

CSE2010 LAB-11

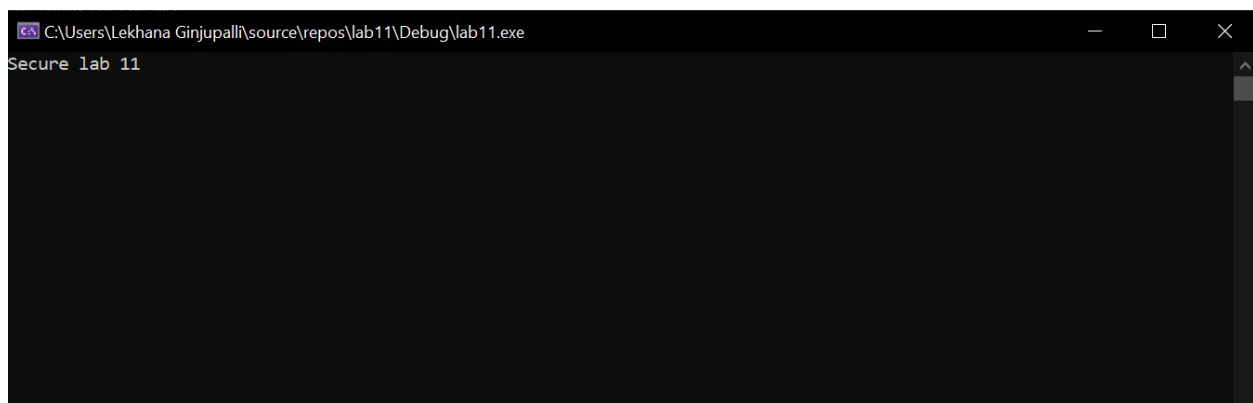
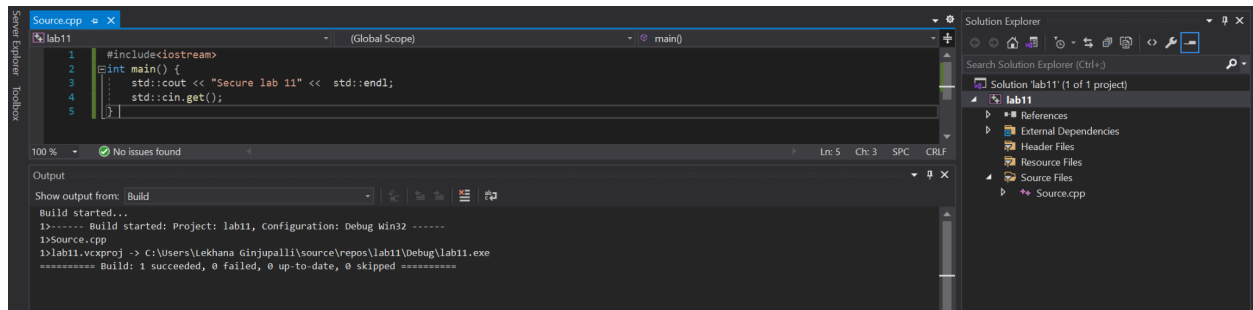
G.Lekhana devasena

18BCE7207

Create a cpp code and build an executable on visual studio

Cpp code:

```
#include<iostream>
int main() {
    std::cout << "Secure lab 11" << std::endl;
    std::cin.get();
}
```



DEP and ASLR status in process explorer:-

vcpkgsvr.exe	< 0.01	43,108 K	10,220 K	10630	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
VsDebugConsole.exe		1,124 K	5,988 K	13456	Visual Studio Debugger Cons...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		7,188 K	16,724 K	14368	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
lab11.exe		680 K	4,332 K	2660			Disabled (permane...	
mspdbsrv.exe		15,588 K	17,964 K	10284	Microsoft® Program Database	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		1,232 K	6,144 K	13324	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
wpscloudsvr.exe	0.01	54,208 K	76,936 K	6964	WPS Office service program f...	Zhuhai Kingsoft Office Soft...	Enabled (permane...	ASLR
wpscenter.exe	0.02	50,864 K	77,420 K	3612	WPS Office service program f...	Zhuhai Kingsoft Office Soft...	Enabled (permane...	ASLR

Here DEP is disabled.

Enabling dEP,ASLR AND SEH in project properties:-

Configuration: Active(Debug) Platform: Active(Win32) Configuration Manager...

Configuration Properties

- General
- Advanced
- Debugging
- VC++ Directories
- C/C++
- Linker
 - General
 - Input
 - Manifest File
 - Debugging
 - System
 - Optimization
 - Embedded IDL
 - Windows Metadata
 - Advanced
 - All Options
 - Command Line
- Manifest Tool
- XML Document Generator
- Browse Information

Look for options or switches:

Profile

Profile	No
Profile Guided Database	\$(OutDir)\$(TargetName).pgd
Randomized Base Address	Yes (/DYNAMICBASE)
References	
Register Output	No
SectionAlignment	
Set Checksum	No
Show Progress	Not Set
Specify Section Attributes	
Stack Commit Size	
Stack Reserve Size	
Strip Private Symbols	
SubSystem	Console (/SUBSYSTEM:CONSOLE)
Suppress Startup Banner	Yes (/NOLOGO)
Swap Run From CD	No

Randomized Base Address

Randomized Base Address. (/DYNAMICBASE[:NO])

OK Cancel Apply

Configuration: Active(Debug) Platform: Active(Win32) Configuration Manager...

Configuration Properties

- General
- Advanced
- Debugging
- VC++ Directories
- C/C++
- Linker
 - General
 - Input
 - Manifest File
 - Debugging
 - System
 - Optimization
 - Embedded IDL
 - Windows Metadata
 - Advanced
 - All Options
 - Command Line
- Manifest Tool
- XML Document Generator
- Browse Information

Look for options or switches:

Add Module to Assembly

Additional Dependencies kernel32.lib;user32.lib;gdi32.lib;winspool.lib;comdlg32.lib;adv...

Additional Library Directories

Additional Manifest Dependencies

Additional Options

Allow Isolation Yes

Assembly Link Resource

Base Address

CET Shadow Stack Compatible

CLR Image Type Default image type

CLR Thread Attribute

CLR Unmanaged Code Check

Create Hot Patchable Image

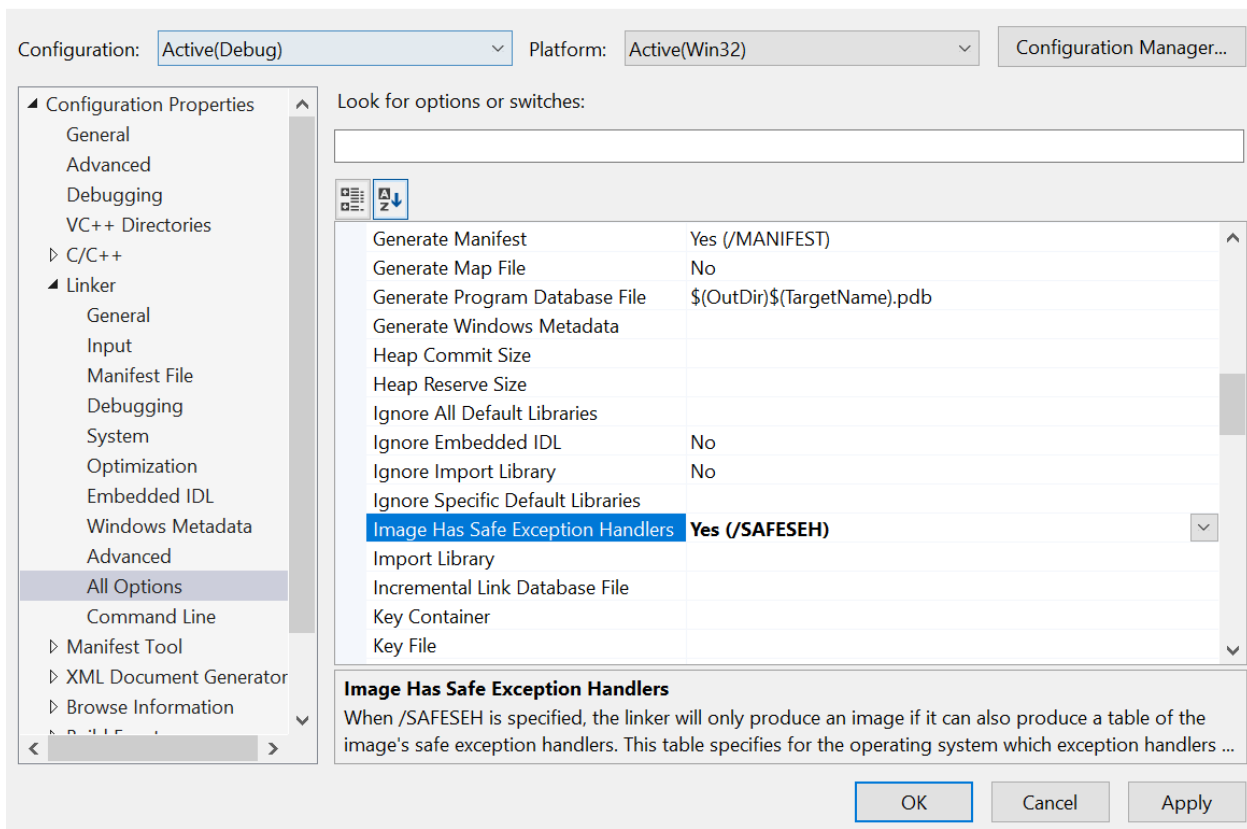
Data Execution Prevention (DEP) Yes (/NXCOMPAT)

Debuggable Assembly

Data Execution Prevention (DEP)

Marks an executable as having been tested to be compatible with Windows Data Execution Prevention feature. (/NXCOMPAT[:NO])

OK Cancel Apply



Now rebuild and run the project. Verify the status in process explorer:-

devenv.exe	3.32	2,08,192 K	3,33,472 K	6512	Microsoft Visual Studio 2019	Microsoft Corporation	Enabled (permane...	ASLR
PerfWatson2.exe	0.01	44,428 K	66,460 K	3616	PerfWatson2.exe	Microsoft Corporation	Enabled (permane...	ASLR
Microsoft.ServiceHub.Contr...	0.01	36,292 K	52,168 K	15732	Microsoft.ServiceHub.Controll...	Microsoft	Enabled (permane...	ASLR
ServiceHub.IdentityHost.e...	0.02	38,316 K	64,612 K	4320	ServiceHub.IdentityHost.exe	Microsoft	Enabled (permane...	ASLR
ServiceHub.SettingsHost...	0.01	40,376 K	66,388 K	8580	ServiceHub.SettingsHost.exe	Microsoft	Enabled (permane...	ASLR
ServiceHub.VSDetoured...	0.03	44,604 K	75,544 K	7072	ServiceHub.VSDetouredHost...	Microsoft	Enabled (permane...	ASLR
ServiceHub.Host.CLR.x86...	0.05	35,828 K	56,508 K	10748	ServiceHub.Host.CLR.x86	Microsoft	Enabled (permane...	ASLR
ServiceHub.ThreadedWait...	0.01	51,408 K	77,644 K	14516	ServiceHub.ThreadedWaitDi...	Microsoft	Enabled (permane...	ASLR
ServiceHub.Host.CLR.x86...	0.01	41,580 K	77,488 K	13348	ServiceHub.Host.CLR.x86	Microsoft	Enabled (permane...	ASLR
ServiceHub.TestWindowS...	0.03	50,216 K	67,432 K	8356	ServiceHub.TestWindowStor...	Microsoft	Enabled (permane...	ASLR
ServiceHub.DataWarehou...	1.63	70,940 K	87,916 K	13344	ServiceHub.DataWarehouse...	Microsoft	Enabled (permane...	ASLR
vcpkgssrv.exe	< 0.01	43,092 K	16,052 K	13268	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	
MSBuild.exe	0.01	28,544 K	43,732 K	12072	MSBuild.exe	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		6,336 K	11,028 K	5760	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
VsDebugConsole.exe		1,116 K	6,004 K	13808	Visual Studio Debugger Cons...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		7,180 K	16,708 K	8432	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
lab11.exe		768 K	4,424 K	5716			Enabled (permane...	ASLR