

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 120L020829 \_

学 生 袁野 \_

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。

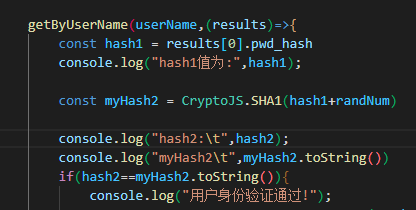
**二、实验内容**

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。

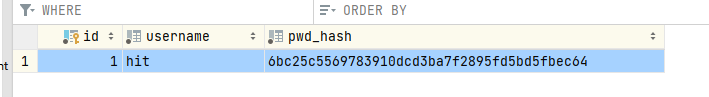
# 三、实验过程

服务器端和客户端都使用JavaScript语言编写。

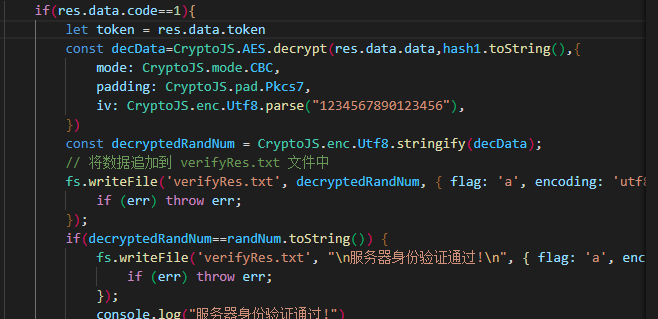
大致流程是，客户端向服务器端发送用户名，hash2和认证码，服务器端从数据库中查询该用户名对应的hash1，与认证码连接后求哈希，比较结果与发来的hash2是否相同。如果相同则验证成功，此时服务器端使用AES加密，将hash1作为密钥，加密认证码并发送给客户端，如果客户端解密出的认证码和它之前发送的相同，则它验证服务器的身份也成功。



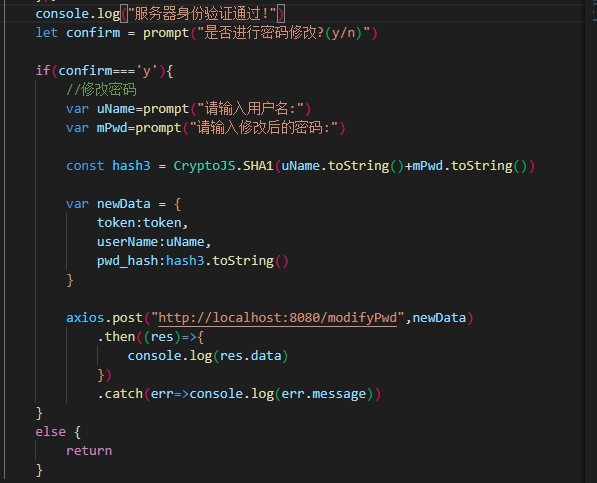
如图，使用js的mysql模块，查询用户名对应的hash1。



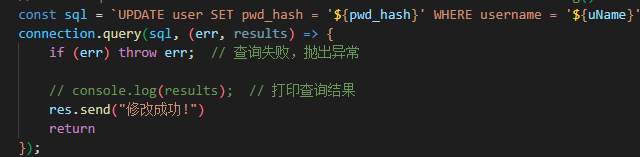
将查询到的hash1与认证码连接后，使用SHA1函数求哈希，比较与发送来的hash2是否相同。



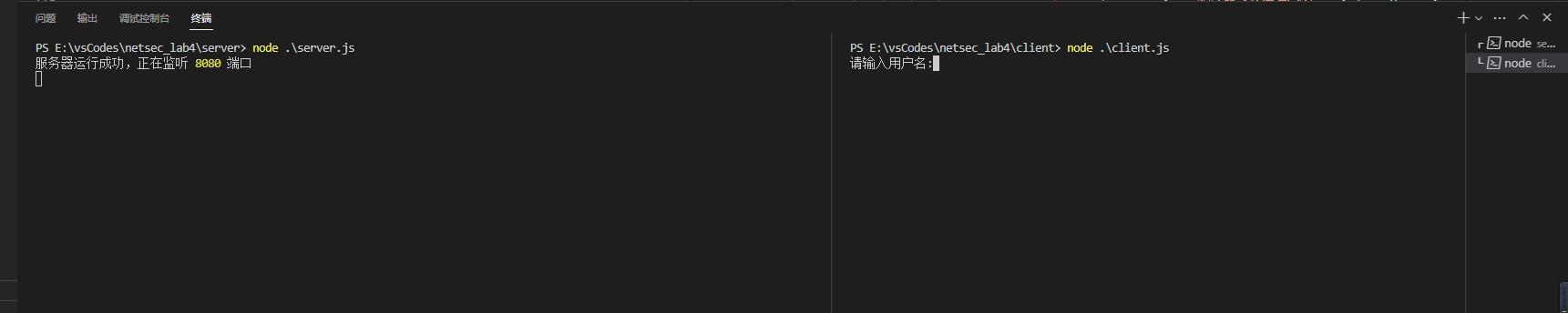
客户端接收到服务端的响应后，使用AES的解密函数，将hash1作为密钥解密数据，比较解密的数据与之前生成的认证码是否相同，如果相同则说明服务器身份验证通过。验证通过之后可以选择修改密码：



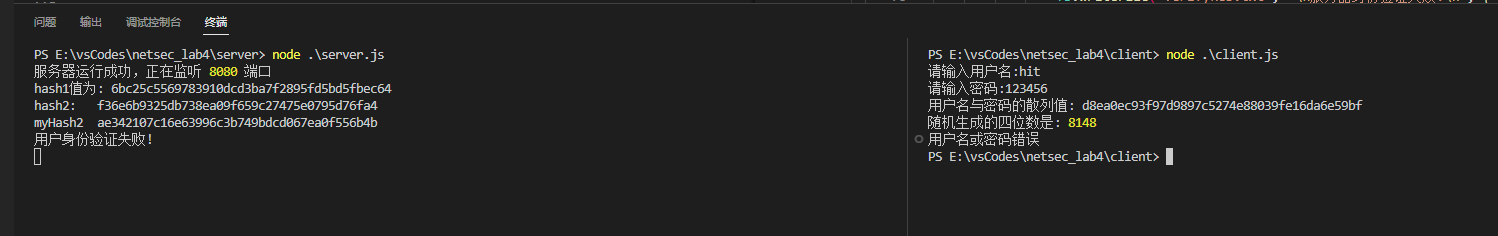
将新的用户名和密码的hash发送给服务端，服务端使用update语句修改数据库中的数据即可。



实验演示：



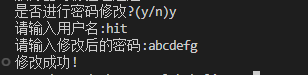
启动程序。



输入错误的密码后服务器会返回错误信息，客户端程序将被终止。



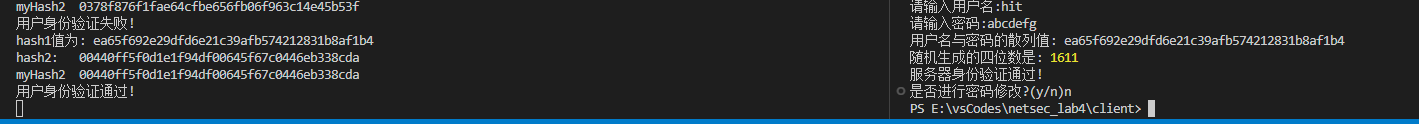
输入正确的密码后即可登录成功，同时如果服务器身份验证通过则可已选择是否修改密码。



现在将密码由原来的111111修改为abcdefg，再次运行客户端程序输入原来的密码



可以看到111111已经无法再登录



使用abcdefg登录成功。

**四、心得体会：**

通过这次实验，学习了如何使用js编写简单的前后端程序，并且学会了如何使用js连接本地的mysql数据库并执行sql语句。同时还对服务器与客户端的身份认证过程有了更深刻 的理解，更加清晰地学习了认证的每个流程。