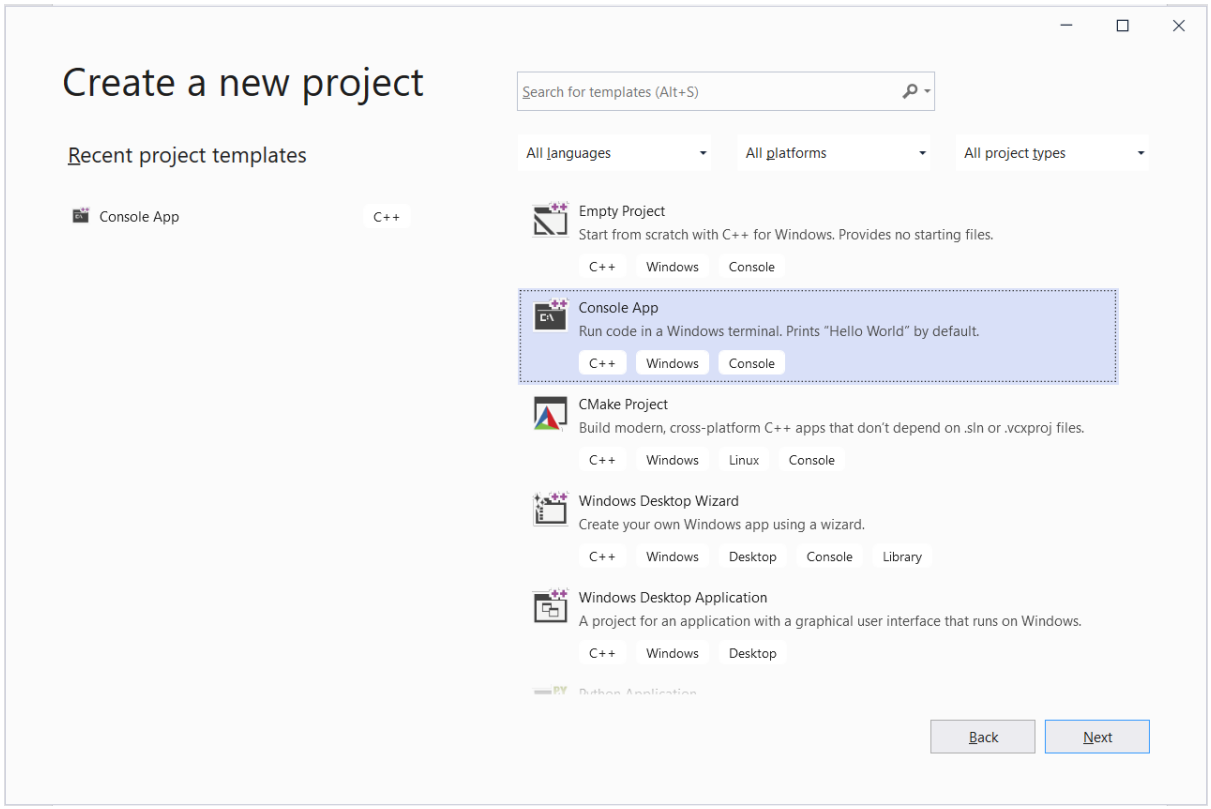
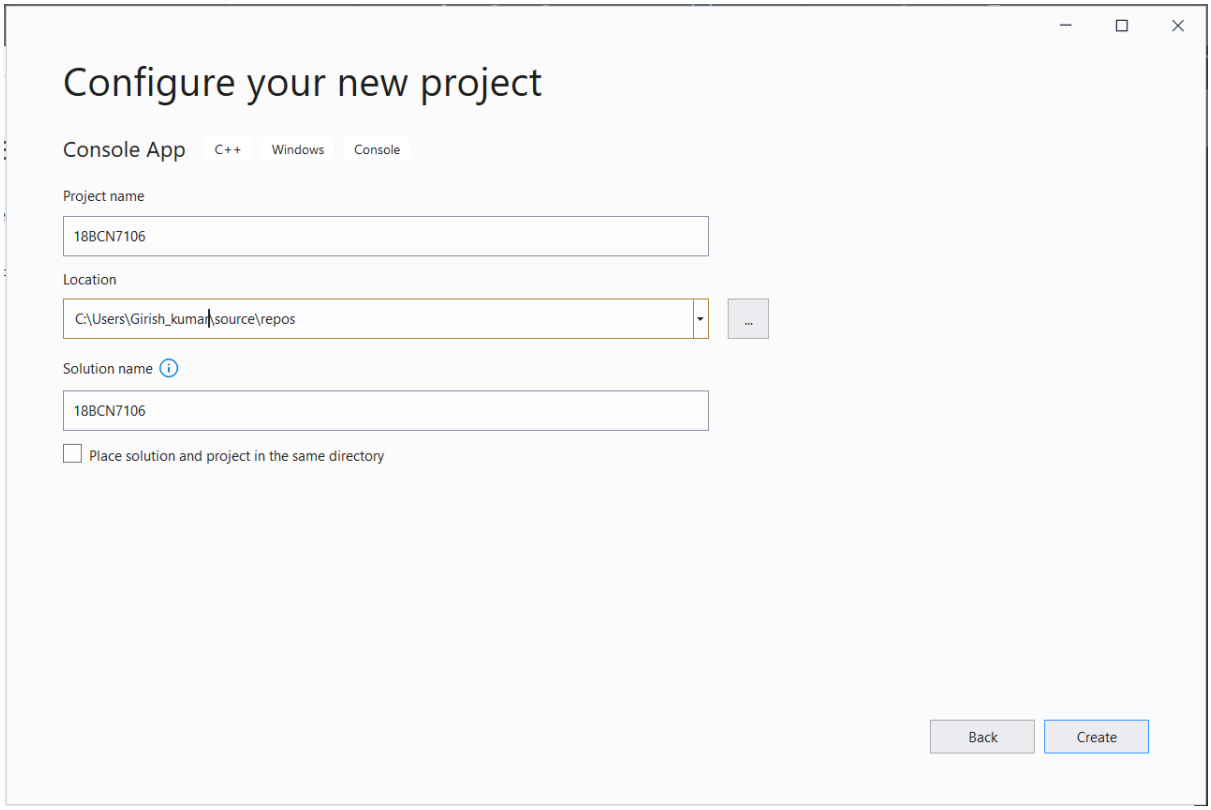
Secure Coding Lab - 11

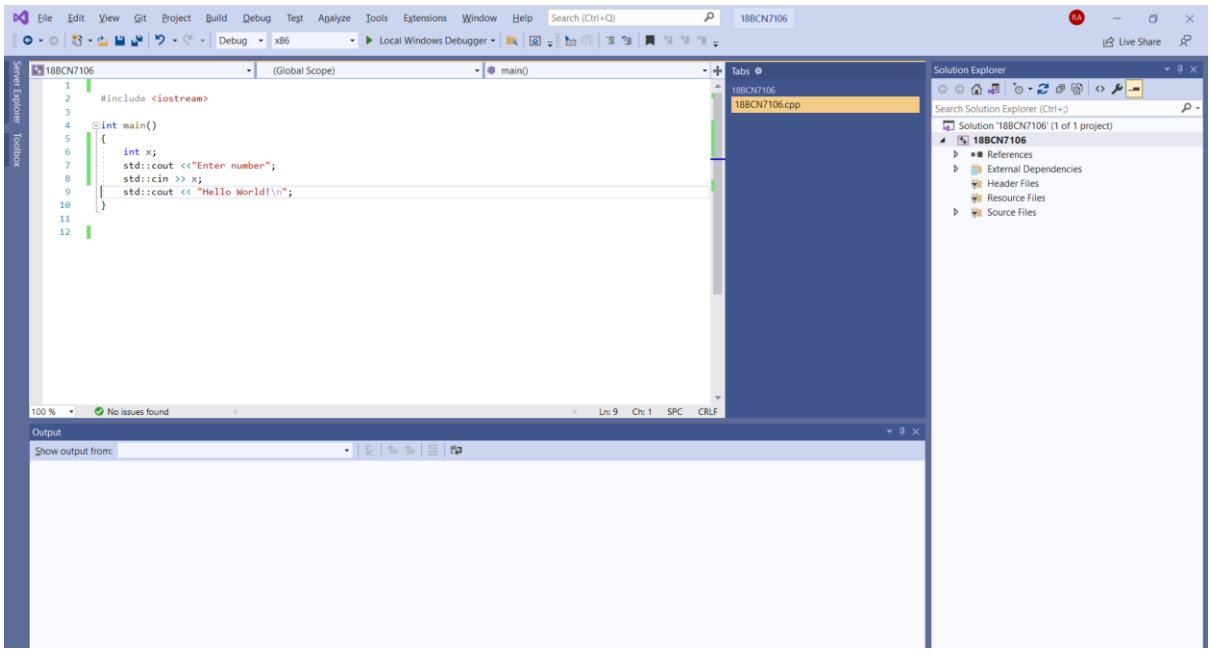
Name: S V Girish Kumar

Reg. No: 18BCN7106

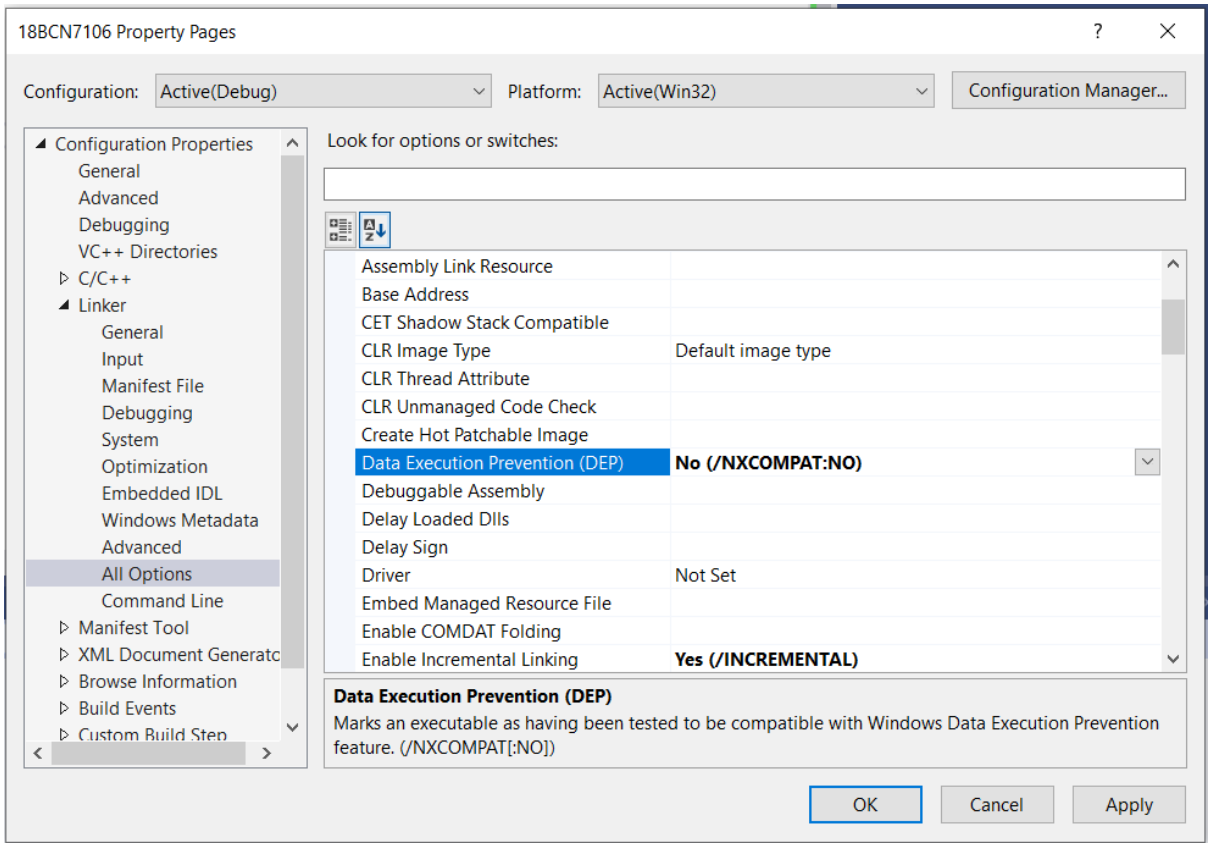
After Downloading the Visual Studio and Process Explorer, creating the new project in visual Studio.

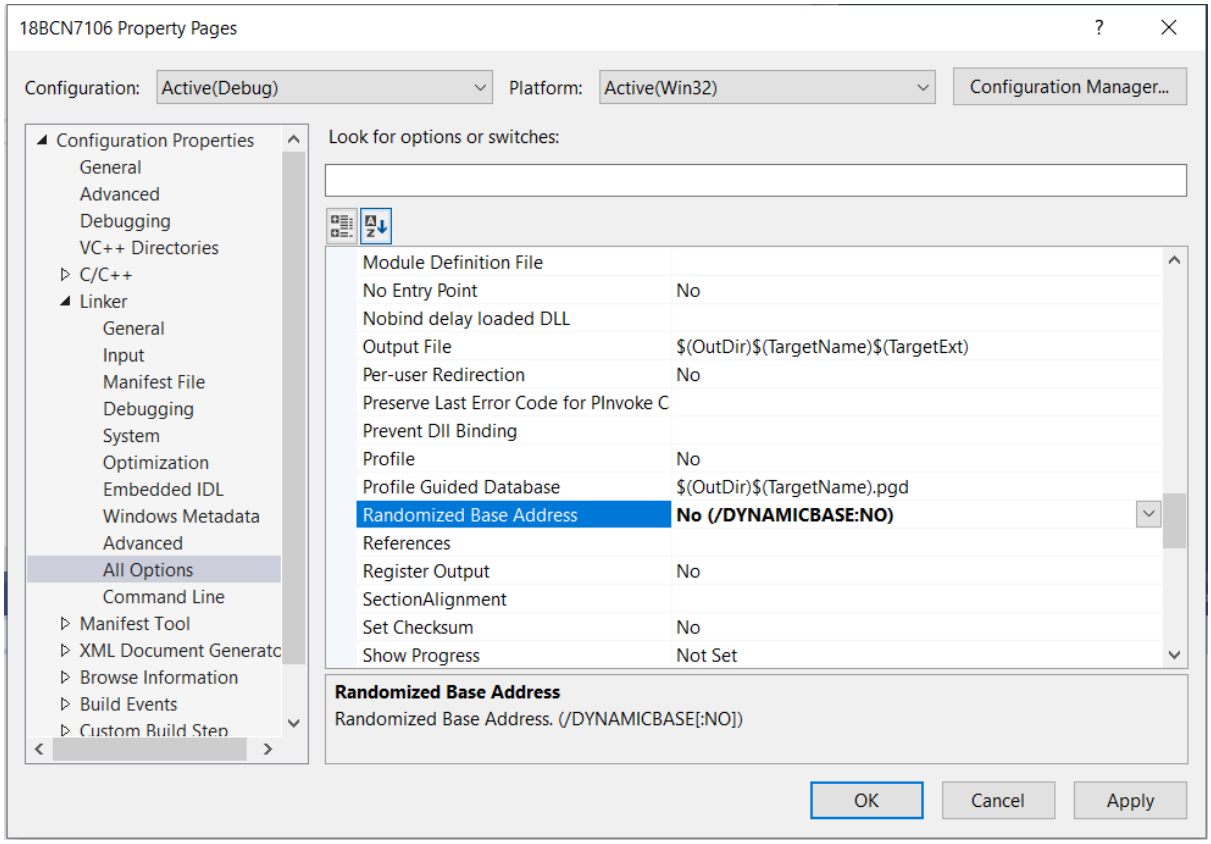


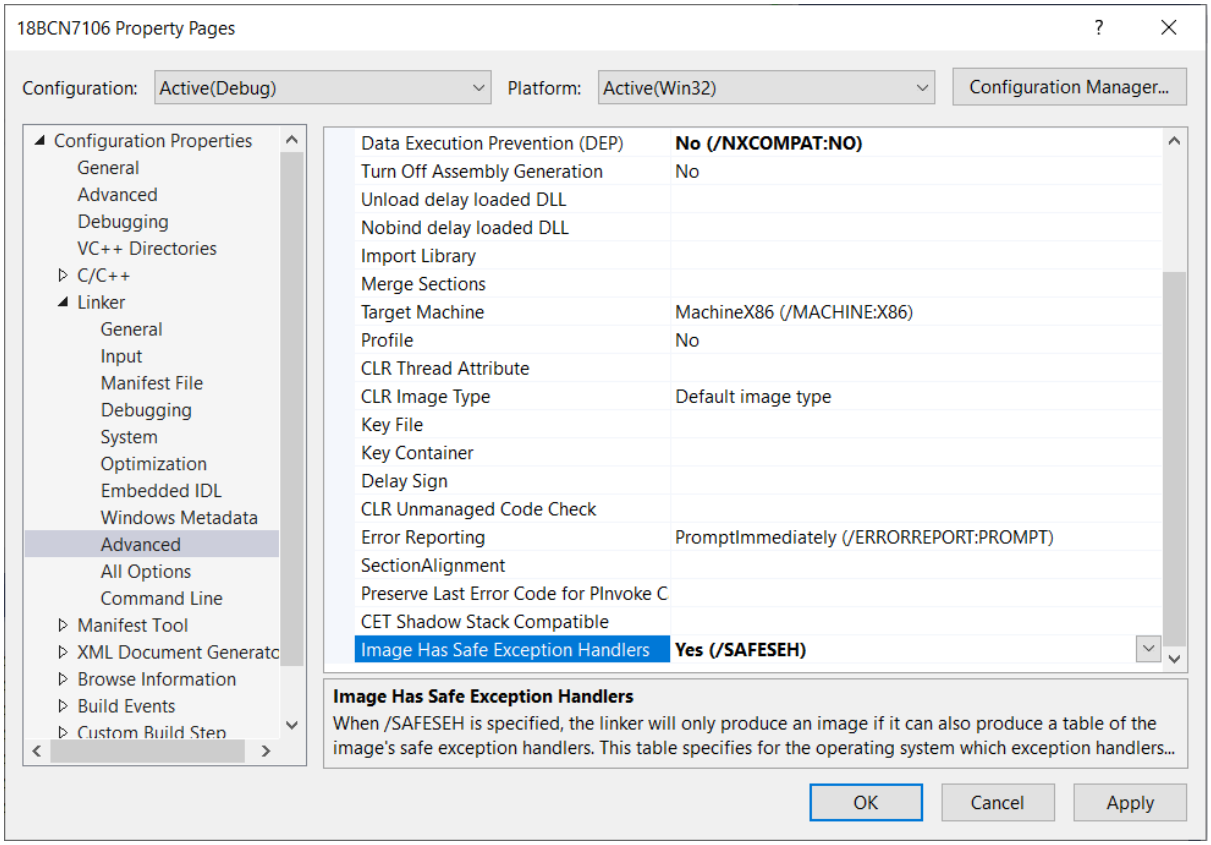




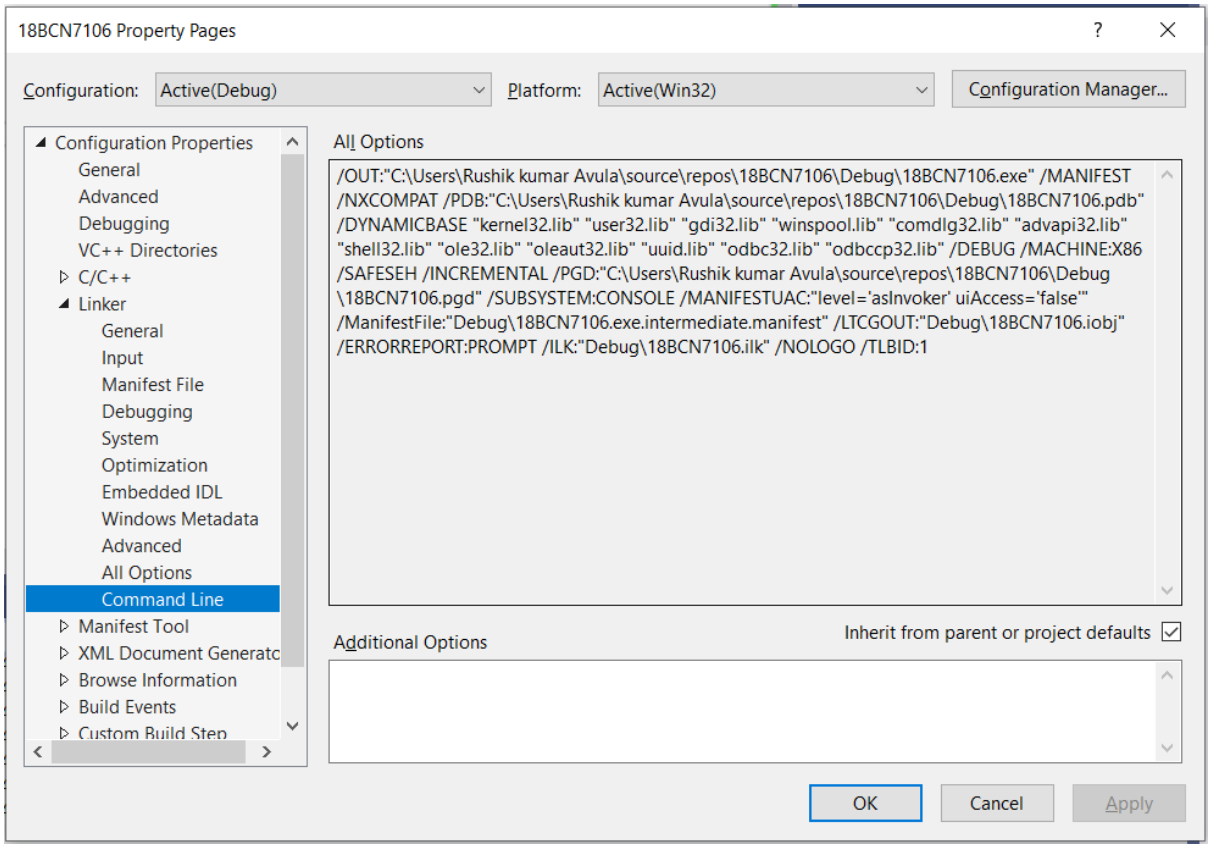
Visiting properties of the project and verifying the DEP, ASLR and SEH properties.


18BCN7106 Property Pages
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 Generatc
Browse Information
Build Events
Custom Build Step
Look for options or switches:
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)
No (/NXCOMPAT:NO)
Debuggable Assembly
Delay Loaded Dlls
Delay Sign
Driver
Not Set
Embed Managed Resource File
Enable COMDAT Folding
Enable Incremental Linking
Yes (/INCREMENTAL)
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

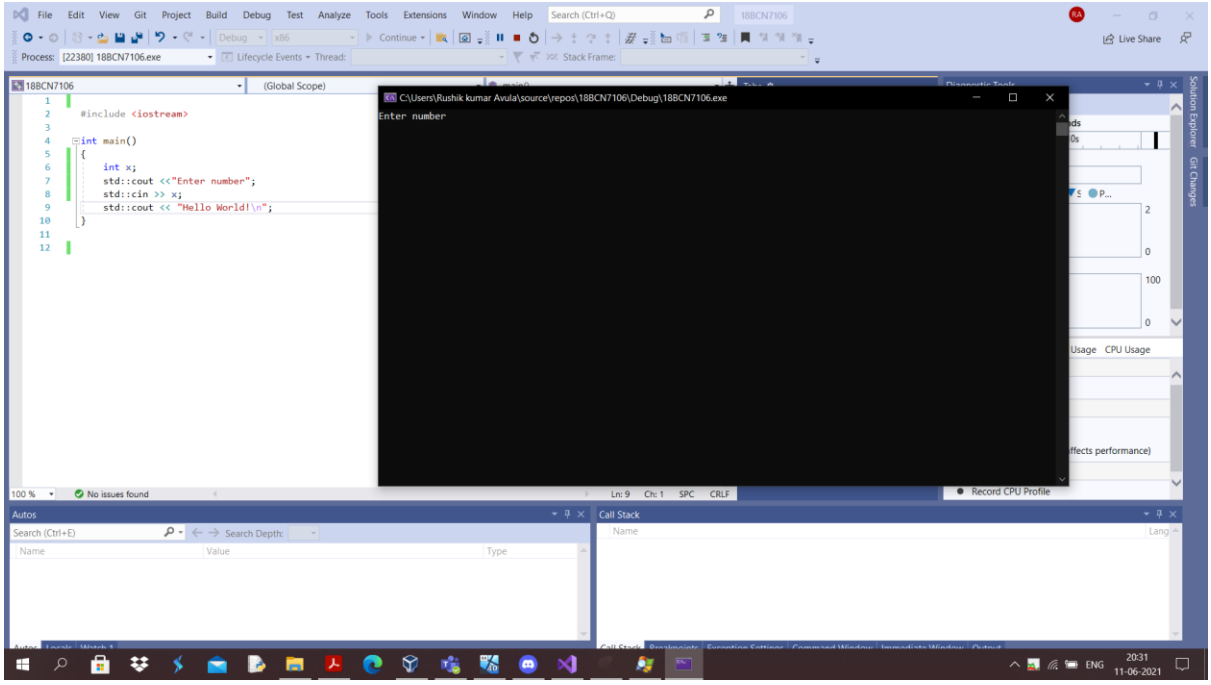

18BCN7106 Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
XML Document Generatc
Browse Information
Build Events
Custom Build Step
Look for options or switches:
Module Definition File
No Entry Point
No
Nobind delay loaded DLL
Output File
$(OutDir)$(TargetName)$(TargetExt)
Per-user Redirection
No
Preserve Last Error Code for PInvoke C
Prevent Dll Binding
Profile
No
Profile Guided Database
$(OutDir)$(TargetName).pgd
Randomized Base Address
No (/DYNAMICBASE:NO)
References
Register Output
No
SectionAlignment
Set Checksum
No
Show Progress
Not Set
Randomized Base Address
Randomized Base Address. (/DYNAMICBASE[:NO])
OK
Cancel
Apply



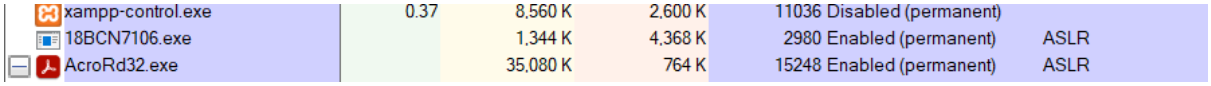
Now I changed the default options to NO for checking them in Process Explorer.



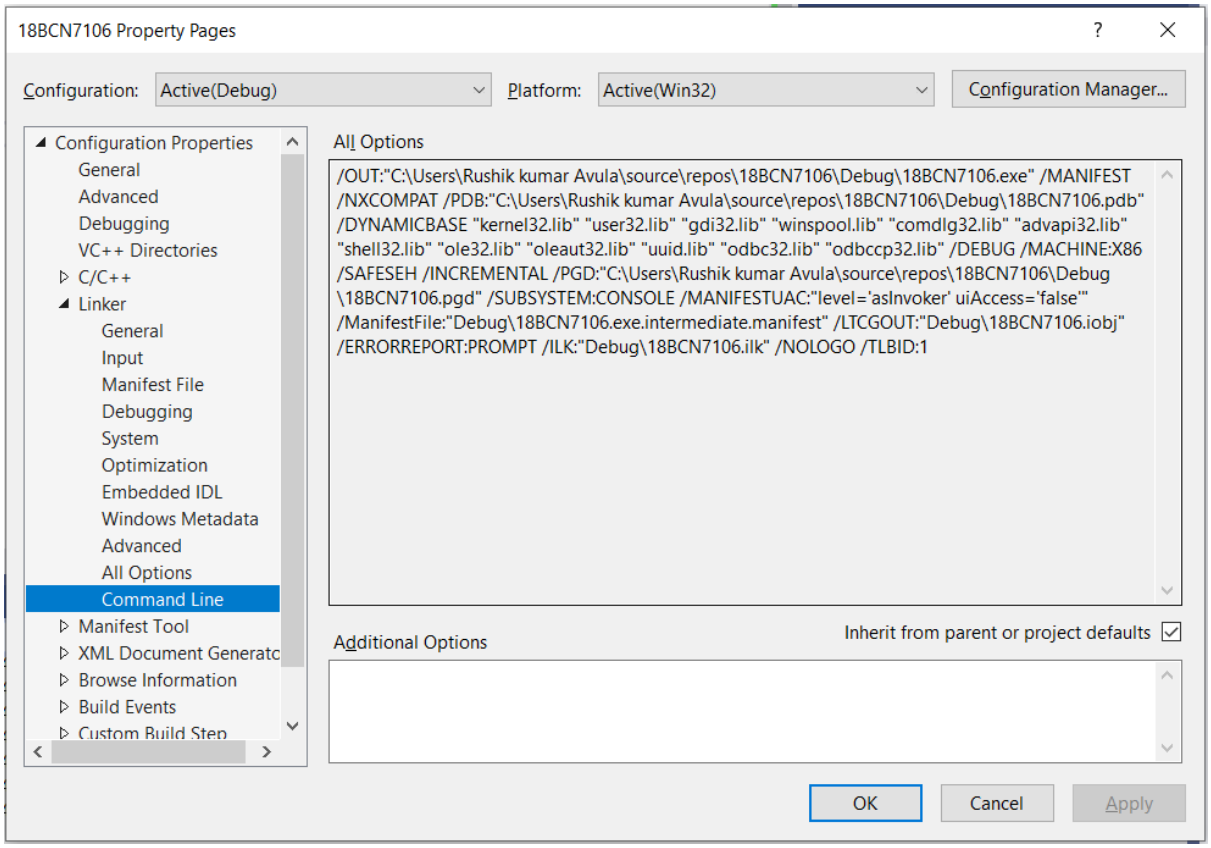
I run the CPP file to get the exe as follows :



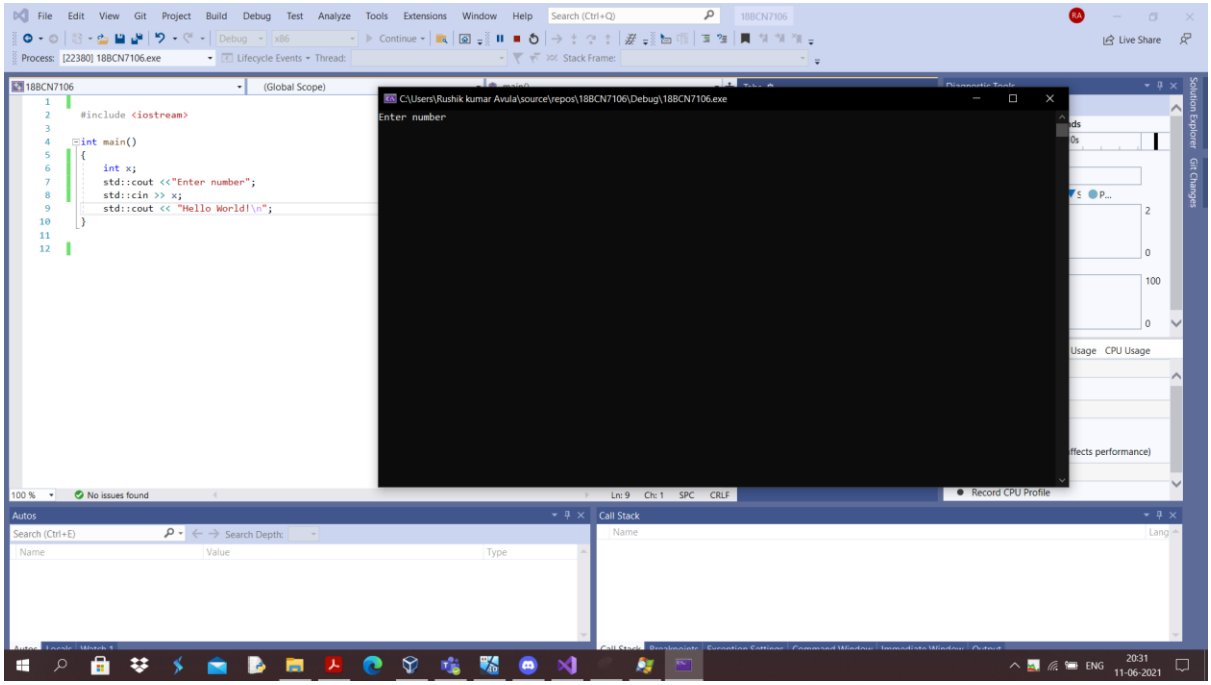
Now I started the Process Explorer to check the DEP and ASLR status.

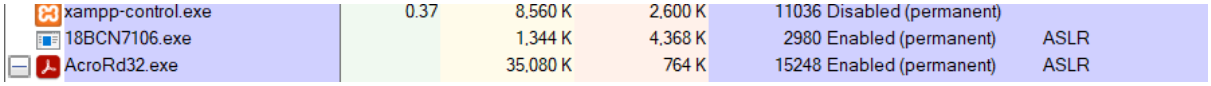


Again, I enabled the DEP and ASLR as well as SEH.



After Executing again :





xampp-control.exe	0.37	8,560 K	2,600 K	11036 Disabled (permanent)	
18BCN7106.exe		1,344 K	4,368 K	2980 Enabled (permanent)	ASLR
AcroRd32.exe		35,080 K	764 K	15248 Enabled (permanent)	ASLR