

SECURE CODING LAB

LAB-11

SLOT-L39+L40

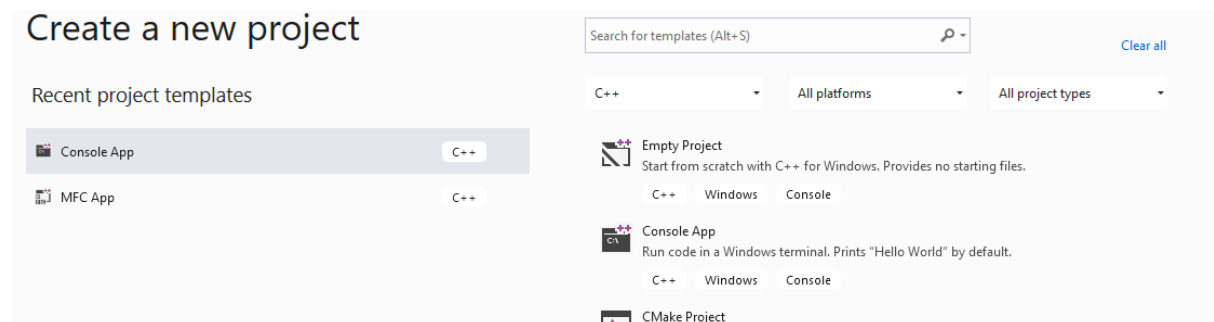
18BCN7128

SEGU NAIMISHA

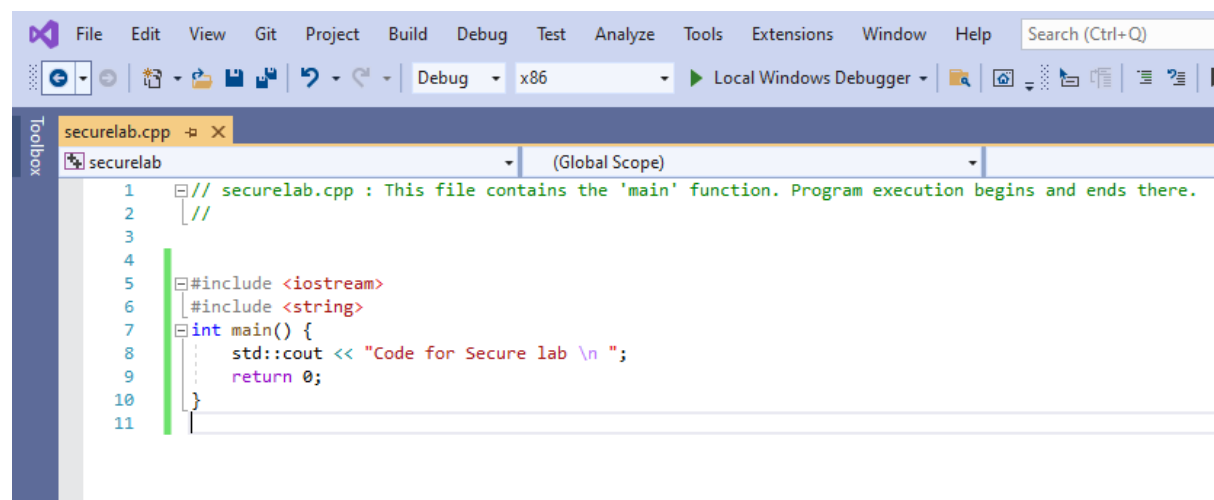
Question: Creating secure and safe executable

Sol:

Download and installing visual studio



C++ code



Run and executing the code:

```
Microsoft Visual Studio Debug Console

Code for Secure lab

C:\Users\Naimisha Segu\source\repos\securelab\Debug\securelab.exe (process 9272) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .
```

Download process explorer

Process Explorer - Sysinternals: www.sysinternals.com [NAIMISHA\Naimisha Segu]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		19,808 K	61,636 K	96		
System Idle Process		60 K	8 K	0		
System	1.86	212 K	5,400 K	4		
Interrupts	2.34	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,164 K	376 K	420		
Memory Compression	< 0.01	2,372 K	1,20,488 K	2324		
csrss.exe	0.06	1,892 K	4,192 K	632		
wininit.exe		1,360 K	4,440 K	728		
services.exe	0.40	7,180 K	10,332 K	872		
svchost.exe		1,016 K	3,072 K	1012	Host Process for Windows S...	Microsoft Corporation
svchost.exe	6.01	14,188 K	24,180 K	448	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		13,244 K	22,060 K	5984		
StartMenuExperience...		29,284 K	35,604 K	8300		
RuntimeBroker.exe		6,328 K	15,840 K	8436	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	0.01	16,536 K	34,732 K	9032	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		3,956 K	2,468 K	4192	Host Process for Setting Syn...	Microsoft Corporation
YourPhone.exe	Susp...	21,488 K	3,080 K	9360	YourPhone	Microsoft Corporation
RuntimeBroker.exe		7,332 K	18,004 K	9456	Runtime Broker	Microsoft Corporation
dllhost.exe		3,924 K	10,064 K	9744	COM Surrogate	Microsoft Corporation
WmiPrvSE.exe		6,376 K	16,216 K	9176		
RuntimeBroker.exe		2,632 K	9,616 K	10252	Runtime Broker	Microsoft Corporation
SearchUI.exe	Susp...	1,53,652 K	69,060 K	10384	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		2,168 K	7,176 K	12216	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		10,524 K	21,592 K	9492	Application Frame Host	Microsoft Corporation
RuntimeBroker.exe		3,416 K	12,968 K	8668	Runtime Broker	Microsoft Corporation
DellMobileConnect...		64,292 K	15,116 K	1520	DellMobileConnectClient	Screenovate Technologie...
DellMobileConnectUni...		17,040 K	12,832 K	10544	DellMobileConnectUniversal...	Screenovate Technologie...
ShellExperienceHost...	Susp...	14,936 K	11,248 K	13936	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		3,524 K	10,588 K	14028	Runtime Broker	Microsoft Corporation

Process explorer and verify the DEP & ASLR status

Process Explorer - Sysinternals: www.sysinternals.com [NAIMISHA\Naimisha Segu]

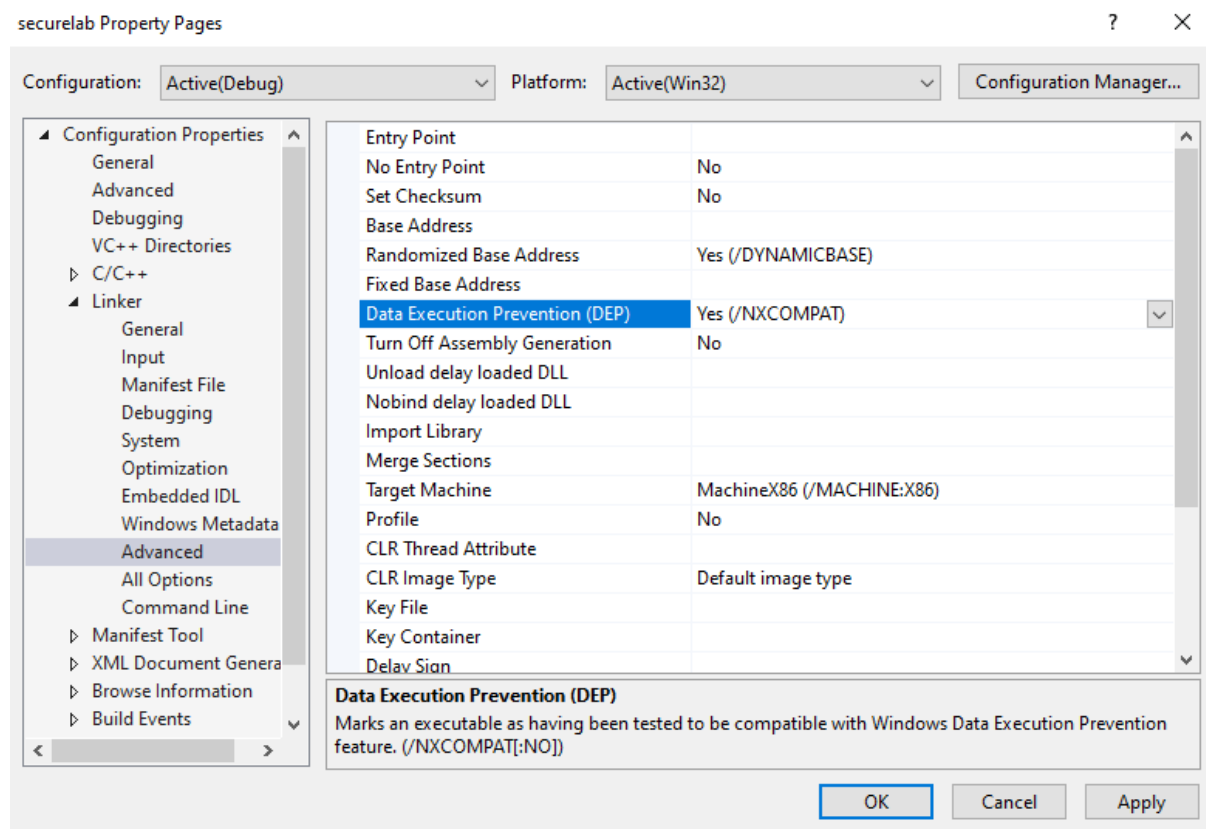
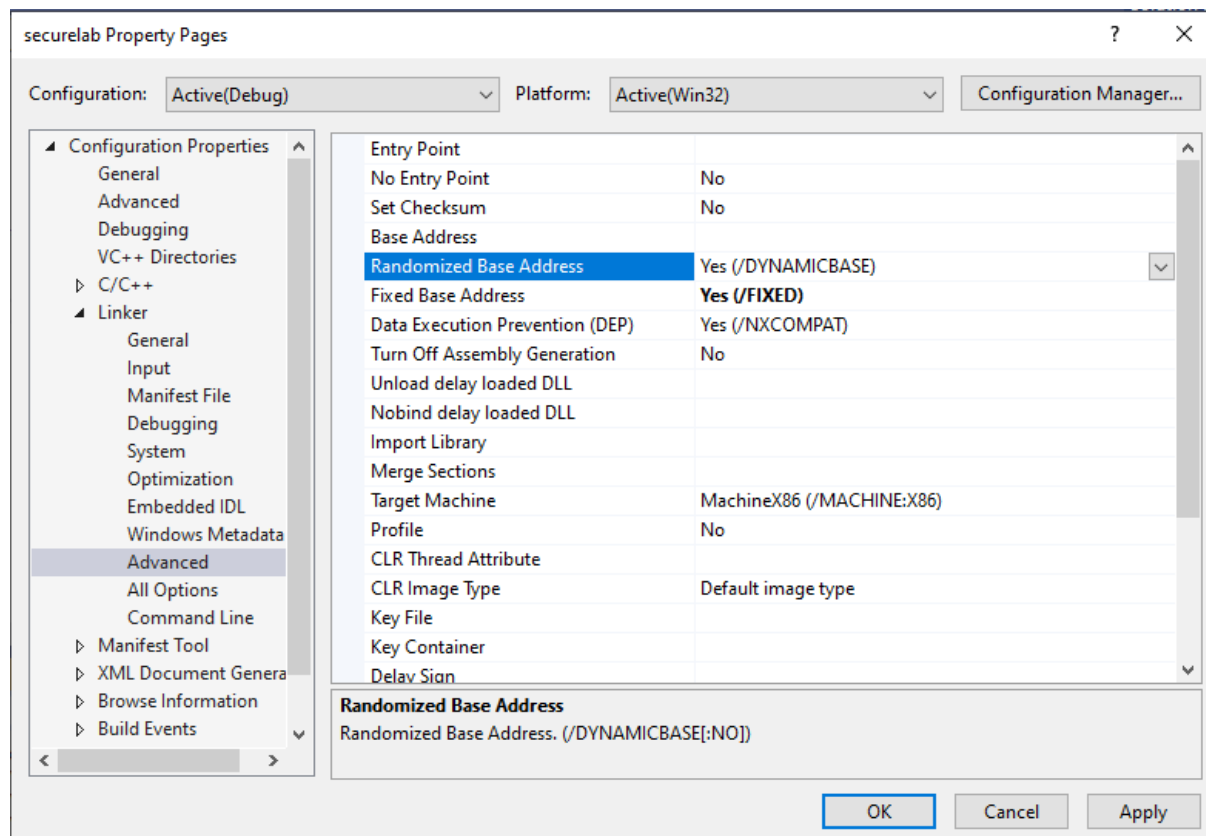
File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
ServiceHub.ThreadedWaitDialo...	2.77	50,588 K	28,164 K	15496	ServiceHub.Threaded...	Microsoft	Enabled (permane...	ASLR
ServiceHub.VSDetouredHost.exe	0.05	37,320 K	16,936 K	12900	ServiceHub.VSDetour...	Microsoft	Enabled (permane...	ASLR
ApplicationFrameHost.exe		10,444 K	18,844 K	9492	Application Frame Host	Microsoft Corporation	Enabled (permane...	ASLR
CompPkgSrv.exe		1,828 K	7,580 K	7976	Component Package ...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		7,240 K	16,192 K	1556	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
devenv.exe	3.59	3,48,968 K	2,91,084 K	11536	Microsoft Visual Studio...	Microsoft Corporation	Enabled (permane...	ASLR
dllhost.exe		5,460 K	11,920 K	9744	COM Surrogate	Microsoft Corporation	Enabled (permane...	ASLR
dllhost.exe		4,004 K	9,444 K	12848	COM Surrogate	Microsoft Corporation	n/a	ASLR
explorer.exe	0.97	80,656 K	1,18,704 K	7924	Windows Explorer	Microsoft Corporation	Enabled (permane...	ASLR
lsass.exe		8,280 K	14,484 K	884	Local Security Authorit...	Microsoft Corporation	n/a	ASLR
msdtc.exe		2,840 K	6,852 K	1240	Microsoft Distributed T...	Microsoft Corporation	n/a	ASLR

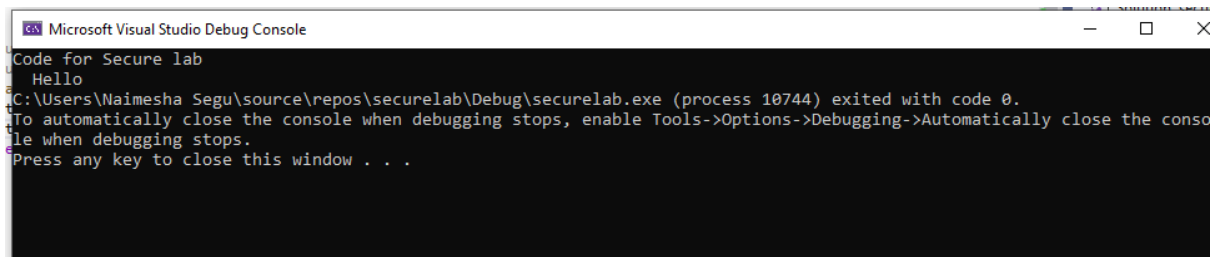
Enable software DEP, ASLR and SEH in the visual studio and rebuild the same executable

Configuration Properties > Linker > Advanced property page

Modifying the Randomized Base Address property.

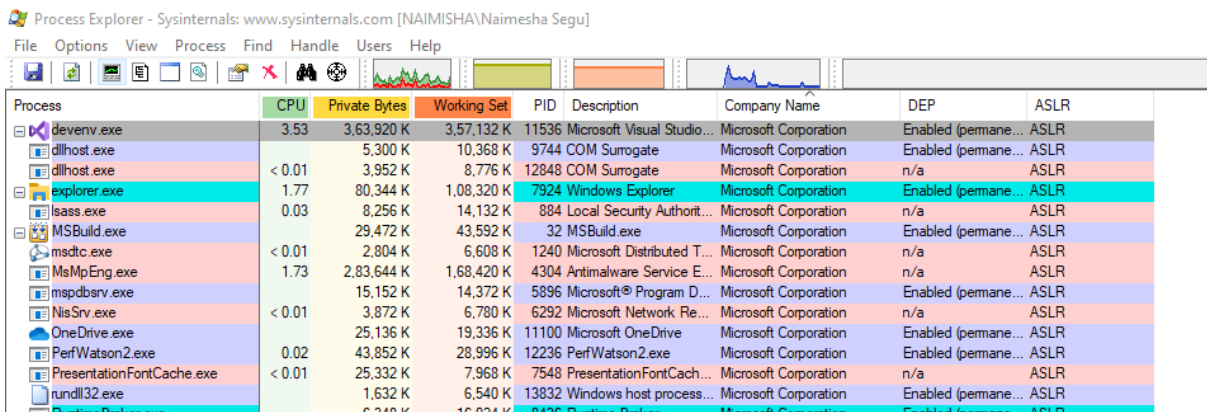


Again, running the executable



```
Microsoft Visual Studio Debug Console
Code for Secure lab
Hello
C:\Users\Naimesha Segu\source\repos\securelab\Debug\securelab.exe (process 10744) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .
```

And, verifying the DEP & ASLR status in the process explorer



Process Explorer - Sysinternals: www.sysinternals.com [NAIMISHA\Naimesha Segu]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
devenv.exe	3.53	3,63,920 K	3,57,132 K	11536	Microsoft Visual Studio...	Microsoft Corporation	Enabled (permane...	ASLR
dllhost.exe		5,300 K	10,368 K	9744	COM Surrogate	Microsoft Corporation	Enabled (permane...	ASLR
dllhost.exe	< 0.01	3,952 K	8,776 K	12848	COM Surrogate	Microsoft Corporation	n/a	ASLR
explorer.exe	1.77	80,344 K	1,08,320 K	7924	Windows Explorer	Microsoft Corporation	Enabled (permane...	ASLR
lsass.exe	0.03	8,256 K	14,132 K	884	Local Security Authorit...	Microsoft Corporation	n/a	ASLR
MSBuild.exe		29,472 K	43,592 K	32	MSBuild.exe	Microsoft Corporation	Enabled (permane...	ASLR
msdtc.exe	< 0.01	2,804 K	6,608 K	1240	Microsoft Distributed T...	Microsoft Corporation	n/a	ASLR
MsMpEng.exe	1.73	2,83,644 K	1,68,420 K	4304	Antimalware Service E...	Microsoft Corporation	n/a	ASLR
mspdbsrv.exe		15,152 K	14,372 K	5896	Microsoft® Program D...	Microsoft Corporation	Enabled (permane...	ASLR
NisSrv.exe	< 0.01	3,872 K	6,780 K	6292	Microsoft Network Re...	Microsoft Corporation	n/a	ASLR
OneDrive.exe		25,136 K	19,336 K	11100	Microsoft OneDrive	Microsoft Corporation	Enabled (permane...	ASLR
PerfWatson2.exe	0.02	43,852 K	28,996 K	12236	PerfWatson2.exe	Microsoft Corporation	Enabled (permane...	ASLR
PresentationFontCache.exe	< 0.01	25,332 K	7,968 K	7548	PresentationFontCach...	Microsoft Corporation	n/a	ASLR
rundll32.exe		1,632 K	6,540 K	13832	Windows host process...	Microsoft Corporation	Enabled (permane...	ASLR
System.Diagnostics...		5,248 K	16,024 K	8426	System.Diagnostics...	Microsoft Corporation	Enabled (permane...	ASLR