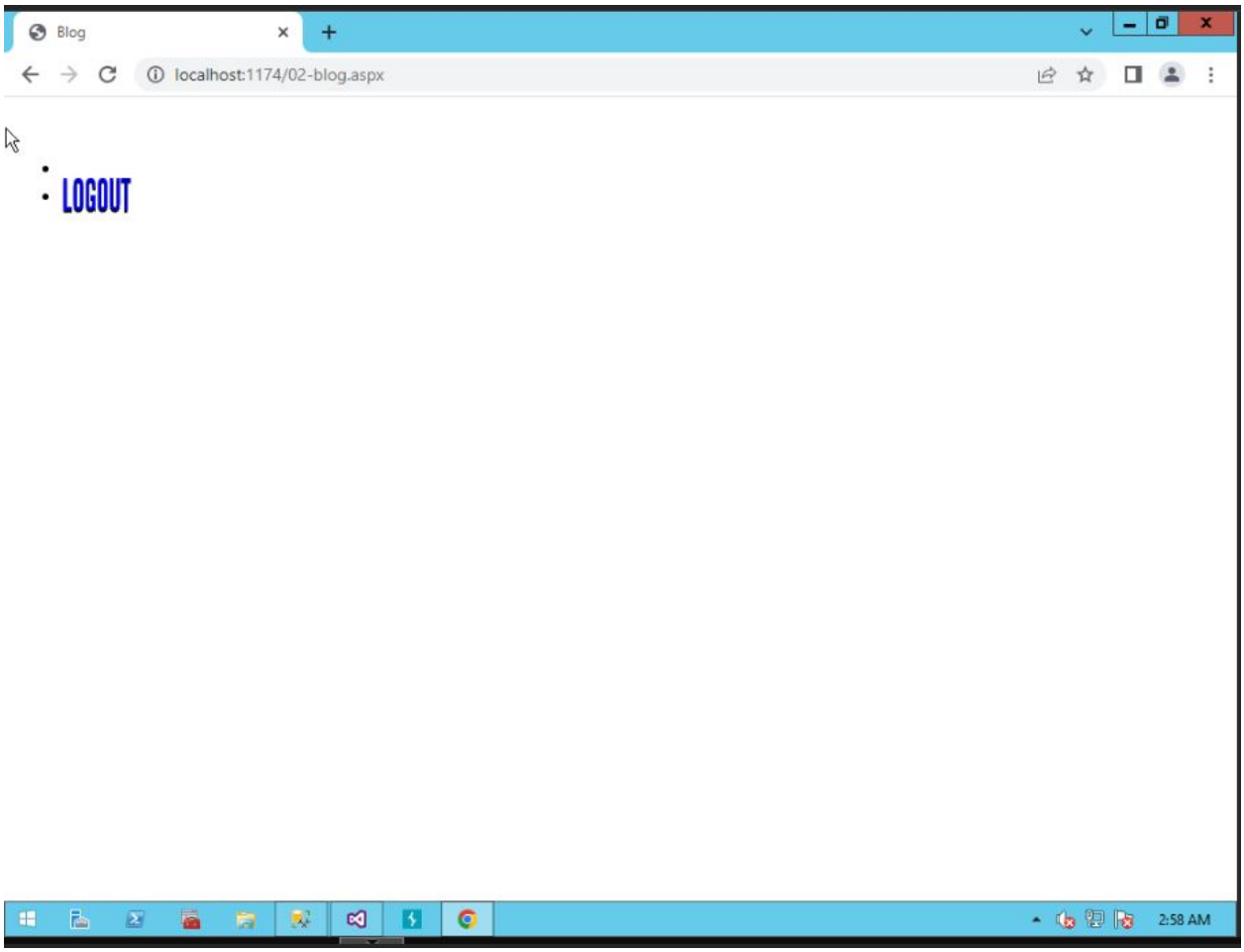
Assignment 3 – Database Attacks and Defense

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



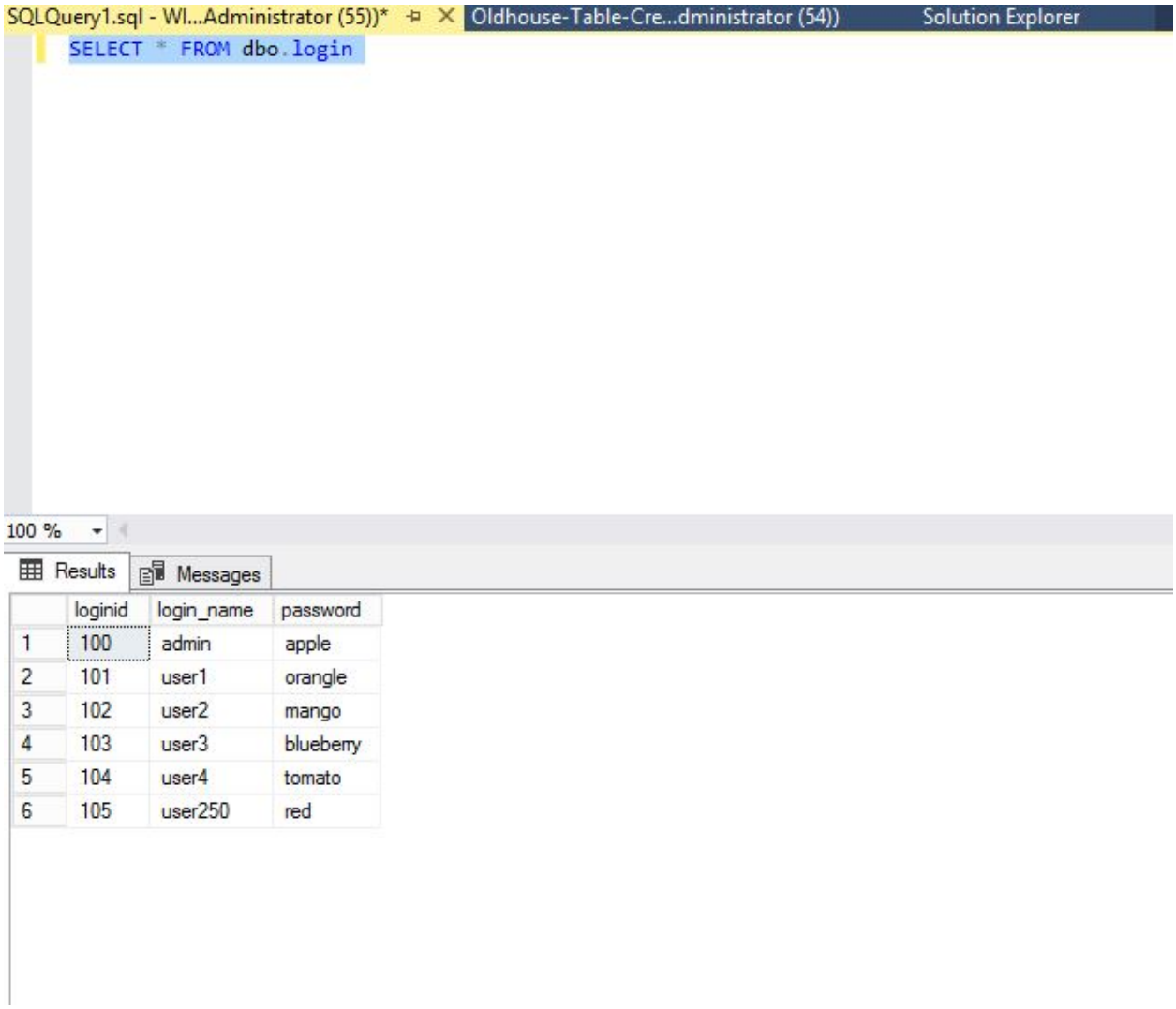
- **(Task # 2)** Enter the following injection in **Login name** box and make the Password box blank.

    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

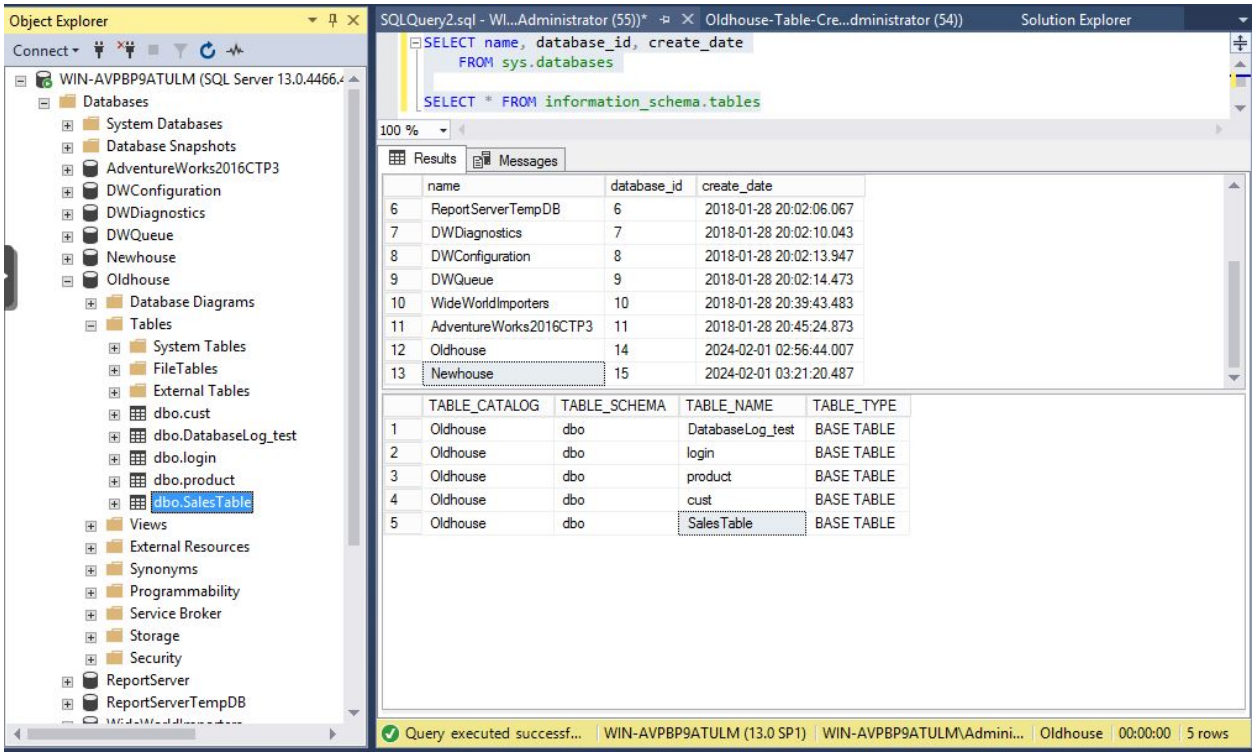
       WHERE login_name='admin'; INSERT INTO login VALUES ('user250', 'red');--
       AND login_password=''

2. **Task #2B**: Go to the SQL Server and confirm that the account (‘user250’, ‘red’) is indeed created in the login table. Provide a screenshot of the records in the table.



	loginid	login_name	password
1	100	admin	apple
2	101	user1	orangle
3	102	user2	mango
4	103	user3	blueberry
5	104	user4	tomato
6	105	user250	red

- **(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

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 2A-2E-94-82-B7-C8
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::30bd:7a57:a0ed:44e3%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.48(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 310801758
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-31-0A-87-2A-2E-94-82-B7-C8
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{9F9EB500-4E5B-4FF1-B937-037BB7970BD2}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   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.

QEMU machine emulators and t...	0%	1.4 MB
Runtime Broker	0%	2.2 MB
Sink to receive asynchronous ca...	0%	0.8 MB
Spooler SubSystem App	0%	2.2 MB
SQL Full Text host	0%	1.0 MB
SQL Full-text Filter Daemon Lau...	0%	0.6 MB
Sql Server Telemetry Client	0%	11.2 MB
Sql Server Telemetry Client	0%	12.5 MB
Sql Server Telemetry Client	0%	15.1 MB
SQL Server VSS Writer - 64 Bit	0%	1.0 MB
SQL Server Windows NT - 64 Bit	0%	1,101.7 MB
TCP/IP Ping Command	0%	0.5 MB
VsHub.exe (32 bit)	0%	16.1 MB
Windows Command Processor	0%	0.3 MB
Windows Update	0%	1.1 MB
WMI Provider Host	1.1%	4.4 MB