

网络安全实验报告

题 目 基于口令的认证过程实现

专 业 信息安全

学 号 120L020121

学 生 刘旭

指 导 教 师 王彦

# 一、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、实验内容**

1. 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。
2. 服务器端以数据库（如access）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。

# 三、实验过程

**实验基本信息：**

实验环境：windows 10 编程语言Python

## 1. 需求分析

需要实现以下功能：

客户端：输入用户名、口令和认证码，计算散列值1和散列值2，并将其发送给服务器端。

服务器端：保存用户名和散列值1的对应关系，接收客户端传送的用户名、散列值2和认证码明文，计算散列值2'并进行比较，如果认证成功，则使用散列值1加密认证码并发送给客户端。

客户端：接收服务器端发送的加密认证码，解密后将其写入指定文件。

用户：可以修改自己的密码，可以在服务器端进行相应的修改。

## 2. 程序结构

Client.py：客户端，用于与服务器进行通信和交互，发送和接收数据。可以实现用户登录的功能。

Server.py：服务器端，用于接收客户端的请求，处理请求并向客户端发送响应。可以实现用户认证的功能。

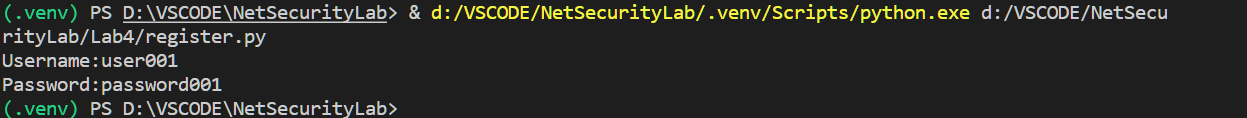
Register.py：注册账号，提供用户注册功能，包括输入用户名和密码，将用户信息保存到数据库中。

Change\_password.py：修改账号密码，提供用户修改密码功能，包括输入旧密码和新密码，将新密码保存到数据库中。

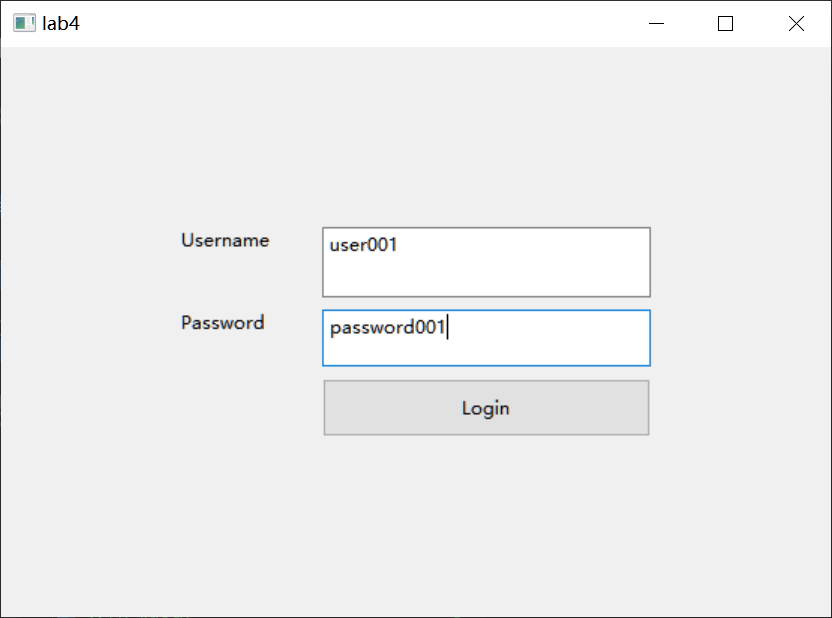
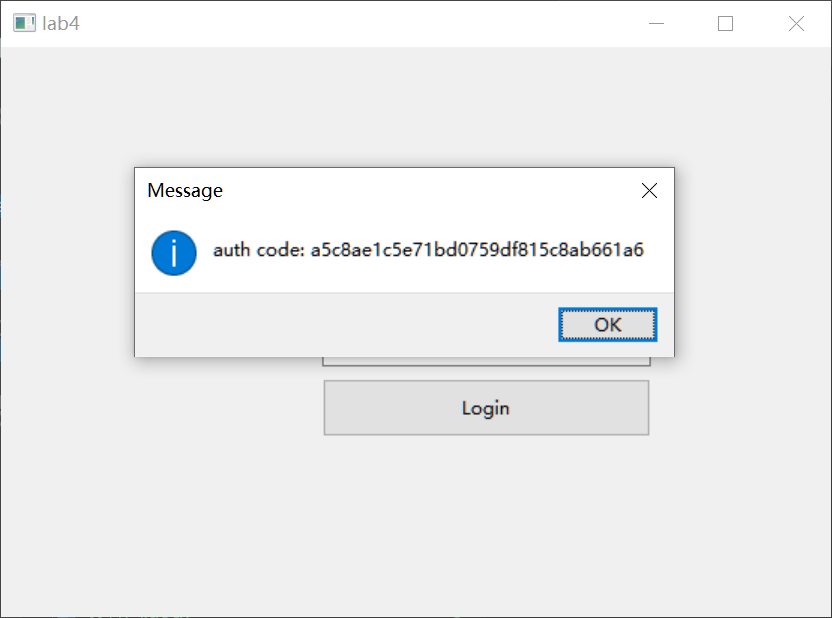
Scheme.py：用到的加密函数，包括哈希函数、认证码等，用于对用户密码进行加密和解密，保证用户信息的安全性。

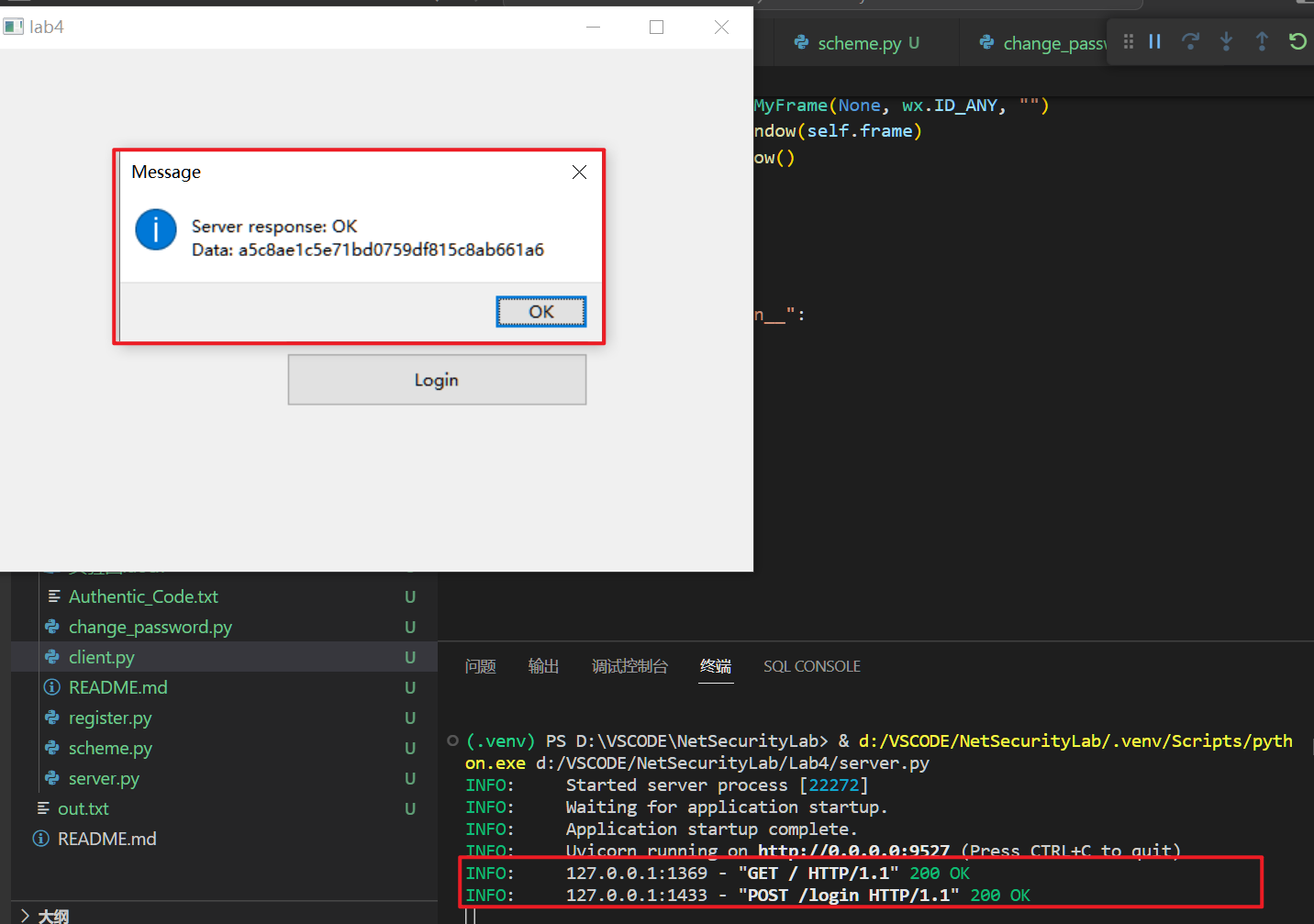
# 四、实验结果

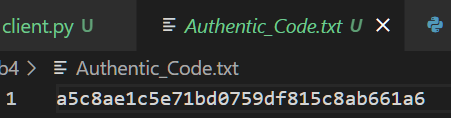
注册账号：

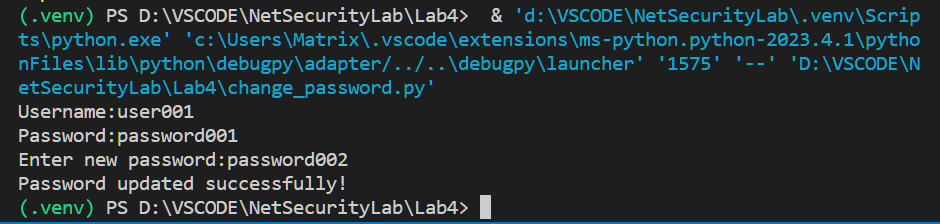


登陆：

登陆成功：

生成的文件内容：

修改密码：

# 五、心得体会 （出现问题分析）

在这个实验中，我学习了密码学中常用的散列函数及其应用。通过实验，我深刻认识到密码学在信息安全中的重要性。

在实验过程中，我遇到了一些问题。首先，我在计算散列值1时，由于没有使用适当的编码方式，导致计算结果与服务器端不一致，无法完成认证。解决方案是使用统一的编码方式，例如UTF-8。

其次，我在修改密码时遇到了一些困难。由于密码是加密存储在服务器端的，我需要先解密密码，再进行修改。但是，如果在解密过程中出现错误，可能导致密码数据损坏。解决方案是在修改密码前，先备份原始密码数据，以防止数据损坏。

通过这个实验，我不仅掌握了密码学的基本知识，还学会了如何应对实际情况中的问题。同时，我也更加认识到信息安全的重要性，希望在以后的学习和工作中，能够更加注重信息安全。