**2023年春季学期**

**网络安全第四次试验**

学号：120L020322

姓名：刘祚甫

指导教师：王彦

实验时间：2023.3.31

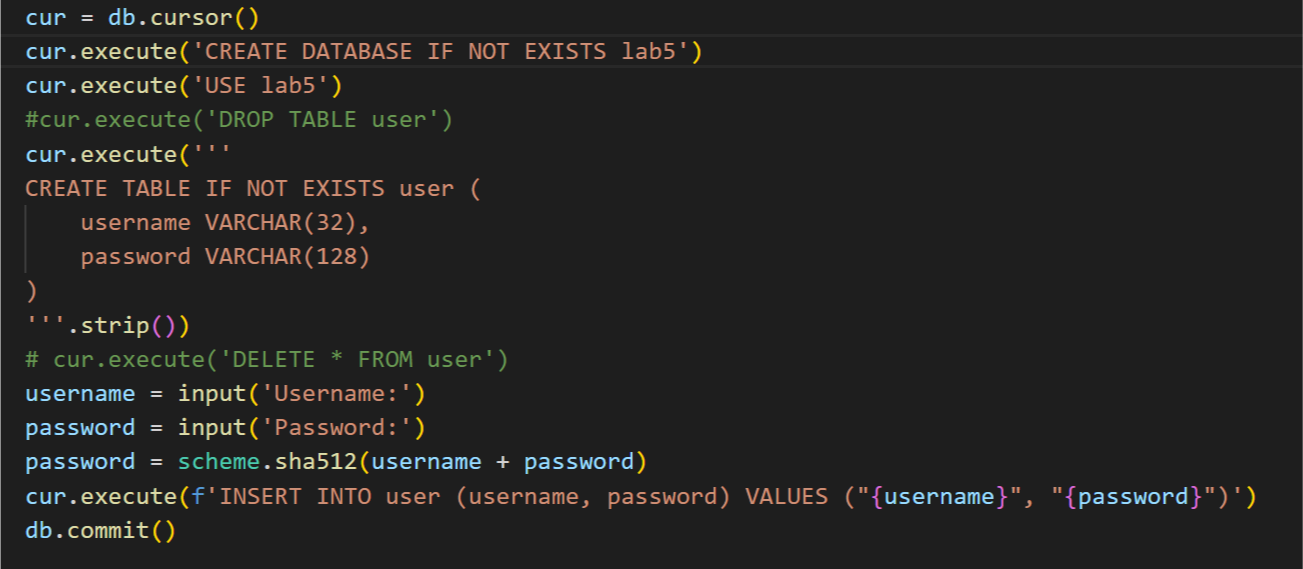
1. **实验目的**

掌握随机函数的使用，掌握散列函数，加解密函数的使用。包的格式与发包的顺序，可以等同于协议的三要素。掌握程序与数据库的链接。

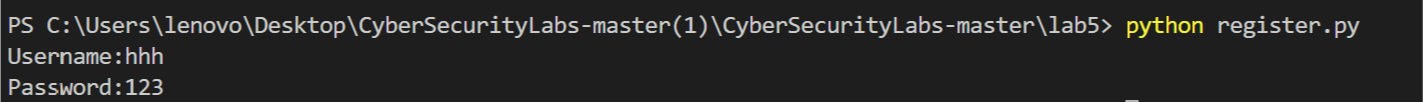
**二、实验原理**

客户端输入用户名，口令，随机产生认证码，使用散列函数计算用户名与口令的散列值1，使用散列值1与认证码计算散列值2，将用户名，散列值2，认证码明文传送到服务器端。

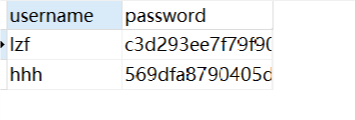
服务器端以数据库保存用户名和散列值1的对应关系。收到客户端信息后，以同样的方法计算散列值2’。 如散列值2’=散列值2，则认证成功，成功后用散列值1加密认证码发送给客户端。客户端解密后写到指定文件。用户可以修改自己的密码。



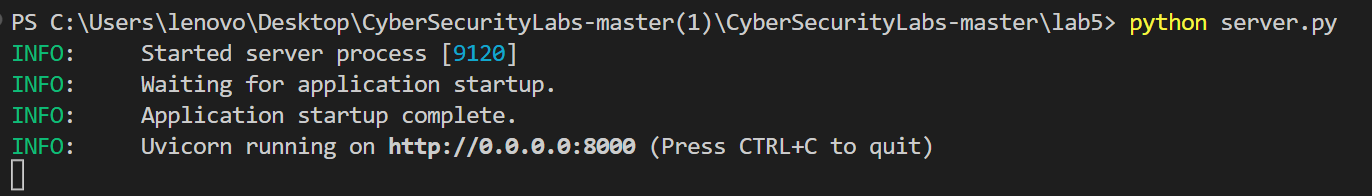
register.py文件的作用是注册登录账号。Cur是一个游标，用于进行数据库操作。输入用户名和密码，即可创建新账号：

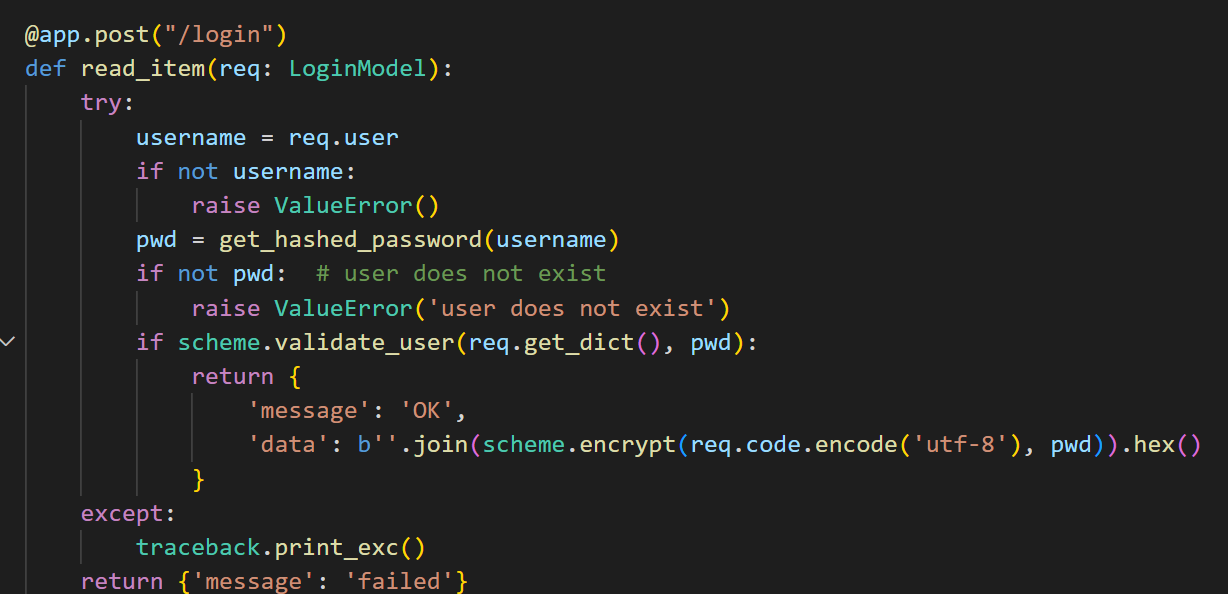


用sha256函数将密码的hash值存储到数据库中

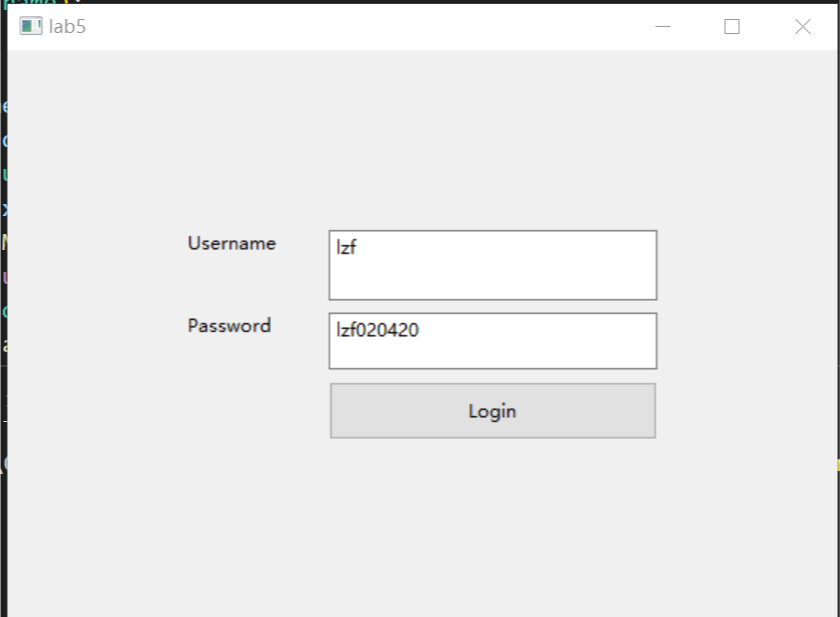


创建好账号密码后，运行server.py文件，让服务器对应的8000端口开始监听，等待客户端的连接。

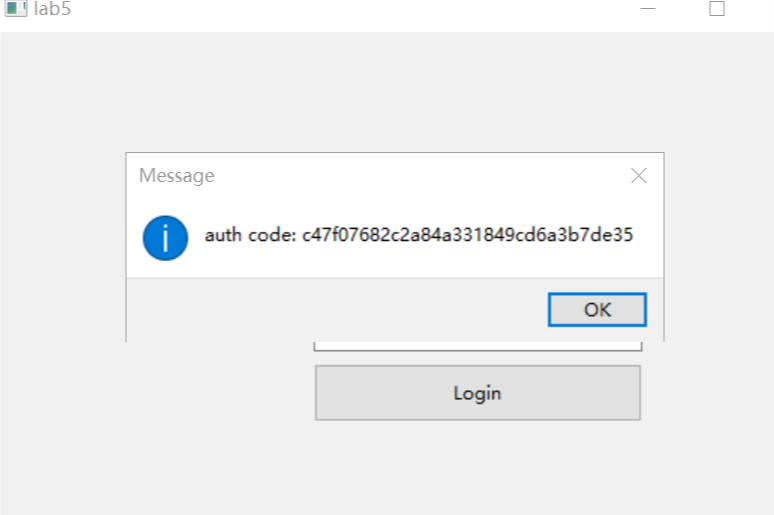


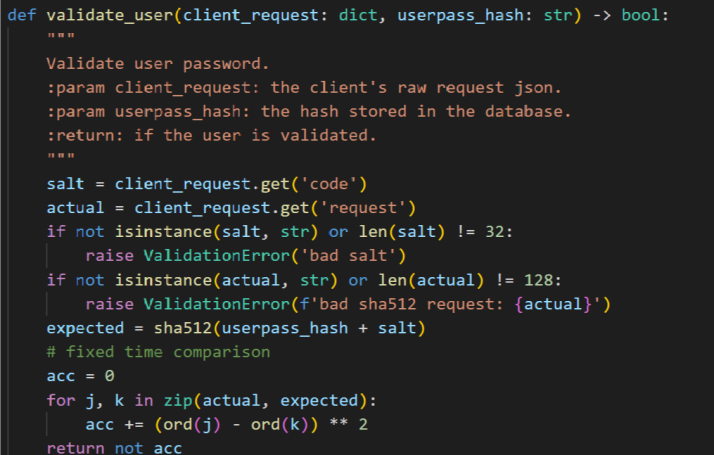


接下来的操作就是运行客户端文件，连接客户端和服务器，进行通信。运行文件后弹出gui窗口，输入账号和登录密码



程序会先随机生成一个盐值（随机认证码），并显示出来





服务器认证成功后，开始传输数据，将数据显示出来并打印在文件里

