# Assignment #4: Database Attacks and Defense

|  |
| --- |
| * This is an individual assignment and is worth 20 points. * The due date is Thursday, Feb 17th, Midnight. * 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. * When you take a screenshot, please zoom in so that the results are recognizable. When the screenshot is too small, I will deduct points. |

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

Graphical user interface, text, application

Description automatically generated

* **(Task # 2)** Enter the following injection in the **Username** box and leave the Password box blank.

1. **Task #2A:** What is the constructed query that is passed on to SQL Server? Refer to the class slides for ideas.

**The constructed query is SQL Data Manipulation language that adds a new username and password into the login table by pretending to be the administrator.**

1. **Task #2B**: Go to the SQL Server and confirm that the account (‘user600’, ‘blue’) is indeed created in the login table. Provide a screenshot of the records in the table.

A picture containing text, screenshot, computer, computer

Description automatically generated

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

A picture containing text, screenshot, computer, computer

Description automatically generated

* **(Task # 4)** Go to the directory **c:\Test\** in Windows 2016 Server and locate **ipconfig3.txt** file. Open the file and take a screenshot of its content.

A picture containing text, screenshot, computer, computer

Description automatically generated

* **(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 has worked.

Graphical user interface, application, table, Word

Description automatically generated