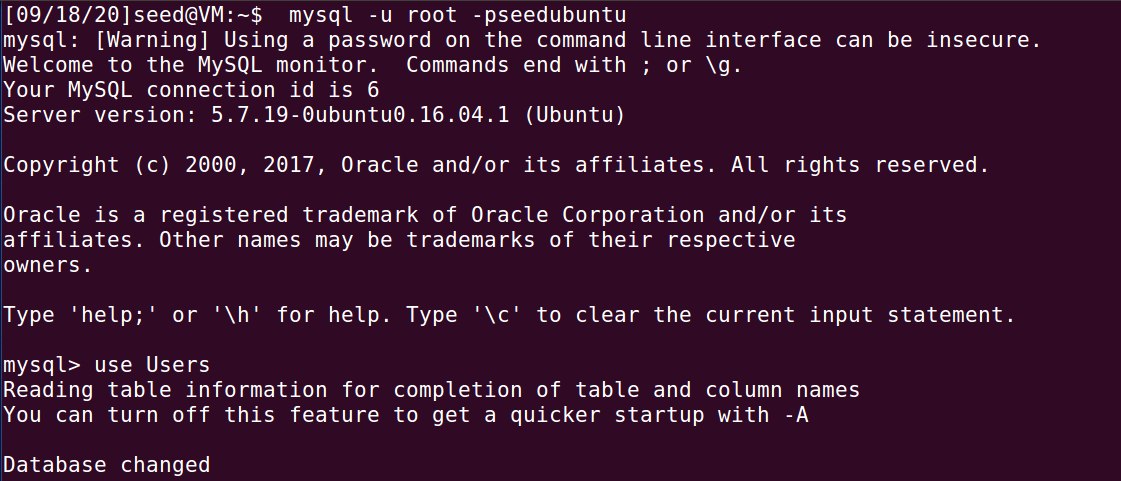
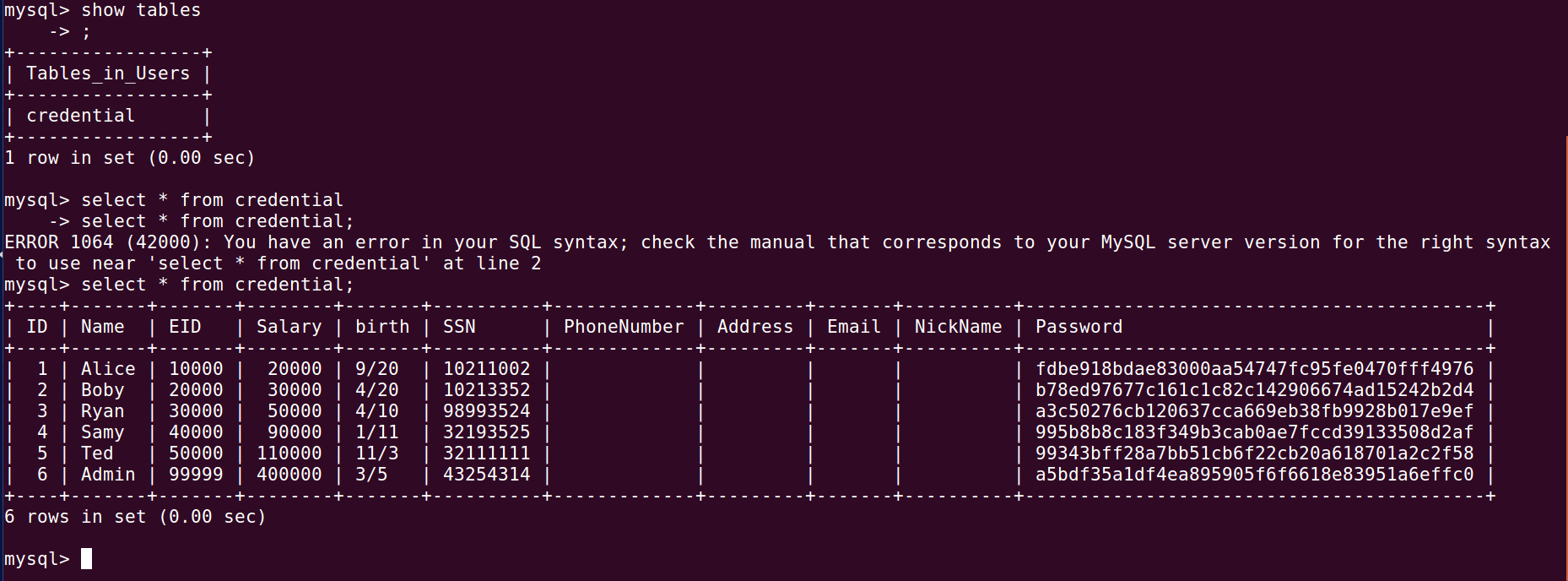
**Lab6-Report**

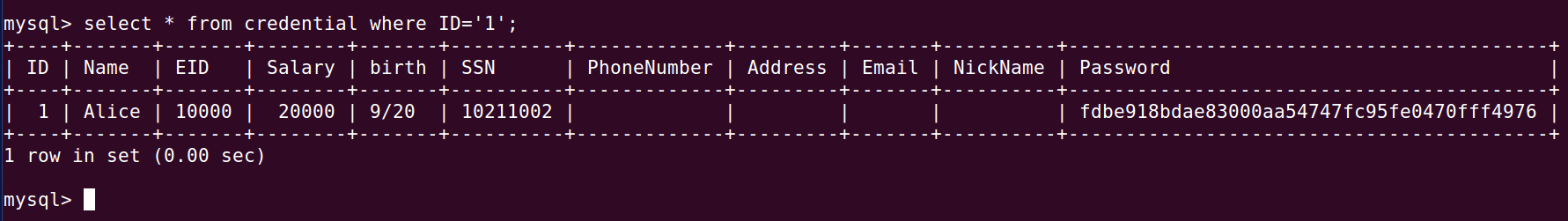
57118103 郭欣然

**Task1:Get Familiar with SQL Statements**

熟悉SQL命令。数据库为Users，包含一个名为credential的表;表存储每位员工的个人资料(如eid、密码、薪资、ssn等)。管理员admin可以查看所有员工的个人资料，但每个员工只能查看自己的信息。使用mysql查询所有员工信息。

命令如下，含义依次为：进入Users数据库；查询Users数据库包含的表；使用SQL语句查询Alice的所有信息



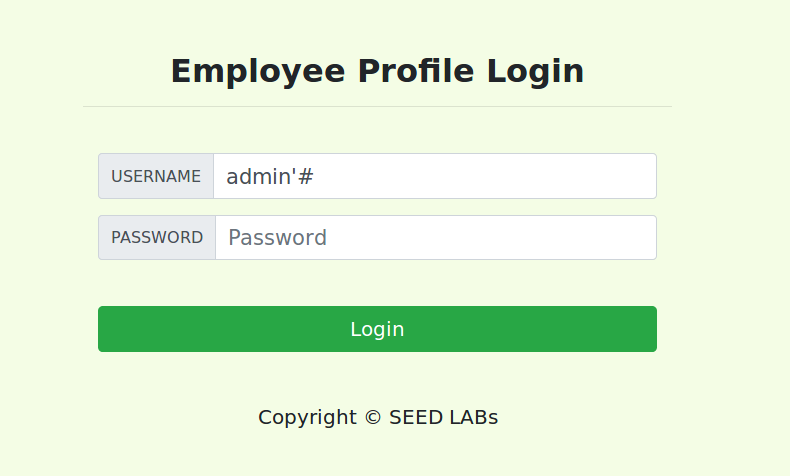


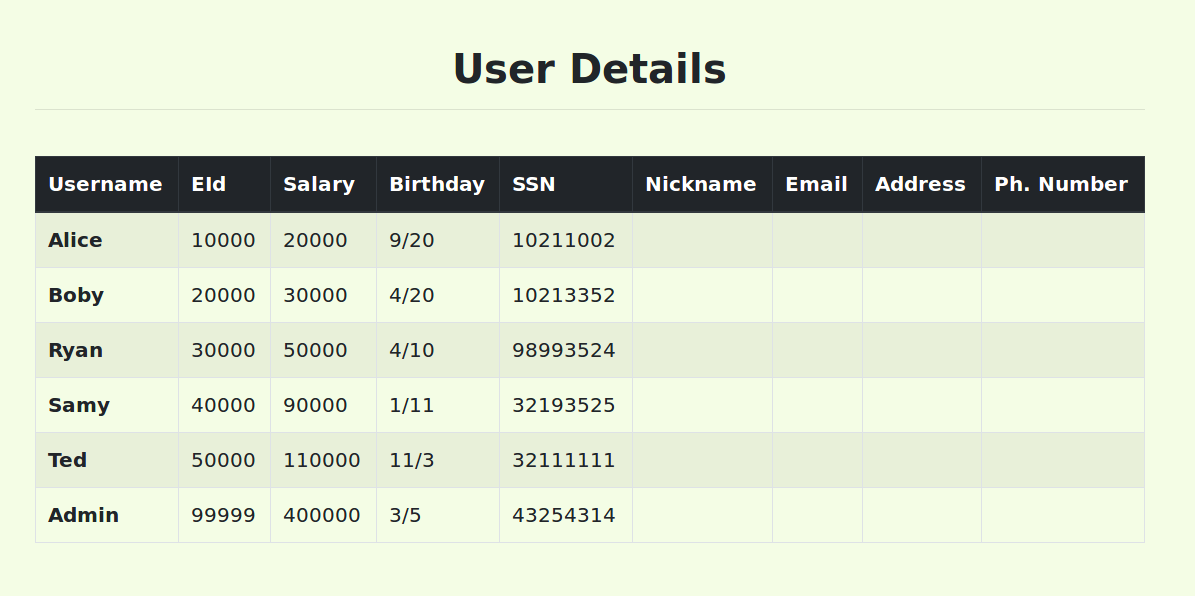
**Task2: SQL Injection Attack on SELECT Statement**

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

假设知道管理员的帐户名为admin，但不知道密码，希望以管理员身份进入系统并查看到所有员工信息。

分析代码,通过sql注入技术，在username中输入admin’#即可成功以admin的身份登入.原因是,第一个单引号会闭合eid=’$input\_eid’,使条件变成了eid=’admin’#,#会把后面的语句都注释掉,所以相当于不用输入密码直接登入admin

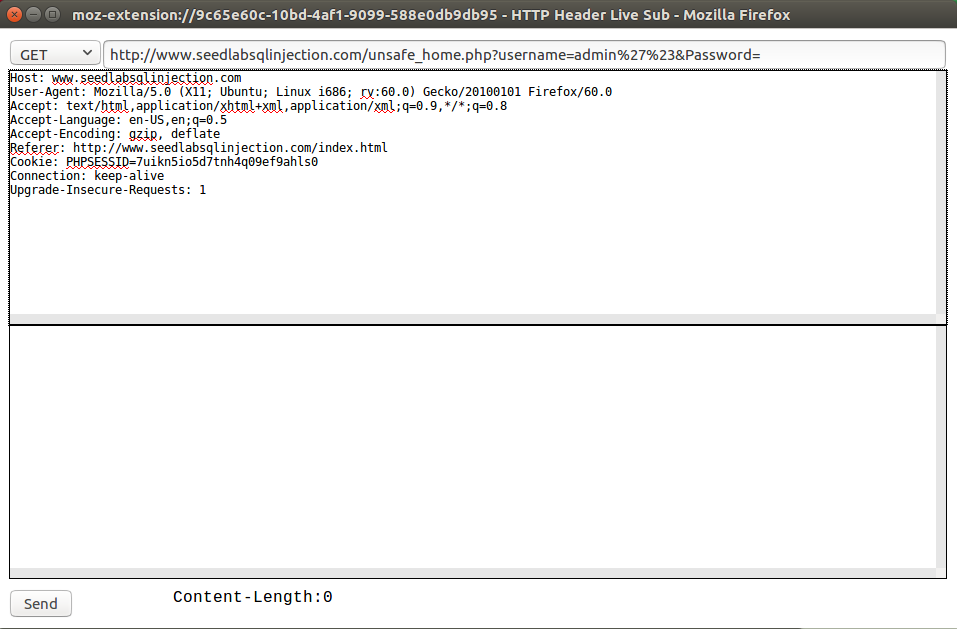




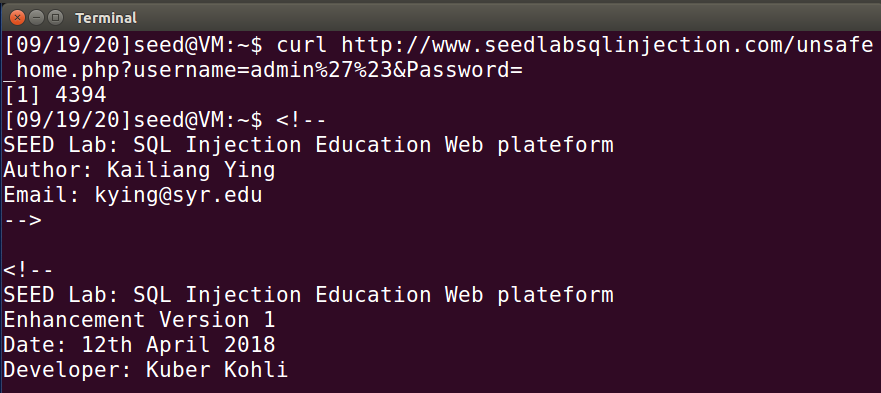
**Task 2.2: SQL Injection Attack from command line**

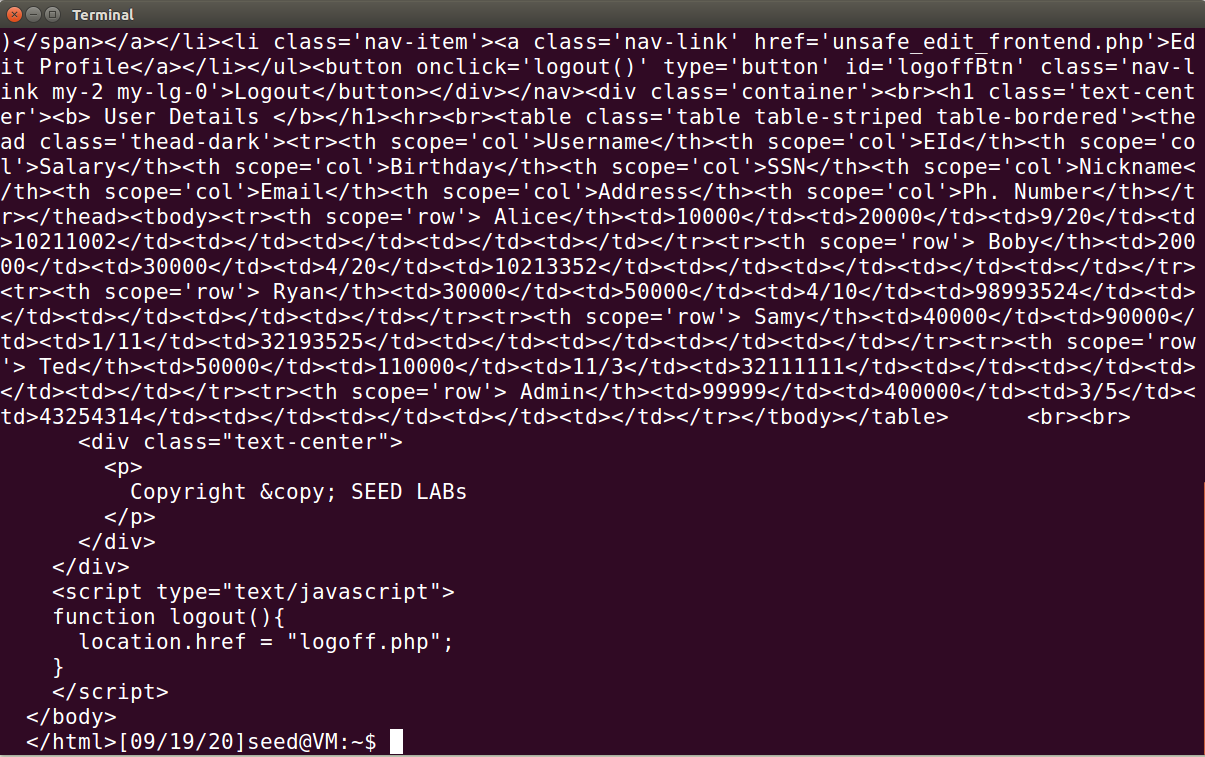
与上一任务类似，将网页进行sql注入变成从命令行登录页面，查看所有员工的信息。同样只知道管理员的帐户名，即admin，但不知道密码。

使用curl命令,为了得到命令格式，在网页下进行sql注入并用live工具抓包，下图为抓到的登录请求http报文，从url中可以看到符号‘改为%27，符号#改为%23

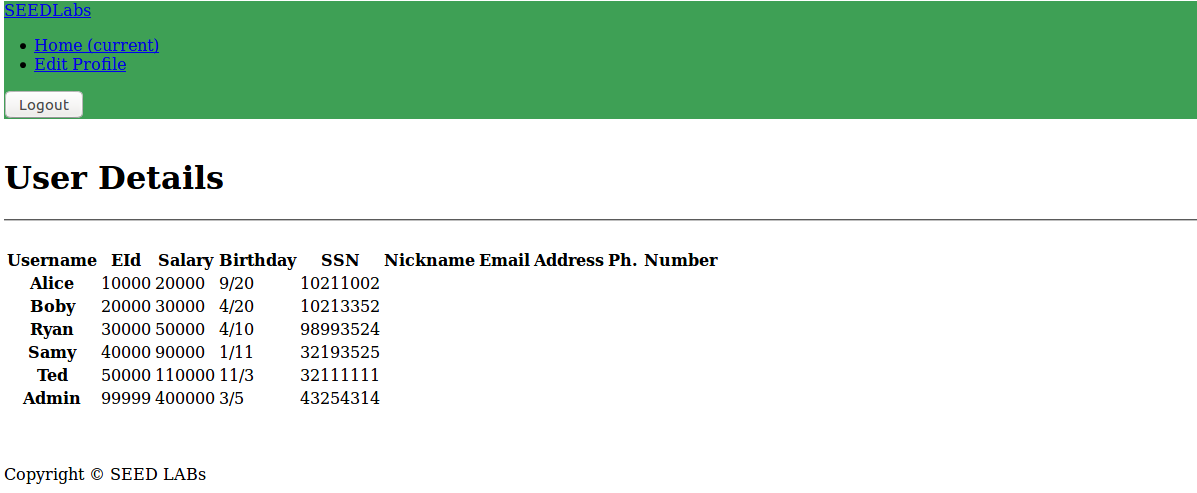


仿照上述请求格式进行sql注入，结果如下，可以看到在终端中以网页源代码形式显示了所有员工的信息





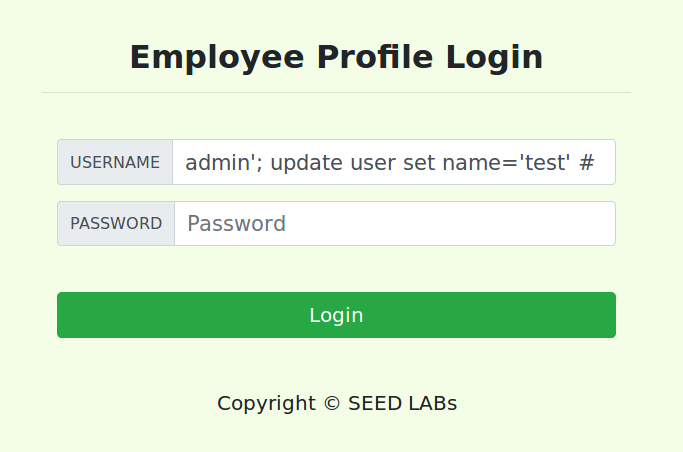
将代码复制到一个html文件中并使用浏览器打开，得到网页版数据：



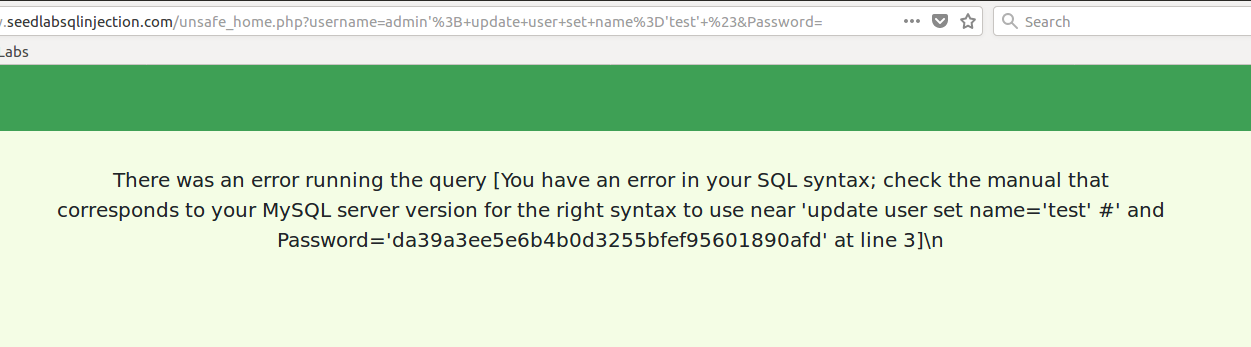
**Task 2.3: Append a new SQL statement**

上面的任务只是查看数据库中的信息，我们希望可以通过类似方法修改数据库信息。方法是使用sql注入攻击将一条sql语句转换为两条sql语句,第二个是用update或delete语句。在sql中，分号用于分隔两个sql语句。请描述如何使用登录页面让服务器运行两条sql语句。尝试从数据库中删除一条记录，并描述观察结果。

根据以上要求，我们注入语句admin'; update user set name='test' #



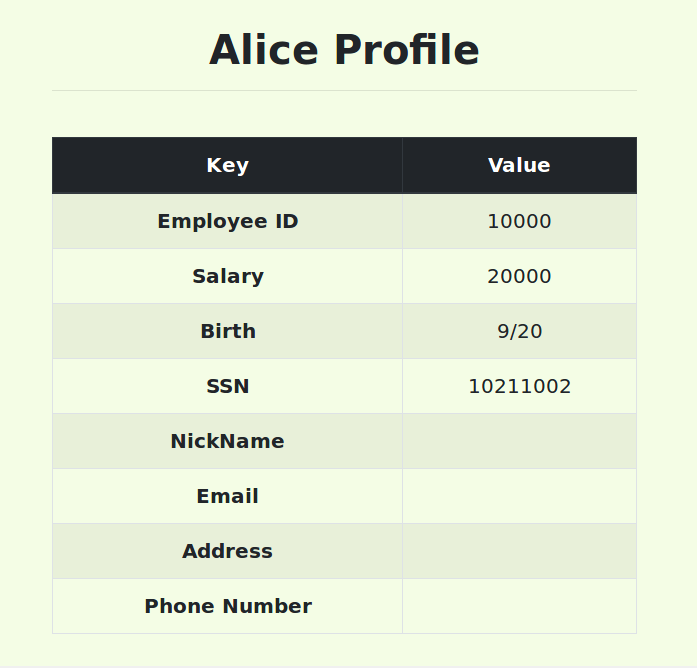
发现出现以下错误提示，这是因为在MySQL中有一种特殊的保护机制，mysq\_query不允许提交多个请求，导致两个用分号隔开的连续请求就会报错。



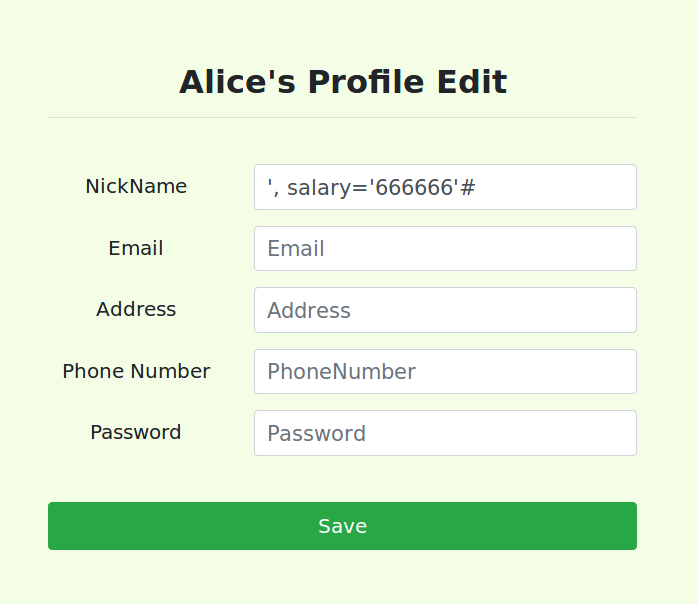
**Task3：SQL Injection Attackon UPDATE Statement**

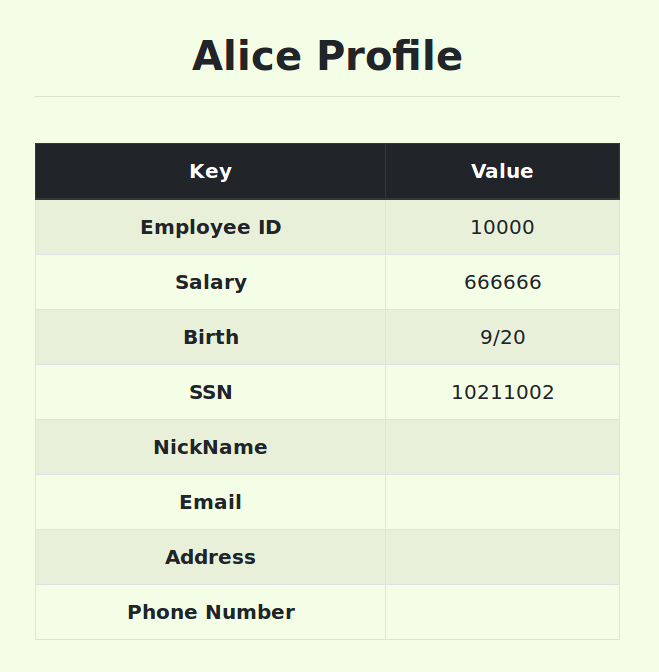
**Task 3.1: Modify your own salary**

Alice想修改自己的工资使工资多一些，进入账号查看初始工资为20000



进入edit profile界面，与上述任务原理类似，运用sql注入手段，通过分析代码,在nickname输入框中输入语句', salary='666666'#即可修改工资为666666

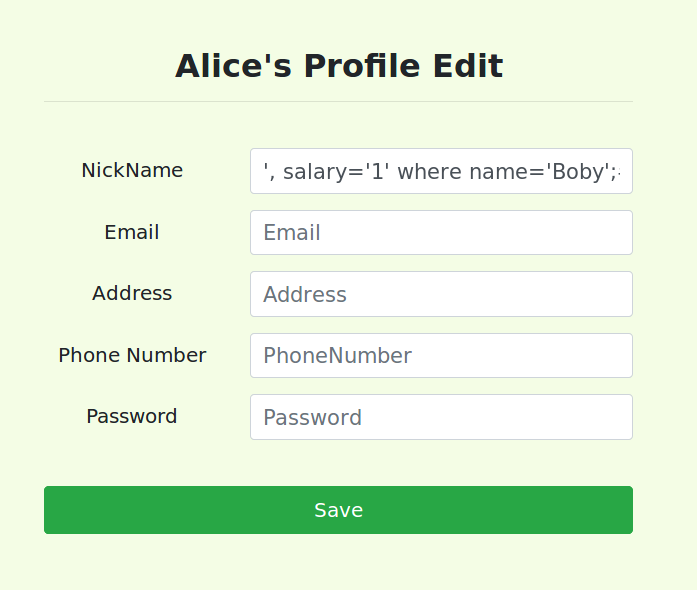




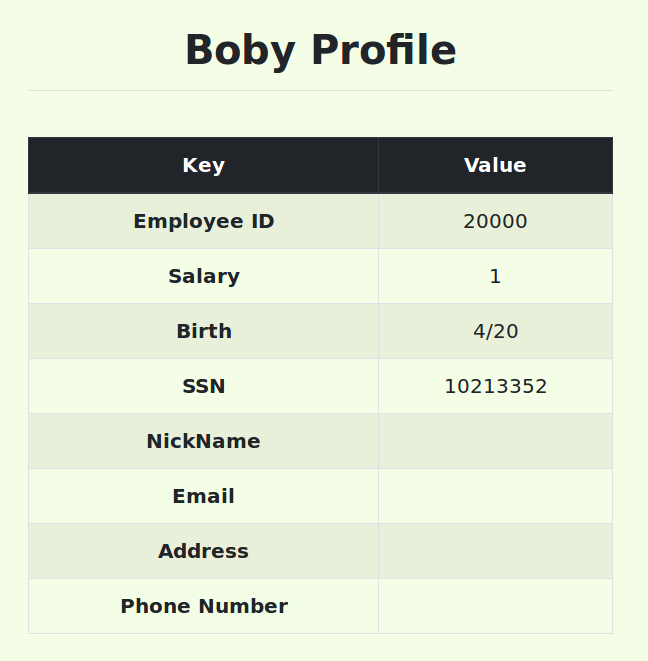
**Task3.2: Modify other people’ salary.**

Alice想修改Boby工资为1 dollar，WHERE 子句用于提取那些满足指定条件的记录。

这里alice修改别人的工资，因此需要加上where语句指定name=boby

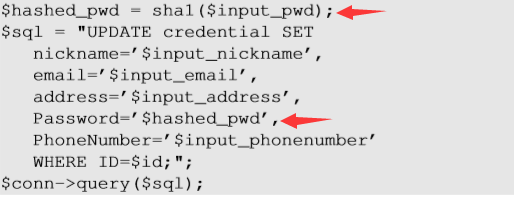


登录boby账户查看发现工资已经被修改为1 dollar

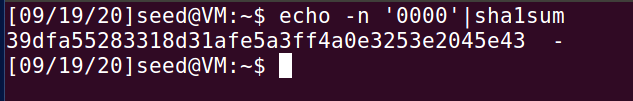


**Task 3.3: Modify other people’ password**

Alice想修改boby的密码，根据代码我们可以知道，密码是以hash格式来存储的

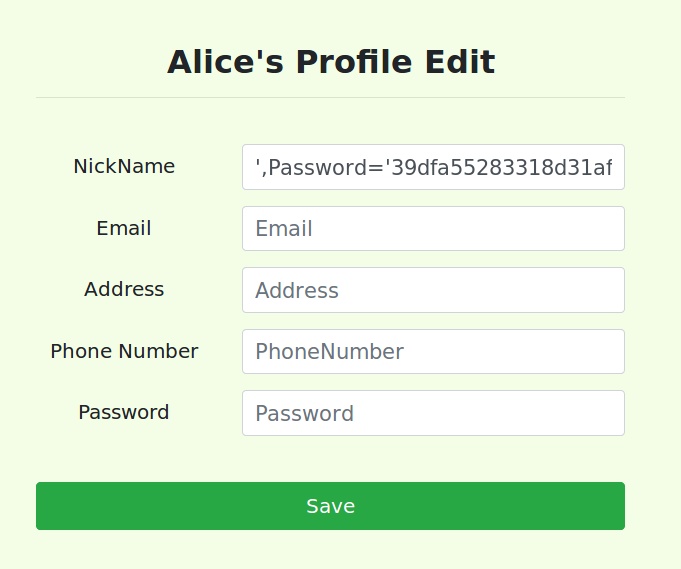


因此首先通过命令得到密码的hash值，这里希望修改boby密码为0000

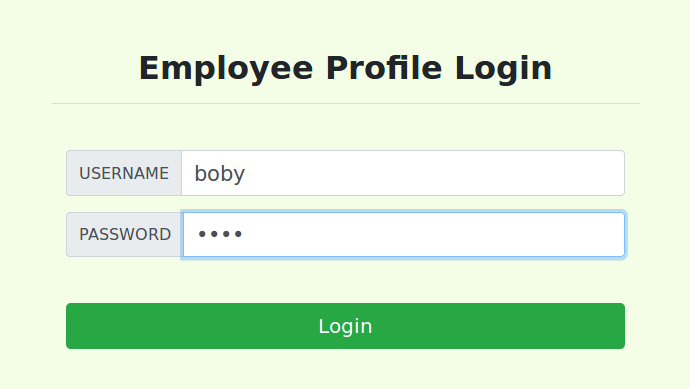


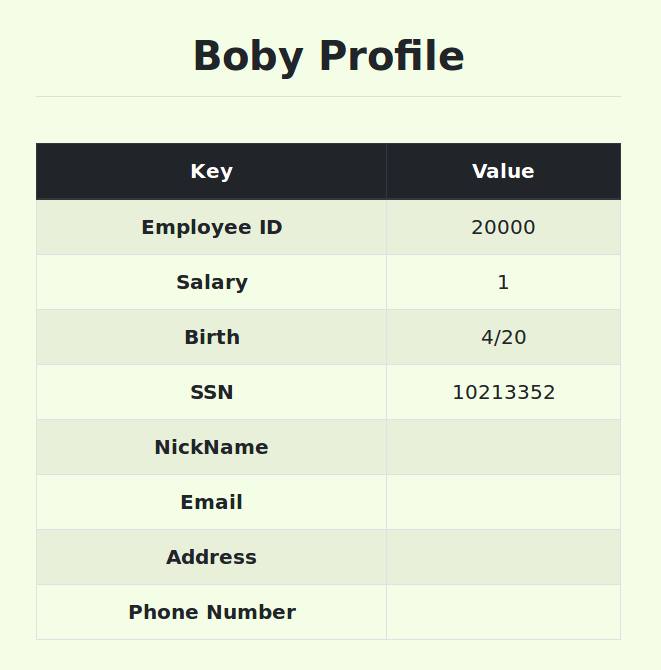
在alice的profile中进行sql注入修改boby密码为0000

',Password='39dfa55283318d31afe5a3ff4a0e3253e2045e43' where Name='Boby'#



登录boby账号，密码输入0000，发现登录成功

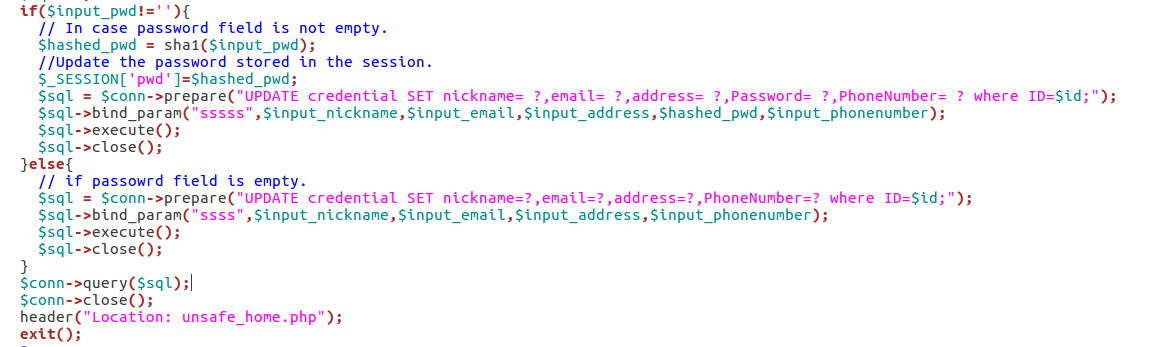




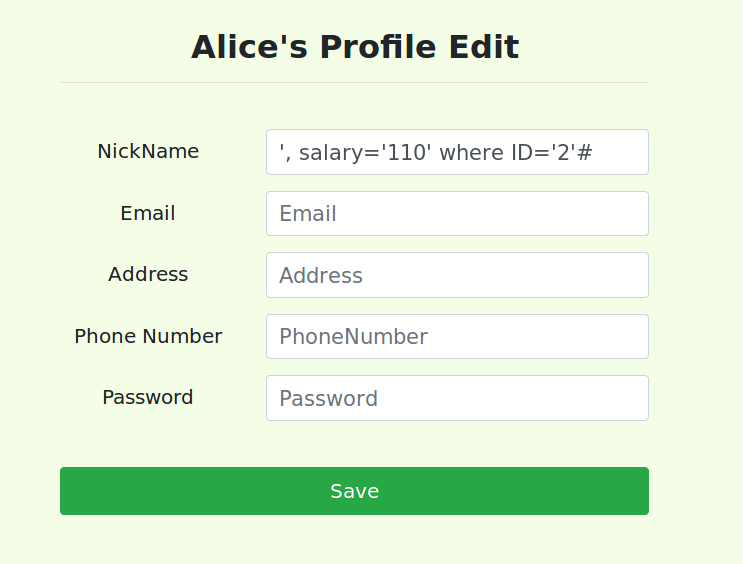
**Task4: Countermeasure—Prepared Statement**

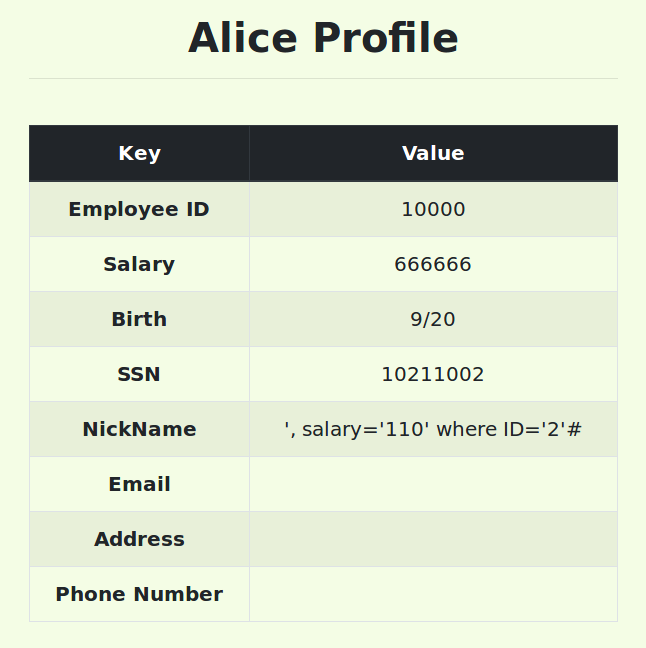
修改网页php文件，使sql注入无法成功

更改Unsafe\_edit\_backend.php代码：

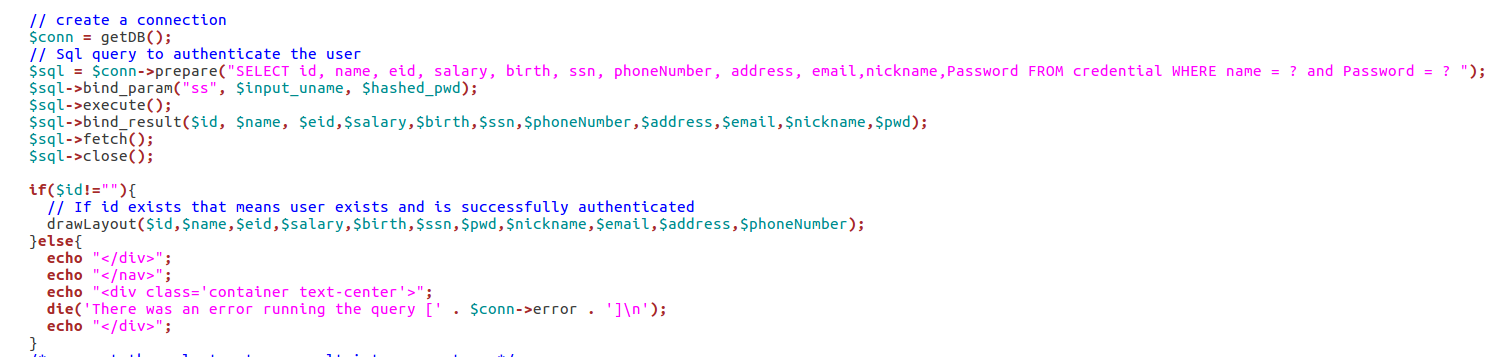


攻击修改个人信息发现sql命令被识别为数据，攻击失败。

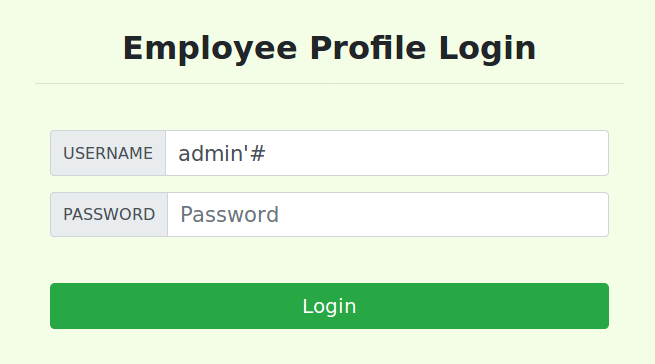


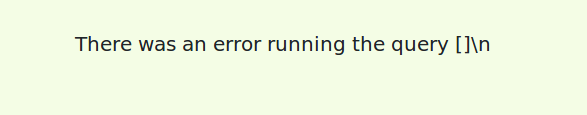


更改Unsafe\_home.php代码如下：



尝试使用sql注入手段登录admin，发现攻击失败





而正常输入用户名密码可以登录成功

