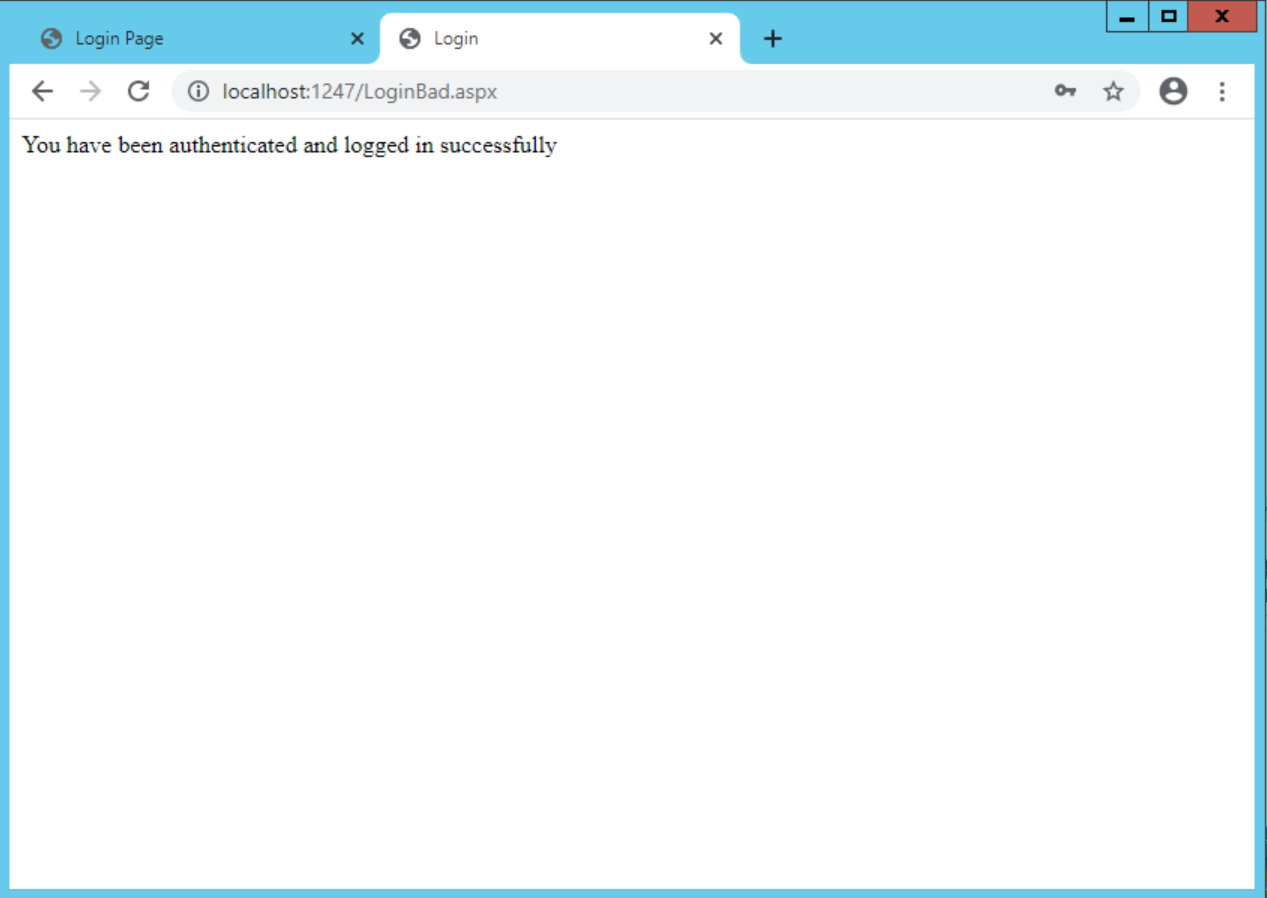
# Lab: SQLi

|  |
| --- |
| * This is due tonight and worth 10 points. * Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab\_SQLi\_ImG.docx). |

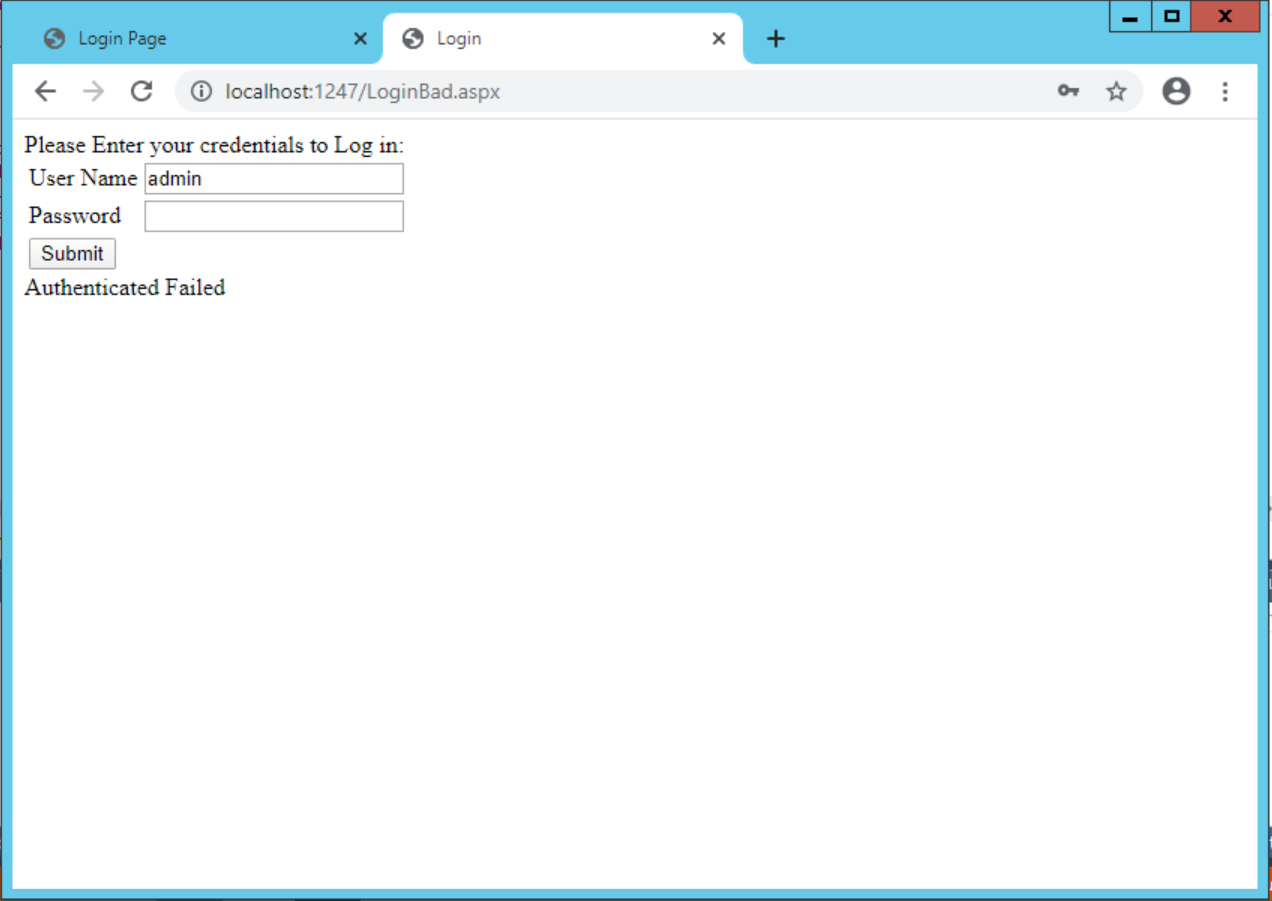
# [Task] SQL Injection

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

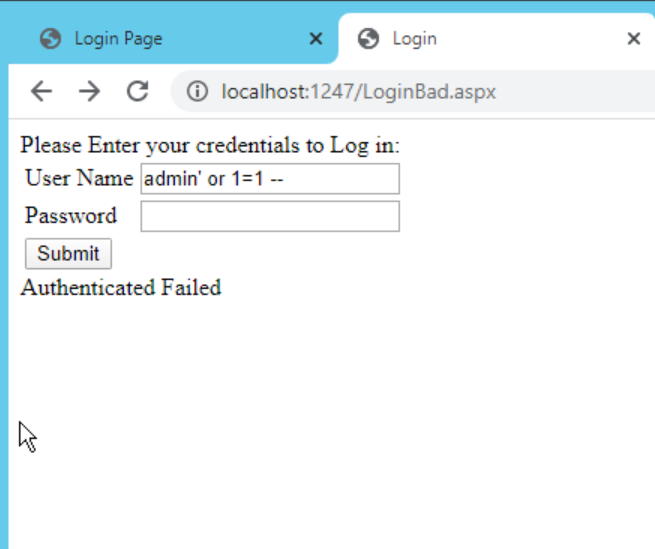
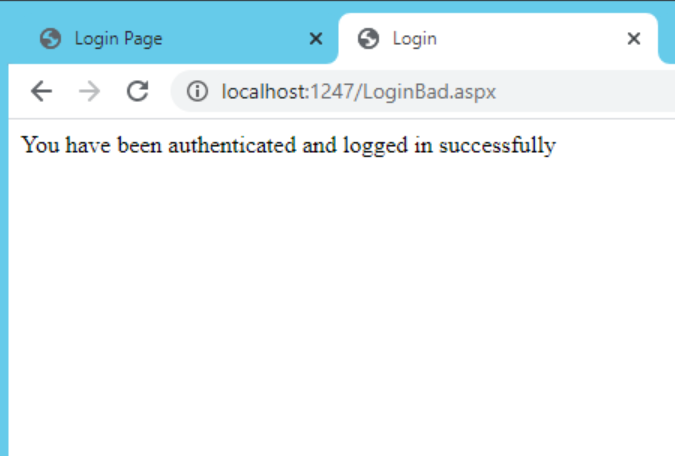
1.a Enter “admin” / “monkey” for login. Report the result in a screenshot.



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



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.

Using “admin’ or 1=1 –” successfully got me past the login screen. Also works if I enter the username “admin and the password “test’ or ‘1’=‘1”.

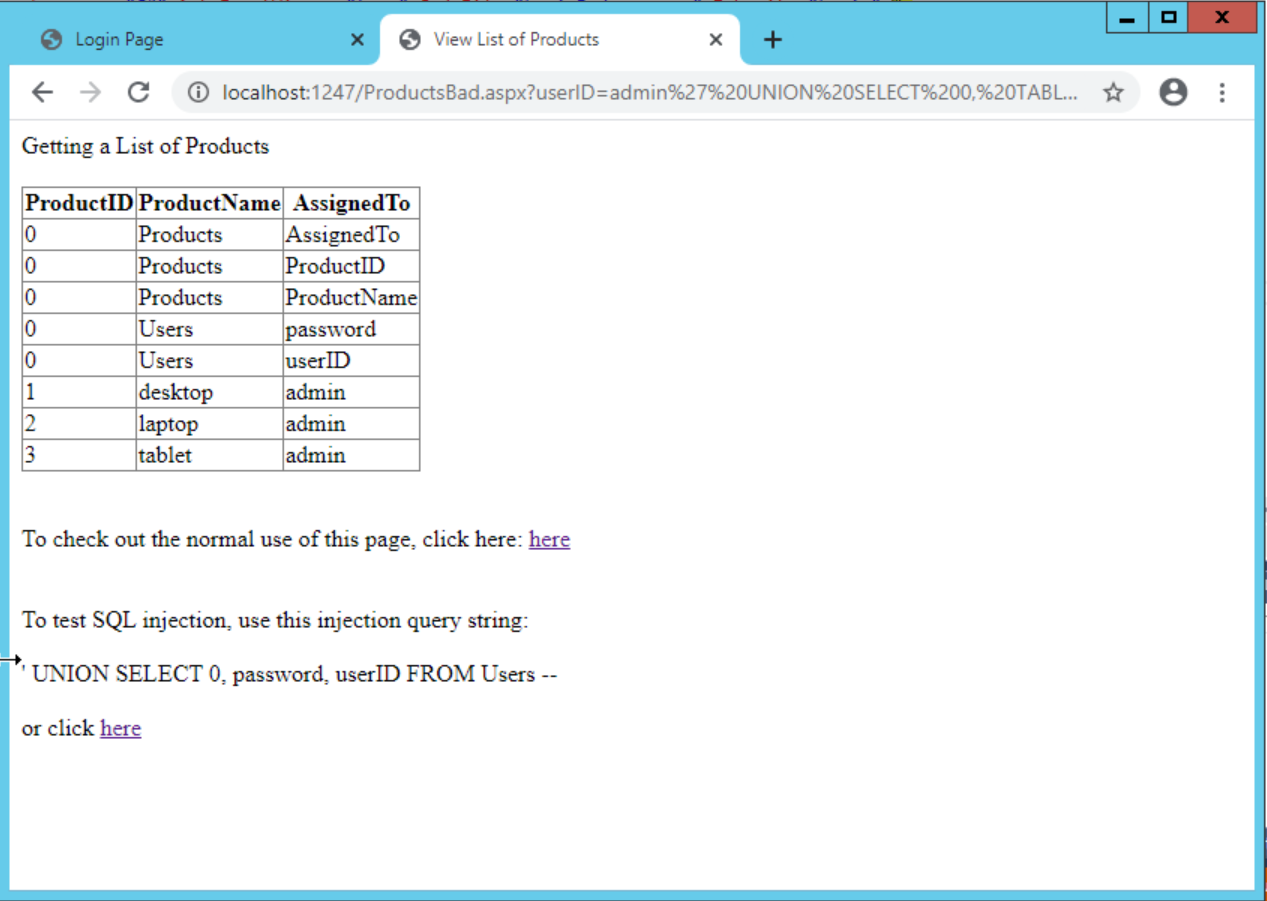
Click the link to test out the **BAD product** page.

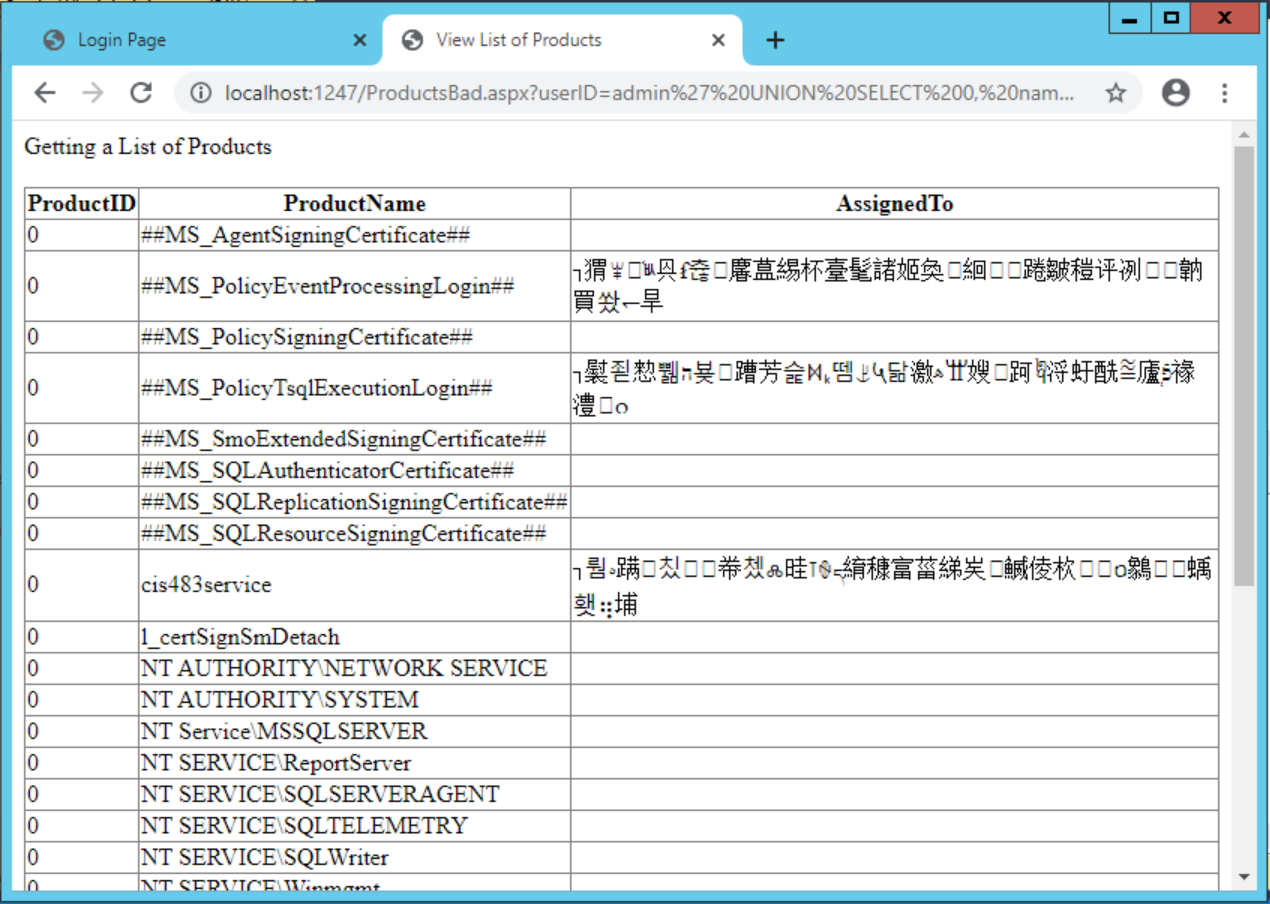
3. Click the link at the bottom of the page. Explain how you’ve got that result.

The first column is null from our select, the second column is passwords, and the third column is user IDs. This works because we injected our own code and joined the Users table to the Product table.

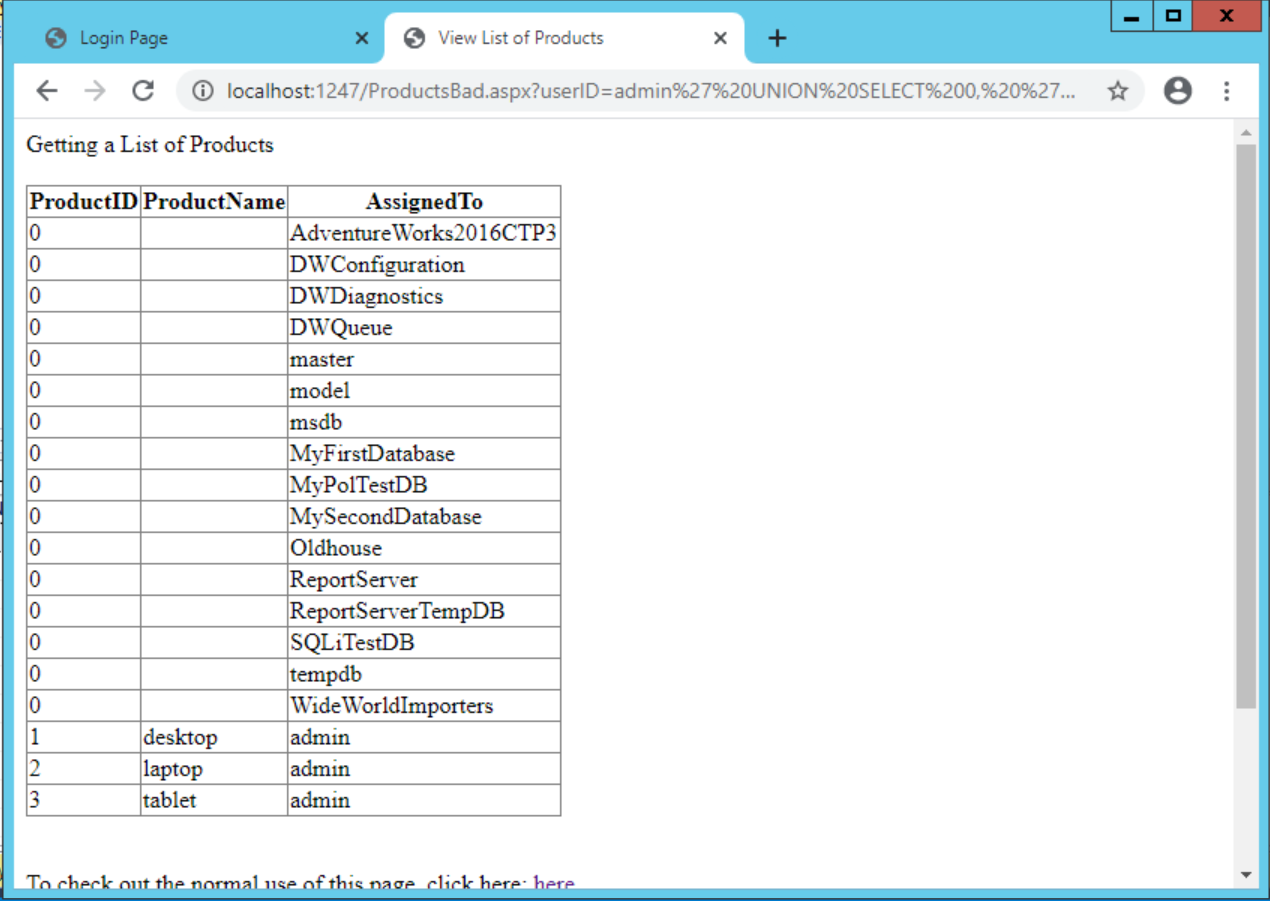
Stay on the **BAD product** test page for the remaining questions.

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.”

 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.



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.



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.

