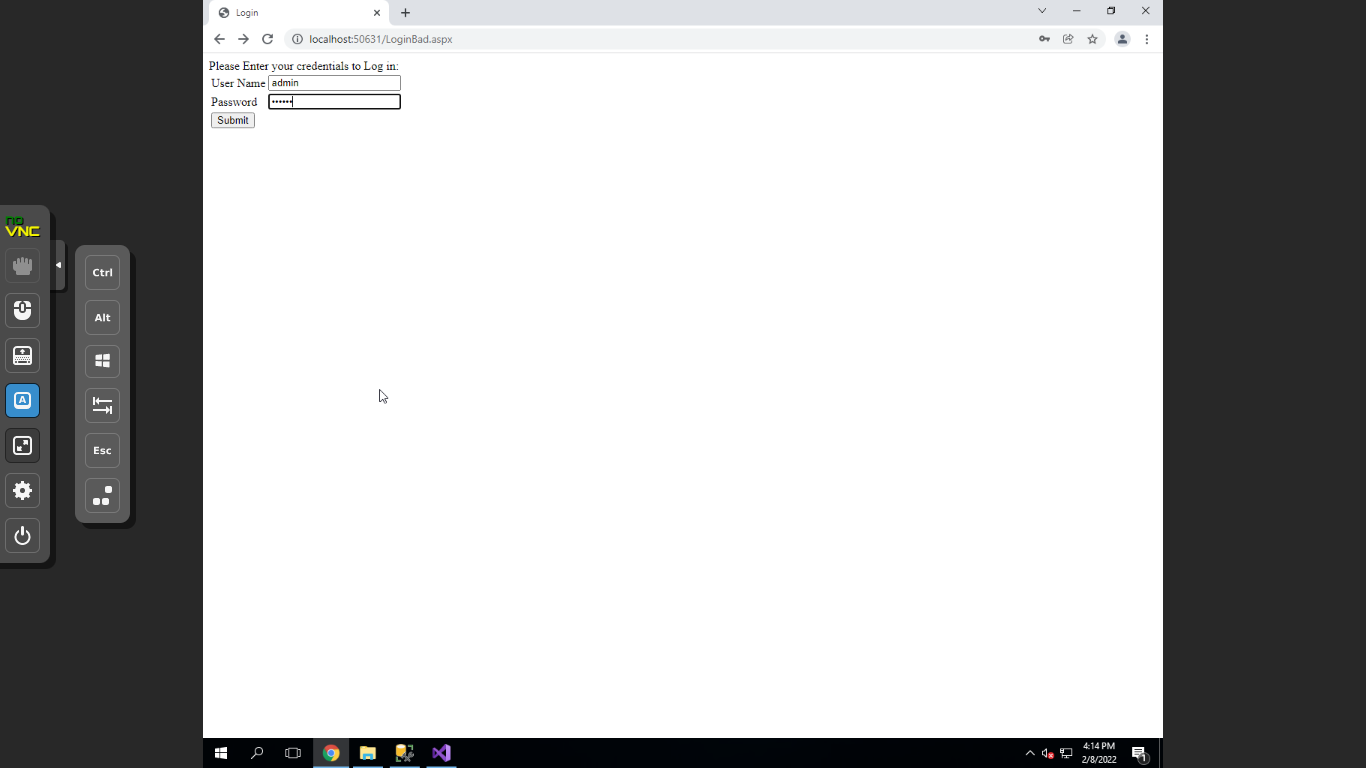
# Lab: SQLi

|  |
| --- |
| * This lab is due tonight. It is worth 5 points and graded as pass/fail. * Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab\_SQLi\_ImG.docx). |

# [Task] SQL Injection

Click the link to test out the **BAD login** page. And answer the following two questions.

1.a Enter “admin” / “monkey” for login. Report the result in a screenshot.



Graphical user interface, application, Word

Description automatically generated

1.b Enter "admin" for User Name and any arbitrary password for Password. Report the result in a screenshot.

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

2. Use an injection and show that you can log in without using any credentials. Show the injection you used. Report the result after the successful injection in a screenshot.

Graphical user interface, application, Word

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

Injection Password used: **‘ or 1=1--+**

Click the link to test out the **BAD product** page.

3. Click the link at the bottom of the page. Explain how you’ve got that result.

The UNION injection query searches for the name and passwords of users as well as the products due to the UNION command.

Stay on the **BAD product** test page for the remaining questions.

4. Create an injection to figure out Table Name, Column Name in the database you currently are connected to. Use Union and Information schema view. Report the result in a screenshot. [Hint: Apply the class slide with the title “Attacks using UNION.”

Graphical user interface, text, application

Description automatically generated

5. Create an injection to list all the logins and their passwords in the current MSSQL instance. Use Union and Catalog view. Report the result in a screenshot.

Graphical user interface, text, application, email

Description automatically generated

6. Create an injection to list all the database names in the current MSSQL instance. Use Union and Catalog view. Report the result in a screenshot.

Graphical user interface, application

Description automatically generated

7. Create an injection to list all the system tables in the current MSSQL instance. Use Union and Catalog view. Report the result in a screenshot.

