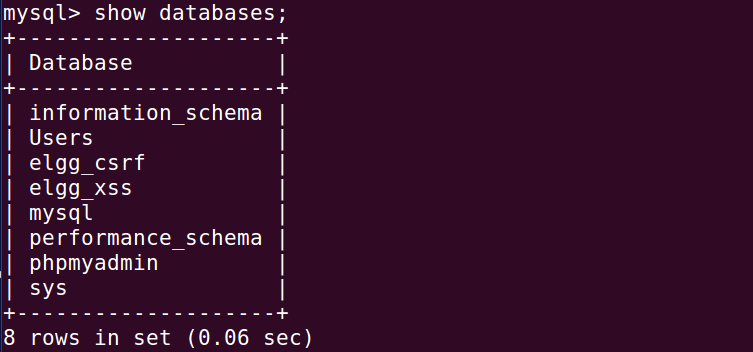
Lab 6

学号：57118104 姓名：郭雅琪

Task1: Get Familiar with SQL Statements

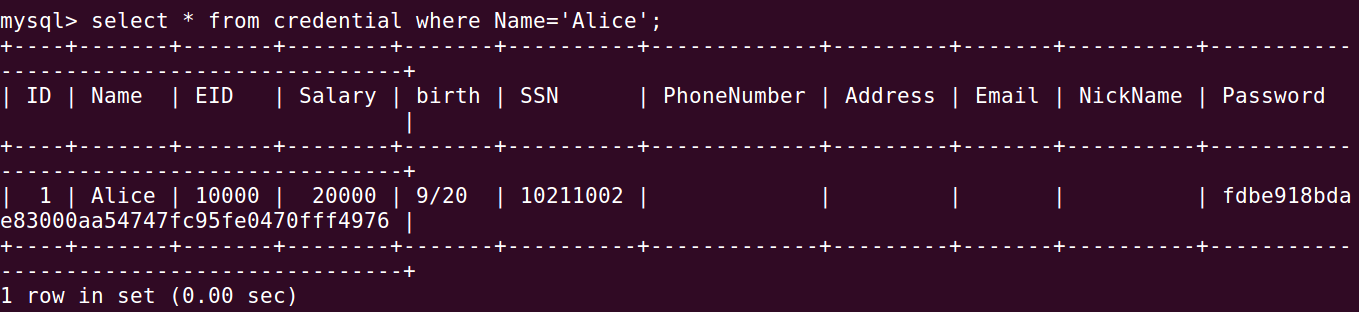
在终端中输入命令 mysql –u root –pseedubutu，进入mysql，使用show databases语句看到所有的数据库。



输入use Users语句，进入Users数据库。使用show tables语句，看到Users中的所有表格。



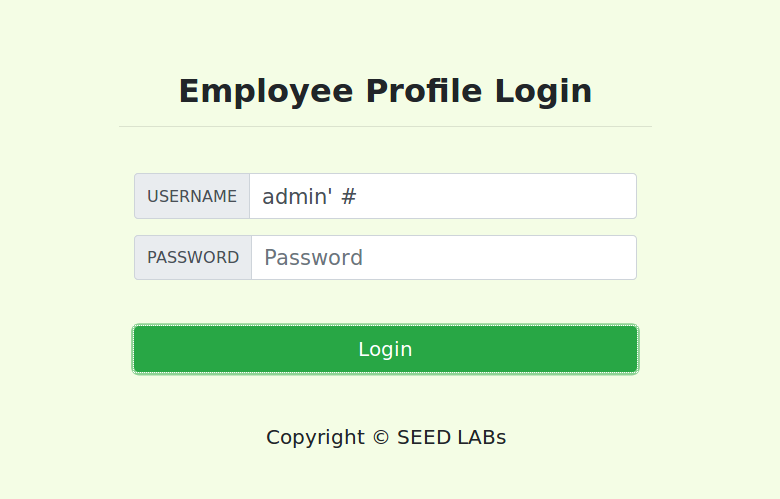
使用语句select \* from credential where Name=’Alice’;找到所有关于alice的信息。



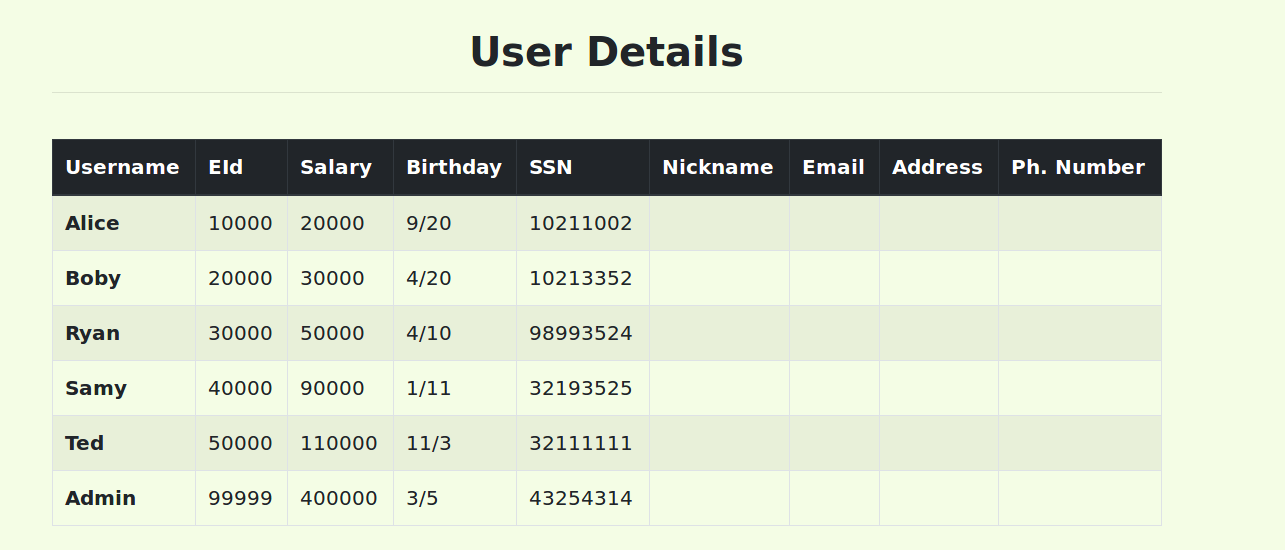
Task 2：SQL Injection Attack on SELECT Statement

Task2.1: SQL Injection Attack on from webpage

在登录用户名的框中输入如下语句：



成功注入，不使用密码进入admin用户。



Task2.2: SQL Injection Attack from command line

在终端中输入 curl ’www.SeedLabSQLInjection.com/unsafe\_home.php?username=admin%27%20%23&Password=111’，其中%27，%20，%23分别是引号，空格，井号的url编码。输入后得到如下结果，成功注入。



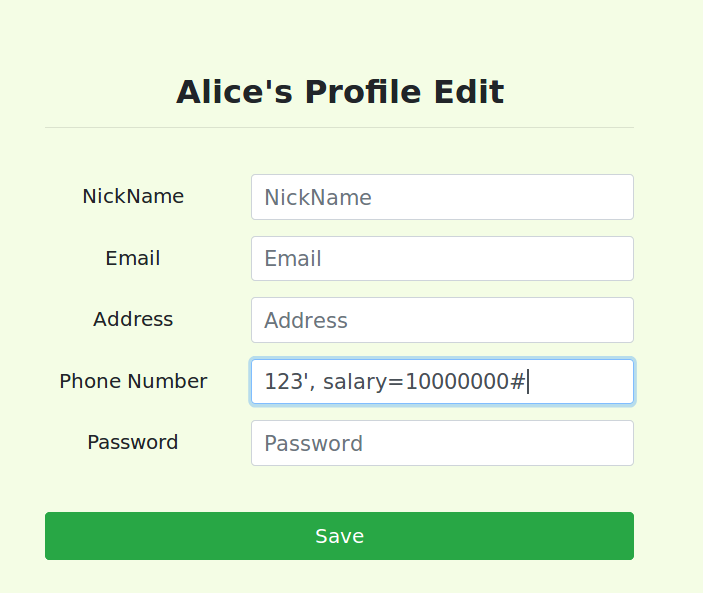
Task2.3: Append a new SQL statement

在网站的输入框中使用union以及堆叠注入都无法成功注入，前者原因是union语句只支持select语句，后者原因是php的mysqli query函数不支持多语句。

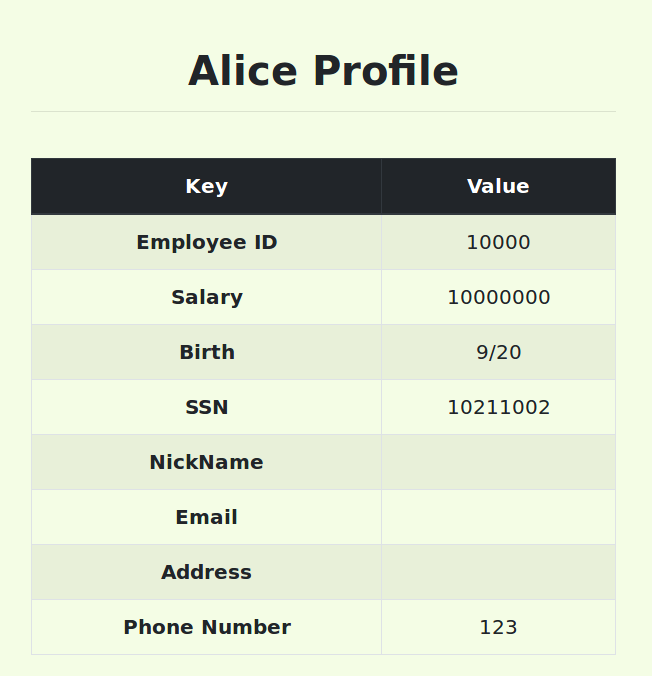
Task 3: SQL Injection Attack on UPDATE Statement

Task3.1: Modify your own salary

登录Alice的账户，进入edit profile页面，在Phone Number中输入如下命令：



保存之后，回到Alice的主页，发现工资被成功修改。

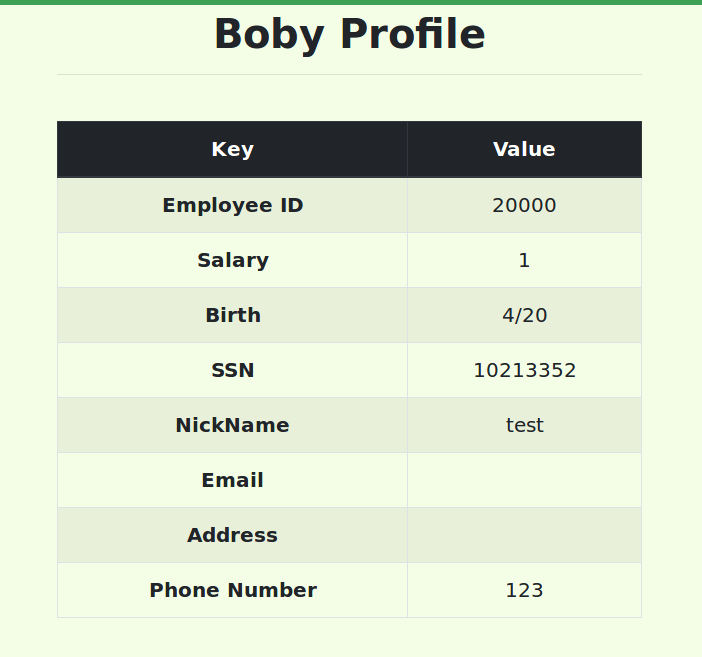


Task3.2: Modify other people’s salary

利用mysql查看boby的具体信息：

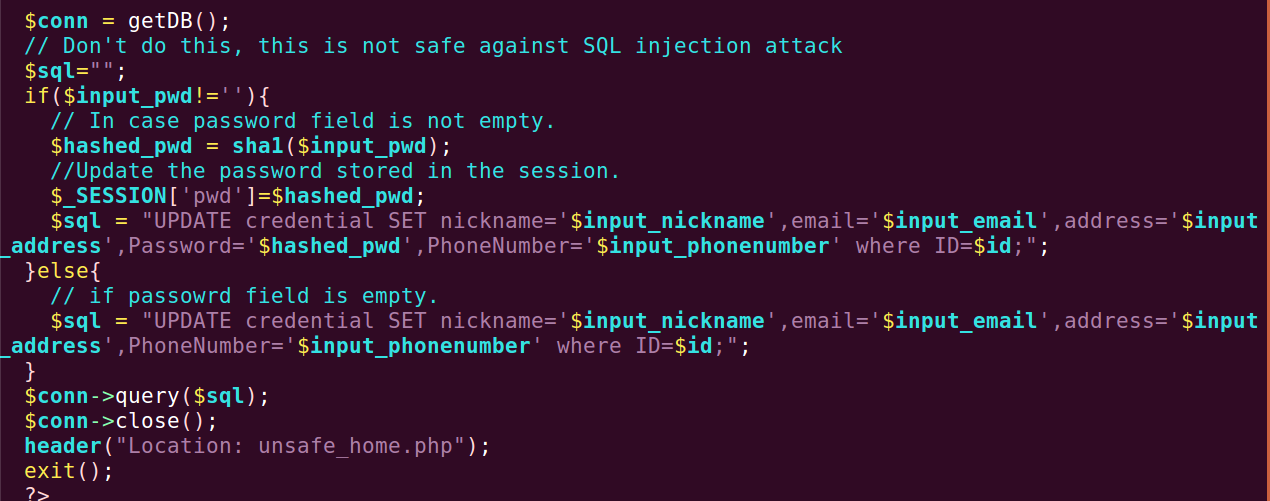


这里利用Boby的eid进行注入。在Alice的Nickname栏中输入test', salary=1, where eid=20000;#。保存之后，登录admin账户，发现修改Boby的工资成功。



Task3.3: Modify other people’s password

这里需要提前查看一下网页的源码，具体内容如下：



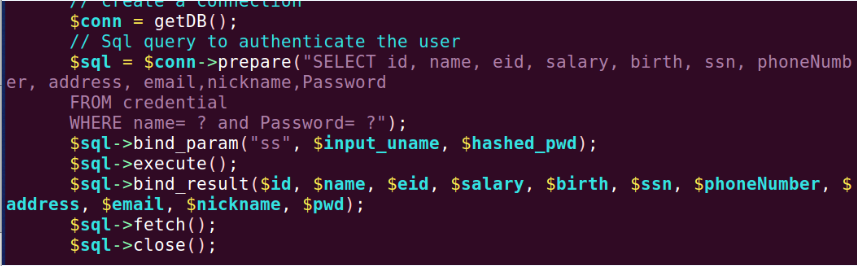
这里后台程序会先检测password是否为空。如果是空的话，会直接更新除了password之外的内容。如果不为空，就将password中的值转为SHA1码之后，和其他信息一起更新。因此这里注入的方法如下：

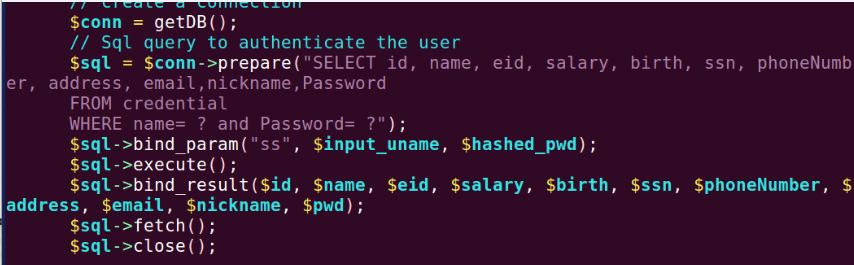
在Alice的email栏中输入p', Password='40bd001563085fc35165329ea1ff5c5ecbdbbeef' where id=2;#（这里的SHA1码代表123），同时也需要在password栏中输入一串密码。但由于email先于password更新，这一段password会被#号注释掉，因此不会起作用。点击保存之后，利用账号密码登录Boby账户，查看mysql中的内容，均发现修改成功。

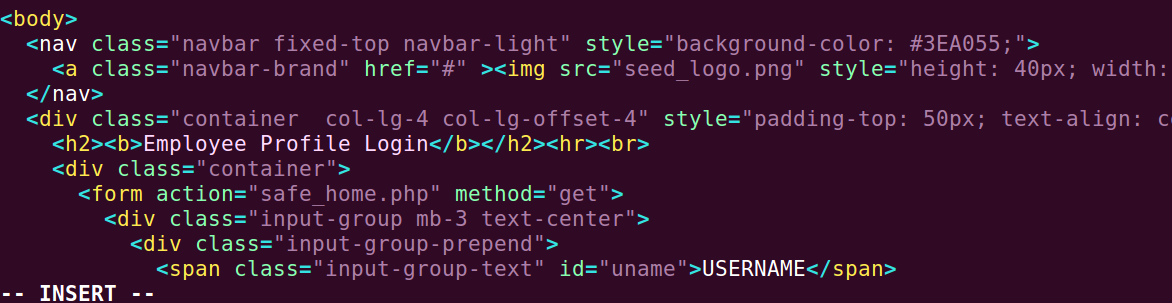


Task 4: Coutermeasure--Prepared Statement

按照实验手册给出的方法修改unsafe\_home.php以及unsafe\_edit\_backend.修改如下：

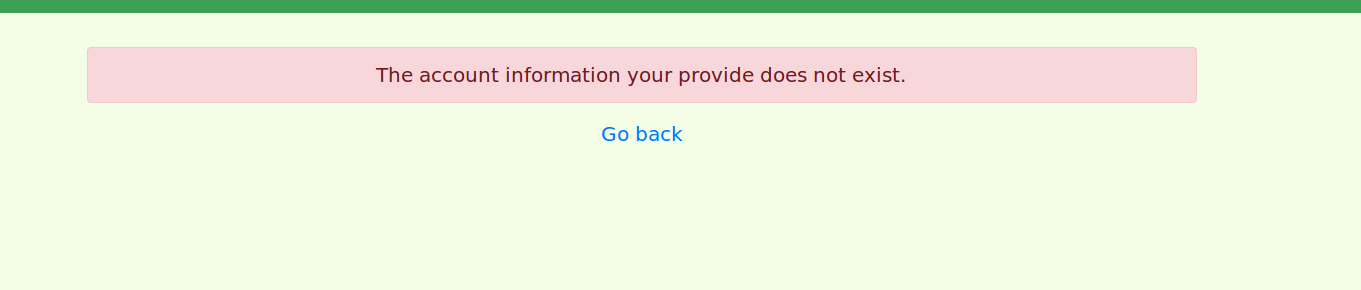


同时修改index.php，以及unsafe\_edit\_frontend.php中的form表单信息，使得页面能跳转到新编写的页面上。





最后进行注入测试，在登录页面尝试登录admin账户发现不成功。



在edit profile页面中修改Alice的工资也不成功。

