

# Secure Coding Lab - 11

Name: Charitha Bodapothula

Reg.No: 19BCN7005

Slot: L23+24

## Lab experiment – Creating secure and safe executable

**Download and install visual studio (recent edition)**

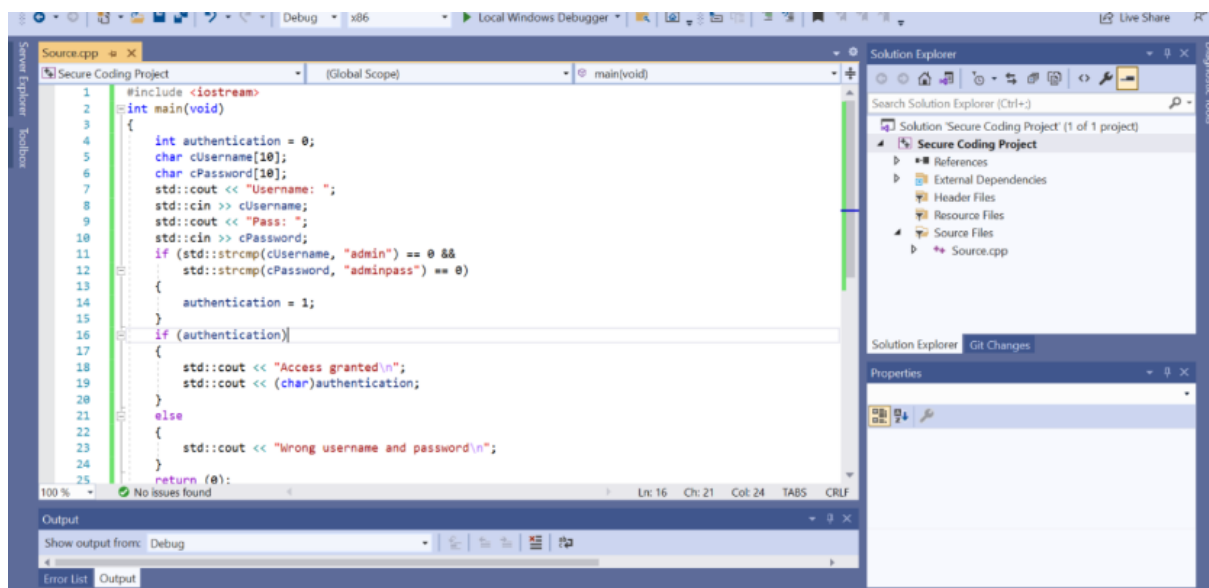
**Write a C++ code of your own to build an executable and run the same.**

**Download process explorer and verify the DEP & ASLR status**

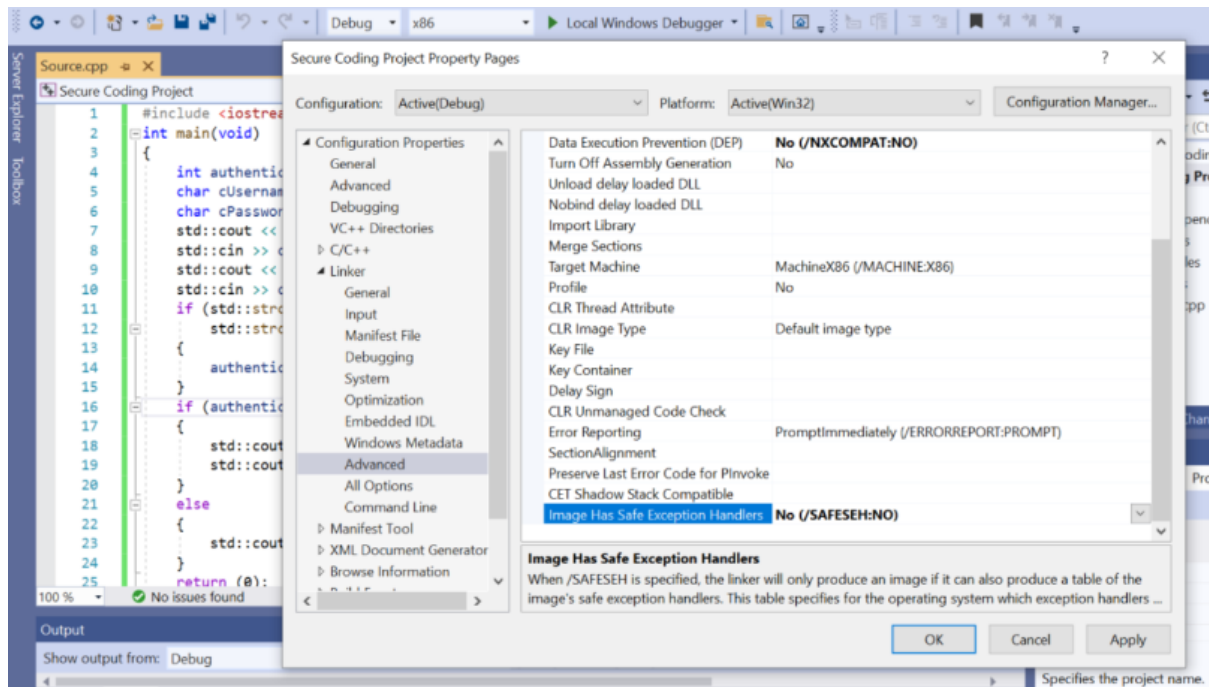
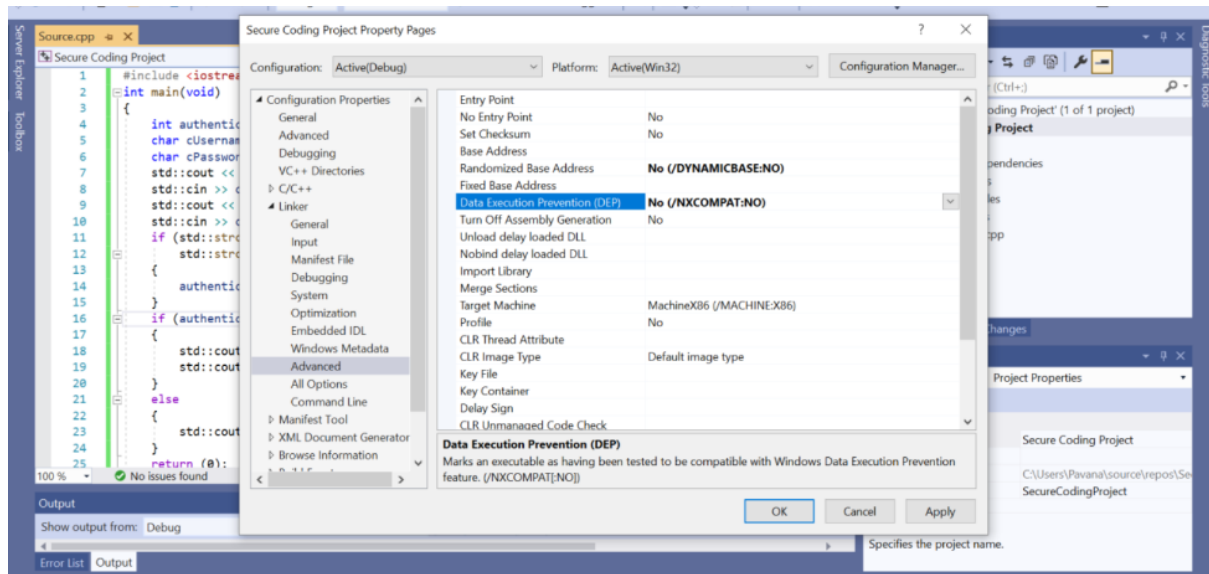
**Enable software DEP, ASLR and SEH in the visual studio and rebuild the same executable**

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

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



Disable DEP, ASLR and SEH



Install Process Explorer

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP
Interrupts	0.53	0 K	0 K	n/a	Hardware Interrupts and DPCs	n/a	n/a
smss.exe		1,072 K	468 K	592	Windows Session Manager	Microsoft Corporation	Enabled
Memory Compression	0.67	1,020 K	36,932 K	2856			Enabled
csrss.exe	< 0.01	2,264 K	3,240 K	760	Client Server Runtime Process	Microsoft Corporation	Enabled
wininit.exe		1,824 K	3,488 K	860	Windows Start-Up Application	Microsoft Corporation	Enabled
services.exe	< 0.01	7,980 K	9,216 K	936	Services and Controller app	Microsoft Corporation	Enabled
svchost.exe	0.12	25,976 K	34,832 K	644	Host Process for Windows S...	Microsoft Corporation	Enabled
dllhost.exe		3,752 K	5,564 K	19052	COM Surrogate	Microsoft Corporation	Enabled
TIWorker.exe		35,184 K	21,772 K	2116	Windows Modules Installer W...	Microsoft Corporation	Enabled
fodhelper.exe		1,408 K	2,244 K	9052	Features On Demand Helper	Microsoft Corporation	Enabled
WmiPrvSE.exe		3,900 K	7,996 K	17988	WMI Provider Host	Microsoft Corporation	Enabled
MoUsocoreWorker.exe		14,108 K	19,260 K	15428	MoUSO Core Worker Process	Microsoft Corporation	Enabled
McVulCtr.exe		8,728 K	4,732 K	22492	McAfee Vulnerability Scanner	McAfee, LLC	Enabled
StartMenuExperienceHos...		27,564 K	76,648 K	1892			Enabled
RuntimeBroker.exe		6,688 K	25,852 K	8284	Runtime Broker	Microsoft Corporation	Enabled
SearchApp.exe	0.53	2,07,364 K	2,60,256 K	11268	Search application	Microsoft Corporation	Enabled
SettingSynchost.exe	< 0.01	11,088 K	31,800 K	23436	Host Process for Setting Syn...	Microsoft Corporation	Enabled
RuntimeBroker.exe		12,940 K	39,656 K	8700	Runtime Broker	Microsoft Corporation	Enabled
YourPhone.exe	Susp...	25,848 K	18,516 K	15972	YourPhone	Microsoft Corporation	Enabled
LockApp.exe	Susp...	13,732 K	46,328 K	16412	LockApp.exe	Microsoft Corporation	Enabled
RuntimeBroker.exe		10,608 K	35,868 K	9888	Runtime Broker	Microsoft Corporation	Enabled
TextInputHost.exe		13,044 K	45,464 K	16860		Microsoft Corporation	Enabled
RuntimeBroker.exe	< 0.01	3,024 K	15,160 K	10628	Runtime Broker	Microsoft Corporation	Enabled
dllhost.exe	0.02	6,624 K	14,396 K	18368	COM Surrogate	Microsoft Corporation	Enabled
RuntimeBroker.exe		7,016 K	25,232 K	20968	Runtime Broker	Microsoft Corporation	Enabled
Cortana.exe	Susp...	31,240 K	58,984 K	19732	Cortana	Microsoft Corporation	Enabled
RuntimeBroker.exe		4,616 K	22,744 K	15880	Runtime Broker	Microsoft Corporation	Enabled
ApplicationFrameHost.exe		24,468 K	40,752 K	3696	Application Frame Host	Microsoft Corporation	Enabled
WinStore.App.exe	Susp...	18,764 K	2,332 K	2124	Store	Microsoft Corporation	Enabled
RuntimeBroker.exe	<						>

Enable DEP and ASLR in the process

Select Columns

Process Network

Process GPU

Handle

DLL

NET

Status Bar

Process Image

Process Performance

Process I/O

Select the columns that will appear on the Process view of Process Explorer.

☒ Process Name
 ☐ Window Title

☒ PID (Process Identifier)
 ☐ Window Status

☐ User Name
 ☐ Session

☒ Description
 ☐ Command Line

☒ Company Name
 ☐ Comment

☐ Verified Signer
 ☐ Autostart Location

☐ Version
 ☐ VirusTotal

☐ Image Path
 ☒ DEP Status

☐ Image Type (64 vs 32-bit)
 ☐ Integrity Level

☐ Package Name
 ☐ Virtualized

☐ DPI Awareness
 ☒ ASLR Enabled

☐ Protection
 ☐ UI Access

☐ Control Flow Guard
 ☐ Enterprise Context

OK

Cancel

DEP status of the project shows disabled



Username: