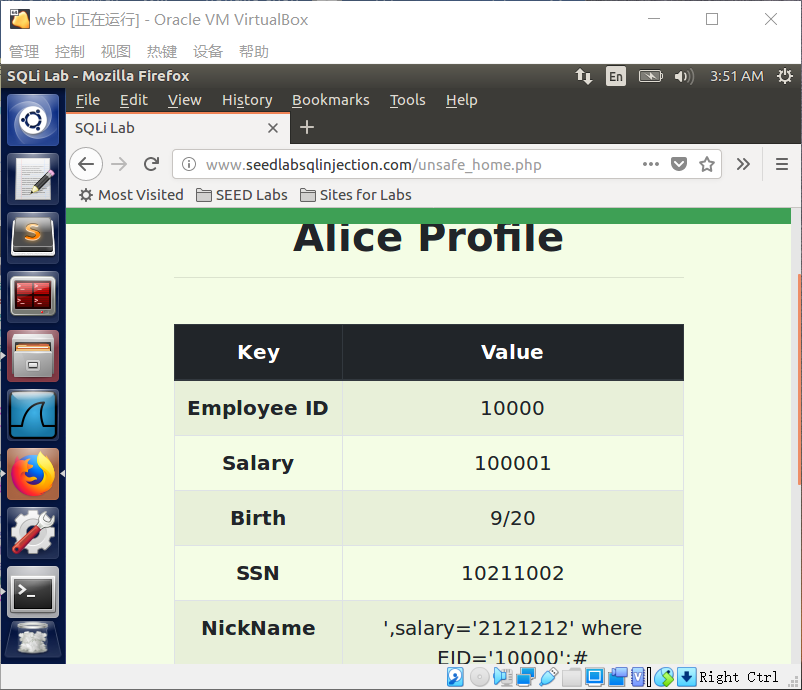
出现下面情况



我们再来修改薪水：



却发现只改了nickname



试一下修改密码，发现也未成功。

