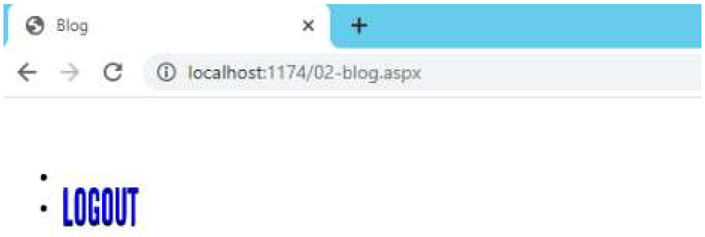
Assignment #4: Database Attacks and Defense

- 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.

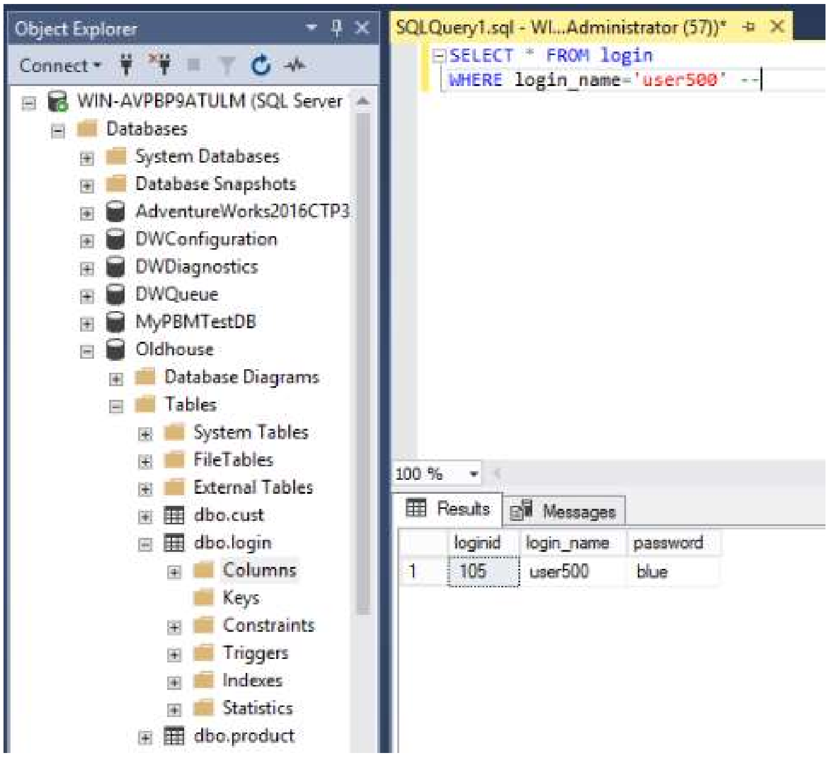


- **(Task # 2)** Enter the following injection in **Login name** box and make the Password box blank.

  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’);--
```

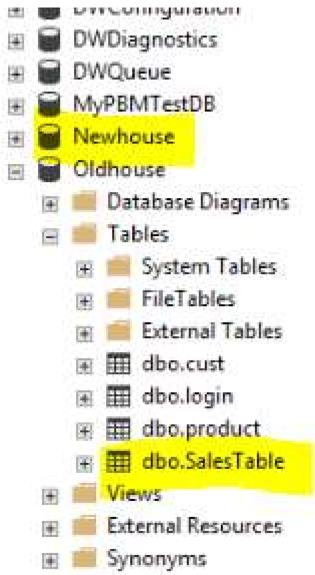
2. **Task #2B**: Go to the SQL Server and confirm that the account ('user500', 'blue') is indeed created in the login table. Provide a screenshot of the records in the table.



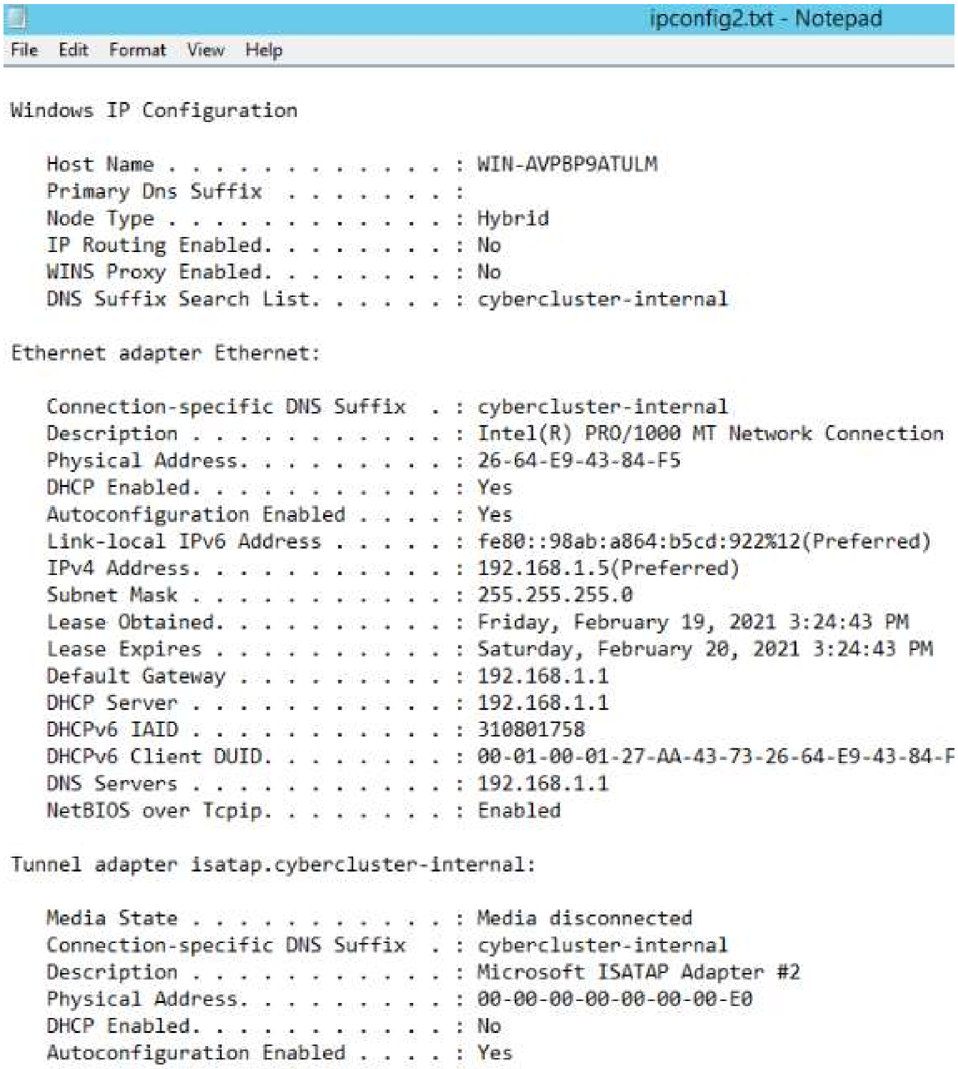
```
SELECT * FROM login
WHERE login_name='user500' --
```

	loginid	login_name	password
1	105	user500	blue

- **(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.

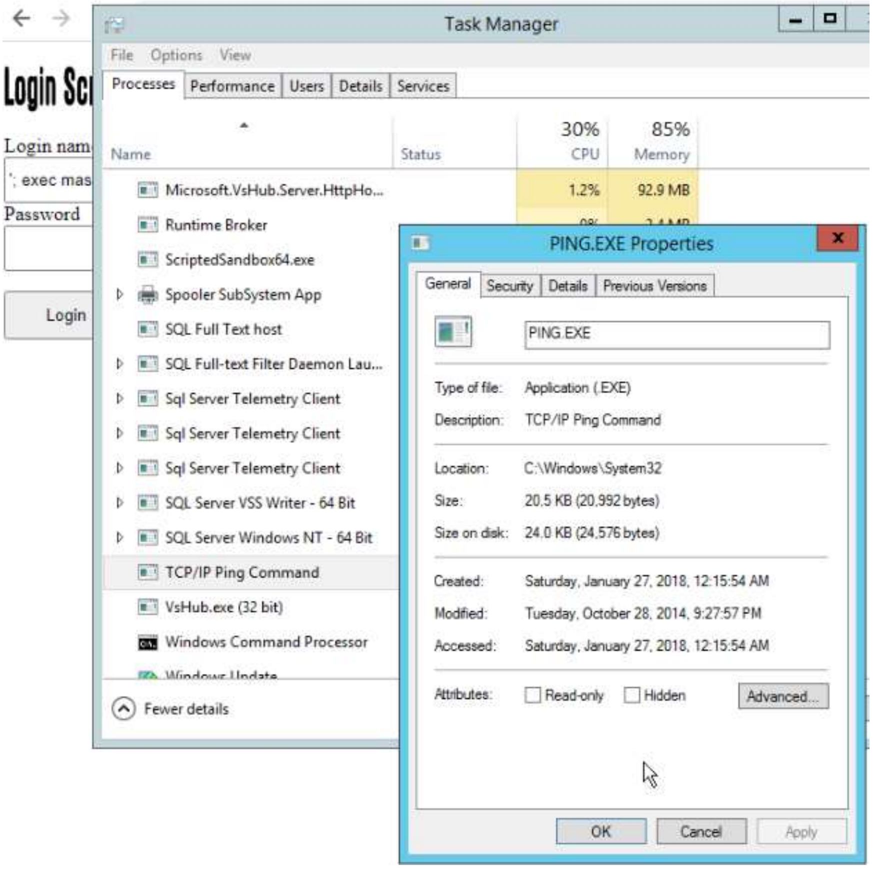


- **(Task # 4)** Go to the directory **c:\Test\** in Windows 2012 Server and locate **ipconfig2.txt** file. Open up the file and take a screenshot of its content.



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-AVPBP9ATULM
   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. . . . . . . . . : 26-64-E9-43-84-F5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::98ab:a864:b5cd:922%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, February 19, 2021 3:24:43 PM
   Lease Expires . . . . . . . . . . : Saturday, February 20, 2021 3:24:43 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 310801758
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-AA-43-73-26-64-E9-43-84-F
   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.



Name	Status	30% CPU	85% Memory
Microsoft.VsHub.Server.HttpHo...		1.2%	92.9 MB
Runtime Broker			
ScriptedSandbox64.exe			
Spooler SubSystem App			
SQL Full Text host			
SQL Full-text Filter Daemon Lau...			
Sql Server Telemetry Client			
Sql Server Telemetry Client			
Sql Server Telemetry Client			
SQL Server VSS Writer - 64 Bit			
SQL Server Windows NT - 64 Bit			
TCP/IP Ping Command			
VsHub.exe (32 bit)			
Windows Command Processor			
Windows Update			

PING.EXE

Type of file: Application (.EXE)

Description: TCP/IP Ping Command

Location: C:\Windows\System32

Size: 20.5 KB (20,992 bytes)

Size on disk: 24.0 KB (24,576 bytes)

Created: Saturday, January 27, 2018, 12:15:54 AM

Modified: Tuesday, October 28, 2014, 9:27:57 PM

Accessed: Saturday, January 27, 2018, 12:15:54 AM

Attributes: □ Read-only □ Hidden