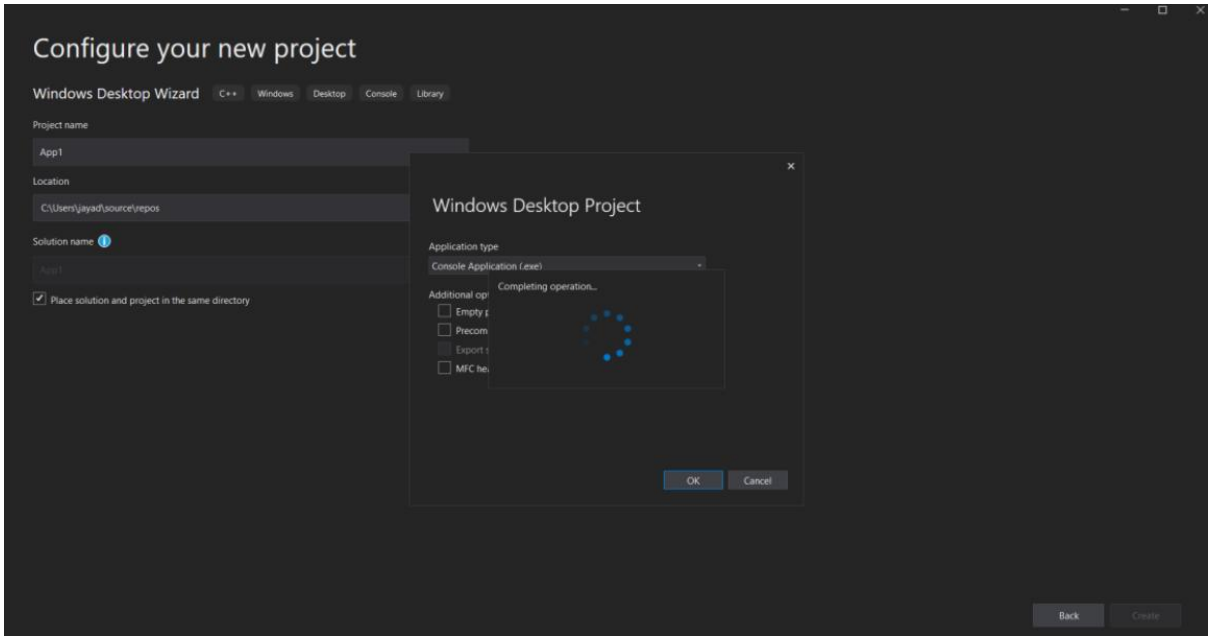
SECURECODING-LAB 11

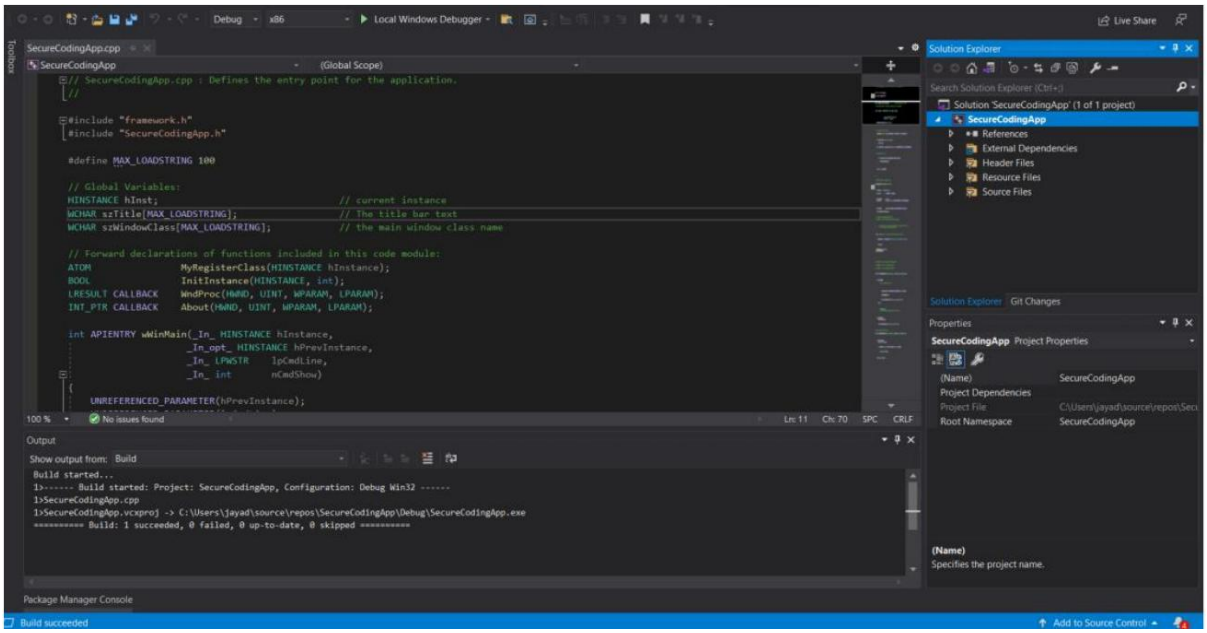
Ch. Sree Vital

18BCE7015

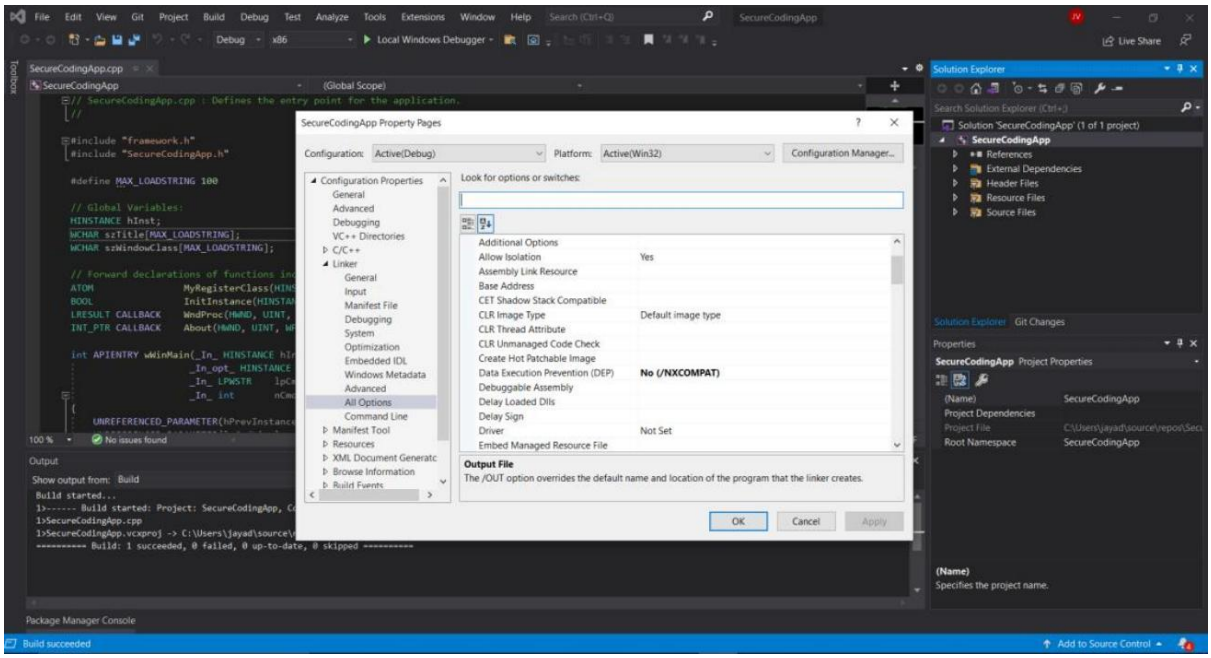
After installing visual studio:

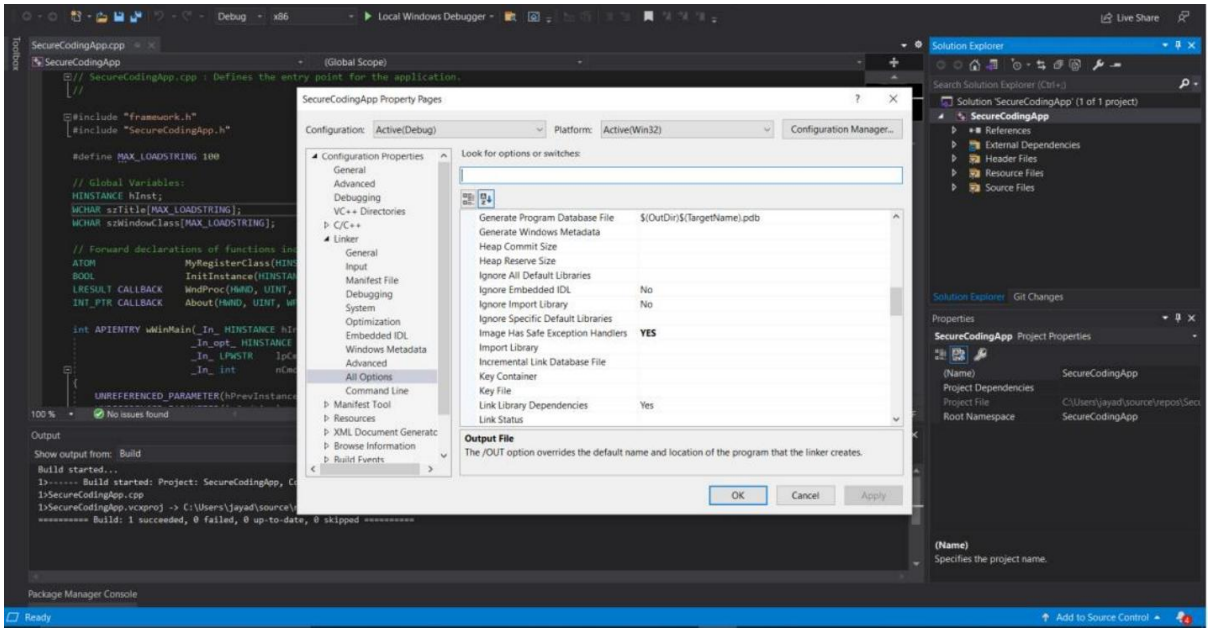


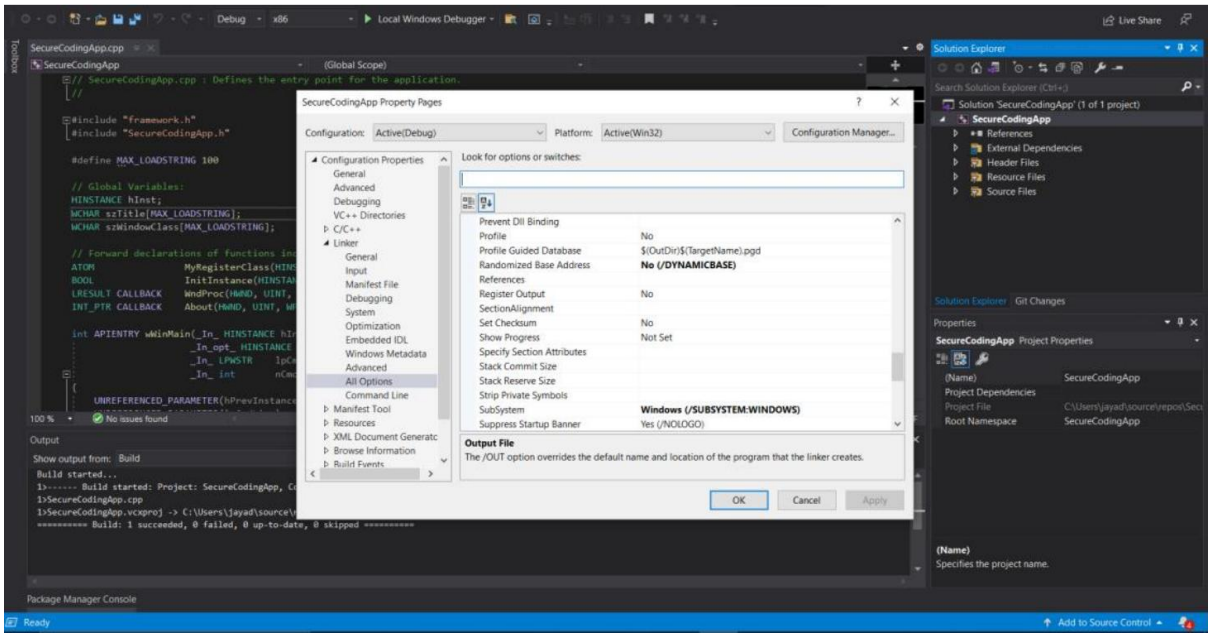
Generating .exe:



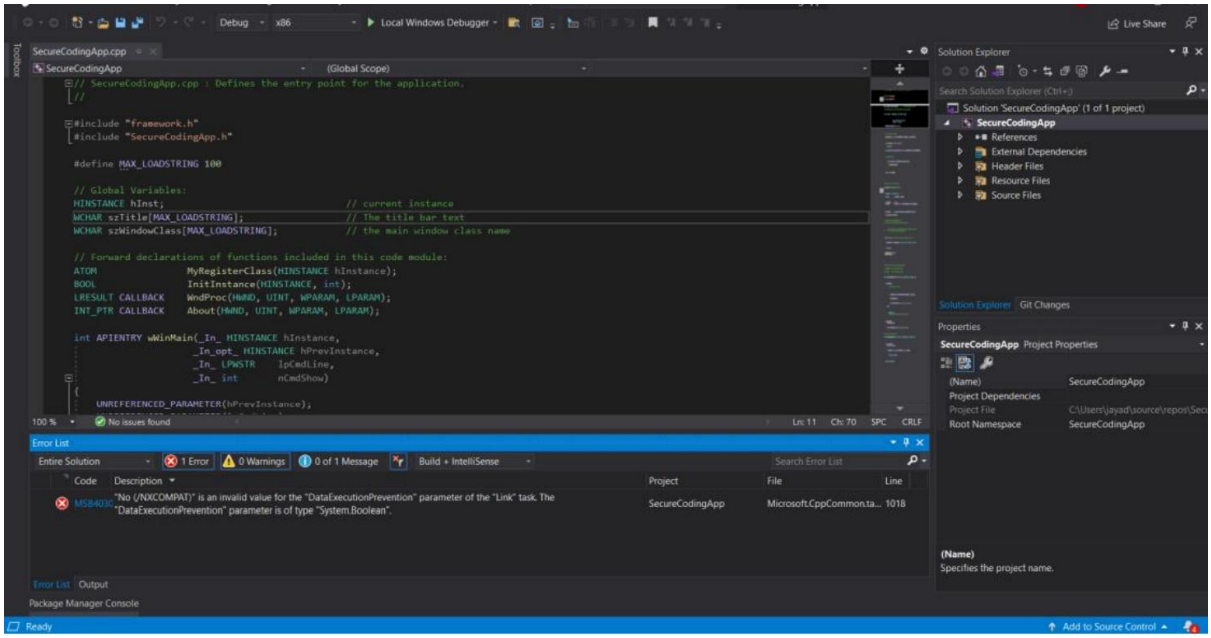
Disabling DER and ASLR:



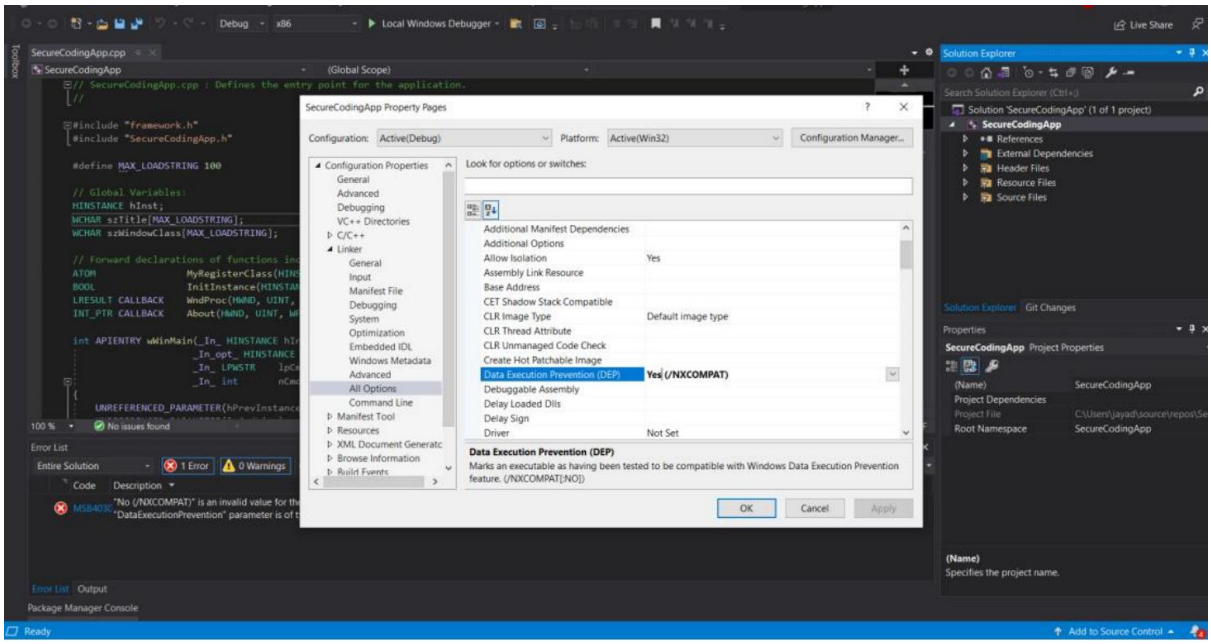

SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
Resources
XML Document Generatc
Browse Information
Build Events
Look for options or switches:
Generate Program Database File $(OutDir)$(TargetName).pdb
Generate Windows Metadata
Heap Commit Size
Heap Reserve Size
Ignore All Default Libraries
Ignore Embedded IDL No
Ignore Import Library No
Ignore Specific Default Libraries
Image Has Safe Exception Handlers YES
Import Library
Incremental Link Database File
Key Container
Key File
Link Library Dependencies Yes
Link Status
Output File
The /OUT option overrides the default name and location of the program that the linker creates.
OK
Cancel
Apply

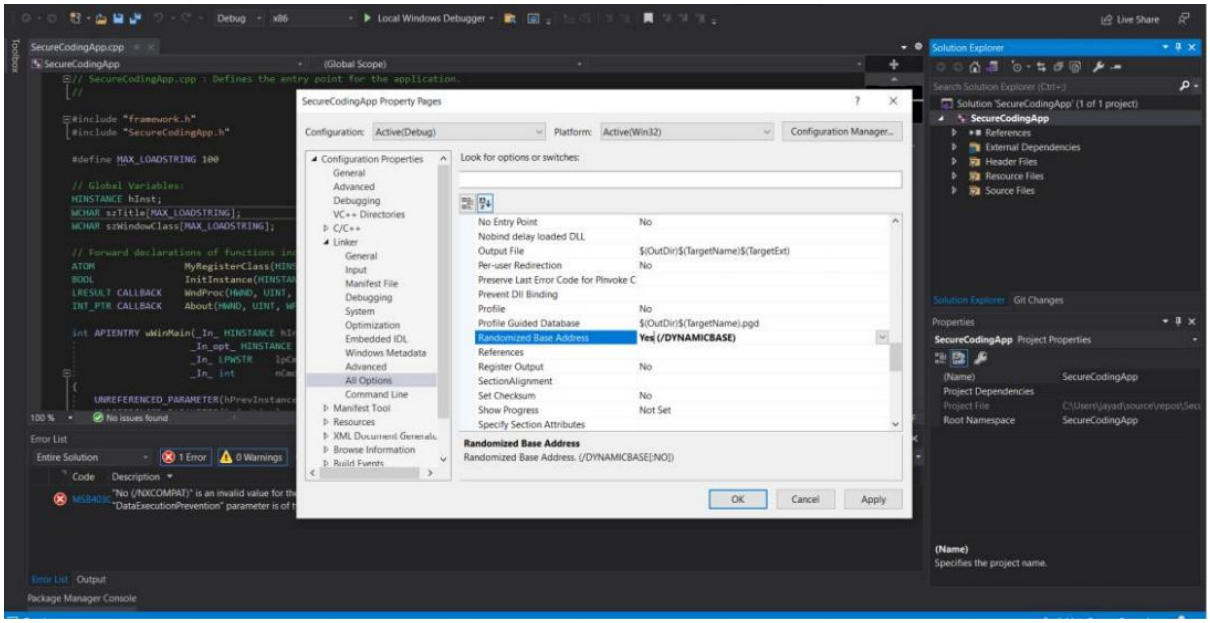

SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Look for options or switches:
Prevent Dll Binding
Profile No
Profile Guided Database $(OutDir)$(TargetName).pgd
Randomized Base Address No (/DYNAMICBASE)
References
Register Output No
SectionAlignment
Set Checksum No
Show Progress Not Set
Specify Section Attributes
Stack Commit Size
Stack Reserve Size
Strip Private Symbols
SubSystem Windows (/SUBSYSTEM:WINDOWS)
Suppress Startup Banner Yes (/NOLOGO)
Output File
The /OUT option overrides the default name and location of the program that the linker creates.
OK
Cancel
Apply

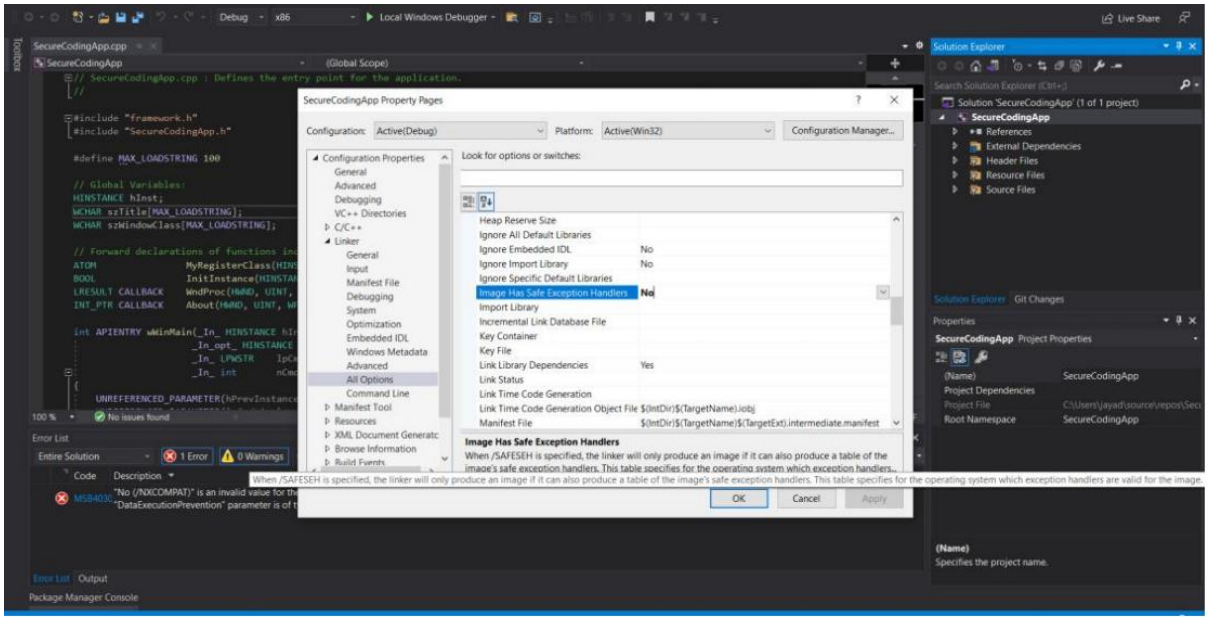
.exe file not created

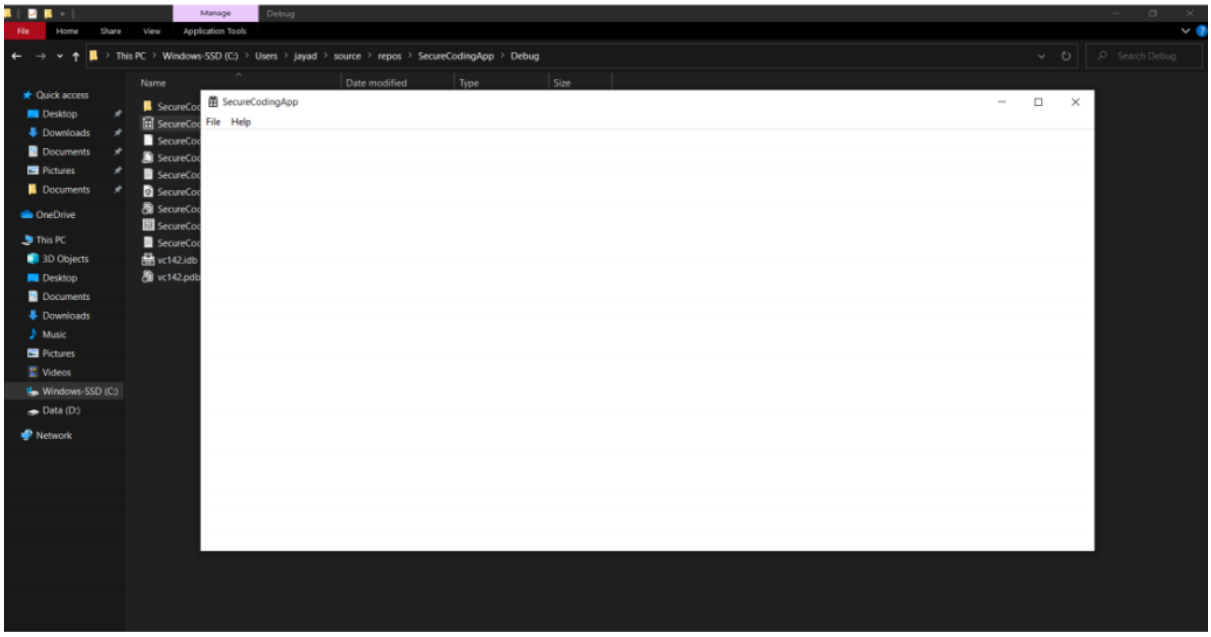


After enabling and running the app:

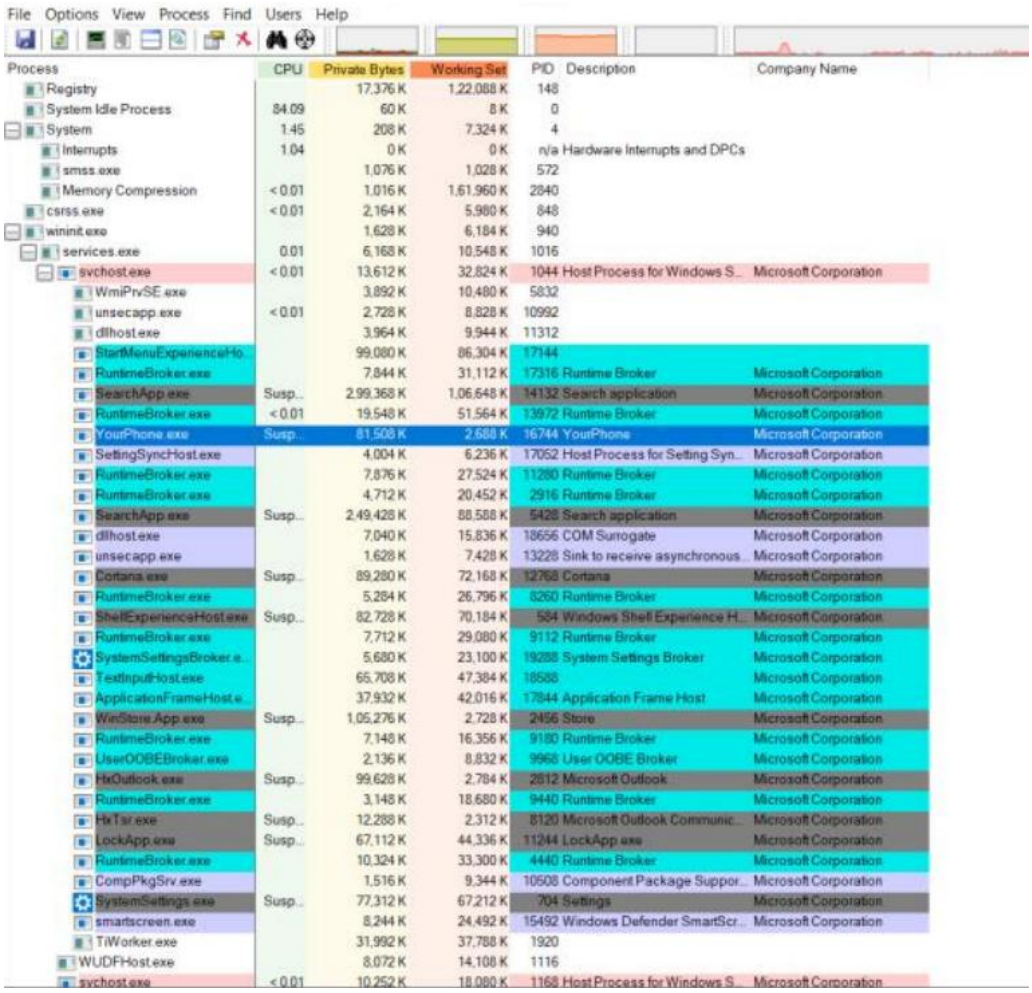


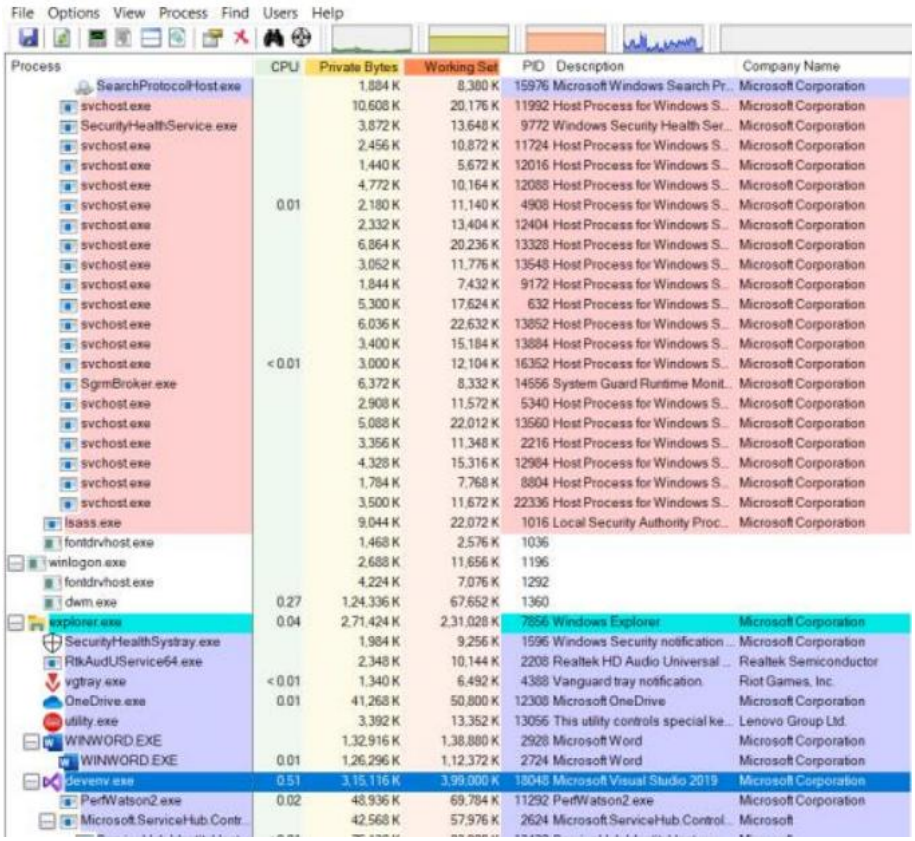

SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
Resources
XML Document Generator
Browse Information
Build Events
Look for options or switches:
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 Yes (/DYNAMICBASE)
References
Register Output No
SectionAlignment
Set Checksum No
Show Progress Not Set
Specify Section Attributes
Randomized Base Address
Randomized Base Address. (/DYNAMICBASE[:NO])
OK
Cancel
Apply

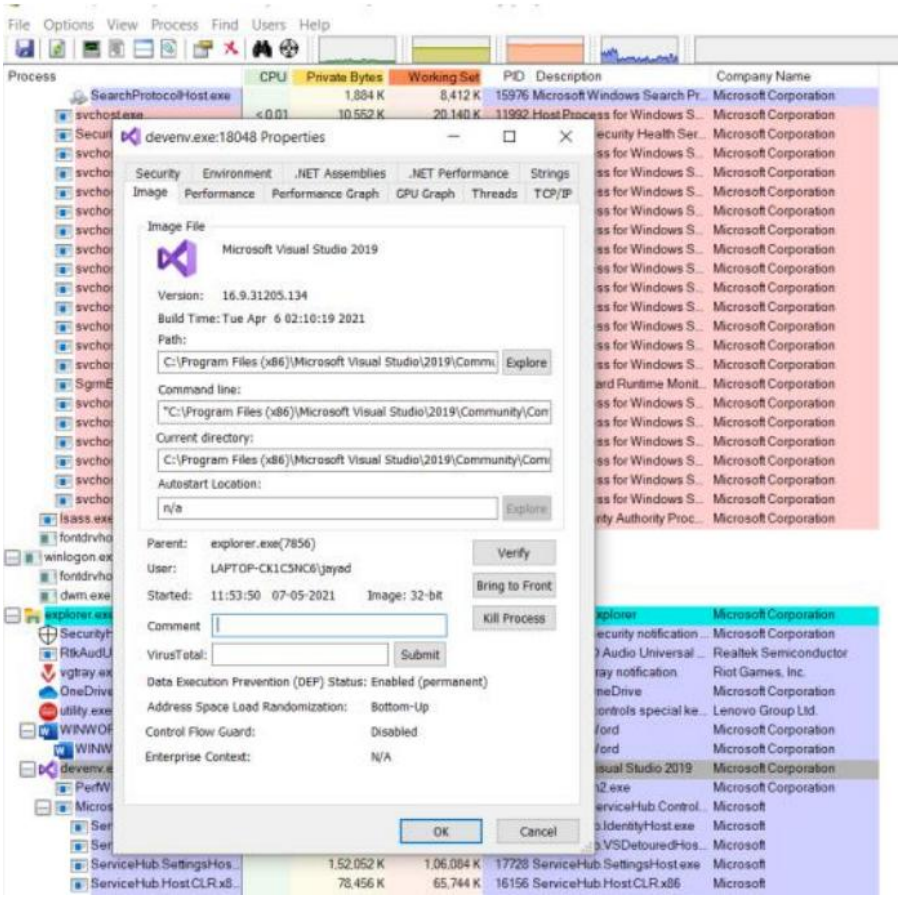

SecureCodingApp Property Pages
Configuration: Active(Debug)
Platform: Active(Win32)
Configuration Manager...
Configuration Properties
General
Advanced
Debugging
VC++ Directories
C/C++
Linker
General
Input
Manifest File
Debugging
System
Optimization
Embedded IDL
Windows Metadata
Advanced
All Options
Command Line
Manifest Tool
Resources
XML Document Generator
Browse Information
Build Events
Look for options or switches:
Heap Reserve Size
Ignore All Default Libraries
Ignore Embedded IDL No
Ignore Import Library No
Ignore Specific Default Libraries
Image Has Safe Exception Handlers No
Import Library
Incremental Link Database File
Key Container
Key File
Link Library Dependencies Yes
Link Status
Link Time Code Generation
Link Time Code Generation Object File $(IntDir)$(TargetName).iobj
Manifest File $(IntDir)$(TargetName)$(TargetExt).intermediate.manifest
Image Has Safe Exception Handlers
When /SAFESEH is specified, the linker will only produce an image if it can also produce a table of the image's safe exception handlers. This table specifies for the operating system which exception handlers are valid for the image.
When /SAFESEH is specified, the linker will only produce an image if it can also produce a table of the image's safe exception handlers. This table specifies for the operating system which exception handlers are valid for the image.
OK
Cancel
Apply



Downloading, installing and analysing through Process Explorer:




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 15976 Microsoft Windows Search Pr... Microsoft Corporation
svchost.exe 10,608 K 20,176 K 11992 Host Process for Windows S... Microsoft Corporation
SecurityHealthService.exe 3,872 K 13,648 K 9772 Windows Security Health Ser... Microsoft Corporation
svchost.exe 2,456 K 10,872 K 11724 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,440 K 5,672 K 12016 Host Process for Windows S... Microsoft Corporation
svchost.exe 4,772 K 10,164 K 12088 Host Process for Windows S... Microsoft Corporation
svchost.exe 0.01 2,180 K 11,140 K 4908 Host Process for Windows S... Microsoft Corporation
svchost.exe 2,332 K 13,404 K 12404 Host Process for Windows S... Microsoft Corporation
svchost.exe 6,864 K 20,236 K 13328 Host Process for Windows S... Microsoft Corporation
svchost.exe 3,052 K 11,776 K 13548 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,844 K 7,432 K 9172 Host Process for Windows S... Microsoft Corporation
svchost.exe 5,300 K 17,624 K 632 Host Process for Windows S... Microsoft Corporation
svchost.exe 6,036 K 22,632 K 13852 Host Process for Windows S... Microsoft Corporation
svchost.exe 3,400 K 15,184 K 13884 Host Process for Windows S... Microsoft Corporation
svchost.exe < 0.01 3,000 K 12,104 K 16352 Host Process for Windows S... Microsoft Corporation
SgrmBroker.exe 6,372 K 8,332 K 14556 System Guard Runtime Monit... Microsoft Corporation
svchost.exe 2,908 K 11,572 K 5340 Host Process for Windows S... Microsoft Corporation
svchost.exe 5,088 K 22,012 K 13560 Host Process for Windows S... Microsoft Corporation
svchost.exe 3,356 K 11,348 K 2216 Host Process for Windows S... Microsoft Corporation
svchost.exe 4,328 K 15,316 K 12984 Host Process for Windows S... Microsoft Corporation
svchost.exe 1,784 K 7,768 K 8804 Host Process for Windows S... Microsoft Corporation
svchost.exe 3,500 K 11,672 K 22336 Host Process for Windows S... Microsoft Corporation
lsass.exe 9,044 K 22,072 K 1016 Local Security Authority Proc... Microsoft Corporation
fontdrvhost.exe 1,468 K 2,576 K 1036
winlogon.exe 2,688 K 11,656 K 1196
fontdrvhost.exe 4,224 K 7,076 K 1292
dwm.exe 0.27 1,24,336 K 67,652 K 1360
explorer.exe 0.04 2,71,424 K 2,31,028 K 7856 Windows Explorer Microsoft Corporation
SecurityHealthSystray.exe 1,984 K 9,256 K 1596 Windows Security notification ... Microsoft Corporation
RtkAudUService64.exe 2,348 K 10,144 K 2208 Realtek HD Audio Universal ... Realtek Semiconductor
vgtray.exe < 0.01 1,340 K 6,492 K 4388 Vanguard tray notification Riot Games, Inc.
OneDrive.exe 0.01 41,268 K 50,800 K 12308 Microsoft OneDrive Microsoft Corporation
utility.exe 3,392 K 13,352 K 13056 This utility controls special ke... Lenovo Group Ltd.
WINWORD.EXE 1,32,916 K 1,38,880 K 2928 Microsoft Word Microsoft Corporation
WINWORD.EXE 0.01 1,26,296 K 1,12,372 K 2724 Microsoft Word Microsoft Corporation
devenv.exe 0.51 3,15,116 K 3,99,000 K 18048 Microsoft Visual Studio 2019 Microsoft Corporation
PerfWatson2.exe 0.02 48,936 K 69,784 K 11292 PerfWatson2.exe Microsoft Corporation
Microsoft.ServiceHub.Contr... 42,568 K 57,976 K 2624 Microsoft.ServiceHub.Control... Microsoft


File Options View Process Find Users Help
Process
CPU
Private Bytes
Working Set
PID
Description
Company Name
devenv.exe:18048 Properties
Security
Environment
.NET Assemblies
.NET Performance
Strings
Image
Performance
Performance Graph
GPU Graph
Threads
TCP/IP
Image File
Microsoft Visual Studio 2019
Version: 16.9.31205.134
Build Time: Tue Apr 6 02:10:19 2021
Path:
C:\Program Files (x86)\Microsoft Visual Studio\2019\Comm
Explore
Command line:
"C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Con
Current directory:
C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Com
Autostart Location:
n/a
Explore
Parent: explorer.exe(7856)
User: LAPTOP-CK1C5NC6\jayad
Started: 11:53:50 07-05-2021 Image: 32-bit
Comment
VirusTotal:
Submit
Verify
Bring to Front
Kill Process
Data Execution Prevention (DEP) Status: Enabled (permanent)
Address Space Load Randomization: Bottom-Up
Control Flow Guard: Disabled
Enterprise Context: N/A
OK
Cancel
SearchProtocolHost.exe
1,884 K
8,412 K
15976 Microsoft Windows Search Pr...
Microsoft Corporation
ServiceHub.SettingsHos...
1,52,052 K
1,06,084 K
17728 ServiceHub.SettingsHost.exe
Microsoft
ServiceHub.Host.CLR.x8...
78,456 K
65,744 K
16156 ServiceHub.Host.CLR.x86
Microsoft