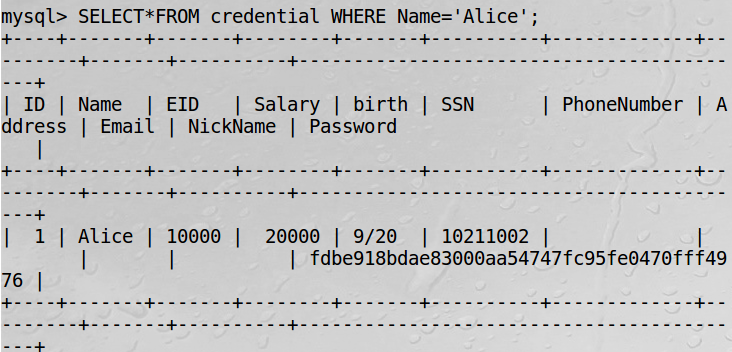
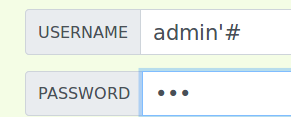
任务一：

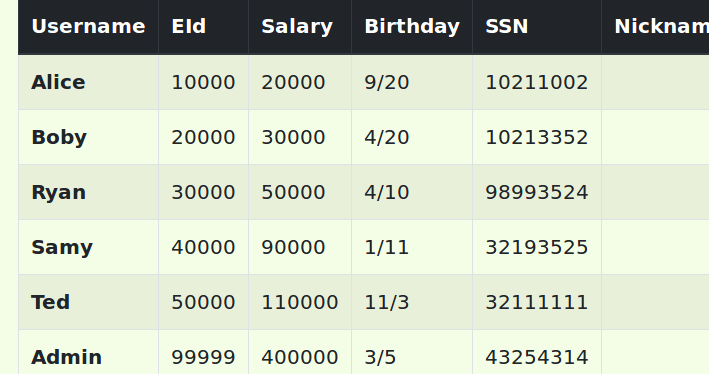
命令行中查看表格：



任务二：

1. 查看所有用户信息：

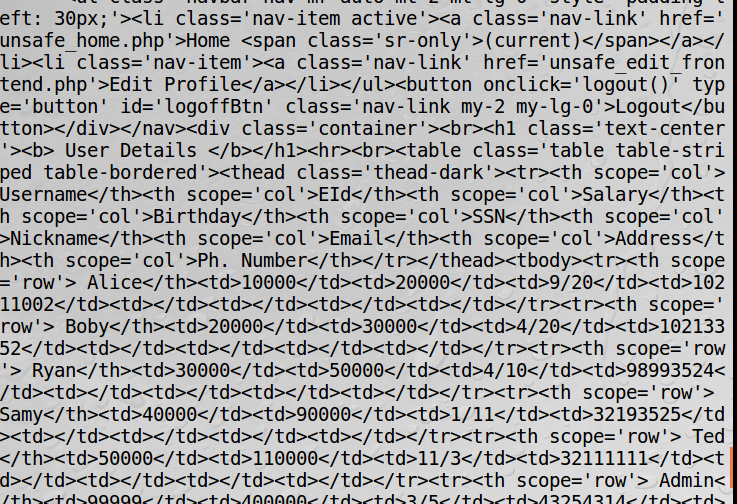


将密码部分注释掉，则输入任意密码可以登录对应账户  


1. 发送curl请求：



将参数写在url中，并将特殊字符用指定数值转义



3、

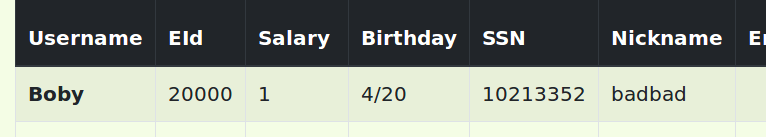
修改文件：



用户名中输入用；相连的两句指令：

Admin’;DELETE FROM credential WHERE name=’Alice’;#

重新登录，alice信息被删除：

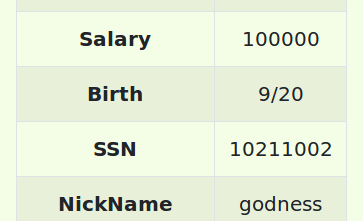


任务三：

1. 在修改信息栏中加入修改薪水的语句

Godness’,salary=100000#

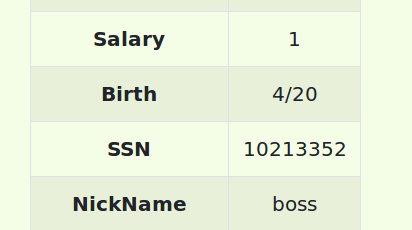
昵称和薪水均被修改：（没有加上where name=’Alice’，所有人nickname被修改）



1. 在alice个人信息的界面加入以下语句：

Boss’,salary=1 where name=’boby’;#

Boby的薪水被修改：

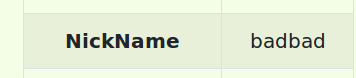


1. 修改alice个人主页：

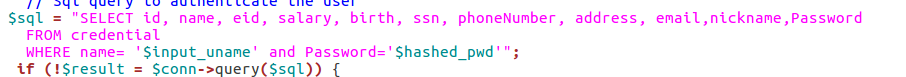
badbad’,Password=’011c945f30ce2cbafc452f39840f025693339c42’ where name=’boby’

其中011c945f30ce2cbafc452f39840f025693339c42为1111的哈希值

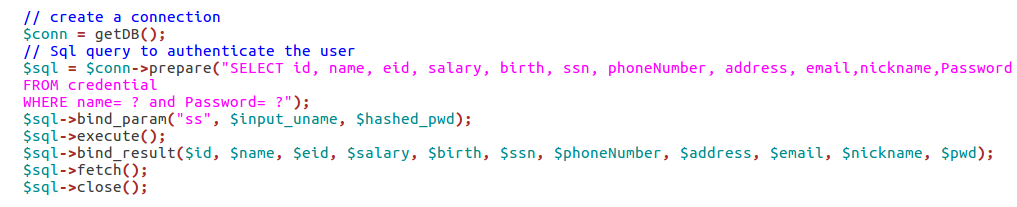
Boby账户可以用1111密码登录，并且nickname被修改：



任务四：

Unsafehome文件：  


没有区分代码和数据

Safehome文件：  


采用了preparedstatement，不将参数简单拼凑为sql语句，而是采用预处理将参数转换为string类型，参数内的特殊字符做预编译处理。使得提供的数据没有经过编译，不会被当作代码执行。

将浏览器网址改为safe



刷新可见注入攻击失败：

