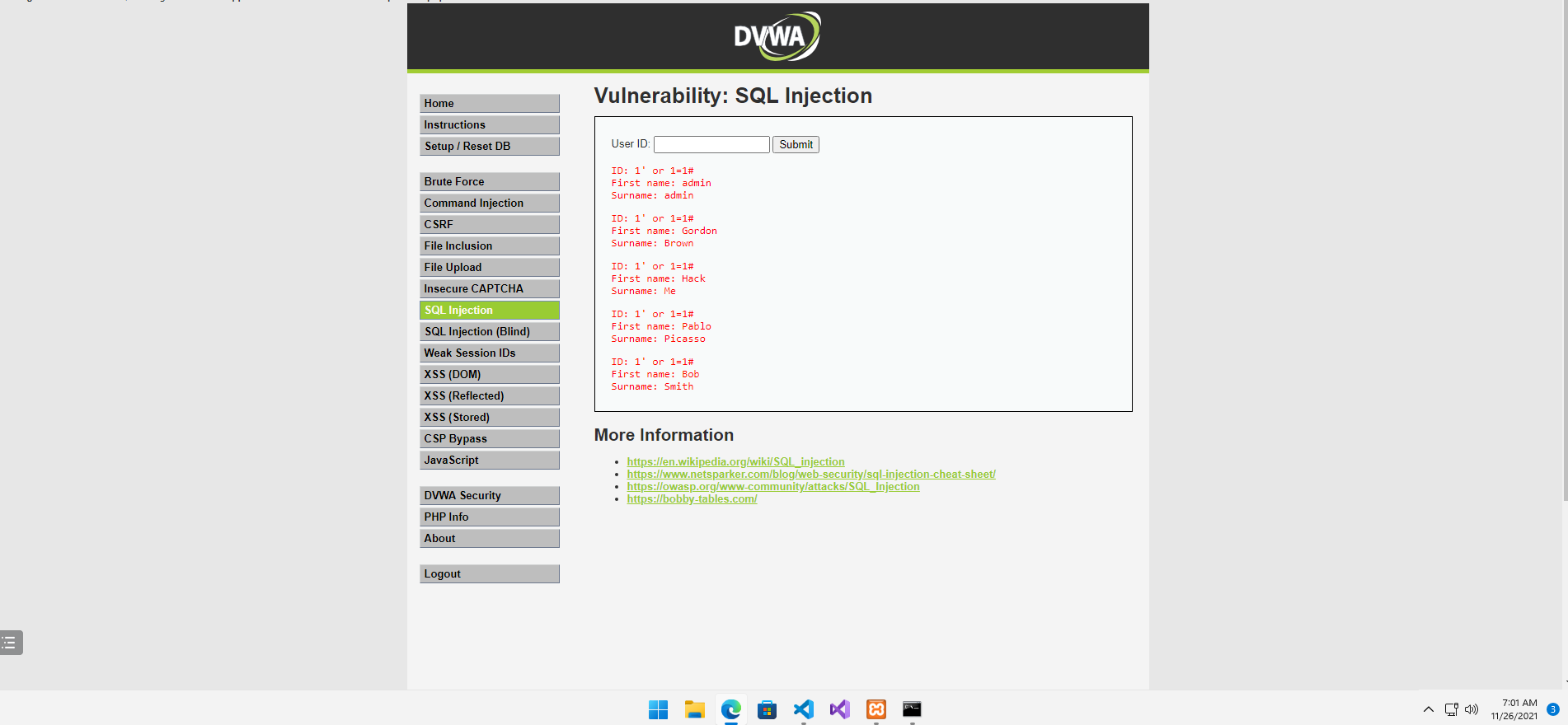
**Homework 3**

Xueli Yang

008737742

1. Describe the SQLi attack you used, how did you cause the user table to be dumped? What was the input string you used?

I changed the security setting into” low” mode and use the input “1’or 1=1#”. It means true and give everything in the table. It will display all the users’ information from the database.

Graphical user interface, application

Description automatically generated

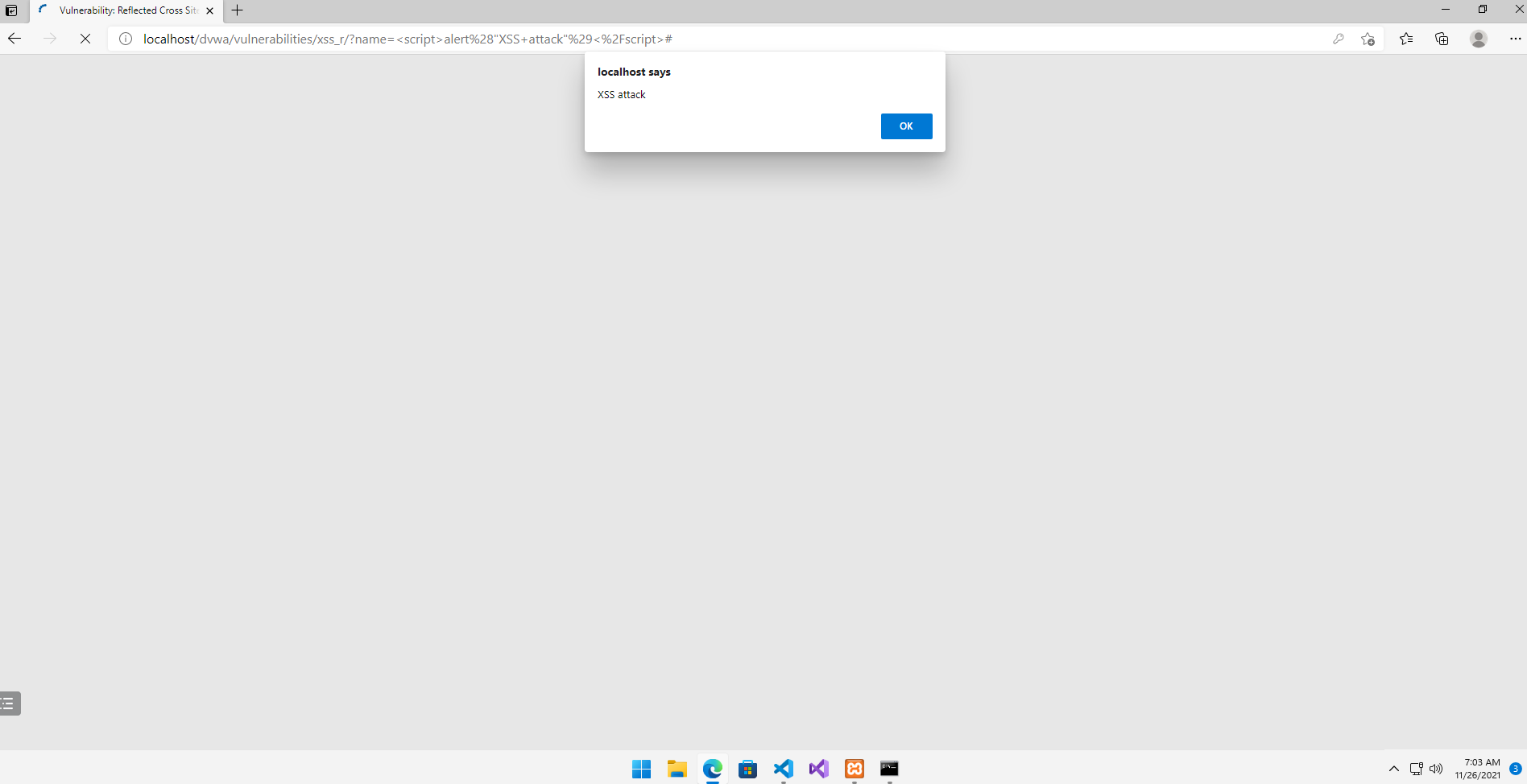
From the picture, I used “1’ and 1=1 union select null, table\_name from information\_schema.tables #” to get the table name. “1’ and 1=1 union select null, column\_name from information\_schema.columns where table\_name = “users”#. To get the column names. Then, use the input as the in the picture, “1’ and 1=1 union select user, password from users#” to get more information like, user First name and Surname.

1. If you switch the security level in DVWA to “Medium”, does the SQLi attack still work?

The SQLi attack will not work.

1. Describe the reflected XSS attack you used, how did it work?

As show in the picture, I used the input to test: <script>alert(“XSS ATTACT’)</script> and when the security was ‘low’, it will go through and will not be detective.



1. If you switch the security level in DVWA to “Medium”, does the XSS attack still work?

No, as show in the picture. It has been detective.

