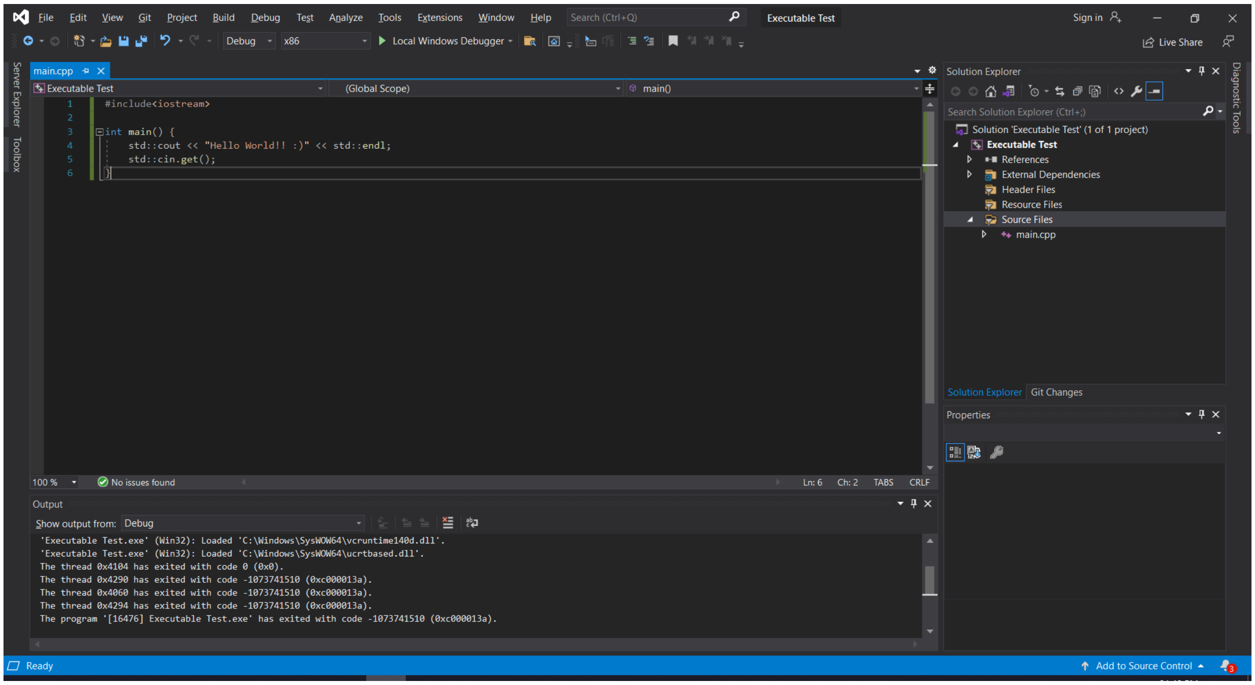
Secure Coding | Lab 11

by prof. Sibi Chakkaravarthy

Sk Saddam Hossain
18BCN7143

Download and install visual studio (recent edition)

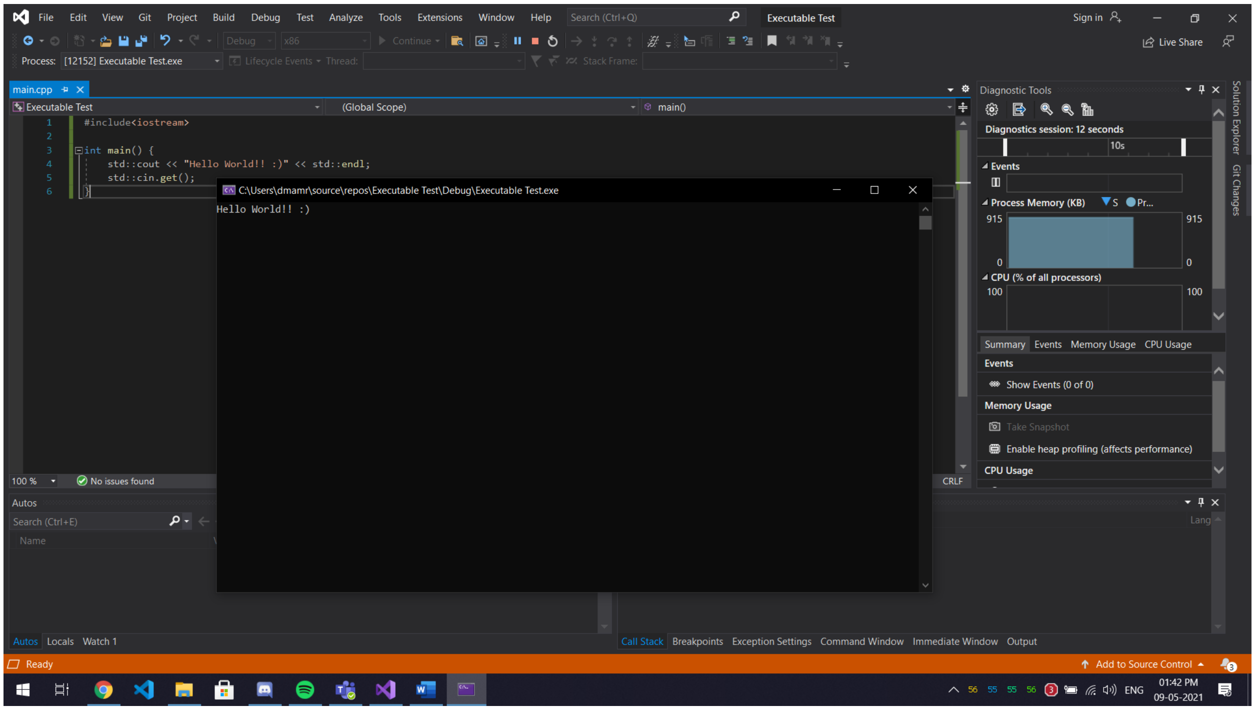
Write a C++ code of your own to build an executable and run the same.



```cpp
#include<iostream>

int main() {
	std::cout << "Hello World!! :)" << std::endl;
	std::cin.get();
}
```

```
'Executable Test.exe' (Win32): Loaded 'C:\Windows\SysWOW64\vcruntime140d.dll'.
'Executable Test.exe' (Win32): Loaded 'C:\Windows\SysWOW64\ucrtbased.dll'.
The thread 0x4104 has exited with code 0 (0x0).
The thread 0x4290 has exited with code -1073741510 (0xc000013a).
The thread 0x4060 has exited with code -1073741510 (0xc000013a).
The thread 0x4294 has exited with code -1073741510 (0xc000013a).
The program '[16476] Executable Test.exe' has exited with code -1073741510 (0xc000013a).
```



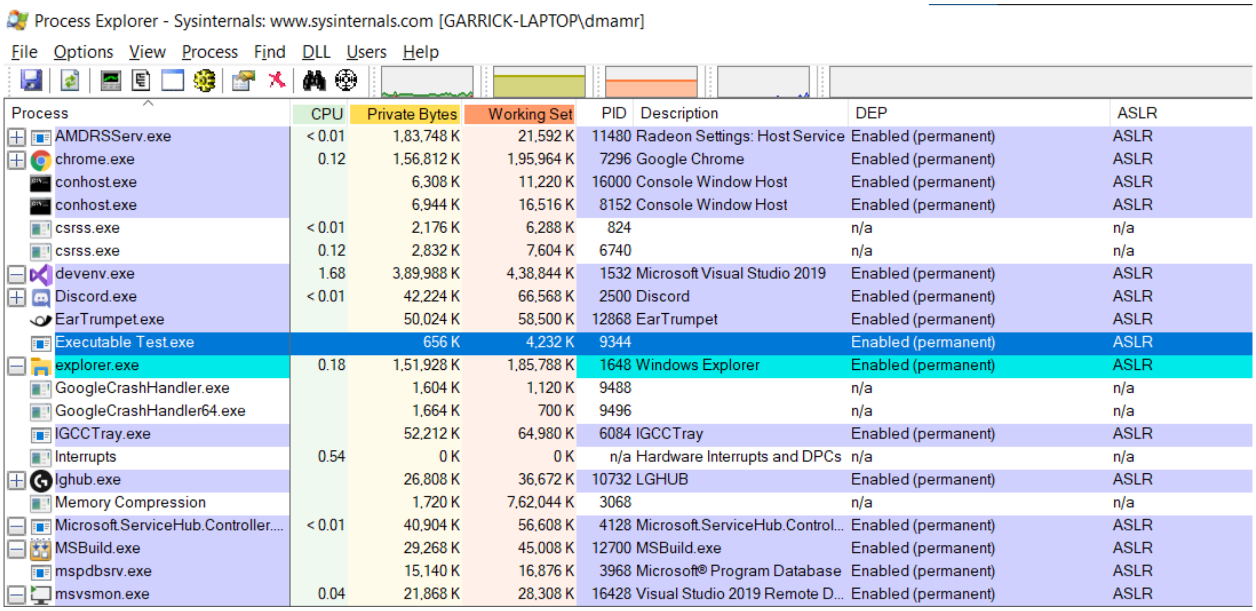
```
#include<iostream>

int main() {
    std::cout << "Hello World!! :)" << std::endl;
    std::cin.get();
}
```

C:\Users\dmamr\source\repos\Executable Test\Debug\Executable Test.exe

```
Hello World!! :)
```

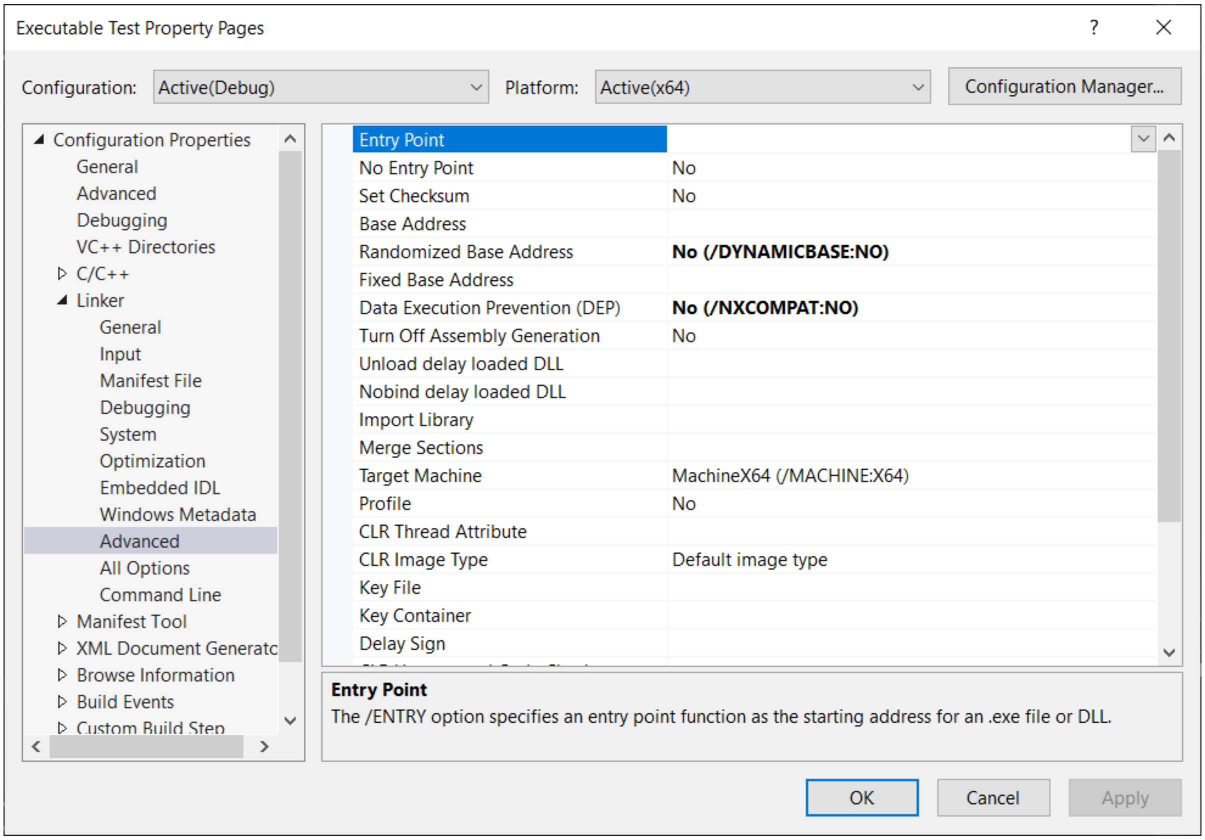
Download process explorer and verify the DEP & ASLR status


Process Explorer - Sysinternals: www.sysinternals.com [GARRICK-LAPTOP\dmamr]
File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	DEP	ASLR
AMDRSServ.exe	< 0.01	1,83,748 K	21,592 K	11480	Radeon Settings: Host Service	Enabled (permanent)	ASLR
chrome.exe	0.12	1,56,812 K	1,95,964 K	7296	Google Chrome	Enabled (permanent)	ASLR
conhost.exe		6,308 K	11,220 K	16000	Console Window Host	Enabled (permanent)	ASLR
conhost.exe		6,944 K	16,516 K	8152	Console Window Host	Enabled (permanent)	ASLR
csrss.exe	< 0.01	2,176 K	6,288 K	824		n/a	n/a
csrss.exe	0.12	2,832 K	7,604 K	6740		n/a	n/a
devenv.exe	1.68	3,89,988 K	4,38,844 K	1532	Microsoft Visual Studio 2019	Enabled (permanent)	ASLR
Discord.exe	< 0.01	42,224 K	66,568 K	2500	Discord	Enabled (permanent)	ASLR
EarTrumpet.exe		50,024 K	58,500 K	12868	EarTrumpet	Enabled (permanent)	ASLR
Executable Test.exe		656 K	4,232 K	9344		Enabled (permanent)	ASLR
explorer.exe	0.18	1,51,928 K	1,85,788 K	1648	Windows Explorer	Enabled (permanent)	ASLR
GoogleCrashHandler.exe		1,604 K	1,120 K	9488		n/a	n/a
GoogleCrashHandler64.exe		1,664 K	700 K	9496		n/a	n/a
IGCCTray.exe		52,212 K	64,980 K	6084	IGCCTray	Enabled (permanent)	ASLR
Interrupts	0.54	0 K	0 K	n/a	Hardware Interrupts and DPCs	n/a	n/a
lghub.exe		26,808 K	36,672 K	10732	LGHUB	Enabled (permanent)	ASLR
Memory Compression		1,720 K	7,62,044 K	3068		n/a	n/a
Microsoft.ServiceHub.Controller....	< 0.01	40,904 K	56,608 K	4128	Microsoft.ServiceHub.Control...	Enabled (permanent)	ASLR
MSBuild.exe		29,268 K	45,008 K	12700	MSBuild.exe	Enabled (permanent)	ASLR
mspdbsrv.exe		15,140 K	16,876 K	3968	Microsoft® Program Database	Enabled (permanent)	ASLR
msvsmon.exe	0.04	21,868 K	28,308 K	16428	Visual Studio 2019 Remote D...	Enabled (permanent)	ASLR

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

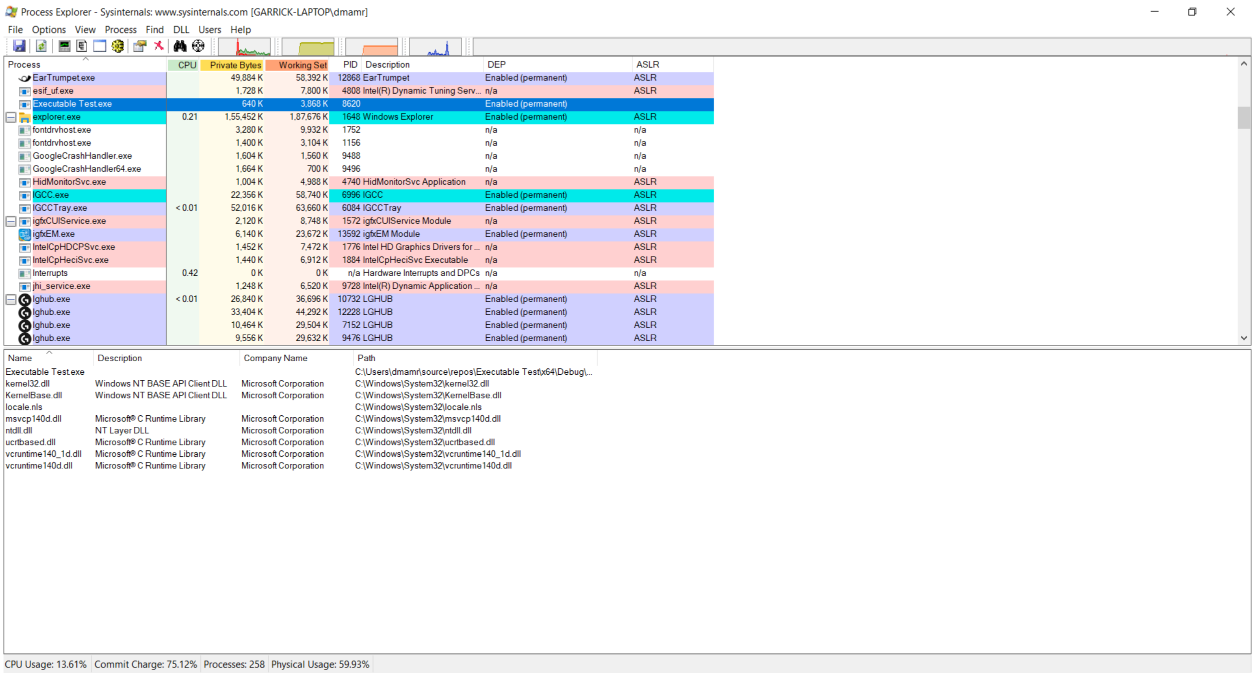
Project > properties > configuration properties > linker



Configuration: Active(Debug) Platform: Active(x64)

Entry Point	
No Entry Point	No
Set Checksum	No
Base Address	
Randomized Base Address	**No (/DYNAMICBASE:NO)**
Fixed Base Address	
Data Execution Prevention (DEP)	**No (/NXCOMPAT:NO)**
Turn Off Assembly Generation	No
Unload delay loaded DLL	
Nobind delay loaded DLL	
Import Library	
Merge Sections	
Target Machine	MachineX64 (/MACHINE:X64)
Profile	No
CLR Thread Attribute	
CLR Image Type	Default image type
Key File	
Key Container	
Delay Sign	

Entry Point
The /ENTRY option specifies an entry point function as the starting address for an .exe file or DLL.



Process Explorer - Sysinternals: www.sysinternals.com [GARRICK-LAPTOP\dmamr]
File
Options
View
Process
Find
DLL
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	DEP	ASLR
EarTrumpet.exe		49,884 K	58,392 K	12868	EarTrumpet	Enabled (permanent)	ASLR
esif_uf.exe		1,728 K	7,800 K	4808	Intel(R) Dynamic Tuning Serv...	n/a	ASLR
Executable Test.exe		640 K	3,868 K	8620		Enabled (permanent)	
explorer.exe	0.21	1,55,452 K	1,87,676 K	1648	Windows Explorer	Enabled (permanent)	ASLR
fontdrvhost.exe		3,280 K	9,932 K	1752		n/a	n/a
fontdrvhost.exe		1,400 K	3,104 K	1156		n/a	n/a
GoogleCrashHandler.exe		1,604 K	1,560 K	9488		n/a	n/a
GoogleCrashHandler64.exe		1,664 K	700 K	9496		n/a	n/a
HidMonitorSvc.exe		1,004 K	4,988 K	4740	HidMonitorSvc Application	n/a	ASLR
IGCC.exe		22,356 K	58,740 K	6996	IGCC	Enabled (permanent)	ASLR
IGCCTray.exe	< 0.01	52,016 K	63,660 K	6084	IGCCTray	Enabled (permanent)	ASLR
igfxCUIService.exe		2,120 K	8,748 K	1572	igfxCUIService Module	n/a	ASLR
igfxEM.exe		6,140 K	23,672 K	13592	igfxEM Module	Enabled (permanent)	ASLR
IntelCpHDCPSvc.exe		1,452 K	7,472 K	1776	Intel HD Graphics Drivers for ...	n/a	ASLR
IntelCpHeciSvc.exe		1,440 K	6,912 K	1884	IntelCpHeciSvc Executable	n/a	ASLR
Interrupts	0.42	0 K	0 K	n/a	Hardware Interrupts and DPCs	n/a	n/a
jhi_service.exe		1,248 K	6,520 K	9728	Intel(R) Dynamic Application ...	n/a	ASLR
lghub.exe	< 0.01	26,840 K	36,696 K	10732	LGHUB	Enabled (permanent)	ASLR
lghub.exe		33,404 K	44,292 K	12228	LGHUB	Enabled (permanent)	ASLR
lghub.exe		10,464 K	29,504 K	7152	LGHUB	Enabled (permanent)	ASLR
lghub.exe		9,556 K	29,632 K	9476	LGHUB	Enabled (permanent)	ASLR

Name	Description	Company Name	Path
Executable Test.exe			C:\Users\dmamr\source\repos\Executable Test\x64\Debug\...
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
locale.nls			C:\Windows\System32\locale.nls
msvcp140d.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp140d.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll
ucrtbased.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\ucrtbased.dll
vcruntime140_1d.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\vcruntime140_1d.dll
vcruntime140d.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\vcruntime140d.dll

CPU Usage: 13.61% Commit Charge: 75.12% Processes: 258 Physical Usage: 59.93%

By Default, in project properties, DEP and ASLR properties are enabled and even upon disabling them, DEP is still in affect