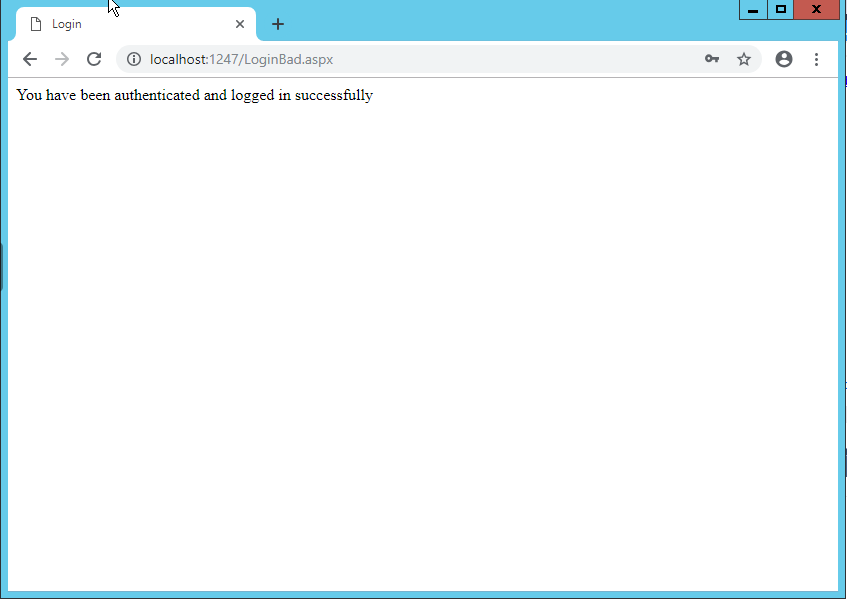
# Lab: SQLi

|  |
| --- |
| * 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). |

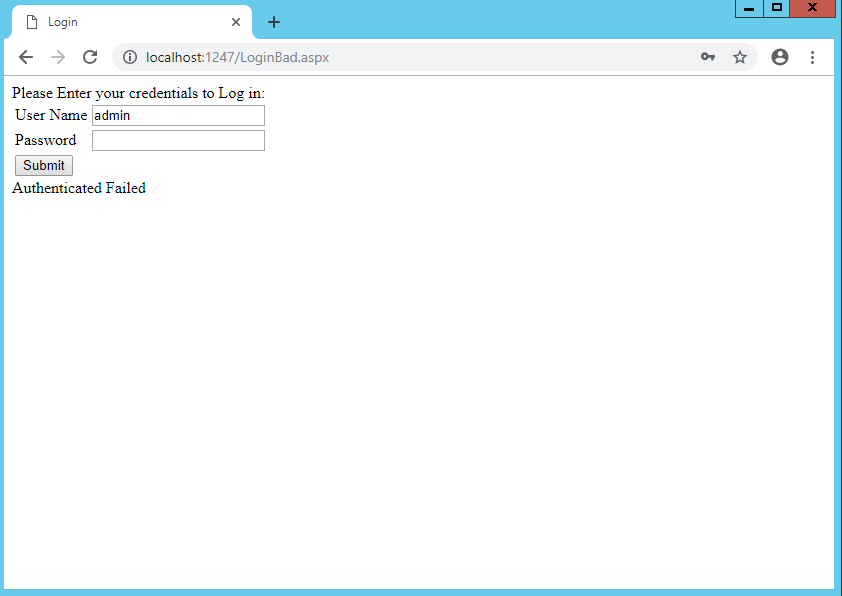
# [Task] SQL Injection

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.



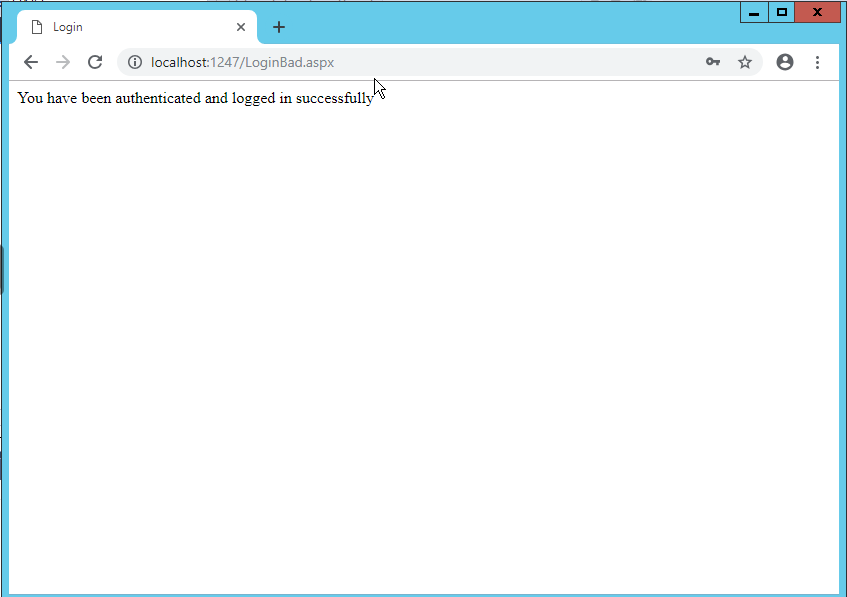
1.b Enter "admin" for User Name and any arbitrary password for Password. Report the result in a screenshot.



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.

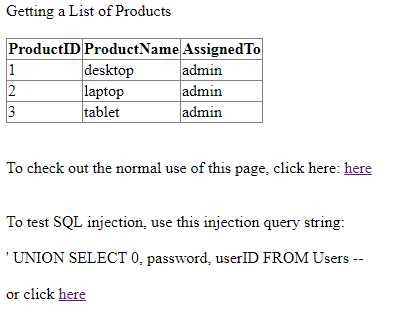
**Username: admin**

**Password: test’ or ‘1’ = ‘1**



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

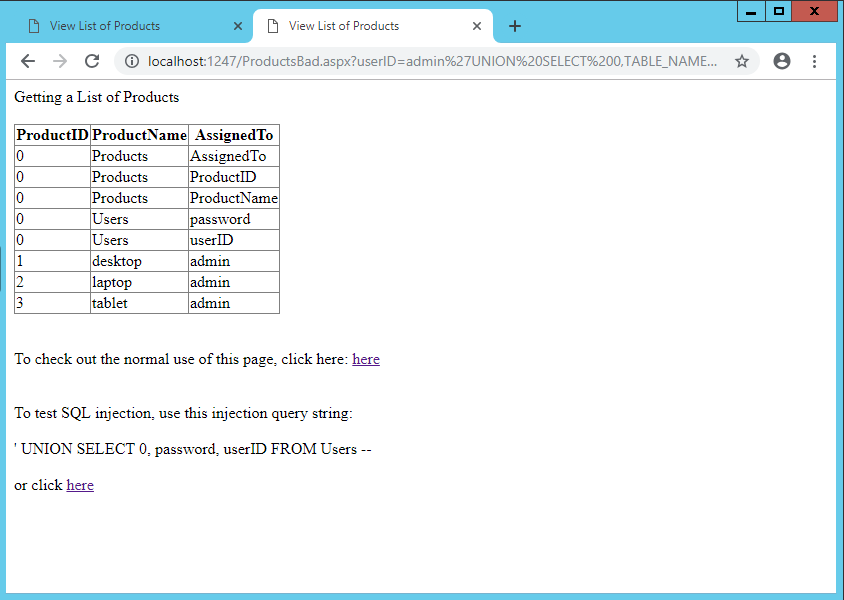
3. Click the link at the bottom of the page. Explain why you get that result.



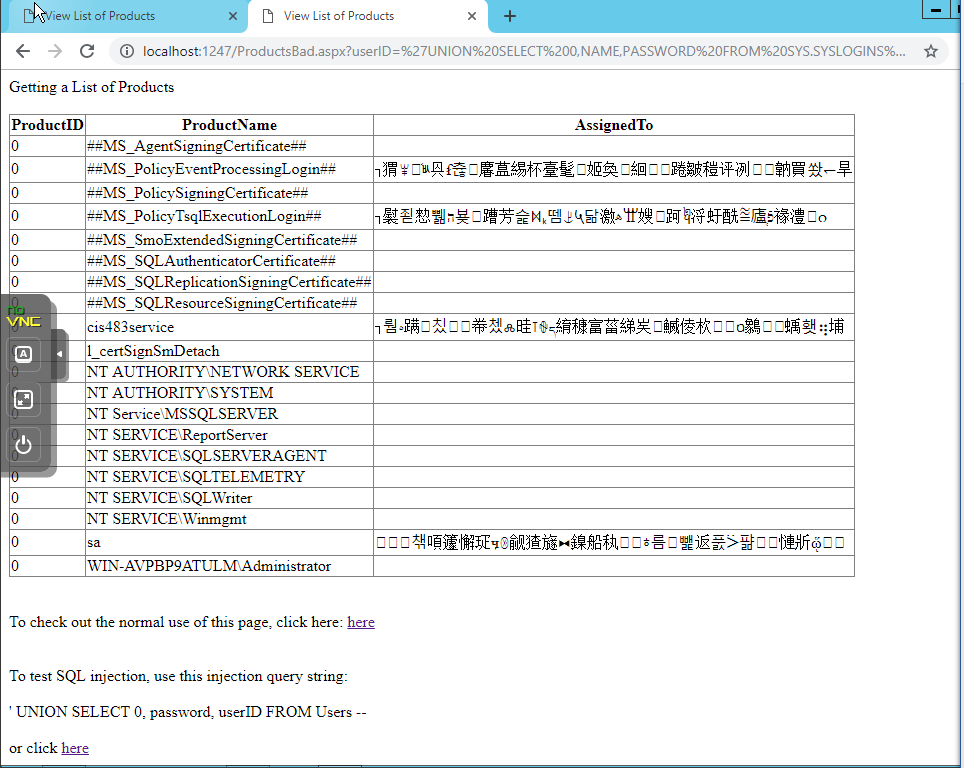
**You are getting the product name (Username) and assigned to (Password) with those who have a product ID of 0.**

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.

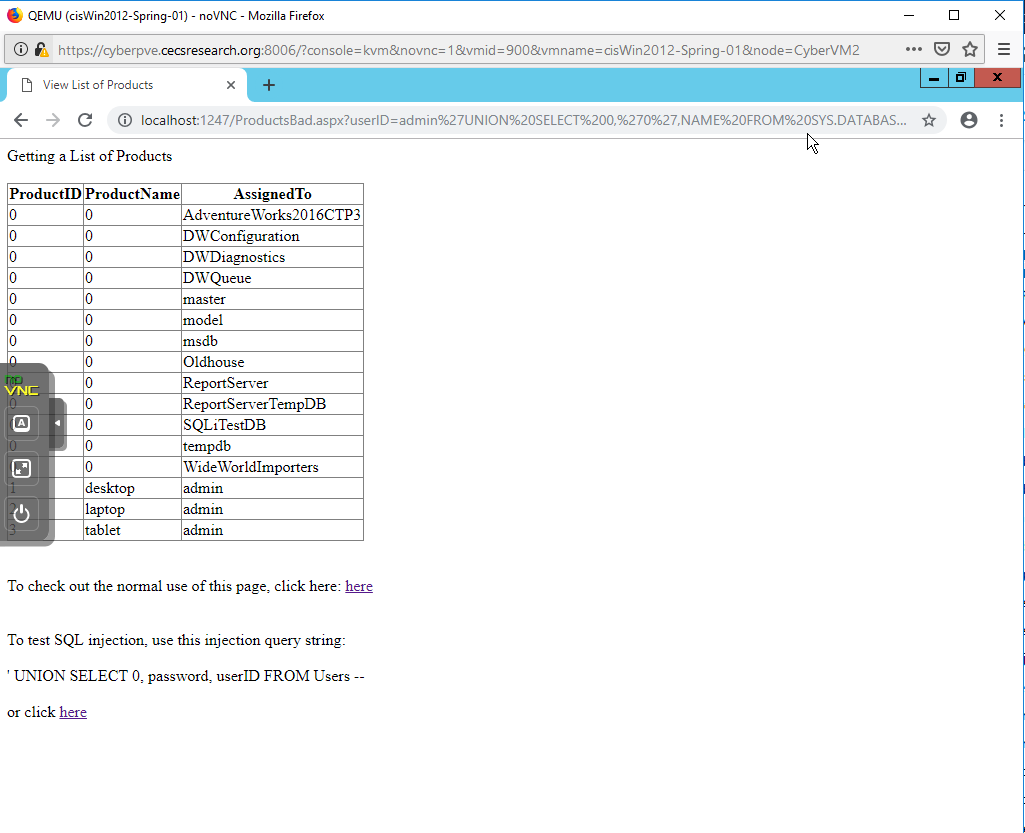


USE SYSTEM SYS LOGINS\_VIEW = SYS.SYSLOGINS

SYS.DATABASES IN SLECT AFTER UNION NEED TO PUT ONE COLUMN FOR DB NAMES

SYS.ALL\_OBJECTS

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.

