

Secure Coding

Lab experiment – Creating secure and safe executable

Download and install visual studio (recent edition)

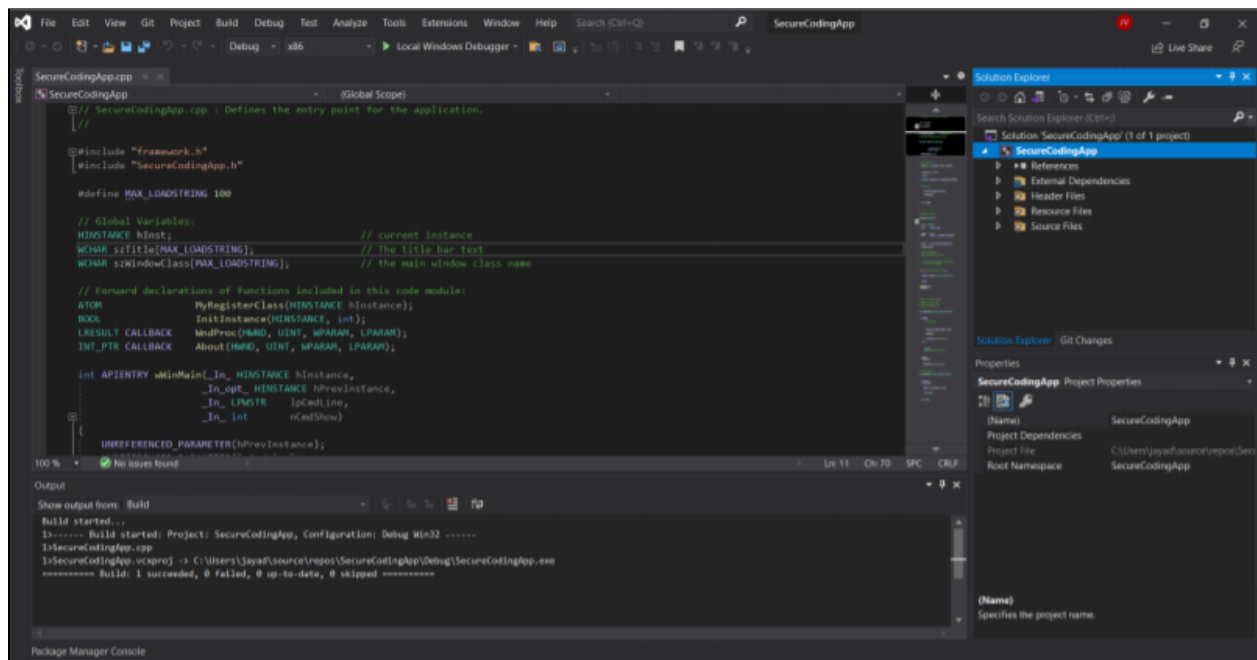
Write a C++ code of your own to build an executable and run the same.

Download process explorer and verify the DEP & ASLR status
Enable software DEP, ASLR and SEH in the visual studio and rebuild the same executable

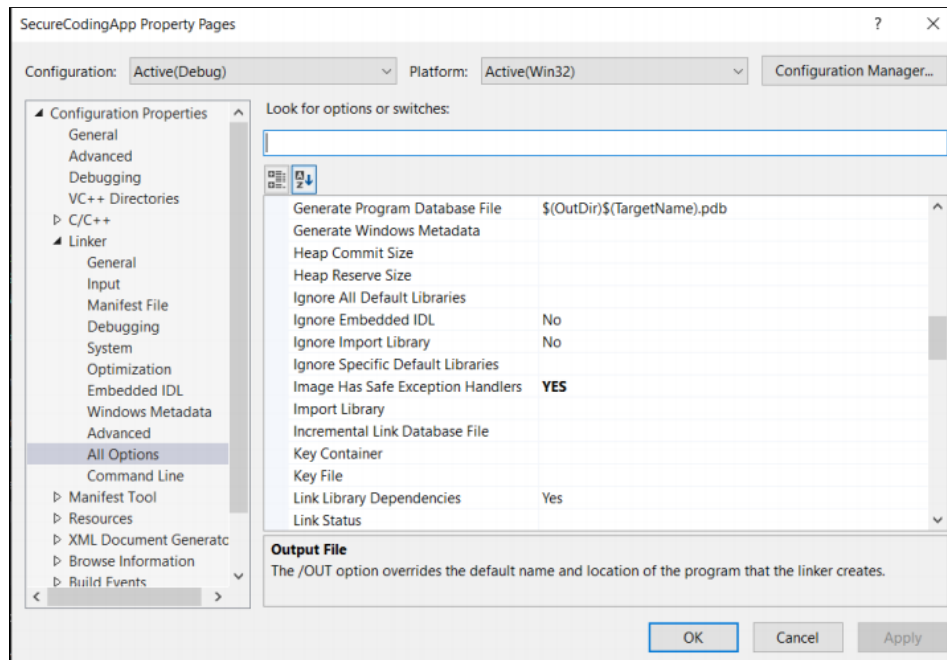
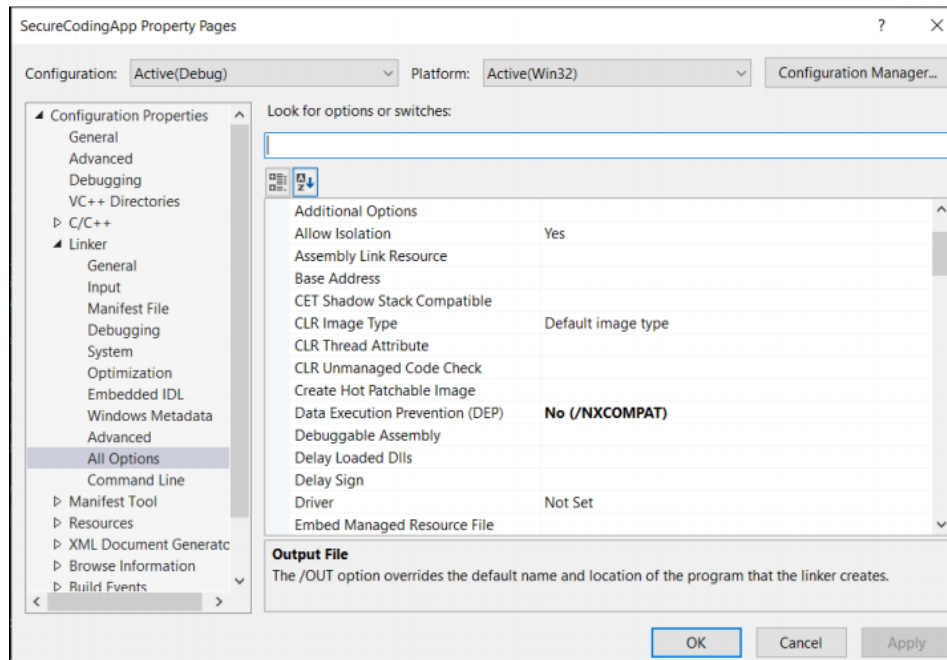
Again, verify the DEP & ASLR status in the process explorer

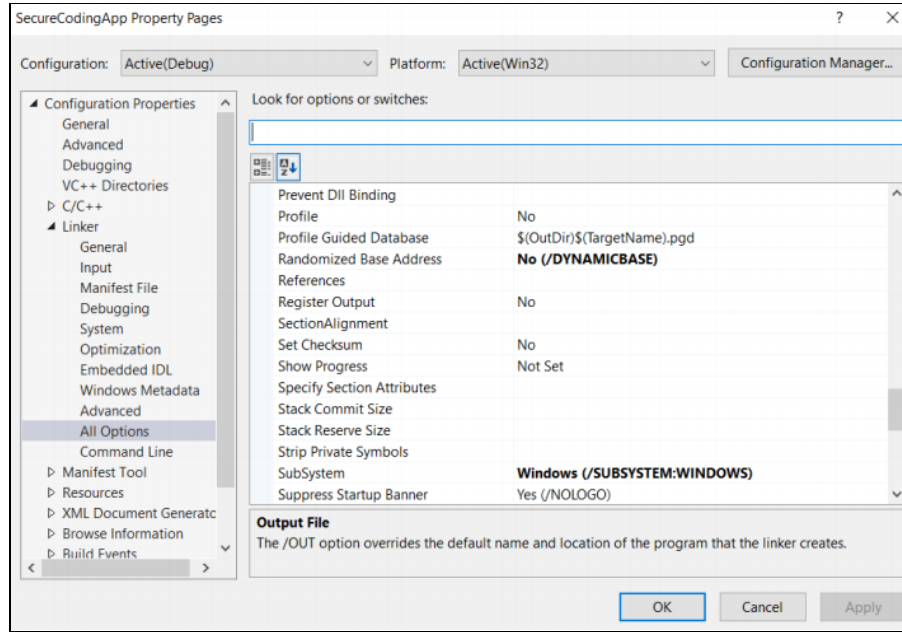
Report the same with separate screenshot - before and after enabling DEP & ASLR.

Building the executable

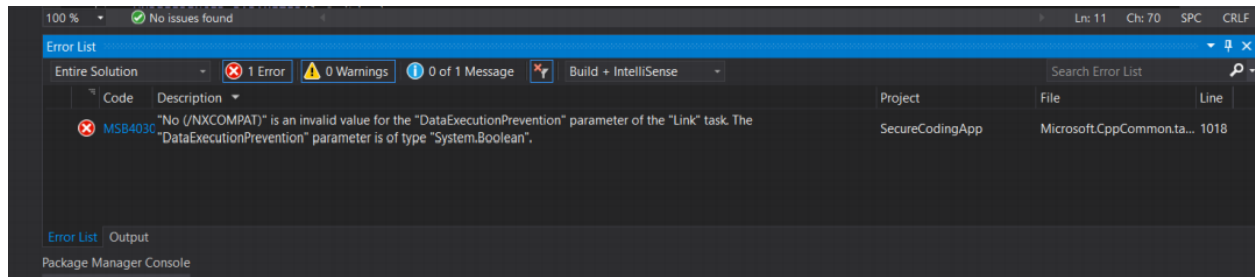


Disabling DEP and ASLR

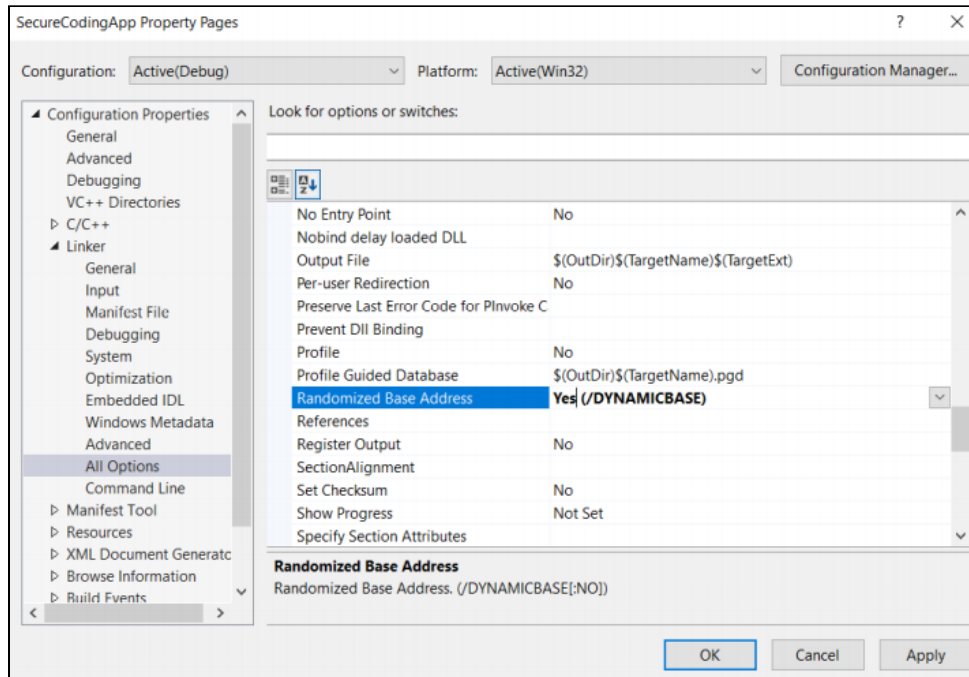
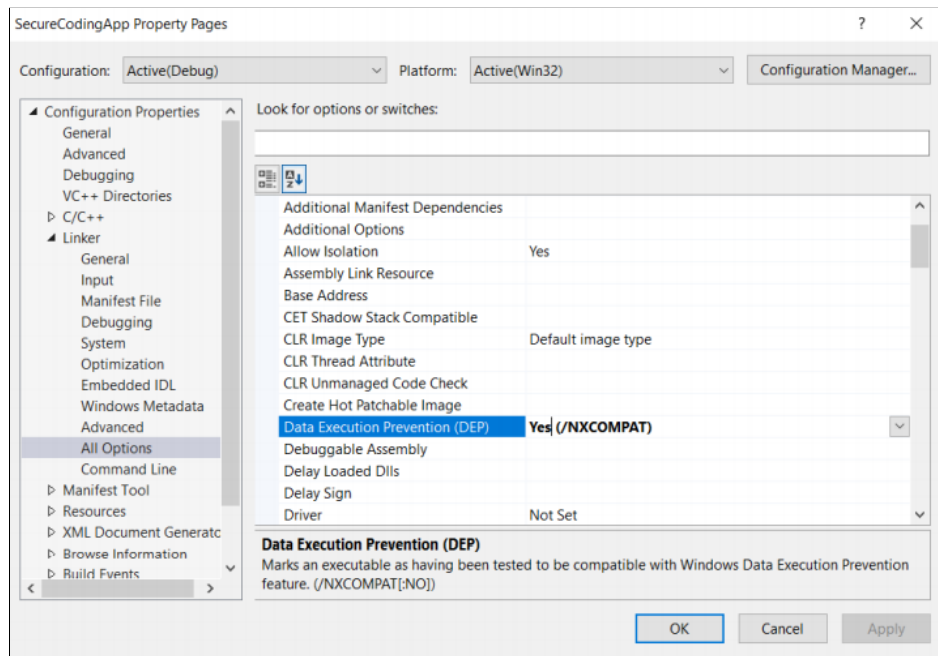




Build failed, exe not generated



Enable DEP and ASLR and re run the APP



Process explorer

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-CKYCSNCP\jayad]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		17.76 K	1,22,088 K	148		
System Idle Process	04.08	8 K	8 K	0		
System	1.45	200 K	7,304 K	4		
Interrupts	1.04	0 K	0 K		ala Hardware Interrupts and DPCs	
smss.exe		1,076 K	1,028 K	572		
Memory Compression	< 0.01	1,016 K	1,61,960 K	2840		
csrss.exe	< 0.01	2,164 K	5,980 K	848		
lsass.exe		1,628 K	6,184 K	940		
services.exe	0.01	6,160 K	10,548 K	1016		
lschost.exe	< 0.01	13,612 K	32,824 K	1044	Host Process for Windows S...	Microsoft Corporation
WinPcapSE.exe		3,892 K	10,480 K	5832		
unsecapp.exe	< 0.01	2,728 K	8,828 K	10982		
drctmon.exe		3,964 K	5,944 K	11512		
RuntimeBroker.exe		99,030 K	86,364 K	37144		
RuntimeBroker.exe		7,844 K	31,112 K	17216	Runtime Broker	Microsoft Corporation
SearchApp.exe	Sup...	2,99,360 K	1,06,648 K	14132	Search application	Microsoft Corporation
RuntimeBroker.exe	< 0.01	19,540 K	51,564 K	17672	Runtime Broker	Microsoft Corporation
lschost.exe	Sup...	8,228 K	12,124 K	17512	Host Process for Windows S...	Microsoft Corporation
RuntimeBroker.exe		4,324 K	8,228 K	17532	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		7,876 K	27,524 K	11280	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		4,712 K	20,452 K	2916	Runtime Broker	Microsoft Corporation
SearchApp.exe	Sup...	2,49,428 K	88,588 K	5428	Search application	Microsoft Corporation
lschost.exe		7,040 K	18,628 K	18836	COM Surrogate	Microsoft Corporation
unsecapp.exe		1,628 K	7,428 K	13228	Task to receive asynchronous...	Microsoft Corporation
csrss.exe	Sup...	89,200 K	72,168 K	12768	csrss.exe	Microsoft Corporation
RuntimeBroker.exe		5,284 K	26,796 K	6260	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Sup...	82,728 K	70,184 K	584	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		7,712 K	20,080 K	9112	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe		23,108 K	10,820 K	10220	System Settings Broker	Microsoft Corporation
TaskHost.exe		65,700 K	47,384 K	10580		Microsoft Corporation
ApplicationFrameHost.exe		37,932 K	42,016 K	17844	Application Frame Host	Microsoft Corporation
WinStoreApp.exe	Sup...	1,05,276 K	7,728 K	2456	Store	Microsoft Corporation
RuntimeBroker.exe		7,140 K	16,364 K	9180	Runtime Broker	Microsoft Corporation
UserVSSDHost.exe		2,136 K	8,832 K	3960	User VSSD Host	Microsoft Corporation
lschost.exe	Sup...	44,604 K	7,744 K	3810	Microsoft Outlook	Microsoft Corporation
RuntimeBroker.exe		1,188 K	18,888 K	5620	Runtime Broker	Microsoft Corporation
NTLDR.exe	Sup...	12,208 K	2,312 K	8120	Microsoft Outlook Communs...	Microsoft Corporation
lschost.exe	Sup...	9,112 K	44,308 K	11296	LSASSP.exe	Microsoft Corporation
RuntimeBroker.exe		10,324 K	33,308 K	4440	Runtime Broker	Microsoft Corporation
CompMgr.exe		1,516 K	8,344 K	10556	Component Package Suppor...	Microsoft Corporation
SystemSettings.exe	Sup...	77,312 K	67,212 K	764	Settings	Microsoft Corporation
smartscreen.exe		8,244 K	24,482 K	15482	Windows Defender SmartScr...	Microsoft Corporation
TlWorker.exe		31,992 K	37,788 K	1920		
WUDFHost.exe		8,072 K	14,108 K	1116		
lschost.exe	< 0.01	30,252 K	18,088 K	11888	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 13.91% Commit Charge: 61.17% Processes: 241 Physical Memory: 72.84%

Process Explorer - Sysinternals: www.sysinternals.com [LAPTOP-CKYCSNCP\jayad]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
SearchProtocolHost.exe		1,884 K	8,380 K	15876	Microsoft Windows Search Pr...	Microsoft Corporation
lschost.exe		10,608 K	20,176 K	11980	Host Process for Windows S...	Microsoft Corporation
SecurityHealthService.exe		3,872 K	12,648 K	9172	Windows Security Health Ser...	Microsoft Corporation
lschost.exe		2,464 K	10,872 K	11724	Host Process for Windows S...	Microsoft Corporation
lschost.exe		1,440 K	5,672 K	12016	Host Process for Windows S...	Microsoft Corporation
lschost.exe		4,772 K	10,164 K	12088	Host Process for Windows S...	Microsoft Corporation
lschost.exe	0.01	2,180 K	11,140 K	4968	Host Process for Windows S...	Microsoft Corporation
lschost.exe		2,332 K	13,404 K	12484	Host Process for Windows S...	Microsoft Corporation
lschost.exe		6,864 K	20,236 K	13328	Host Process for Windows S...	Microsoft Corporation
lschost.exe		3,052 K	11,776 K	13548	Host Process for Windows S...	Microsoft Corporation
lschost.exe		1,844 K	7,432 K	9172	Host Process for Windows S...	Microsoft Corporation
lschost.exe		5,300 K	17,624 K	632	Host Process for Windows S...	Microsoft Corporation
lschost.exe		6,036 K	22,632 K	13852	Host Process for Windows S...	Microsoft Corporation
lschost.exe		3,400 K	15,184 K	13884	Host Process for Windows S...	Microsoft Corporation
lschost.exe	< 0.01	3,000 K	12,104 K	16362	Host Process for Windows S...	Microsoft Corporation
Sysmon.exe		6,372 K	8,332 K	14556	System Guard Runtime Monit...	Microsoft Corporation
lschost.exe		2,900 K	11,572 K	6340	Host Process for Windows S...	Microsoft Corporation
lschost.exe		5,080 K	22,012 K	13660	Host Process for Windows S...	Microsoft Corporation
lschost.exe		3,396 K	11,348 K	2216	Host Process for Windows S...	Microsoft Corporation
lschost.exe		4,320 K	15,316 K	12664	Host Process for Windows S...	Microsoft Corporation
lschost.exe		1,784 K	7,768 K	8884	Host Process for Windows S...	Microsoft Corporation
lschost.exe		3,600 K	11,672 K	22336	Host Process for Windows S...	Microsoft Corporation
lschost.exe		9,044 K	22,072 K	1016	Local Security Authority Proc...	Microsoft Corporation
lschost.exe		1,468 K	2,576 K	1036		
lschost.exe		2,600 K	11,656 K	1196		
lschost.exe		4,224 K	7,076 K	1292		
lschost.exe	0.27	1,24,336 K	67,652 K	1360		
lschost.exe	0.04	2,71,424 K	2,31,028 K	7656	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,984 K	9,256 K	1586	Windows Security notification...	Microsoft Corporation
lschost.exe		2,340 K	10,144 K	2258	Realtek HD Audio Universal	Realtek Semiconductor
lschost.exe	< 0.01	1,340 K	6,480 K	4388	Vanguard tray notification	Riot Games, Inc.
lschost.exe	0.01	41,260 K	50,800 K	12368	Microsoft OneDrive	Microsoft Corporation
lschost.exe		3,392 K	13,352 K	13656	This utility controls special h...	Lenovo Group Ltd.
WINWORD.EXE		1,32,916 K	1,38,880 K	2920	Microsoft Word	Microsoft Corporation
lschost.exe	0.01	1,26,296 K	1,12,372 K	2224	Microsoft Word	Microsoft Corporation
lschost.exe	0.1	3,75,116 K	3,70,028 K	10248	Microsoft Visual Studio 2019	Microsoft Corporation
lschost.exe	0.02	43,936 K	69,784 K	11292	PerfWattson2.exe	Microsoft Corporation
Microsoft ServiceHub Cont...		42,560 K	57,976 K	2624	Microsoft ServiceHub Control...	Microsoft
ServiceHub IdentityHost...	< 0.01	75,132 K	83,920 K	13432	ServiceHub IdentityHost.exe	Microsoft
ServiceHub VSDesktop...		1,43,624 K	78,512 K	13744	ServiceHub VSDesktopHost...	Microsoft
ServiceHub SettingsHost...		1,51,612 K	1,05,912 K	17728	ServiceHub SettingsHost.exe	Microsoft
ServiceHub Host CLR.x64...	< 0.01	78,466 K	65,744 K	16156	ServiceHub Host CLR.x64...	Microsoft
ServiceHub ThreadedW...		95,324 K	91,528 K	6732	ServiceHub ThreadedWaiDi...	Microsoft
ServiceHub Host CLR.x64...		1,85,800 K	83,028 K	6856	ServiceHub Host CLR.x64...	Microsoft
ServiceHub TestWindo...	< 0.01	62,640 K	73,428 K	864	ServiceHub TestWindowStu...	Microsoft

CPU Usage: 11.72% Commit Charge: 62.07% Processes: 234 Physical Memory: 71.29%

