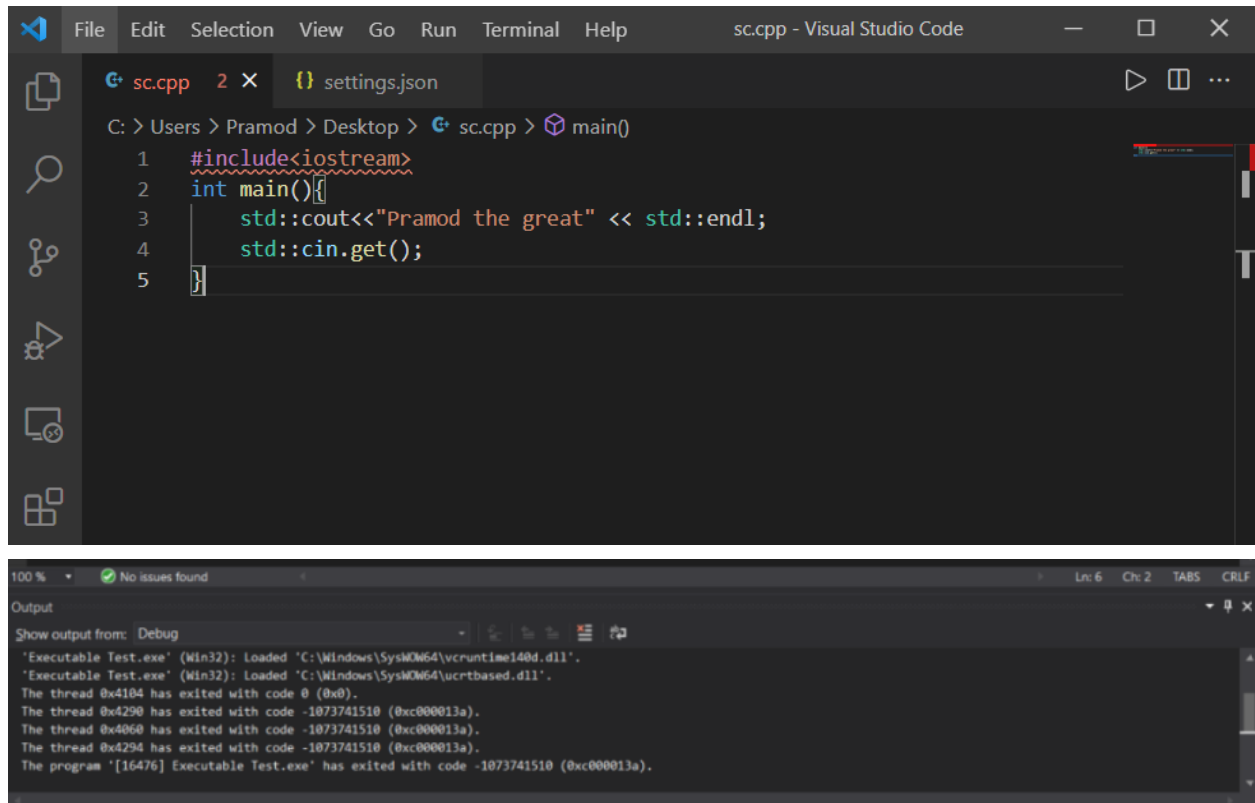


LAB-11: SECURE CODING

N. Satya Pramod
18BCE7293

Step 1:

Install visual studio and execute a C++ script.



The screenshot shows the Visual Studio Code editor with a C++ file named `sc.cpp`. The code is as follows:

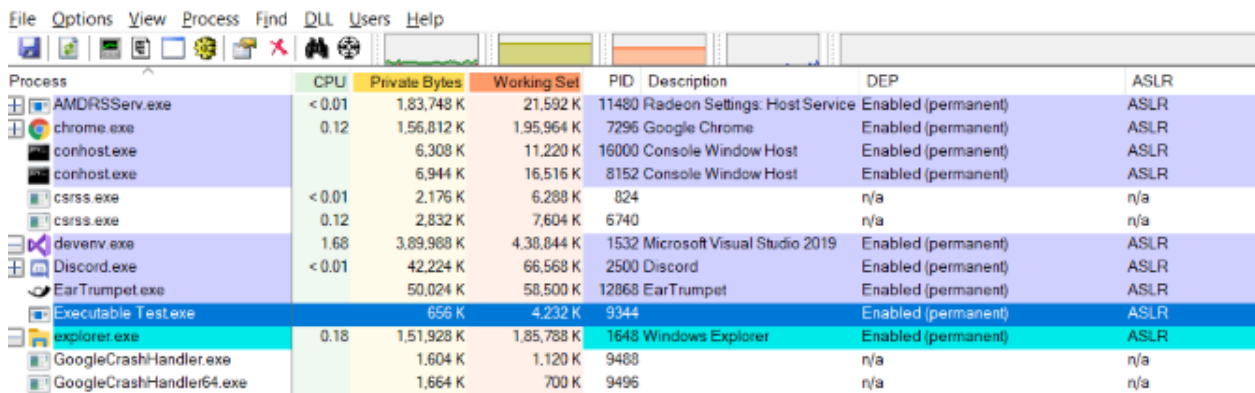
```
1 #include<iostream>
2 int main(){
3     std::cout<<"Pramod the great" << std::endl;
4     std::cin.get();
5 }
```

Below the editor, the Output window shows the debug output:

```
'Executable Test.exe' (Win32): Loaded 'C:\Windows\System64\vcruntime140d.dll'.
'Executable Test.exe' (Win32): Loaded 'C:\Windows\System64\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).
```

Step 2:

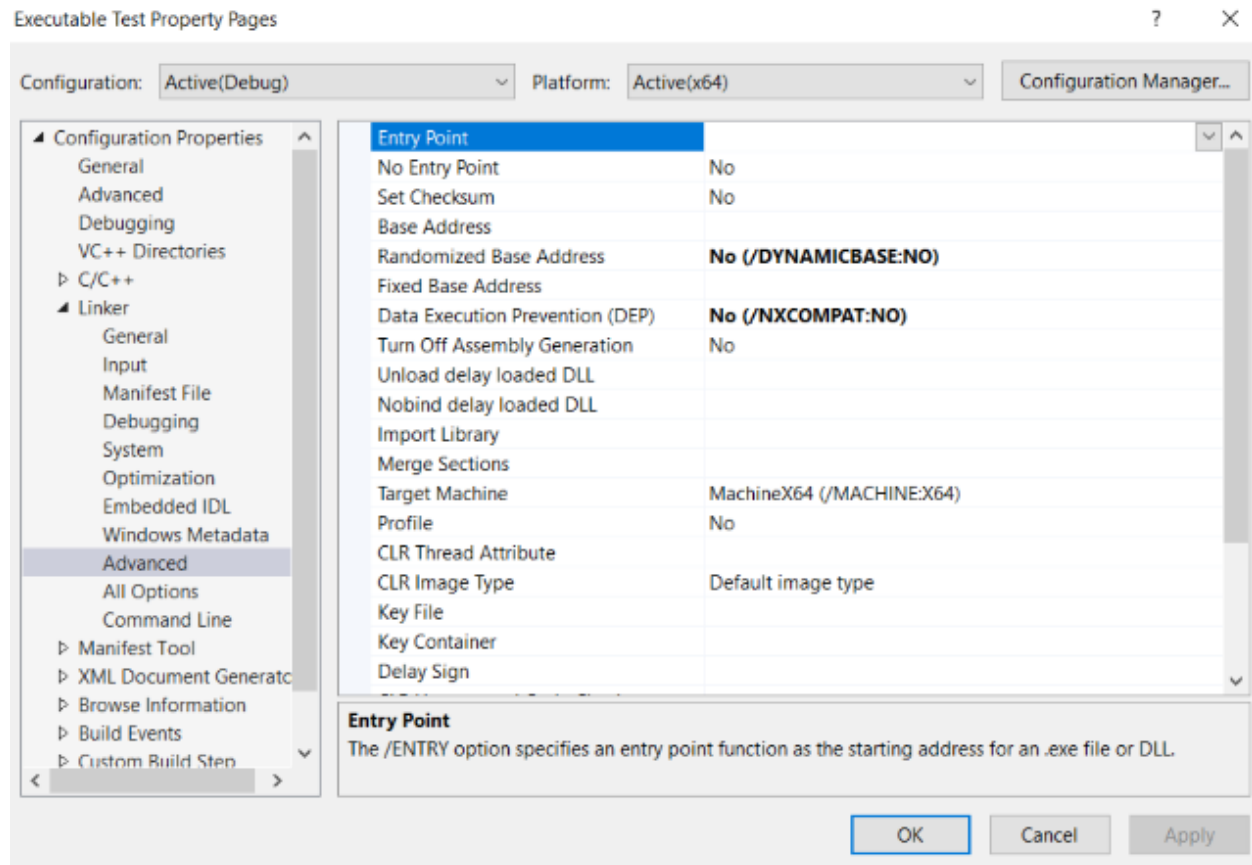
Download process explorer to verify the DEP and ASLR status.



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	12068	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

Step 3:

Disable software DEP, ASLR, and SEH in the visual studio.



Process Explorer - Sysinternals: www.sysinternals.com [GARRICK-LAPTOP\dname]

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	DEP	ASLR
csrss.exe		49,804 K	58,362 K	12868	csrss.exe	Enabled (permanent)	ASLR
csrss.exe		1,728 K	7,800 K	4808	csrss.exe	Enabled (permanent)	ASLR
csrss.exe		640 K	3,060 K	9620	csrss.exe	Enabled (permanent)	ASLR
explorer.exe	0.21	1,55,452 K	1,07,676 K	1648	Windows Explorer	Enabled (permanent)	ASLR
fontdrvhost.exe		3,280 K	8,932 K	1752	fontdrvhost.exe	n/a	n/a
fontdrvhost.exe		1,408 K	3,184 K	1156	fontdrvhost.exe	n/a	n/a
GoogleCrashHandler.exe		1,604 K	1,600 K	9410	GoogleCrashHandler.exe	n/a	n/a
GoogleCrashHandler.exe		1,664 K	700 K	9416	GoogleCrashHandler.exe	n/a	n/a
HostMonitorSvc.exe		1,004 K	4,988 K	4380	HostMonitorSvc Application	n/a	ASLR
ISCC.exe		22,396 K	58,740 K	5996	ISCC	Enabled (permanent)	ASLR
ISCCTray.exe	< 0.01	52,516 K	63,680 K	6004	ISCCTray	Enabled (permanent)	ASLR
lgblService.exe		2,120 K	8,748 K	1572	lgblService Module	n/a	ASLR
lgblService.exe		6,140 K	23,672 K	13932	lgblService Module	Enabled (permanent)	ASLR
IntelCpHDCPSvc.exe		1,452 K	3,472 K	1776	Intel HD Graphics Drivers for ...	n/a	ASLR
IntelCpHDCPSvc.exe		1,440 K	6,912 K	1804	IntelCpHDCPSvc Executable	n/a	ASLR
Interrupts	0.42	0 K	0 K	n/a	Hardware Interrupts and DPCs	n/a	n/a
ISCC.exe	< 0.01	1,248 K	6,520 K	9728	ISCC	n/a	ASLR
lgblService.exe		25,840 K	36,696 K	10732	lgblService	Enabled (permanent)	ASLR
lgblService.exe		33,434 K	44,262 K	12228	lgblService	Enabled (permanent)	ASLR
lgblService.exe		13,464 K	29,564 K	7152	lgblService	Enabled (permanent)	ASLR
lgblService.exe		9,556 K	29,632 K	9476	lgblService	Enabled (permanent)	ASLR

Name	Description	Company Name	Path
Executable Test.exe	Executable Test.exe	Microsoft Corporation	C:\Users\dname\source\repos\Executable Test\obj\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	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\locale.nls
mscrt140d.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\mscrt140d.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

Here DEP is still running even after DEP and ASLR properties are disabled.