# 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.

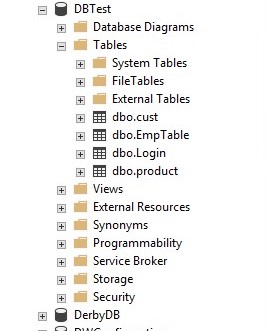
In this task we used admin'; INSERT INTO login VALUES ('user300','orange');-- , this allowed us to send the user and password into the login table in hopes to create the login, so we could access the site.

1. **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.

Table

Description automatically generated

* **(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.
2. 
3. **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.

Table

Description automatically generated with low confidence

* **(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.

Table

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.

Graphical user interface, table

Description automatically generated