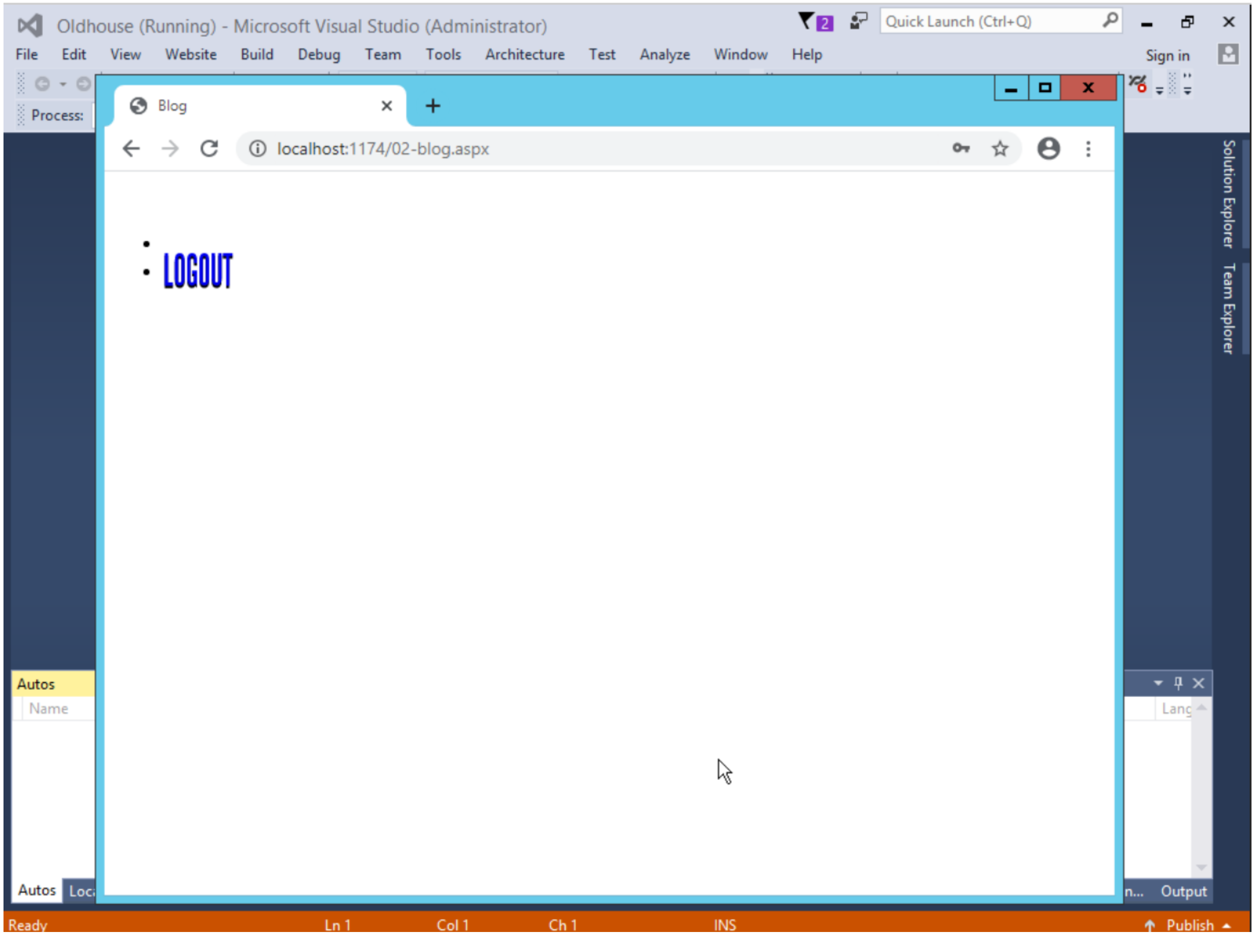
Assignment #4: Database Attacks and Defense

- This is an individual assignment, and is worth 20 points.
- The due date is Saturday, Feb 15th, 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.

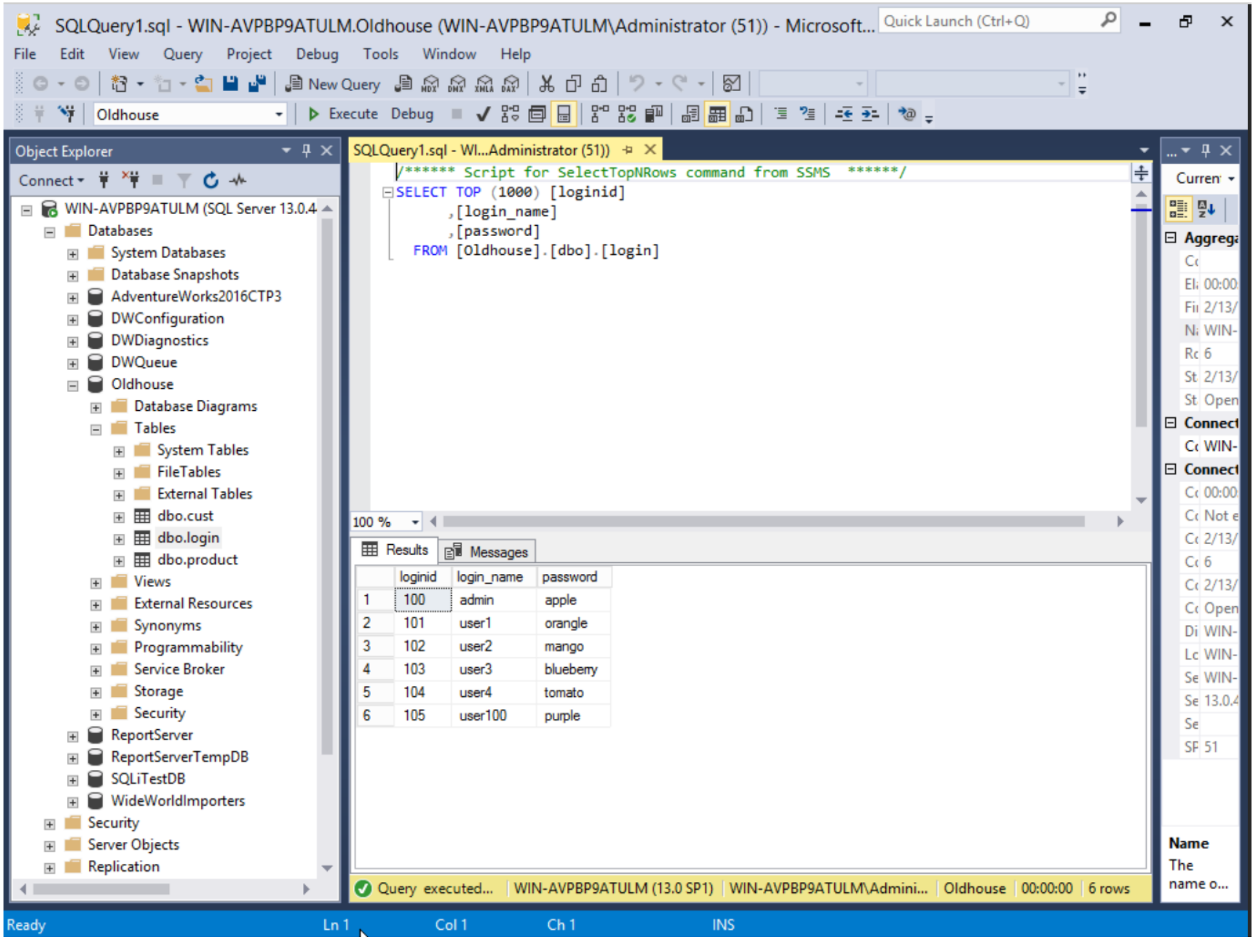


- **(Task # 2)** Enter the following injection in **Login name** box and make the Password box blank.

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 ('user100','purple');--

2. **Task #2B**: Go to the SQL Server and confirm that the account (‘user100’, ‘purple’) is indeed created in the login table. Provide a screenshot of the records in the table.



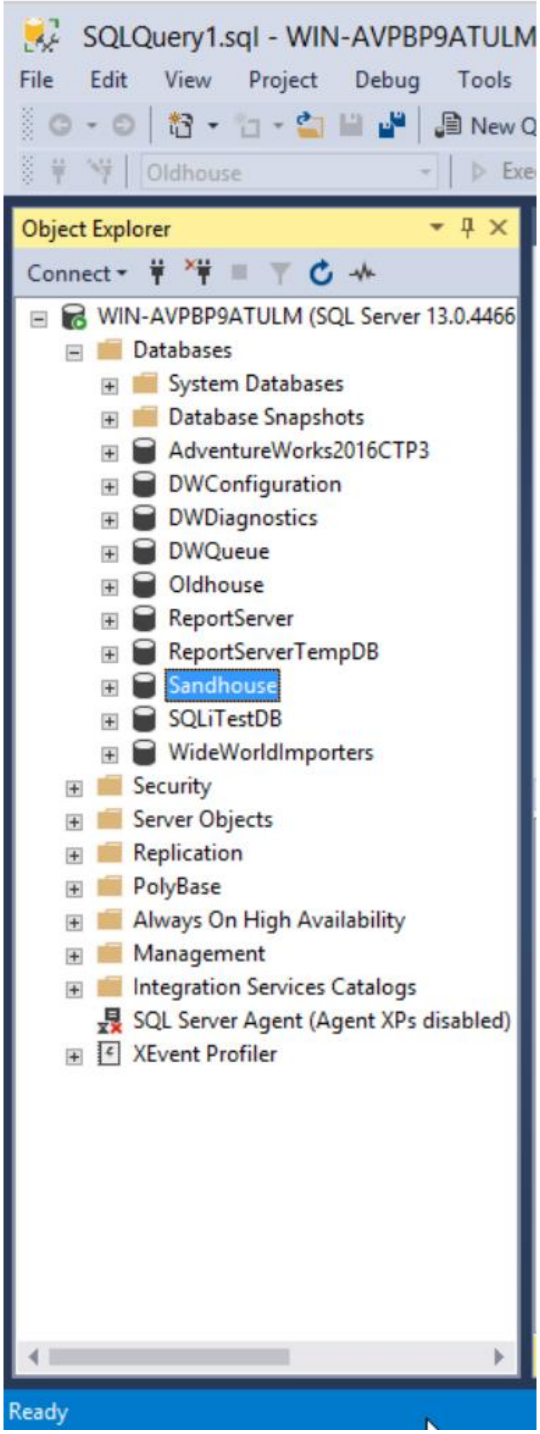
SQLQuery1.sql - WIN-AVPBP9ATULM.Oldhouse (WIN-AVPBP9ATULM\Administrator (51)) - Microsoft...

```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP (1000) [loginid]
      ,[login_name]
      ,[password]
  FROM [Oldhouse].[dbo].[login]
```

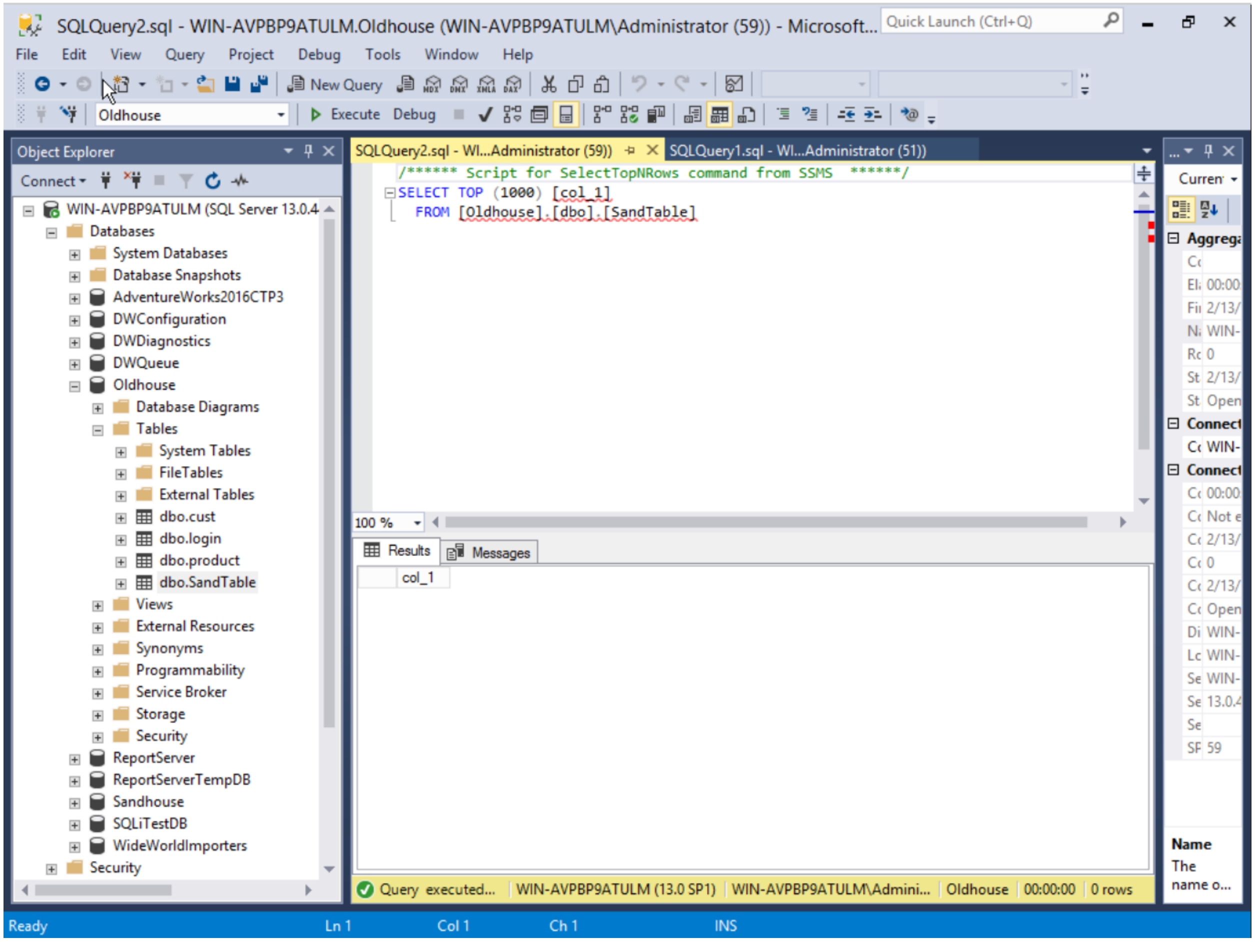
	loginid	login_name	password
1	100	admin	apple
2	101	user1	orangle
3	102	user2	mango
4	103	user3	blueberry
5	104	user4	tomato
6	105	user100	purple

Query executed... | WIN-AVPBP9ATULM (13.0 SP1) | WIN-AVPBP9ATULM\Admini... | Oldhouse | 00:00:00 | 6 rows

- **(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.



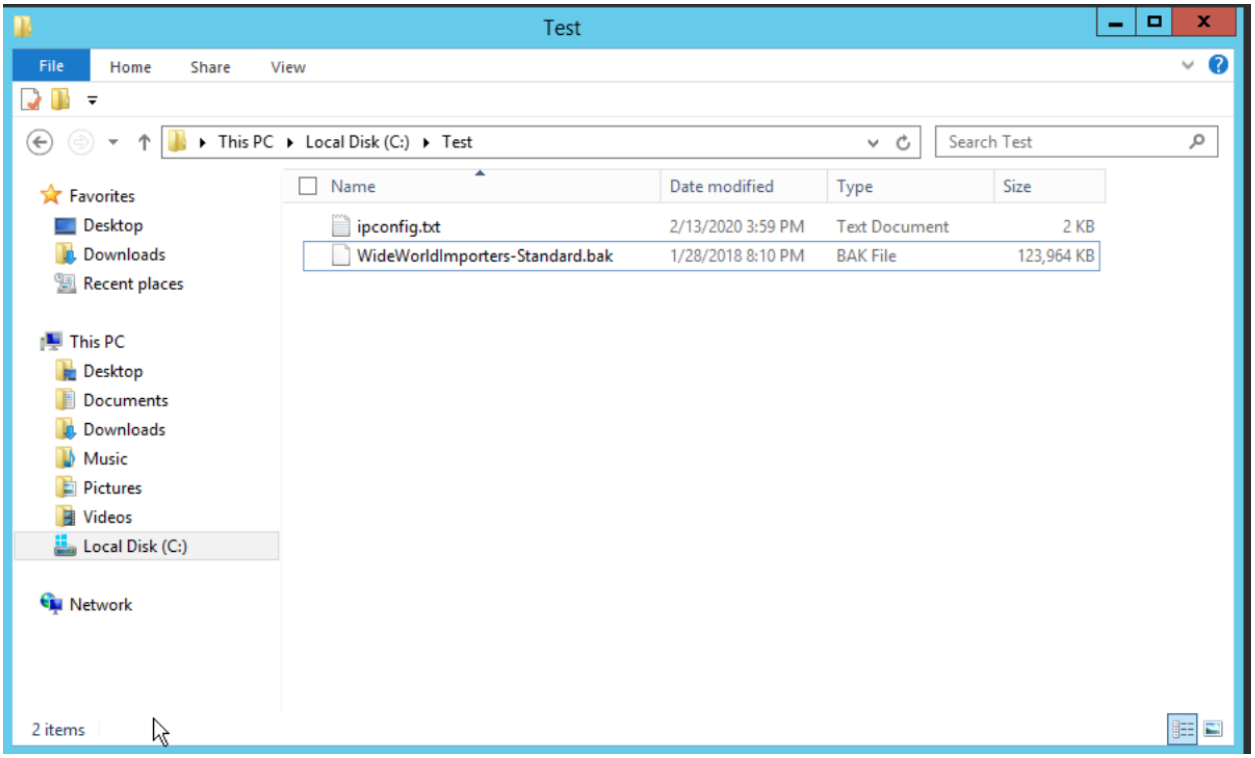
```
WIN-AVPBP9ATULM (SQL Server 13.0.4466
    Databases
        System Databases
        Database Snapshots
        AdventureWorks2016CTP3
        DWConfiguration
        DWDiagnostics
        DWQueue
        Oldhouse
        ReportServer
        ReportServerTempDB
        Sandhouse
        SQLiTestDB
        WideWorldImporters
    Security
    Server Objects
    Replication
    PolyBase
    Always On High Availability
    Management
    Integration Services Catalogs
    SQL Server Agent (Agent XPs disabled)
    XEvent Profiler
```



```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP (1000) [col_1]
  FROM [Oldhouse].[dbo].[SandTable]
```

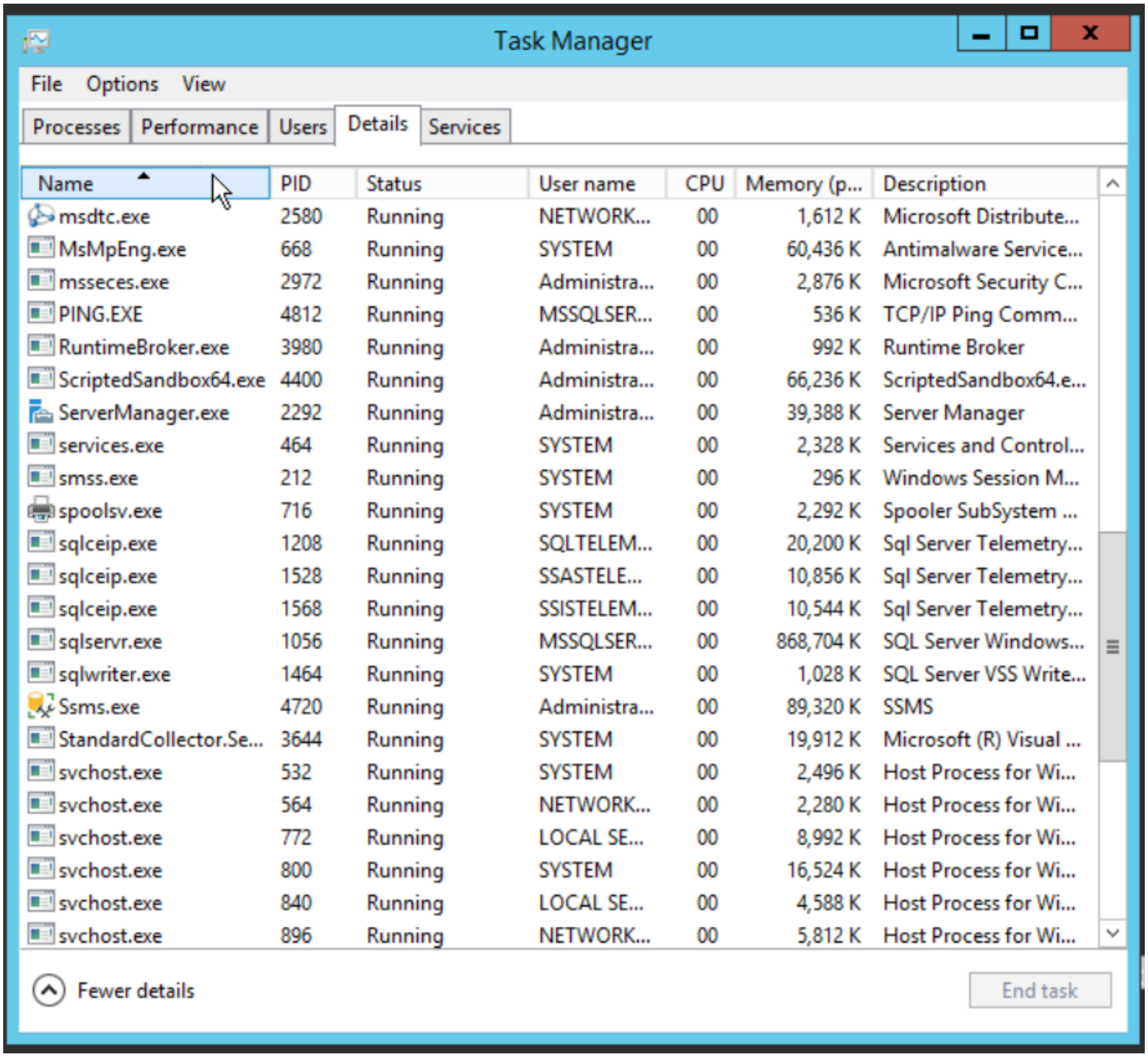
Query executed... | WIN-AVPBP9ATULM (13.0 SP1) | WIN-AVPBP9ATULM\Admini... | Oldhouse | 00:00:00 | 0 rows

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



Name	Date modified	Type	Size
ipconfig.txt	2/13/2020 3:59 PM	Text Document	2 KB
WideWorldImporters-Standard.bak	1/28/2018 8:10 PM	BAK File	123,964 KB

- **(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	PID	Status	User name	CPU	Memory (p...	Description
msdtc.exe	2580	Running	NETWORK...	00	1,612 K	Microsoft Distribute...
MsMpEng.exe	668	Running	SYSTEM	00	60,436 K	Antimalware Service...
msseces.exe	2972	Running	Administra...	00	2,876 K	Microsoft Security C...
PING.EXE	4812	Running	MSSQLSER...	00	536 K	TCP/IP Ping Comm...
RuntimeBroker.exe	3980	Running	Administra...	00	992 K	Runtime Broker
ScriptedSandbox64.exe	4400	Running	Administra...	00	66,236 K	ScriptedSandbox64.e...
ServerManager.exe	2292	Running	Administra...	00	39,388 K	Server Manager
services.exe	464	Running	SYSTEM	00	2,328 K	Services and Control...
smss.exe	212	Running	SYSTEM	00	296 K	Windows Session M...
spoolsv.exe	716	Running	SYSTEM	00	2,292 K	Spooler SubSystem ...
sqlceip.exe	1208	Running	SQLTELEM...	00	20,200 K	Sql Server Telemetry...
sqlceip.exe	1528	Running	SSASTELE...	00	10,856 K	Sql Server Telemetry...
sqlceip.exe	1568	Running	SSISTELEM...	00	10,544 K	Sql Server Telemetry...
sqlservr.exe	1056	Running	MSSQLSER...	00	868,704 K	SQL Server Windows...
sqlwriter.exe	1464	Running	SYSTEM	00	1,028 K	SQL Server VSS Write...
Ssms.exe	4720	Running	Administra...	00	89,320 K	SSMS
StandardCollector.Se...	3644	Running	SYSTEM	00	19,912 K	Microsoft (R) Visual ...
svchost.exe	532	Running	SYSTEM	00	2,496 K	Host Process for Wi...
svchost.exe	564	Running	NETWORK...	00	2,280 K	Host Process for Wi...
svchost.exe	772	Running	LOCAL SE...	00	8,992 K	Host Process for Wi...
svchost.exe	800	Running	SYSTEM	00	16,524 K	Host Process for Wi...
svchost.exe	840	Running	LOCAL SE...	00	4,588 K	Host Process for Wi...
svchost.exe	896	Running	NETWORK...	00	5,812 K	Host Process for Wi...