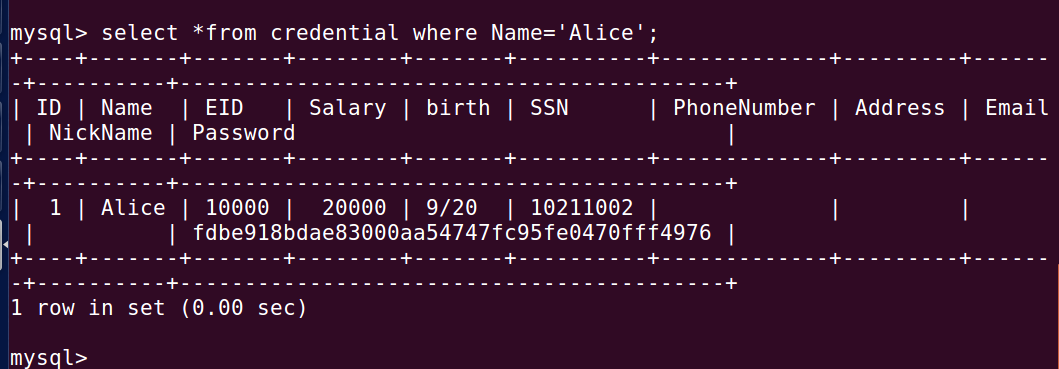
Task1:

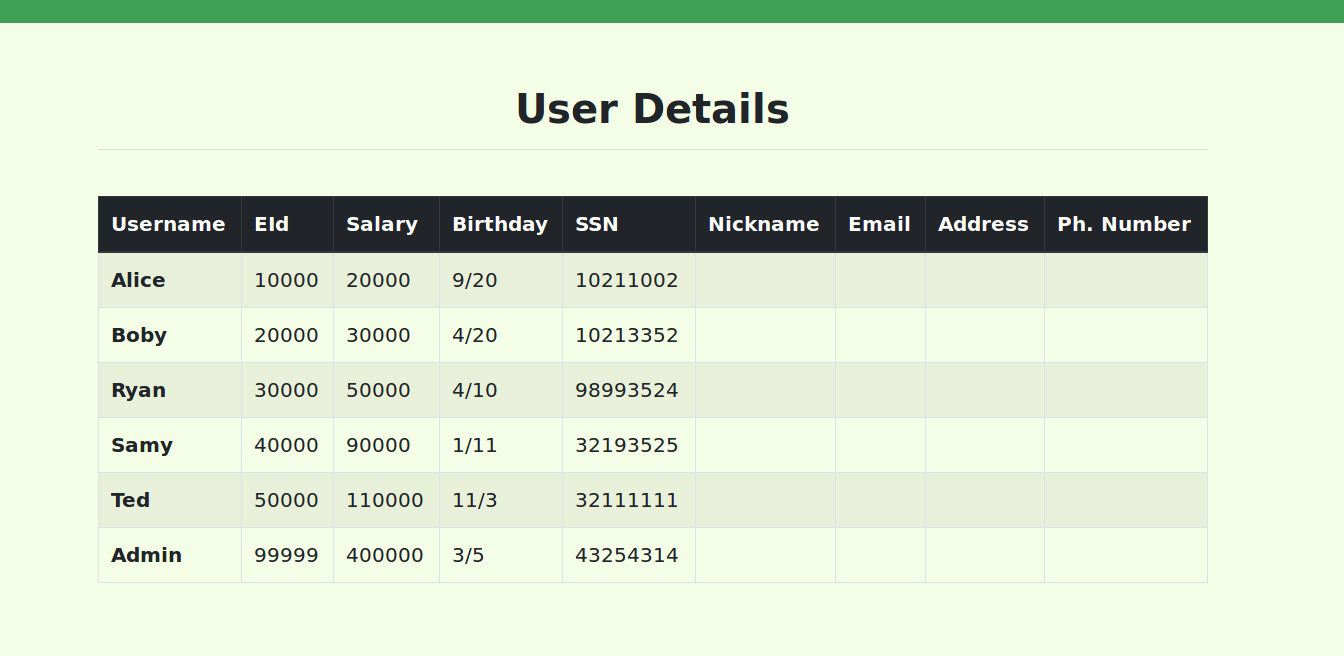
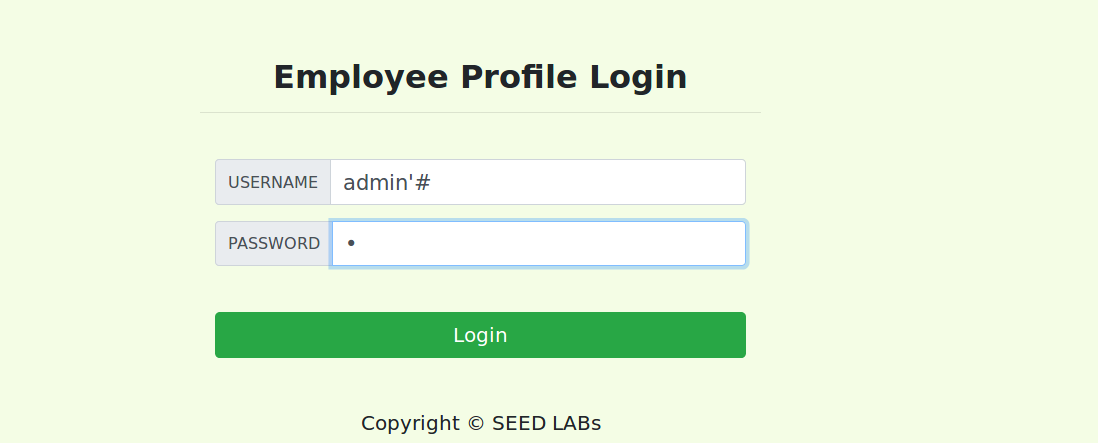
在命令行中进入mysql，输入指令select \*from credential where name=”alice”，得到alice的信息，如图



Task2:

2.1

在用户名输入框中输入admin’#，密码随意输入也可为空，发现成功登陆管理员账户

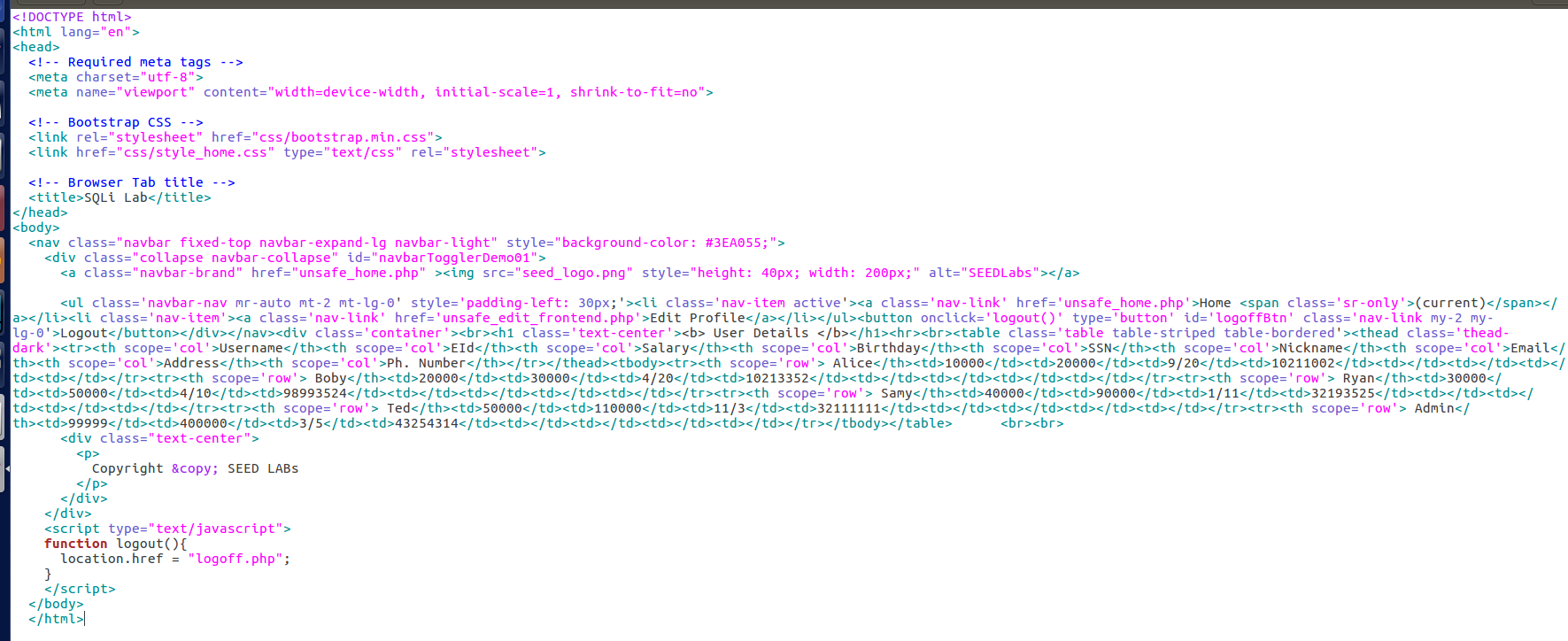


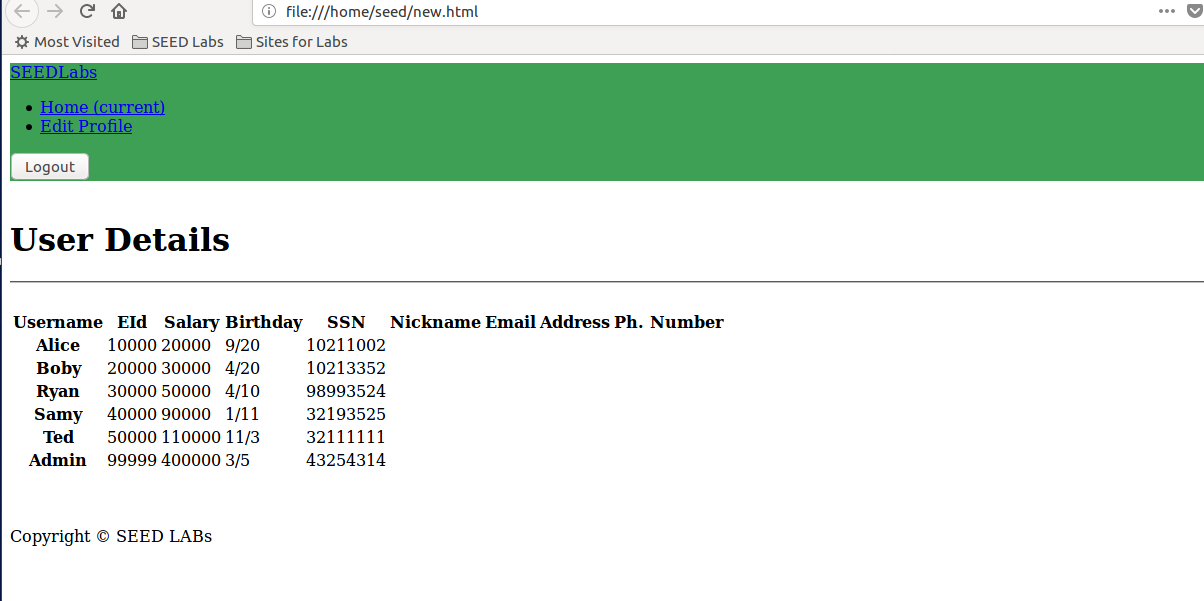
2.2:

在终端中使用crul命令，如图，得到了网页的源码



将源码复制到html文件中，用浏览器打开，看到了所有用户的信息



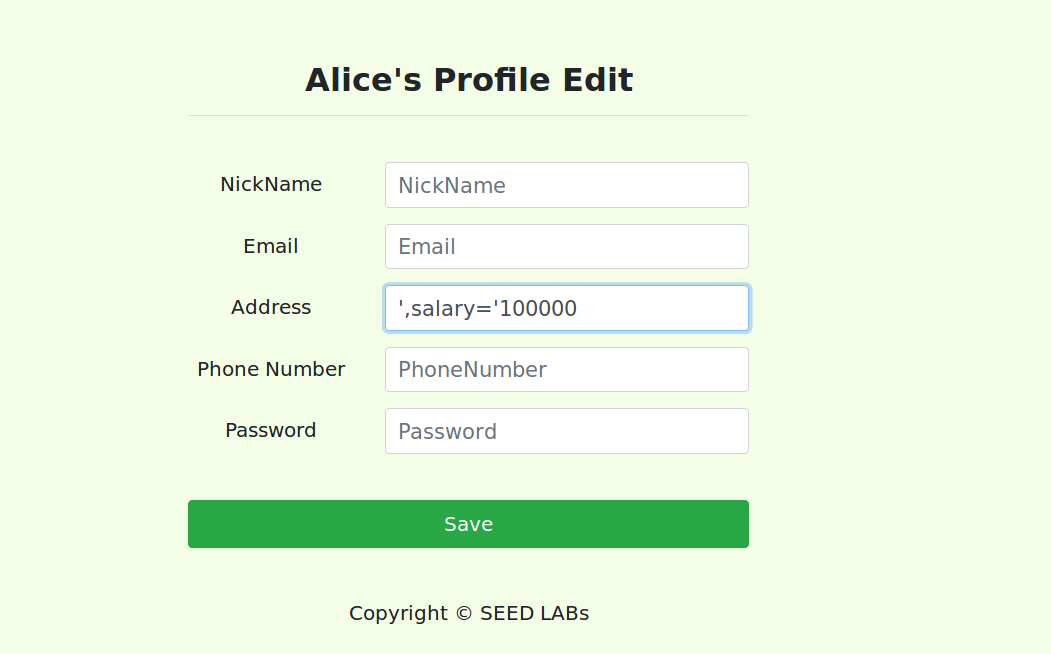


2.3暂时无法成功

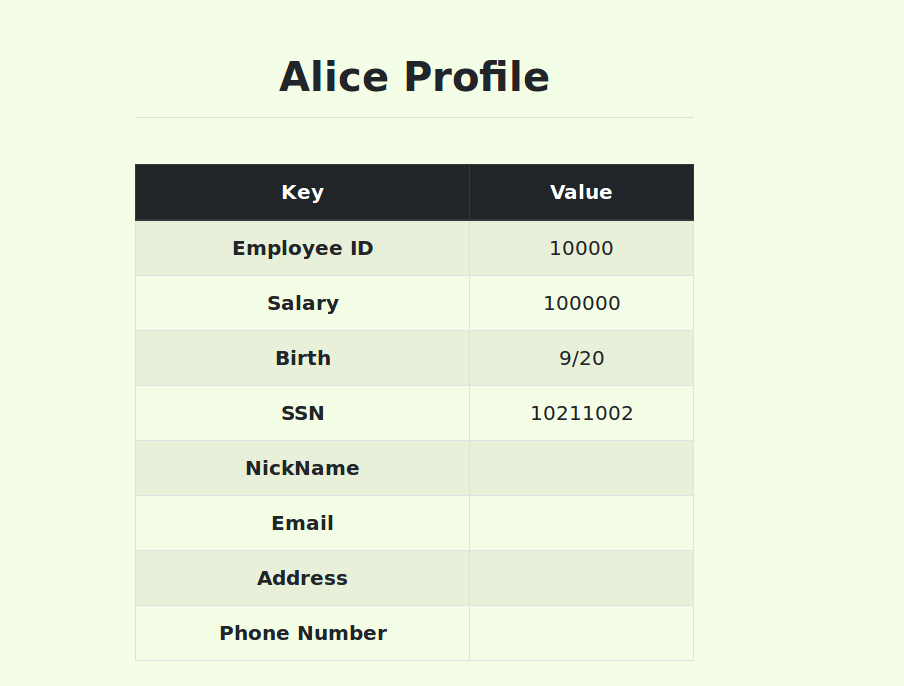
Task3:

3.1

编辑alice的信息，在任意栏输入‘，salary=’100000’

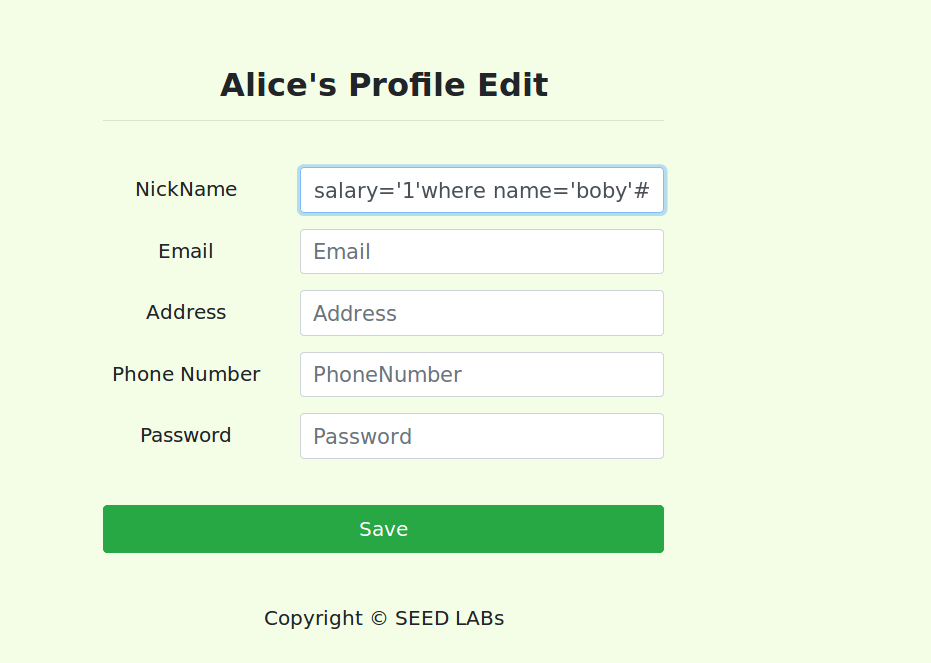


发现alice的工资变成了100000

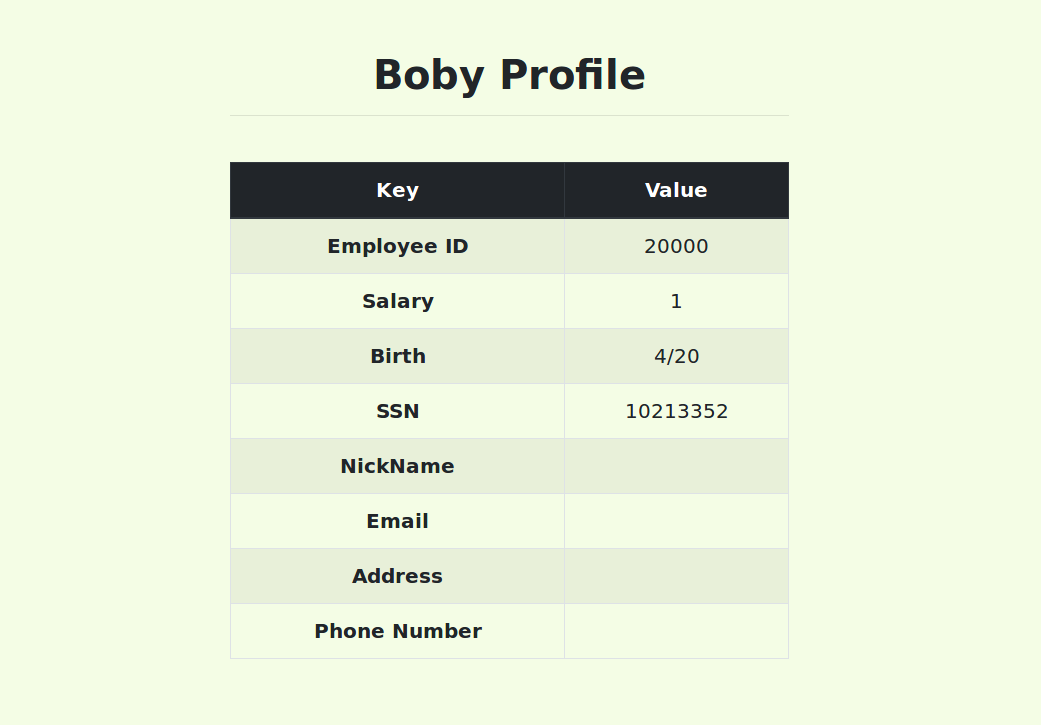


3.2

在alice修改资料界面任意栏输入’,salary=’1’where name=’boby’#



登陆boby账户，发现boby的工资变成1

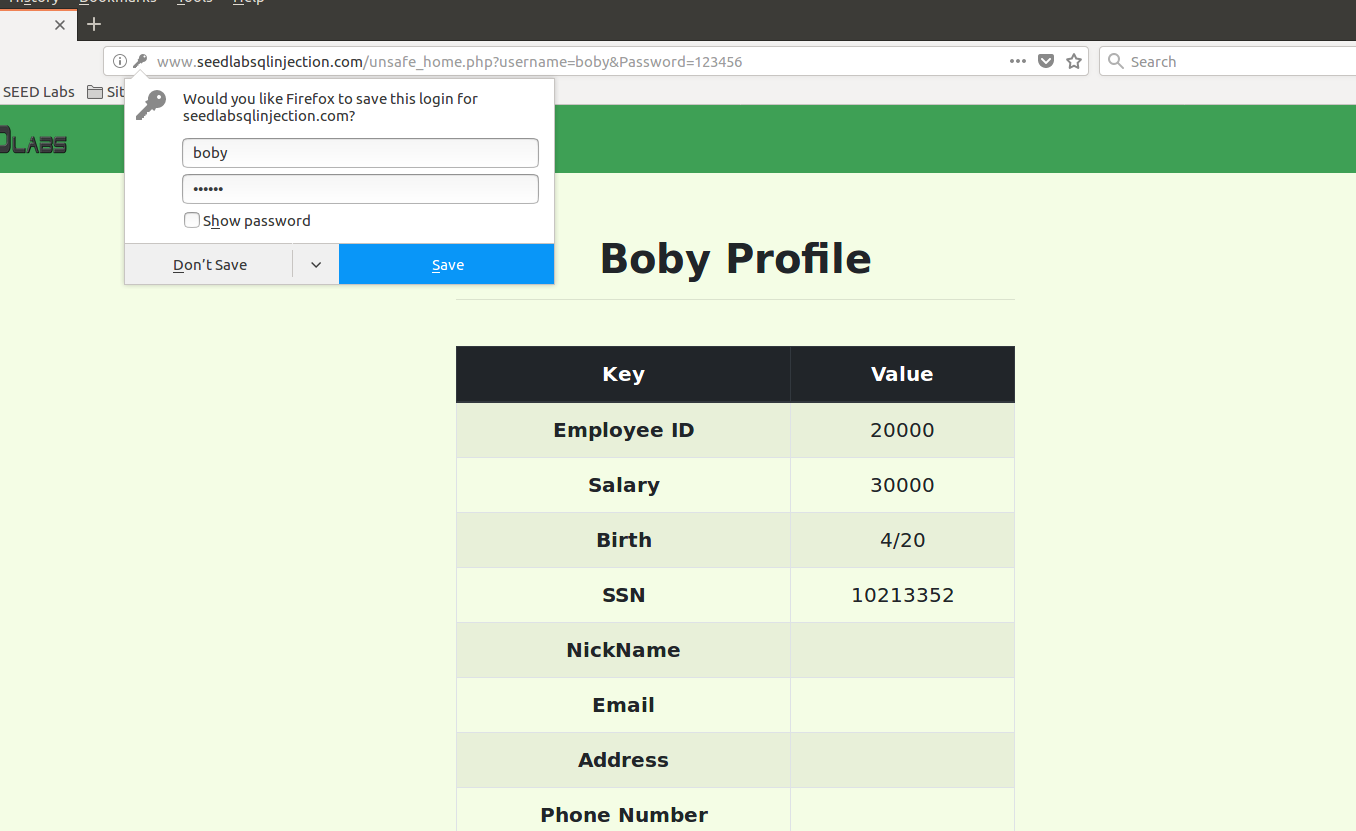


3.3

打算将boby的密码修改为123456，使用sha1加密工具得到123456的hash值为7c4a8d09ca3762af61e59520943dc26494f8941b

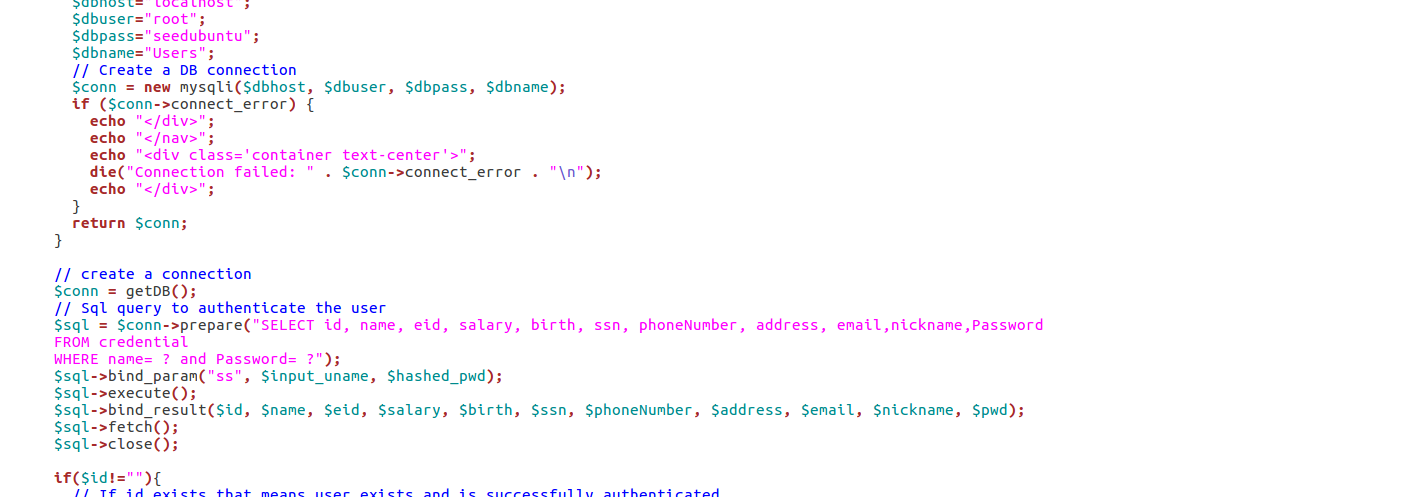
在alice修改资料界面任意栏输入

',password='7c4a8d09ca3762af61e59520943dc26494f8941b'where name='boby'#，再次登陆boby账户，发现登陆密码变为123456

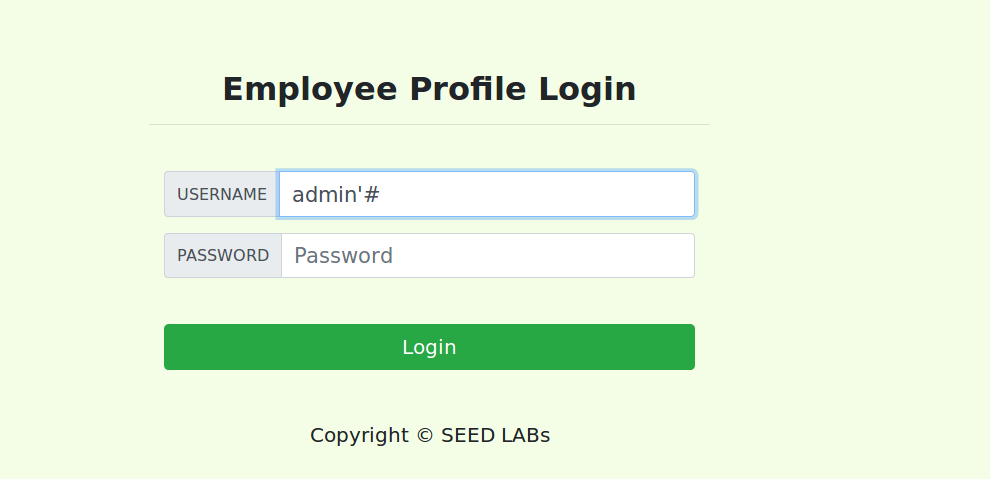


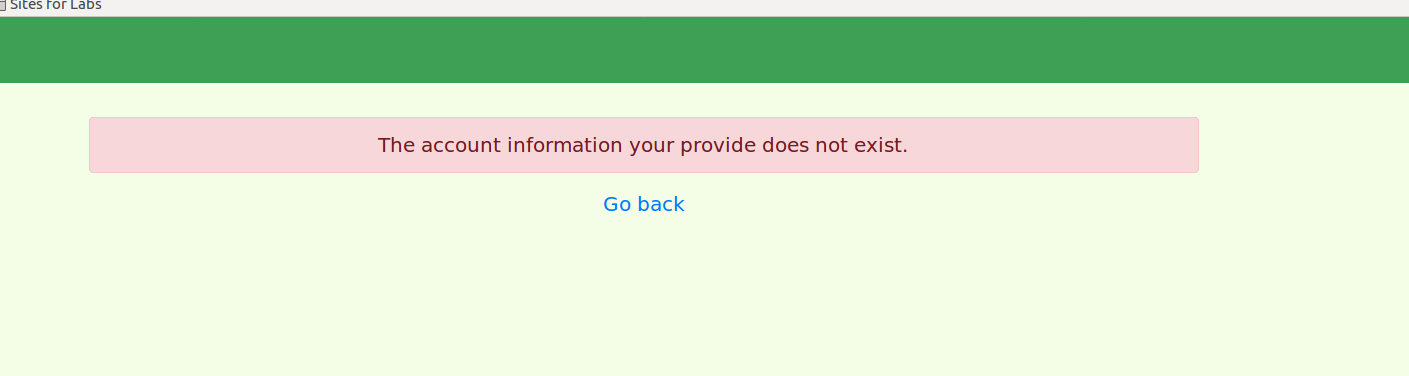
Task4:

修改unsafe\_home.php,修改后代码如图

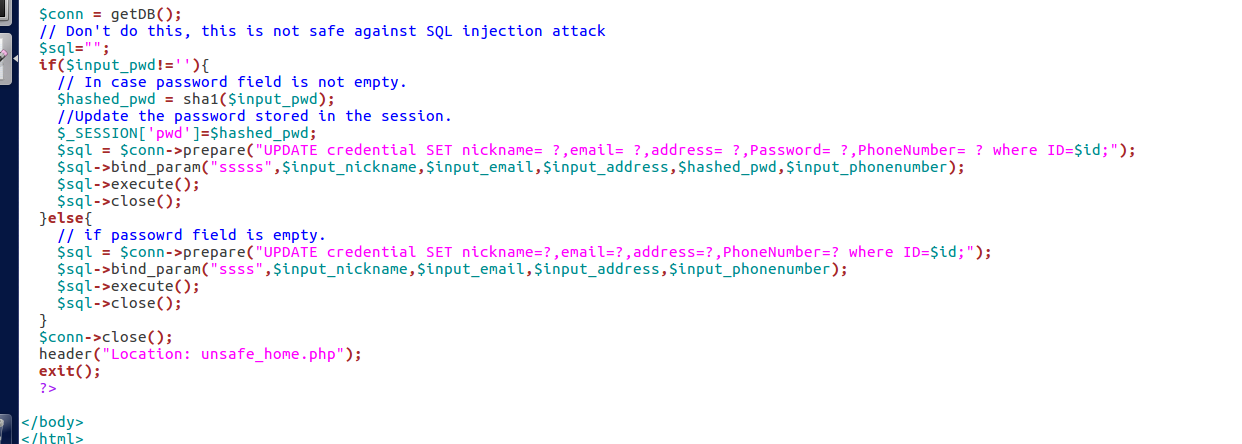


然后使用sql注入攻击登陆账户发现失败





修改unsafe\_edit\_backened.php，修改后代码如图



然后使用sql注入攻击修改他人资料，发现攻击失败

