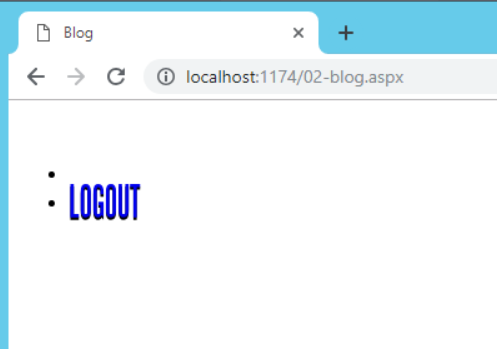
# Assignment #4: Database Attacks and Defense

|  |
| --- |
| * This is an individual assignment, and is worth 20 points. * The due date is Tuesday, Feb 12th, 11:00 AM / 5:30 PM. * You need to provide your answers to the “Homework #4 – Tasks.docx” file. Change the file name following the naming convention suggested below. * Naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Homework #4\_ImG.docx). If you do not follow the convention, I will deduct 1.0. * Do not copy any of the sample screenshots provided as illustrations. |

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

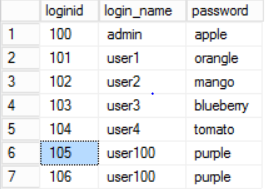


* **(Task # 2)** Enter the following injection in **Login name** box and make the Password box blank.

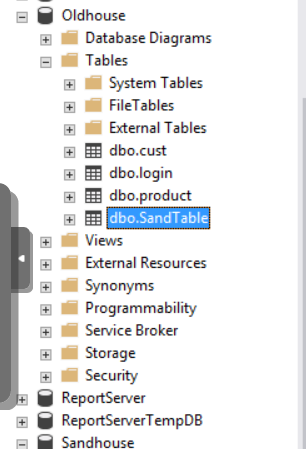
1. **Task #2A:** What is the constructed query that is passed on to SQL Server? If you study the code in **Login.aspx.cs**, you can figure out the constructed query. Also, refer to the class slides for ideas.

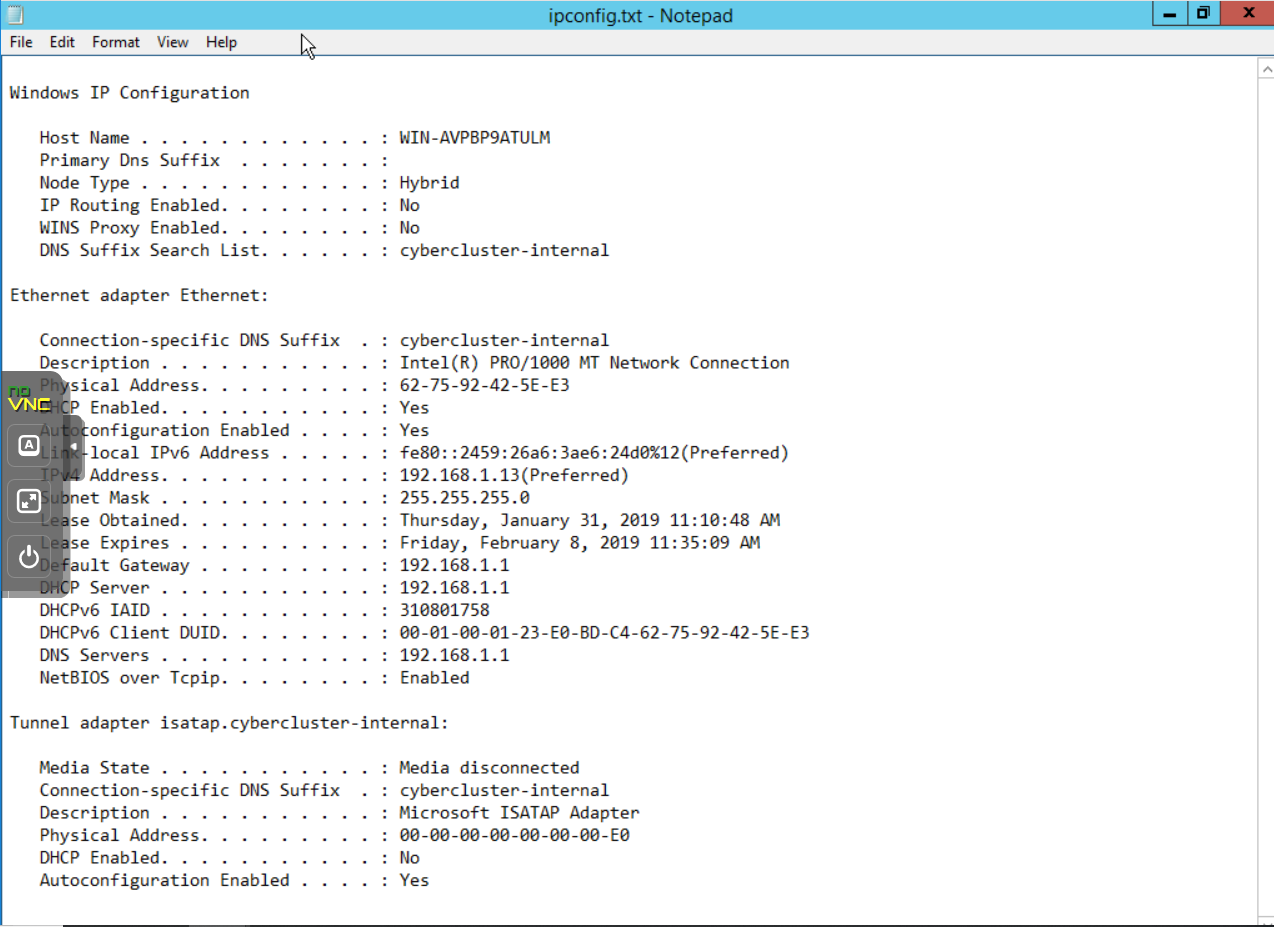
“SELECT \* FROM Login WHERE loginid=’ “ + Session[“userid”] + “’”;

1. **Task #2B**: Go to the SQL Server and confirm that the account (‘user100’, ‘purple’) is indeed created in the login table. Provide a screenshot of the records in the table.



* **(Task # 3)** Enter the following two injections using **Login name** box. Leave the **Password** box blank. Show in screenshots that the database and the table are created. The table will be created in **Oldhouse** database.



* **(Task # 4)** Go to the directory **c:\Test\** in Windows 2012 Server and locate **ipconfig.txt** file. Open up the file and take a screenshot of its content.
*  **(Task # 5)** Take a screenshot of Windows 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 the injection is working.

