

CSE 2010 SECURE CODING
LAB SLOT –L23+L24
NAME-B.PRATYUSH
REGISTRATION NUMBER-19BCN7114
LAB EXPERIMENT 11

Lab experiment – Creating secure and safe executable

Download and install visual studio (recent edition)

Write a C++ code of your own to build an executable and run the same.

Download process explorer and verify the DEP & ASLR status

Enable software DEP, ASLR and SEH in the visual studio and rebuild the same executable

Again, verify the DEP & ASLR status in the process explorer

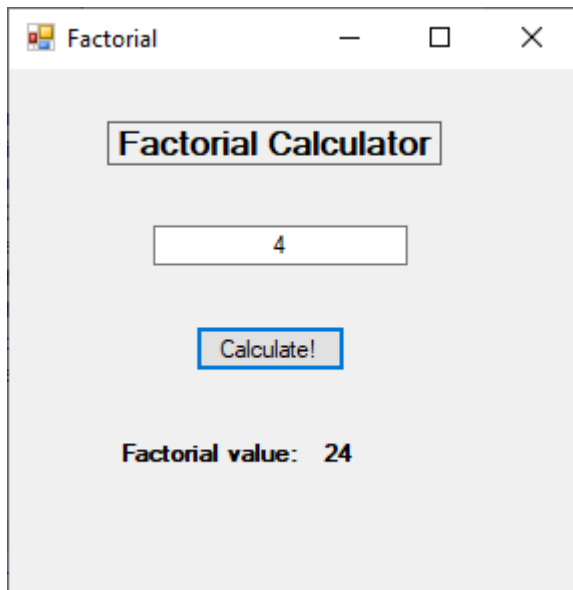
Report the same with separate screenshot - before and after enabling DEP & ASLR.

Happy Learning!!!

Experiment analysis:

1) Create an executable

Executable created: Factorial.exe



Select C++ as the language and open an empty CLR project and select Windows Form.

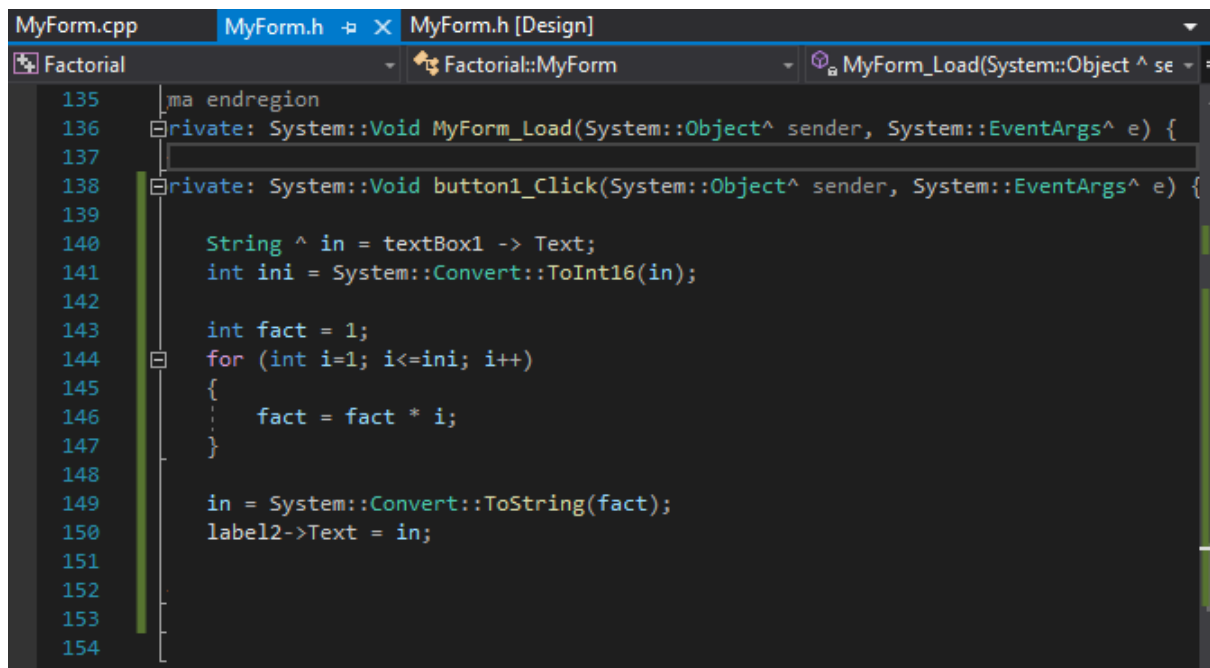
Then create the above GUI by adding labels, textbox and button and make the modifications accordingly.

MyForm.cpp

```
MyForm.cpp  MyForm.h  MyForm.h [Design]
Factorial   (Global Scope)  main(array<String^>^ args)
1  #include "MyForm.h"
2  using namespace System;
3  using namespace System::Windows::Forms;
4  [STAThread]
5  void main(array<String^>^ args)
6  {
7      Application::EnableVisualStyles();
8      Application::SetCompatibleTextRenderingDefault(false);
9      Factorial::MyForm form;
10     Application::Run(% form);
11 }
```

C++ code for the Gui

Now add the functionality to the label and button values and implement the factorial logic.



```
135     ma endregion
136     private: System::Void MyForm_Load(System::Object^ sender, System::EventArgs^ e) {
137
138     private: System::Void button1_Click(System::Object^ sender, System::EventArgs^ e) {
139
140         String ^ in = textBox1 -> Text;
141         int ini = System::Convert::ToInt16(in);
142
143         int fact = 1;
144         for (int i=1; i<=ini; i++)
145         {
146             fact = fact * i;
147         }
148
149         in = System::Convert::ToString(fact);
150         label1->Text = in;
151
152
153
154
155
```

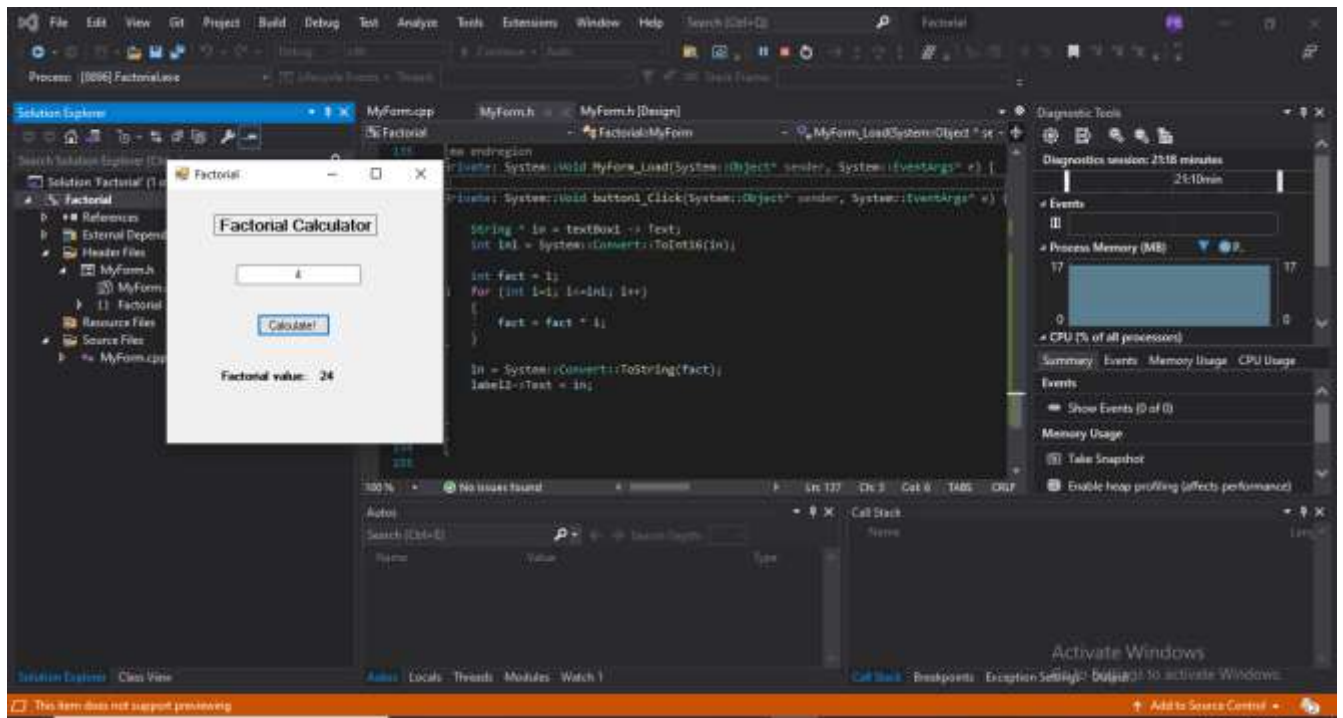
While making the form the code gets auto generated. Later click on particular control option and add functionality to it.

Right click on the Factorial in solution explorer and select “Properties”.

Select Linker and then Select System.

In Sub System option select Windows

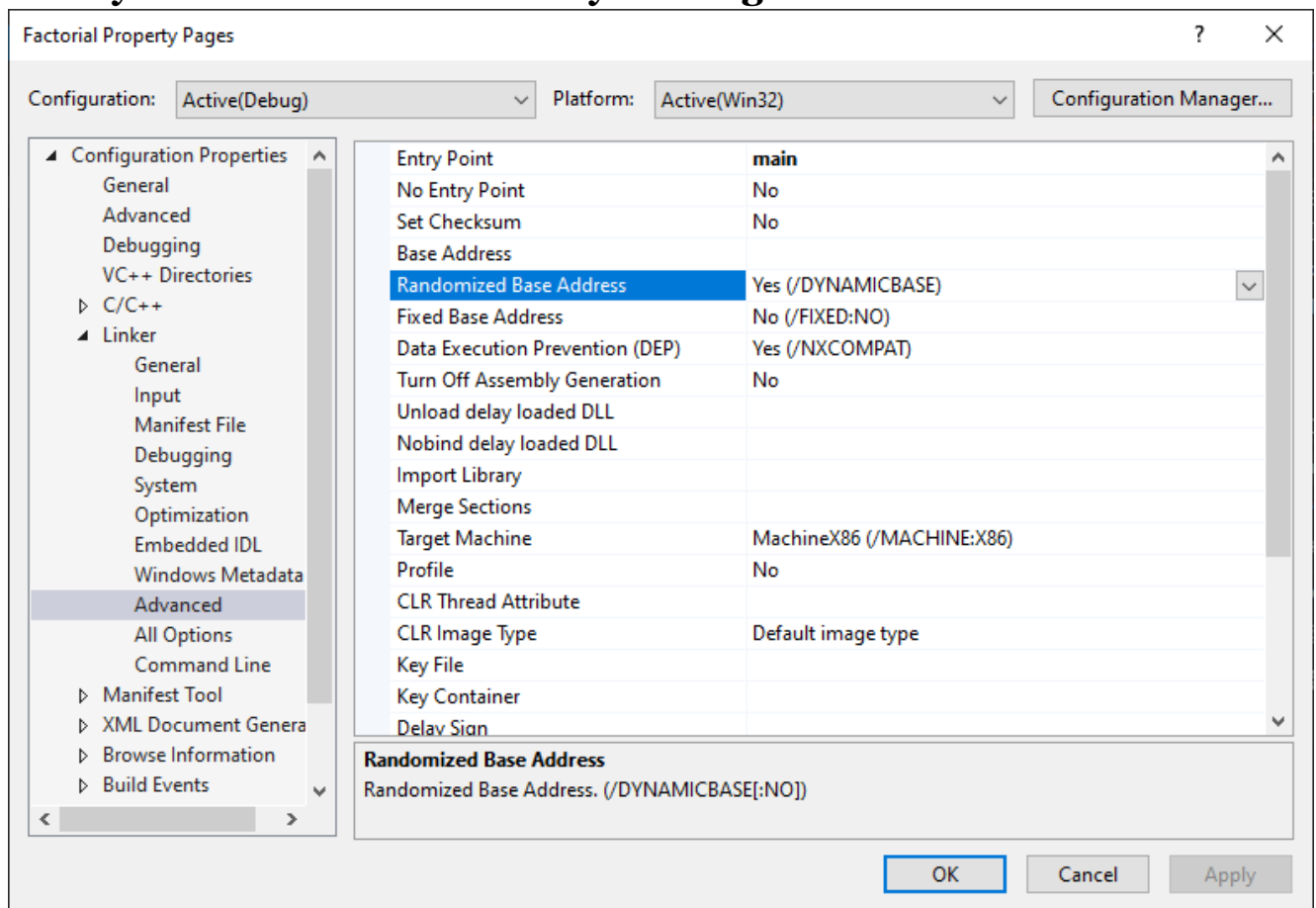
Then go to Advanced option and give “main” in the Entry point option.



TURNING ON DEP AND ASLR

- 2) Now open Process Explorer (Sysinternals) and check the DEP and ASLR status for Factorial.exe

Firstly let us check the status by turning on ASLR and DEP



Check Randomized base address and DEP and make sure it is YES

View Status in process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-2T9KQ2Lanovs]

File Options View Process Find Users Help

Process	Private Bytes	Working Set	PID	Description	Company Name	Version	Window Status	DEP	ASLR
csrss.exe	4,212 K	12,528 K	5452	Realtek HD Audio Manager	Realtek Semiconductor	1.0.0.1110		Enabled (permane...	ASLR
csrss.exe	5,952 K	6,032 K	2716	HD Audio Background Pro...	Realtek Semiconductor	1.0.0.281		Enabled (permane...	ASLR
csrss.exe	26,456 K	16,264 K	6332	Microsoft OneDrive	Microsoft Corporation	21.73.411.2		Enabled (permane...	ASLR
csrss.exe	16,000 K	2,536 K	3796	AnyDesk	AnyDesk Software GmbH	4.2.3.0		Enabled (permane...	ASLR
csrss.exe	6,776 K	372,280 K	247,228 K	Microsoft Visual Studio 2019	Microsoft Corporation	16.0.31313.75	Running	Enabled (permane...	ASLR
csrss.exe	40,380 K	35,260 K	10432	PerfWatson2.exe	Microsoft Corporation	16.0.31227.257		Enabled (permane...	ASLR
csrss.exe	36,836 K	19,900 K	6100	Microsoft ServiceHub Contro...	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	85,060 K	32,236 K	11356	ServiceHub SettingsHost.exe	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	56,152 K	20,396 K	3408	ServiceHub IdentityHost.exe	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	73,092 K	10,228 K	3676	ServiceHub VSDesktopPro...	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	70,640 K	10,432 K	8660	ServiceHub ThreadedWatCh...	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	422,212 K	10,744 K	15944	ServiceHub Host CLP.dll	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	120,444 K	20,964 K	2560	ServiceHub Host CLP.dll	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	50,676 K	16,216 K	3736	ServiceHub TestWorksho...	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	81,168 K	29,156 K	5556	ServiceHub DataWorksho...	Microsoft	2.7.348.34584		Enabled (permane...	ASLR
csrss.exe	8,960 K	7,488 K	2548	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	16.0.31228.75		Enabled (permane...	ASLR
csrss.exe	10,336 K	11,500 K	3936	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	16.0.31228.75		Enabled (permane...	ASLR
csrss.exe	10,300 K	10,044 K	3936				Running	Enabled (permane...	ASLR
csrss.exe	131,220 K	120,276 K	3312	ScriptedSandbox64.exe	Microsoft Corporation	16.0.31227.257		Enabled (permane...	ASLR
csrss.exe	4,180 K	4,220 K	4628	Sysinternals Process Explorer	Sysinternals - www.sysinte...	16.32.0.0		Enabled (permane...	ASLR
csrss.exe	30,516 K	15,380 K	1768	Sysinternals Process Explorer	Sysinternals - www.sysinte...	16.32.0.0	Running	Enabled (permane...	ASLR
csrss.exe	168,016 K	140,204 K	13460	Microsoft Word	Microsoft Corporation	16.0.3371.1206	Running	Enabled (permane...	ASLR
csrss.exe	3,636 K	11,744 K	1752	gdi32.dll	Intel Corporation	6.15.10.3032		Enabled (permane...	ASLR
csrss.exe	2,748 K	9,120 K	1940	gdi32.dll	Intel Corporation	6.15.10.3032		Enabled (permane...	ASLR
csrss.exe	3,096 K	10,224 K	2368					Enabled (permane...	ASLR
csrss.exe	1,204 K	2,236 K	6002	Java Update Scheduler	Oracle Corporation	9.0.0.0		Enabled (permane...	ASLR
csrss.exe	180,730 K	70,060 K	7560	Microsoft Teams	Microsoft Corporation	1.4.0.11161	Running	Enabled (permane...	ASLR
csrss.exe	129,368 K	12,348 K	2336	Microsoft Teams	Microsoft Corporation	1.4.0.11161		Enabled (permane...	ASLR
csrss.exe	17,388 K	15,028 K	4908	Microsoft Teams	Microsoft Corporation	1.4.0.11161		Enabled (permane...	ASLR
csrss.exe	34,292 K	2,668 K	3284	Microsoft Teams	Microsoft Corporation	1.4.0.11161		Enabled (permane...	ASLR
csrss.exe	434,096 K	138,560 K	7188	Microsoft Teams	Microsoft Corporation	1.4.0.11161		Enabled (permane...	ASLR
csrss.exe	11,820 K	9,244 K	7482	Microsoft Teams	Microsoft Corporation	1.4.0.11161		Enabled (permane...	ASLR
csrss.exe	77,420 K	27,232 K	7548	Microsoft Teams	Microsoft Corporation	1.4.0.11161		Enabled (permane...	ASLR
csrss.exe	190,136 K	27,116 K	6688	Microsoft Teams	Microsoft Corporation	1.4.0.11161		Enabled (permane...	ASLR
csrss.exe	83,640 K	104,168 K	6412	Microsoft Edge	Microsoft Corporation	90.0.619.58	Running	Enabled (permane...	ASLR
csrss.exe	6,256 K	1,864 K	7348	Microsoft Edge	Microsoft Corporation	90.0.619.58		Enabled (permane...	ASLR
csrss.exe	180,528 K	83,428 K	376	Microsoft Edge	Microsoft Corporation	90.0.619.58		Enabled (permane...	ASLR
csrss.exe	21,812 K	25,516 K	1892	Microsoft Edge	Microsoft Corporation	90.0.619.58		Enabled (permane...	ASLR

CPU Usage: 67.47% Commit Charge: 82.64% Processes: 153 Physical Usage: 84.84%

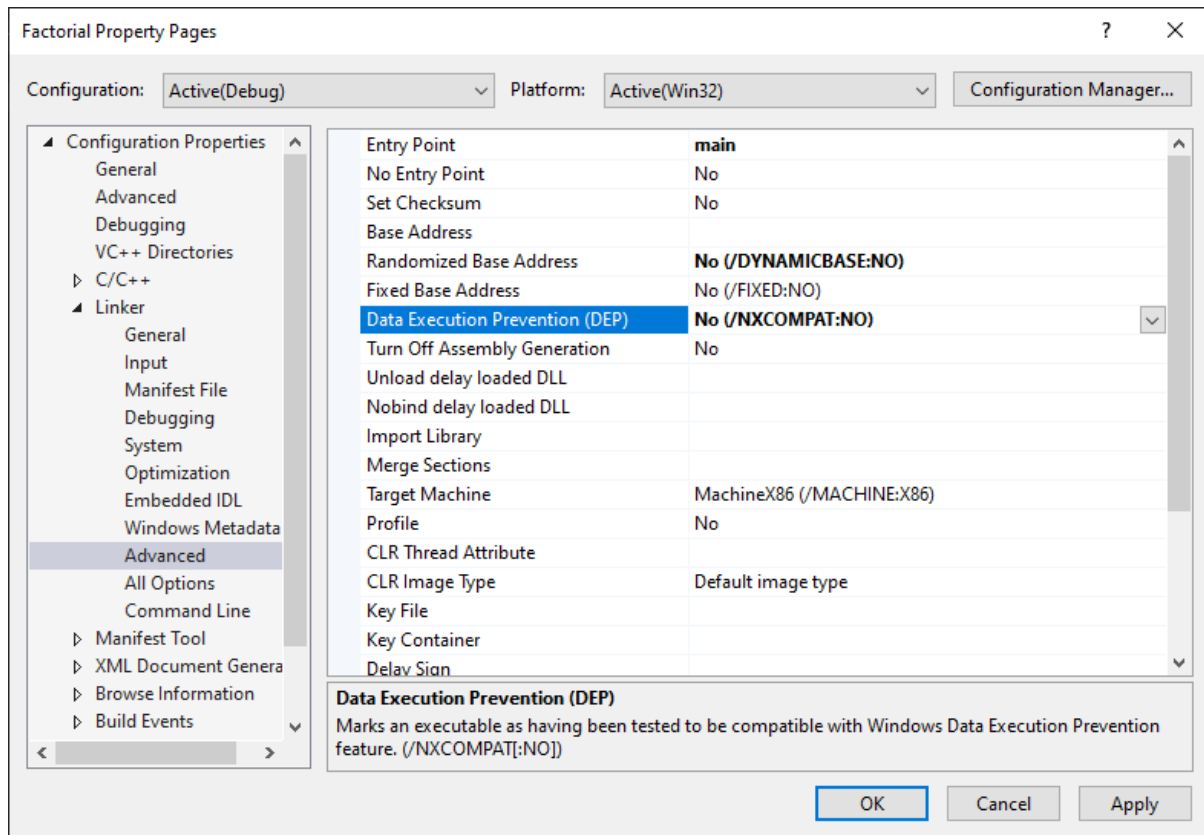
Factorial.exe status

conhost.exe	6,348 K	6,696 K	8936	Console Window Host	Microsoft Corporation	10.0.19041.964	Enabled (permane... ASLR
Factorial.exe	15,368 K	26,704 K	8896			Running	Enabled (permane... ASLR
ScriptedSandbox64.exe	14.87	119,712 K	148,468 K	9312 ScriptedSandbox64.exe	Microsoft Corporation	16.0.31227.257	Enabled (permane... ASLR
procexo.exe	4,180 K	11,188 K	4628	Sysinternals Process Explorer	Sysinternals - www.sysinte...	16.32.0.0	Enabled (permane... ASLR

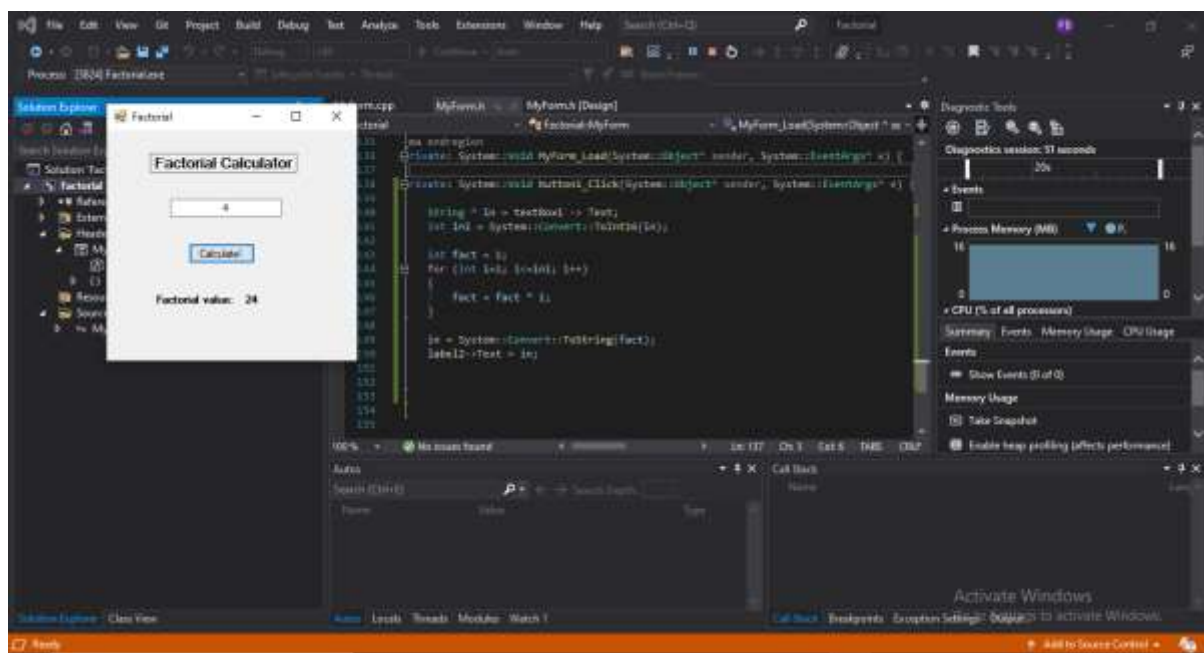
It is enabled

TURNING OFF ASLR AND DEP

Now let us disable the DEP and ASLR and see if it is reflecting in Process Explorer



Run the exe again



Check ASLR and DEP status

ServiceHub.DataWar...	1.5b	86,452 K	59,680 K	5556 ServiceHub.DataWarehouse...	Microsoft	2.7.349.34584	enabled (permane...	ASLR
vcpkgenv.exe	< 0.01	9,960 K	7,468 K	8948 Microsoft (R) Visual C++ Pac...	Microsoft Corporation	16.0.31229.75	Enabled (permane...	
MSBuild.exe		26,880 K	43,764 K	1196 MSBuild.exe	Microsoft Corporation	16.9.0.16703	Enabled (permane...	ASLR
conhost.exe		6,332 K	10,728 K	10276 Console Window Host	Microsoft Corporation	10.0.19041.964	Enabled (permane...	ASLR
Factorial.exe		15,304 K	27,136 K	5824			Running	Disabled (perman...
ScriptedSandbox64.exe	5.86	85,916 K	115,568 K	10584 ScriptedSandbox64.exe	Microsoft Corporation	16.0.31227.257	Enabled (permane...	ASLR
vcpkgenv.exe	0.01	19,320 K	29,012 K	8136 Microsoft (R) Visual C++ Pac...	Microsoft Corporation	16.0.31229.75	Enabled (permane...	
procexp.exe		4,180 K	420 K	4628 Sysinternals Process Explorer	Sysinternals - www.sysinter...	16.32.0.0	Enabled (permane...	ASLR
procexp64.exe	10.90	30,520 K	18,192 K	10760 Sysinternals Process Explorer	Sysinternals - www.sysinter...	16.32.0.0	Running	Enabled (permane...
Microsoft Word		179,144 K	107,608 K	11460 Microsoft Word	Microsoft Corporation	16.0.5211.1000	Running	Enabled (permane...

Here the DEP status is Disabled and ASLR status is off.