**跨站点脚本攻击（XSS）**

姓名：钱煜 学号：57118105

1. 实验目的

了解跨站点脚本攻击(XSS)攻击。

二、实验内容

1.熟悉SQL语句；

2.对SELECT语句的SQL注入攻击；

3.对UPDATE语句的SQL注入攻击；

4.对策-拟备声明。

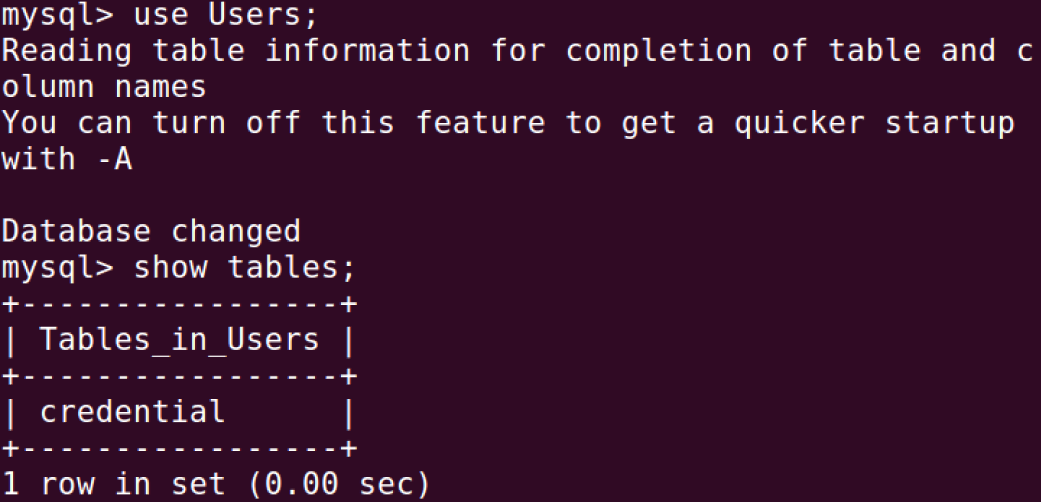
三、实验环境

Virtual Box，Seed Ubuntu 16.04。

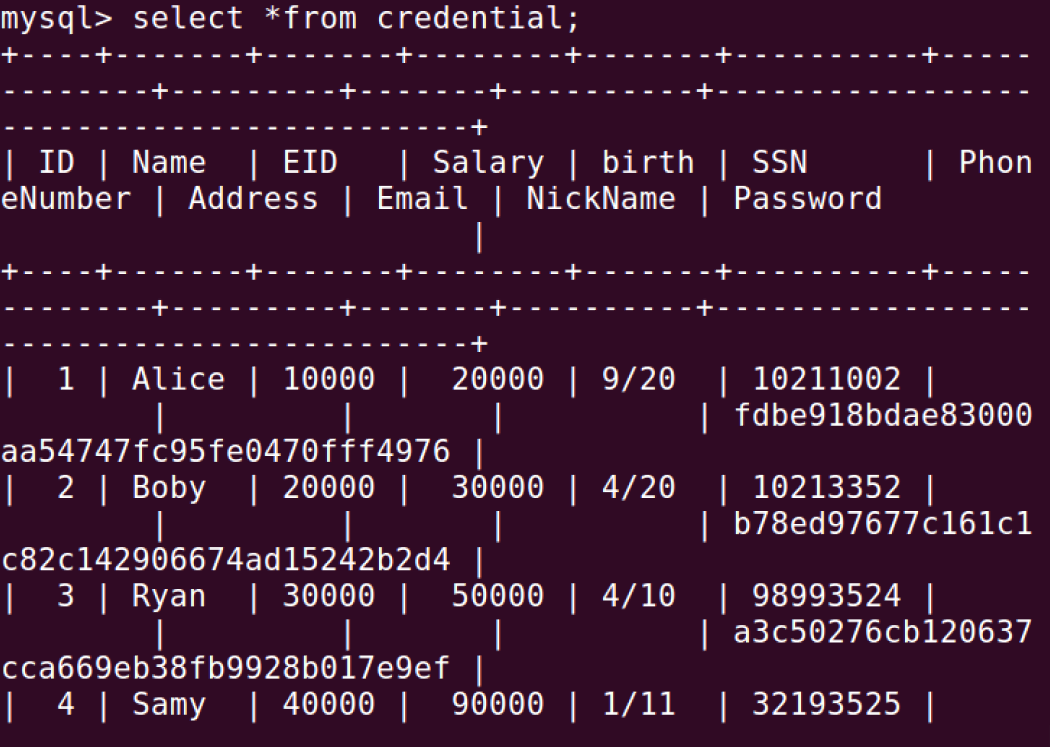
1. 实验

**Task 1.熟悉SQL语句；**

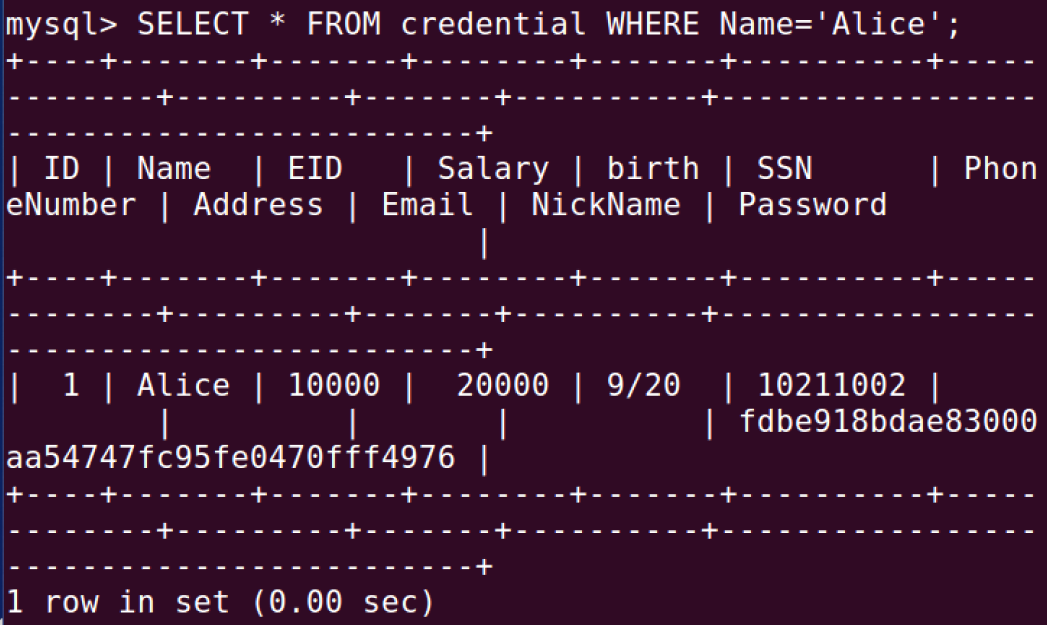
查看SQL表格：



查看credential表格中的内容：

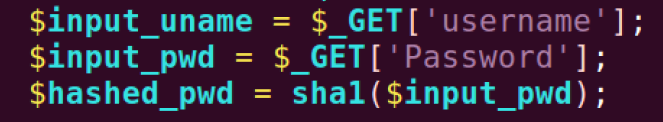


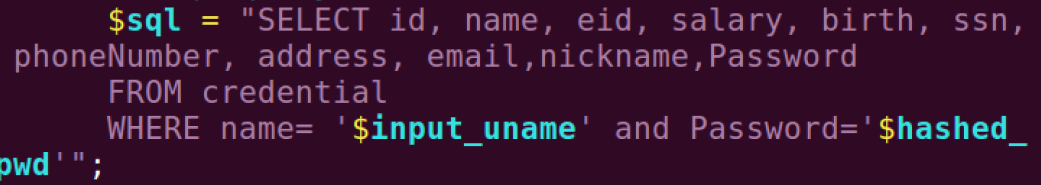
打印Alice的相关信息：



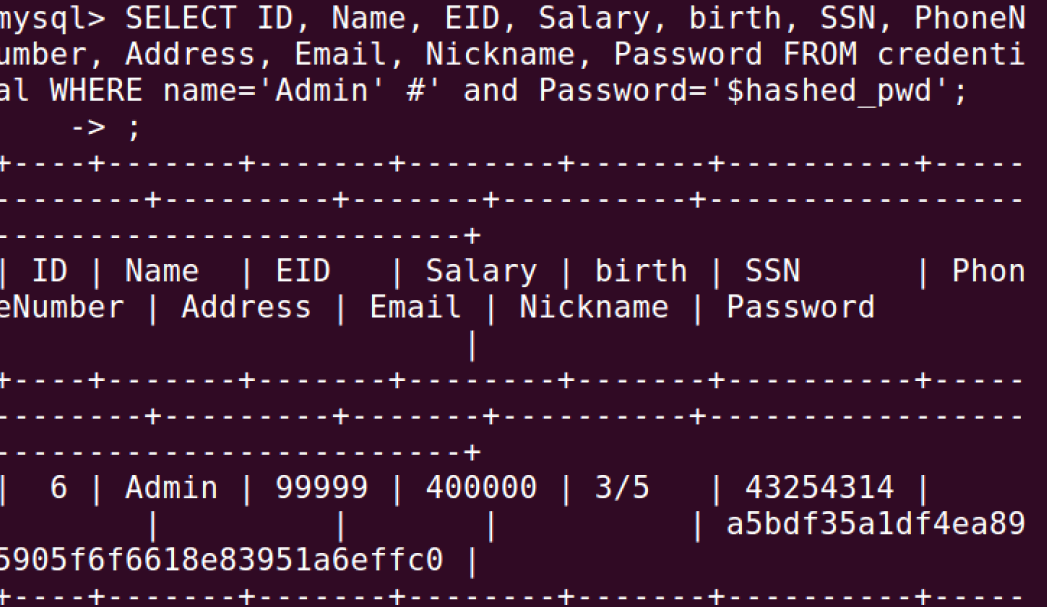
**Task 2.对SELECT语句的SQL注入攻击；**

在unsafe.php文件中找到如图代码：



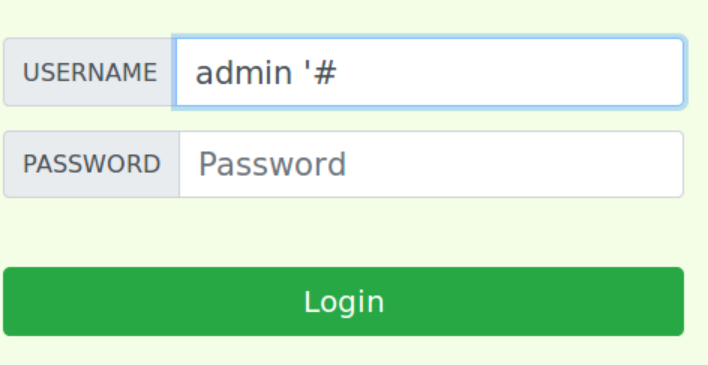


挑选出Admin的相关信息查询：

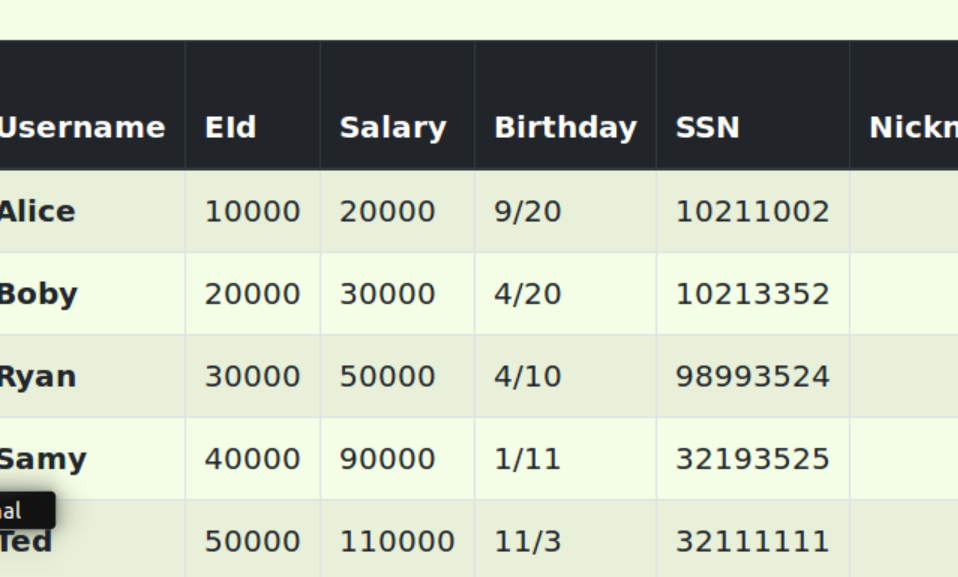


TASK 2.1

注释掉admin，不输入密码直接登陆：

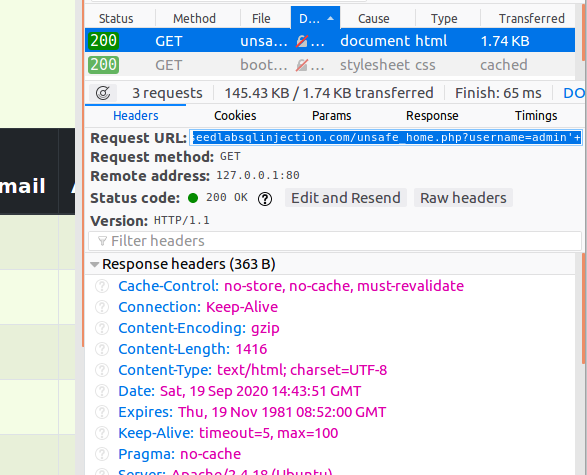


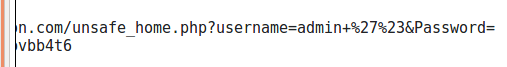
登陆成功：



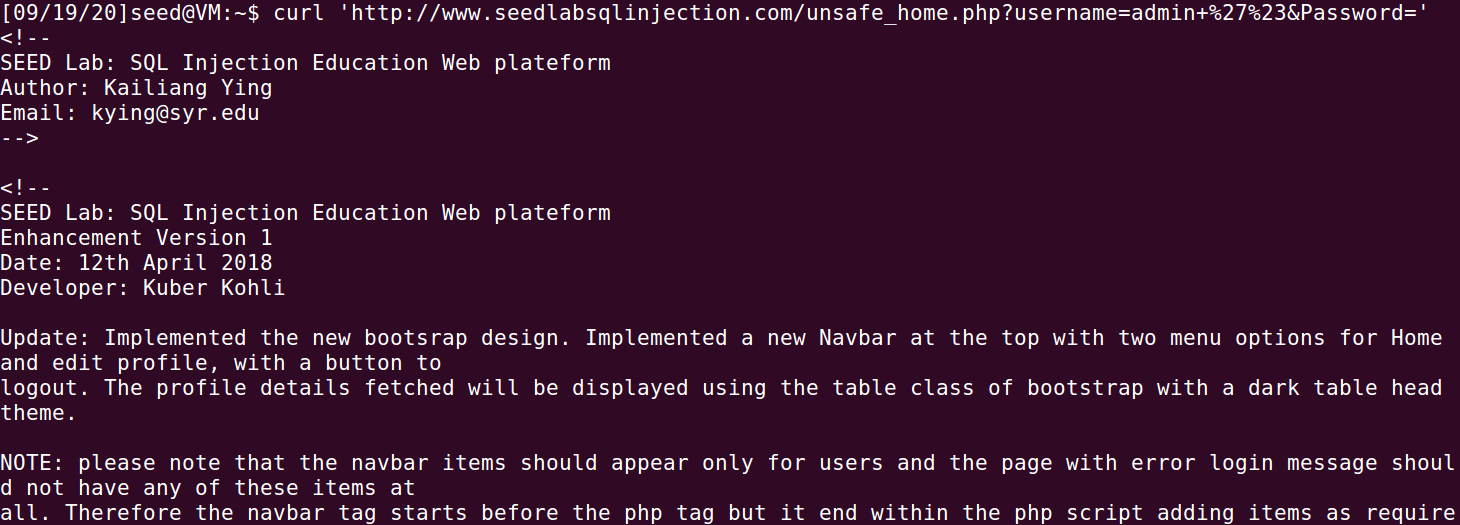
TASK 2.3：

用TASK 2.2的方法登录并捕获Request URL:

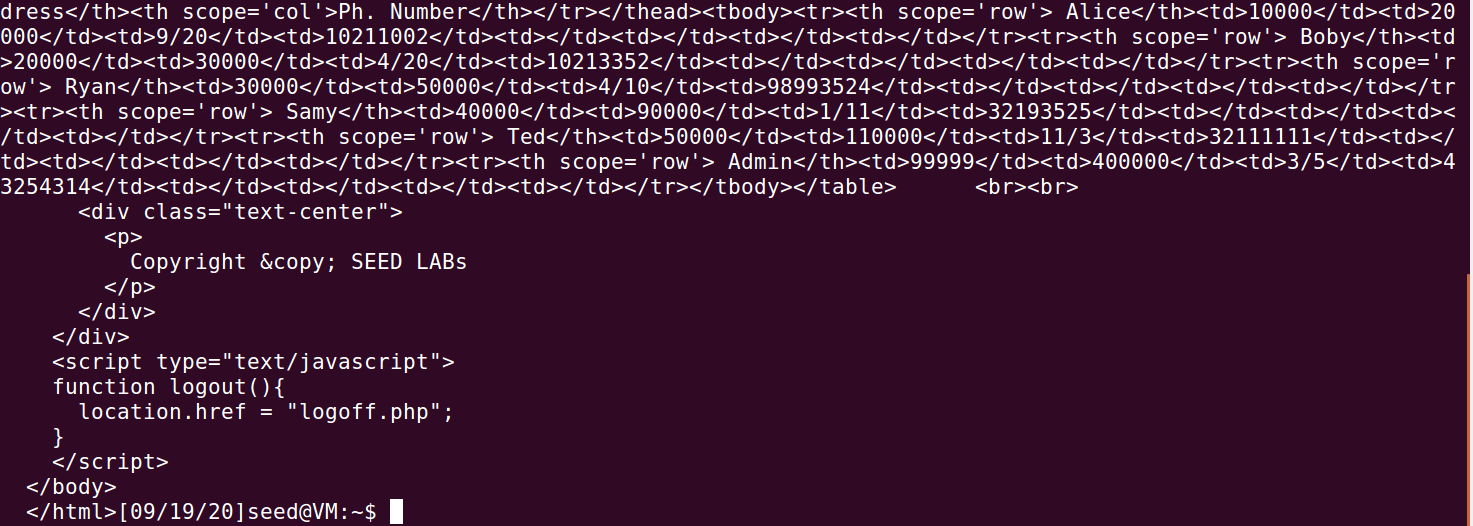




使用curl+语句，获得权限：

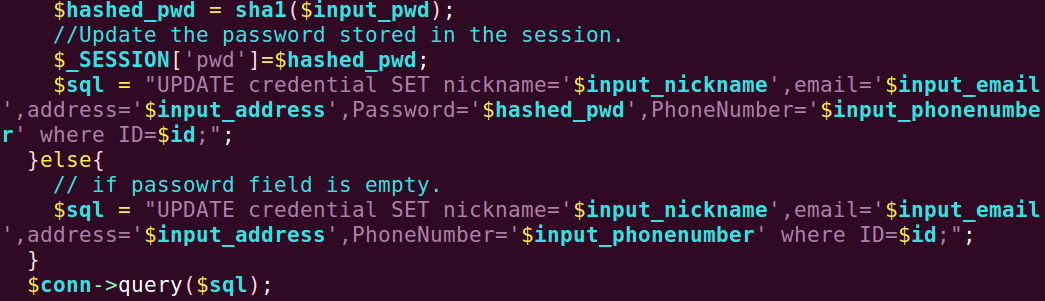




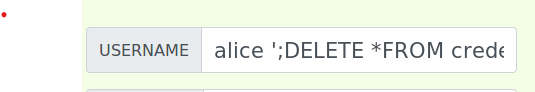


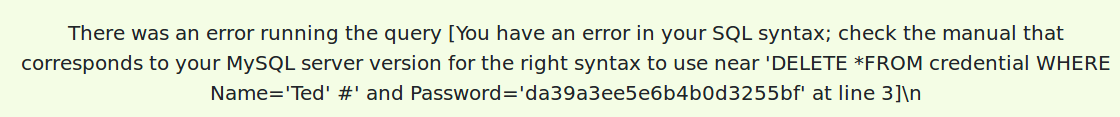
**Task 3.对UPDATE语句的SQL注入攻击；**

查看文件中的内容：



插入两个SQL语句进行尝试：



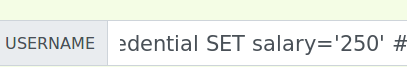


无法在其中插入两个SQL语句并成功执行

则修改unsafe\_home.php文件：



登录界面输入两条语句：



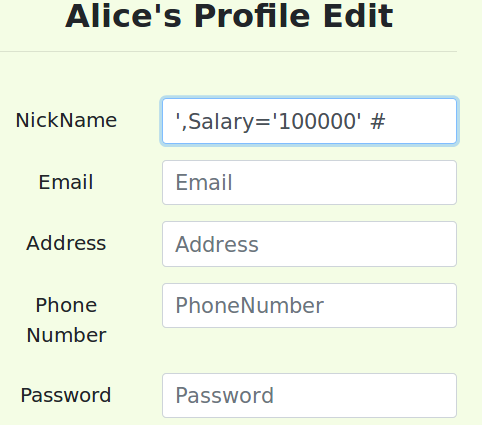
把unsafe\_home.php文件改回原样，登录Alice账号：



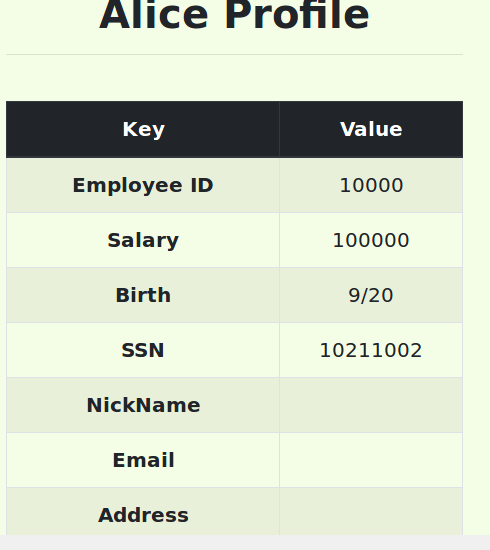
则Salary已被修改。

TASK 3.1

修改Alice账户：

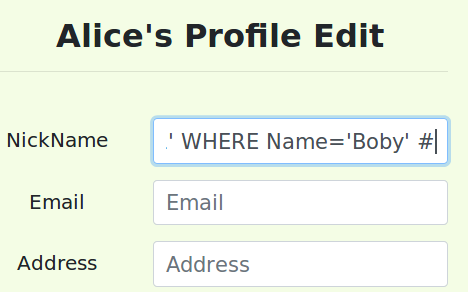


保存后发现已被修改：

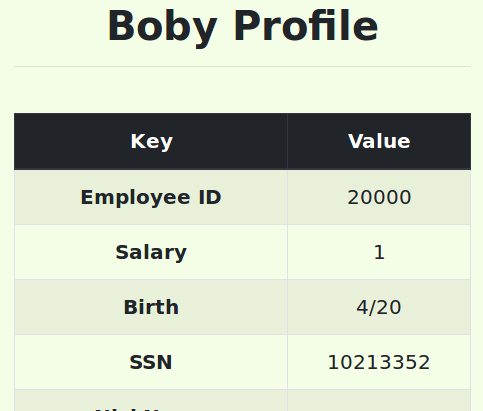


TASK 3.2

再次利用3.1手法修改个人资料：



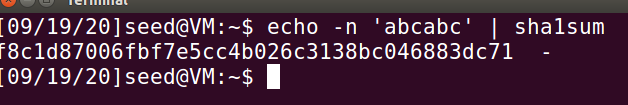
保存后登录Boby的账号：



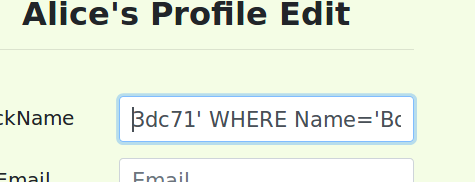
修改成功

TASK 3.3

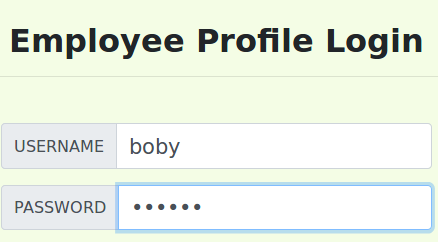
计算加密值：

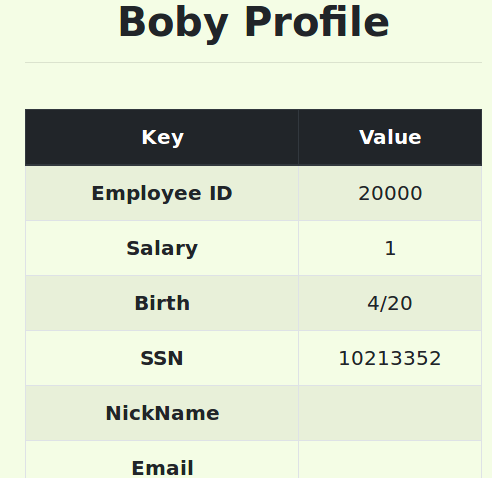


修改Alice的个人资料：



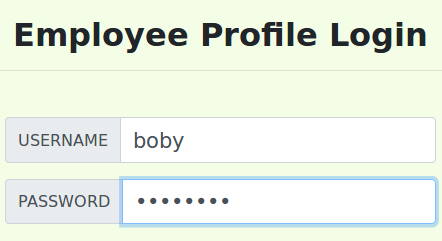
用abcabc登录Boby：



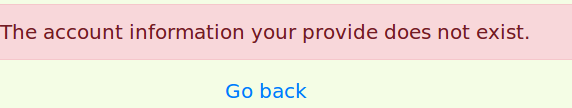


成功登录

如用原密码登录：

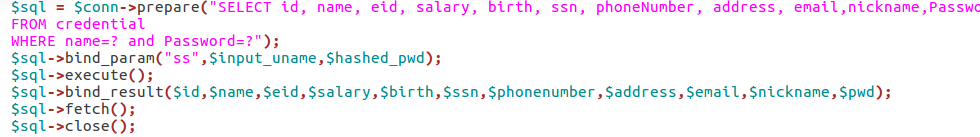


不成功：

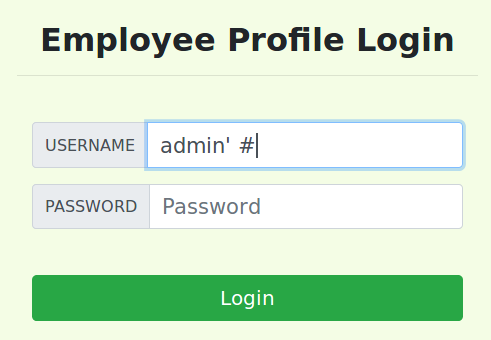


**Task 4.对策-拟备声明**

修改unsafe\_home.php文件：



再次用admin’#登录：



失败：



即SQL攻击注入失败，漏洞修复。