

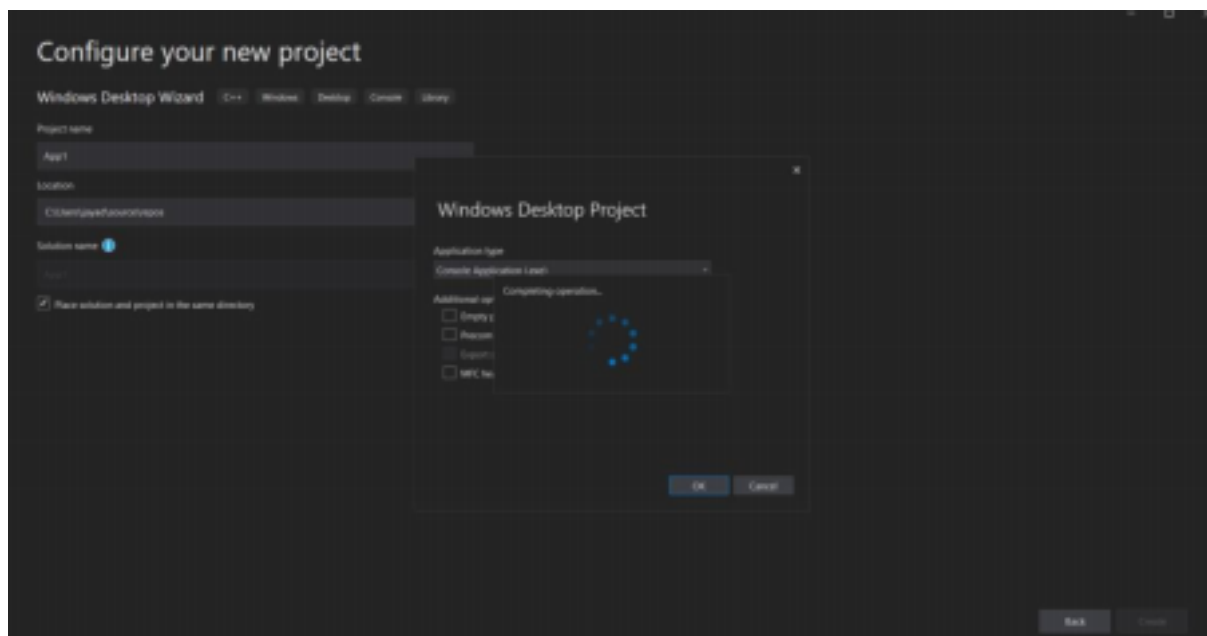
Secure coding

Lab-11

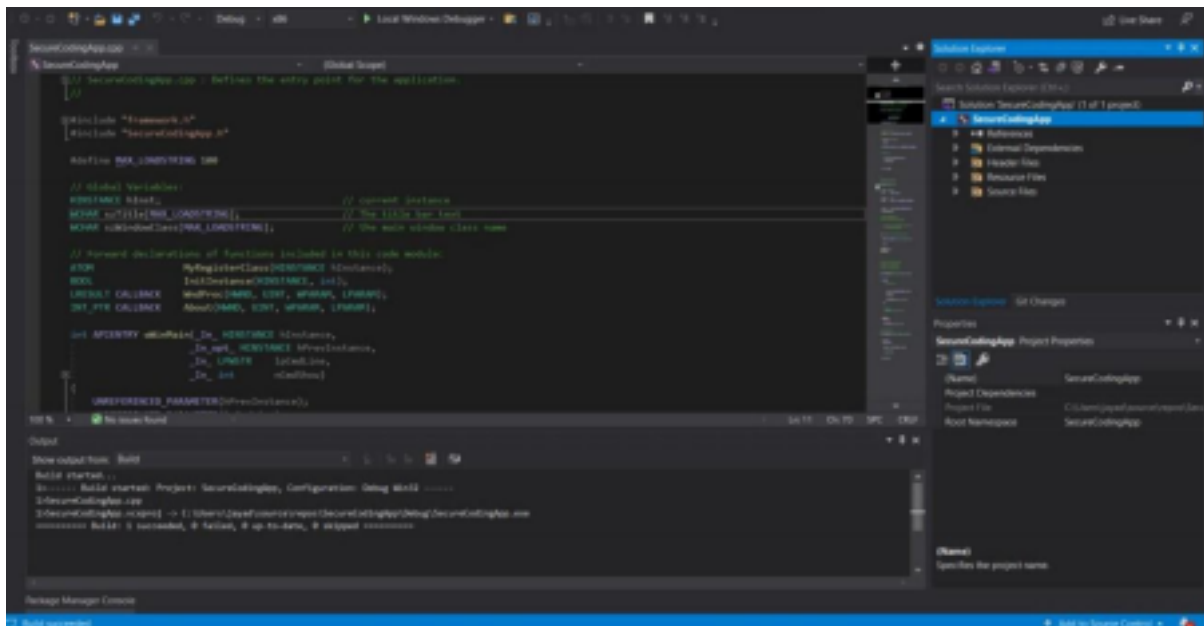
18BCE7103

B.KRANTHI

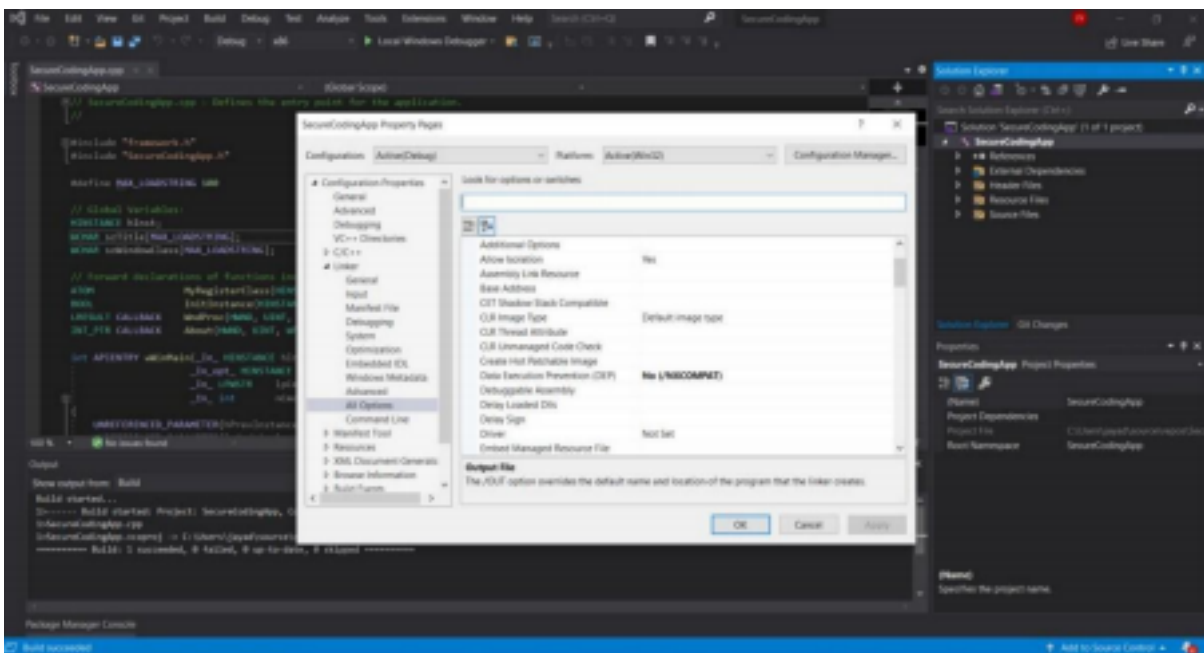
After installing visual studio:



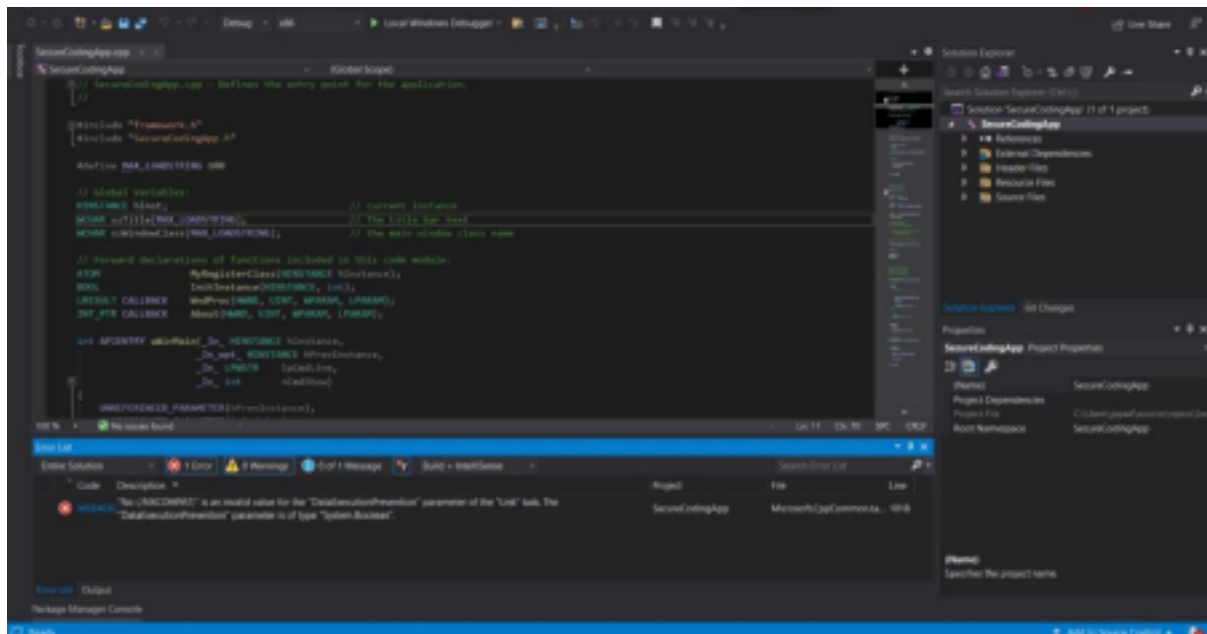
Generating .exe:



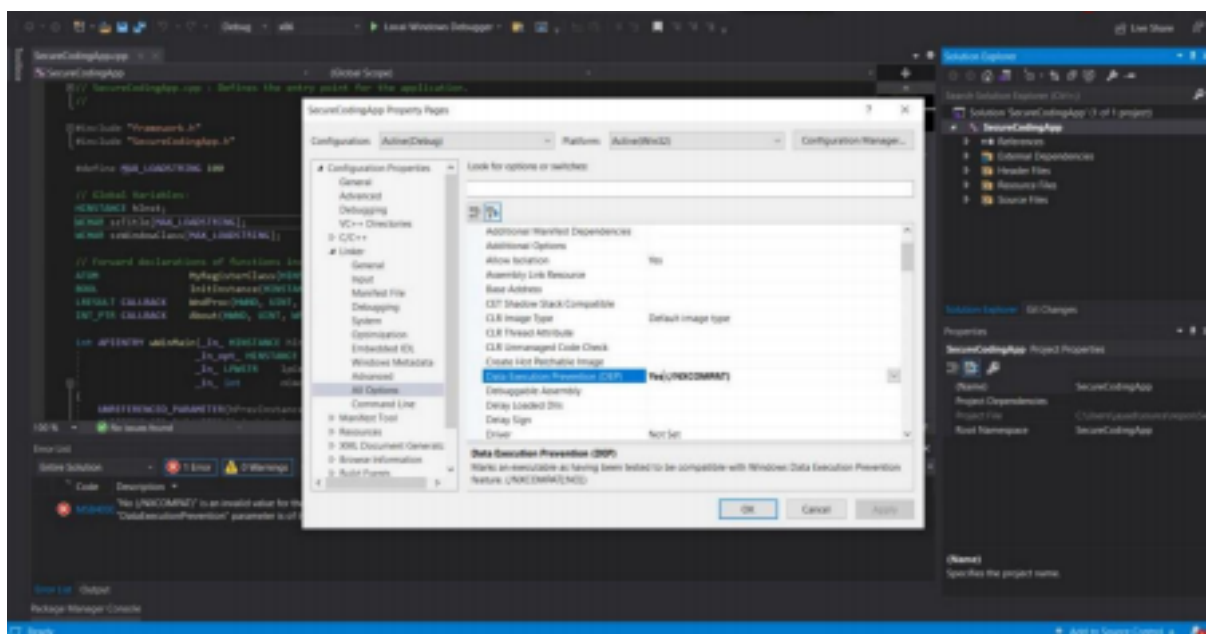
Disabling DER and ASLR:

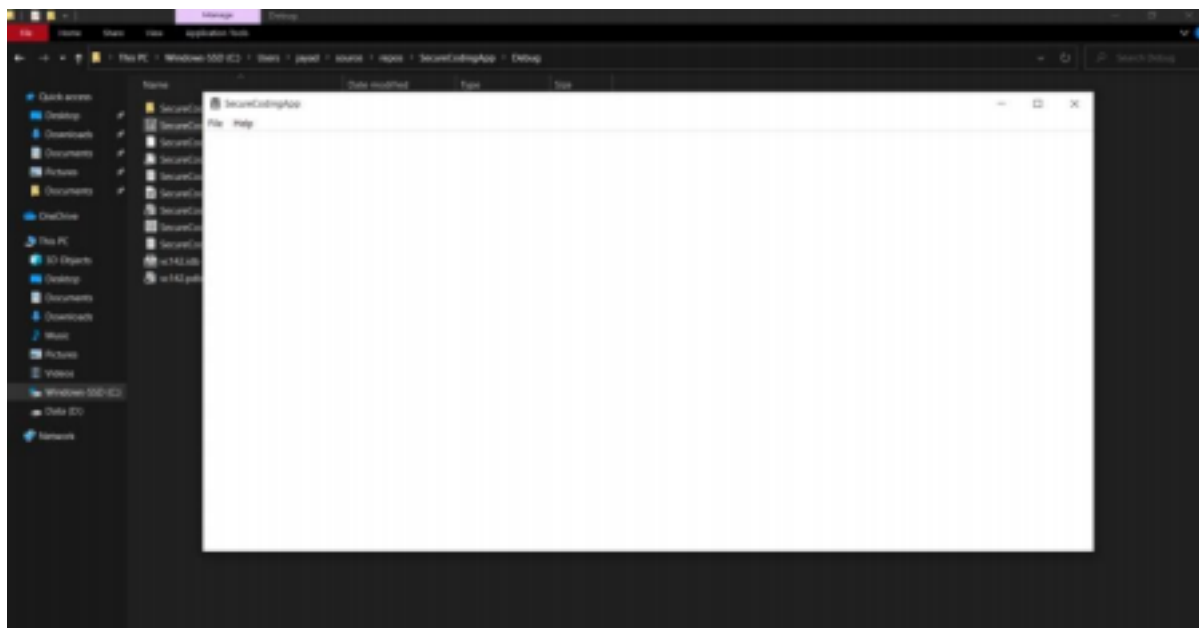


.exe file not created



After enabling and running the app:





Downloading, installing and analysing through Process Explorer:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		17,376 K	1,22,088 K	148		
System Idle Process	84.09	60 K	8 K	0		
System	1.45	208 K	7,324 K	4		
Interrupts	1.04	0 K	0 K		n/a Hardware Interrupts and DPCs	
smss.exe		1,076 K	1,028 K	572		
Memory Compression	< 0.01	1,016 K	1,81,960 K	2040		
csrss.exe	< 0.01	2,164 K	5,900 K	840		
wininit.exe		1,628 K	6,184 K	940		
services.exe	0.01	6,168 K	10,548 K	1016		
svchost.exe	< 0.01	13,612 K	32,824 K	1044	Host Process for Windows S...	Microsoft Corporation
WinPnSE.exe		3,892 K	10,480 K	5832		
umscapp.exe	< 0.01	2,728 K	8,828 K	10992		
dhhost.exe		3,964 K	9,944 K	11312		
StartMenuExperienceHost.exe		99,080 K	86,304 K	17144		
RuntimeBroker.exe		7,844 K	31,112 K	17516	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	2,96,368 K	1,08,648 K	18132	Search application	Microsoft Corporation
RuntimeBroker.exe	< 0.01	18,548 K	51,564 K	18512	Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	81,508 K	2,688 K	18744	YourPhone	Microsoft Corporation
SettingSyncHost.exe		4,804 K	8,236 K	17052	Host Process for Setting Syn...	Microsoft Corporation
RuntimeBroker.exe		7,876 K	27,524 K	11080	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		4,712 K	29,452 K	20516	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	2,49,428 K	88,568 K	5428	Search application	Microsoft Corporation
dhhost.exe		7,940 K	15,836 K	18656	COM Surrogate	Microsoft Corporation
umscapp.exe		1,628 K	7,428 K	13228	Sink to receive asynchronous...	Microsoft Corporation
Cortana.exe	Susp...	88,280 K	72,168 K	12768	Cortana	Microsoft Corporation
RuntimeBroker.exe		5,284 K	26,796 K	8260	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	82,728 K	70,184 K	584	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		7,712 K	29,080 K	9112	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe		5,680 K	23,108 K	18280	System Settings Broker	Microsoft Corporation
TestInputHost.exe		66,708 K	47,384 K	18880		Microsoft Corporation
ApplicationFrameHost.exe		37,932 K	42,016 K	17844	Application Frame Host	Microsoft Corporation
WinStoreApp.exe	Susp...	1,06,276 K	2,728 K	2456	Store	Microsoft Corporation
RuntimeBroker.exe		7,148 K	16,368 K	9180	Runtime Broker	Microsoft Corporation
UserOOBEBroker.exe		2,136 K	8,832 K	9960	User OOBE Broker	Microsoft Corporation
Outlook.exe	Susp...	99,628 K	2,784 K	2812	Microsoft Outlook	Microsoft Corporation
RuntimeBroker.exe		3,148 K	18,680 K	9440	Runtime Broker	Microsoft Corporation
Outlook.exe	Susp...	12,288 K	2,312 K	8120	Microsoft Outlook Communi...	Microsoft Corporation
LockApp.exe	Susp...	67,112 K	44,336 K	11244	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		10,324 K	33,300 K	4440	Runtime Broker	Microsoft Corporation
CompPkgSrv.exe		1,516 K	9,344 K	10628	Component Package Suppor...	Microsoft Corporation
SystemSettings.exe	Susp...	77,312 K	67,212 K	756	Settings	Microsoft Corporation
SmartScreen.exe		8,244 K	24,492 K	15462	Windows Defender SmartSc...	Microsoft Corporation
TIWorker.exe		31,992 K	37,788 K	1920		
WUDFHost.exe		8,872 K	14,108 K	1116		
svchost.exe	< 0.01	10,252 K	18,080 K	7168	Host Process for Windows S...	Microsoft Corporation

www.m
www
www
www
www
www

www
Sign
www
www

www
www
www
www
www

BG Comment

Kill Process



VirusTotal

Submit

Data Execution Prevention (DEP) Status: Enabled (permanent)

