

Secure Coding Lab11

18BCE7338
N.V.Sowmith
Slot: L39+L40

Task - Creating Secure and Safe Executable in Visual Studio

Building the Executable with C++ code

```
#include <iostream>

int main(void)
{
    int authentication = 0;
    char cUsername[10];
    char cPassword[10];

    std::cout << "Username: ";
    std::cin >> cUsername;

    std::cout << "Pass: ";
    std::cin >> cPassword;

    if (std::strcmp(cUsername, "admin") == 0 &&
        std::strcmp(cPassword, "adminpass") == 0)
    {
        authentication = 1;
    }
    if (authentication)
    {
        std::cout << "Access granted\n";
        std::cout << (char)authentication;
```

```

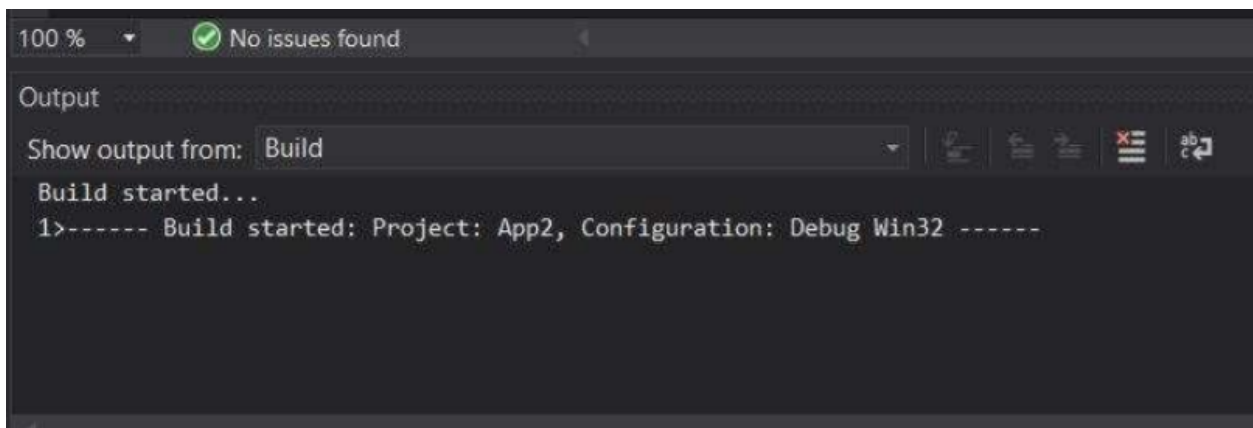
}
else
{
    std::cout << "Wrong username and password\n";
}

return (0);

```



Generating the .exe file



Verifying the DEP & ASLR status in Process Explorer

Microsoft Visual Studio Debug Console

```
Username: admin
Pass: adminpass
Access granted
@
```

< 0.01	43,024 K	19,028 K	9988 Microsoft (R) Visual ...	Microsoft Corporation
	28,612 K	43,636 K	13444 MSBuild.exe	Microsoft Corporation
	6,492 K	11,060 K	20152 Console Window Host	Microsoft Corporation
	1,236 K	6,136 K	5968 Visual Studio Debug...	Microsoft Corporation
	7,188 K	16,284 K	5072 Console Window Host	Microsoft Corporation
	780 K	4,496 K	19128	
< 0.01	44,000 K	86,880 K	16884 Microsoft Edge	Microsoft Corporation
	6,504 K	7,484 K	17008 Microsoft Edge	Microsoft Corporation

Disabling the DEP & ALSR

App2 Property Pages

Configuration: Active(Debug) Platform: Active(Win32) Configuration Manager...

Look for options or switches:

Configuration Properties

- General
- 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
- XAML Compiler
- Browse Information
- Build Events
- Custom Build Step

Additional Dependencies: WindowsApp.lib;% (AdditionalDependencies)

Additional Library Directories

Additional Manifest Dependencies

Additional Options

Allow Isolation: Yes

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

References

/OPT:REF eliminates functions and/or data that are never referenced while /OPT:NOREF keeps functions and/or data that are never referenced.

OK Cancel Apply

Heap Reserve Size	
Ignore All Default Libraries	
Ignore Embedded IDL	No
Ignore Import Library	Yes
Ignore Specific Default Libraries	
Image Has Safe Exception Handlers	YES
Import Library	

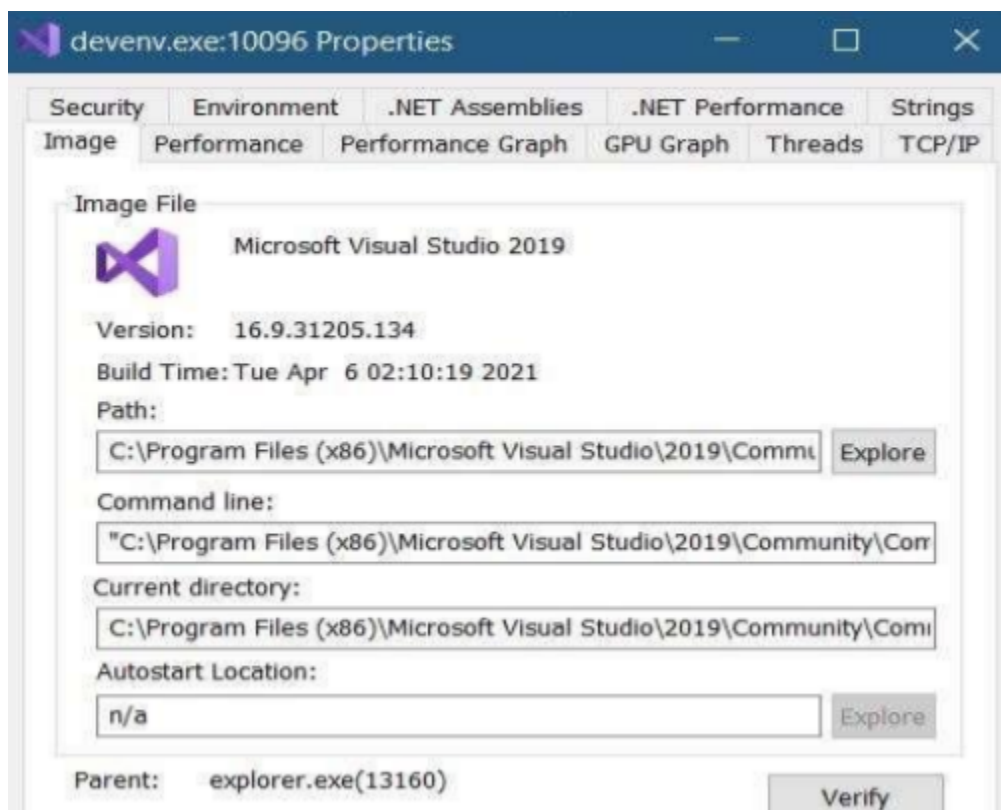
MIDL Commands	
Minimum Required Version	
Module Definition File	
No Entry Point	No
Nobind delay loaded DLL	
Output File	\$(OutDir)\$(TargetName)\$(TargetExt)
Per-user Redirection	No
Preserve Last Error Code for PInvoke C	
Prevent Dll Binding	
Profile	No
Profile Guided Database	\$(OutDir)\$(TargetName).pgd
Randomized Base Address	No (/DYNAMICBASE:NO)
References	
Register Output	No
SectionAlignment	

We can see DEP is disabled and no ASLR

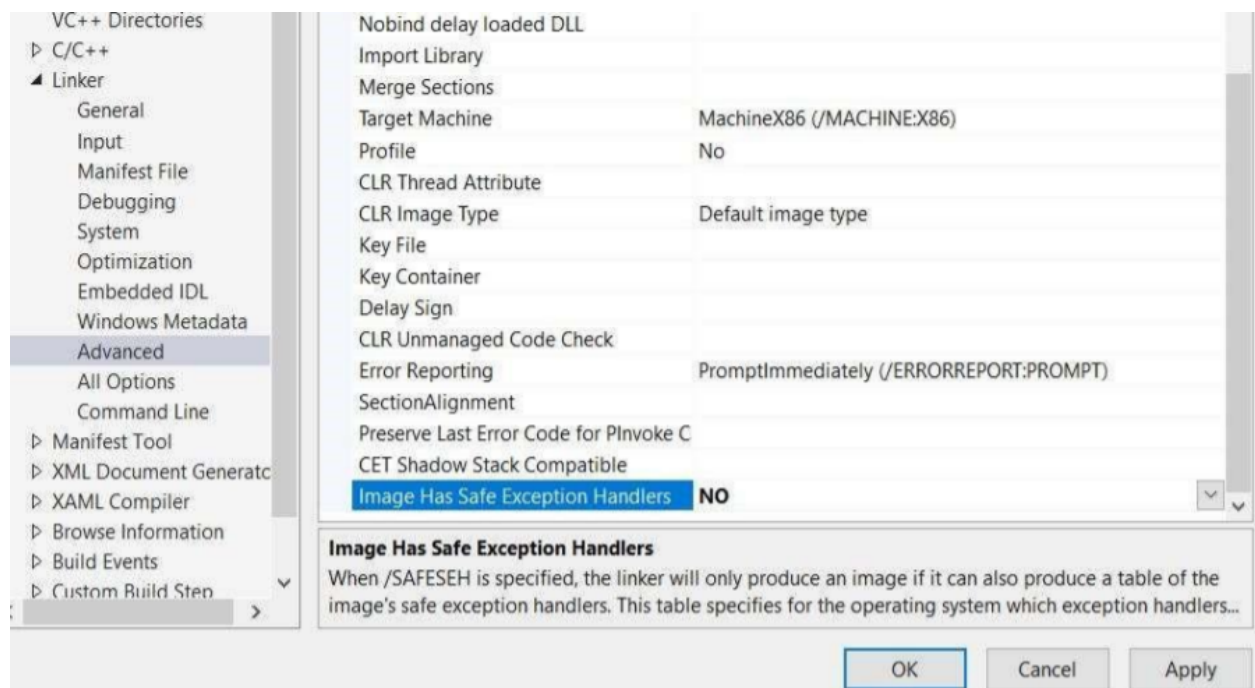
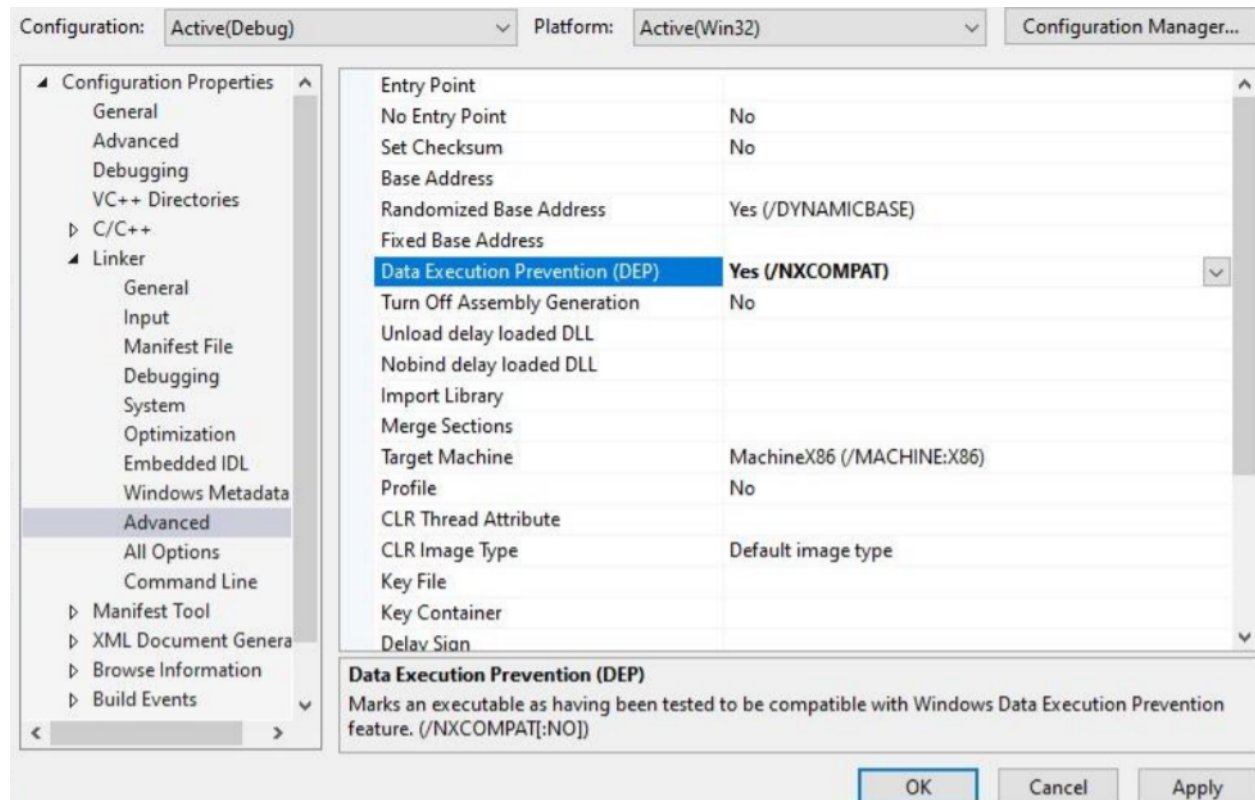
After disabling the DEP system will not allow to build the .exe file

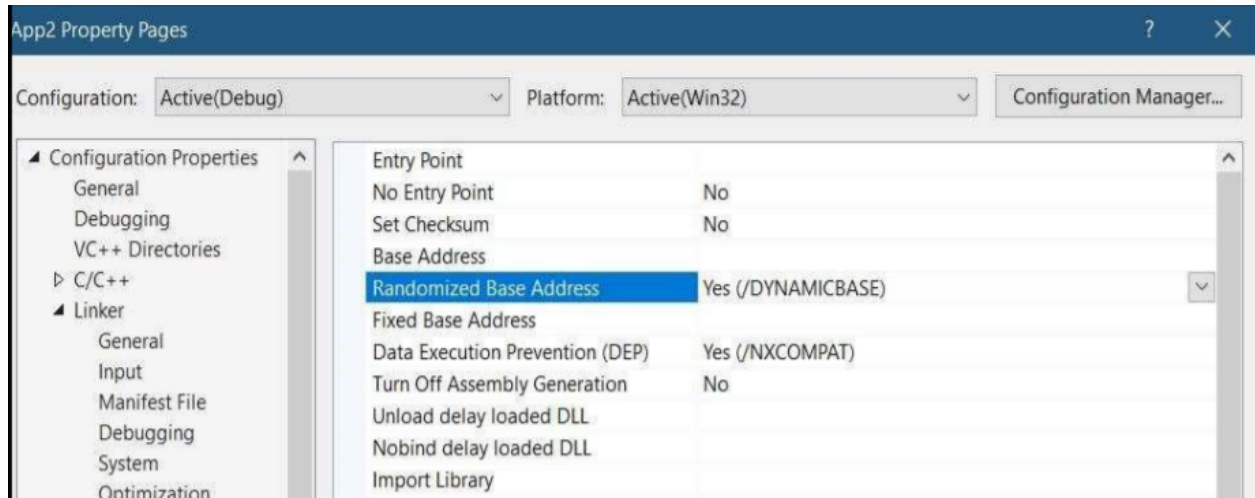


So need to enable DEP again



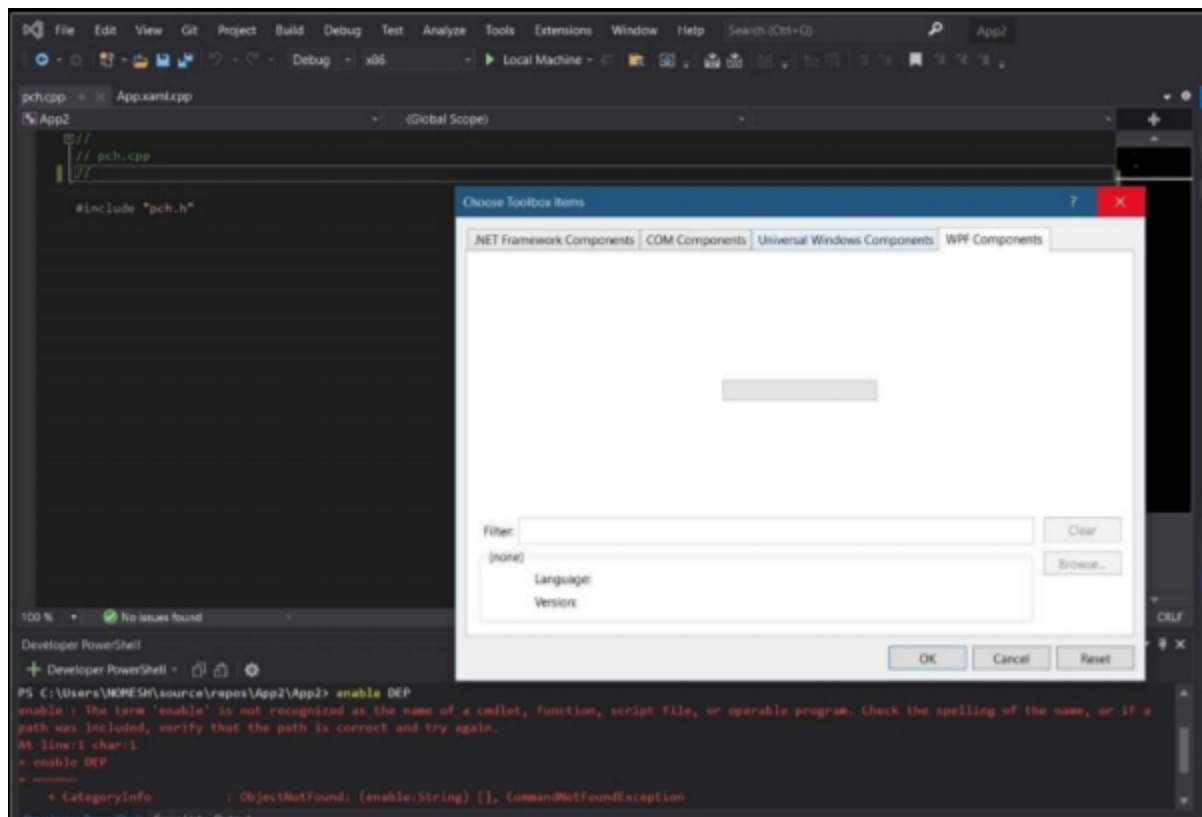
Rebuilding the same Executable after Enabling the DEP & ASLR



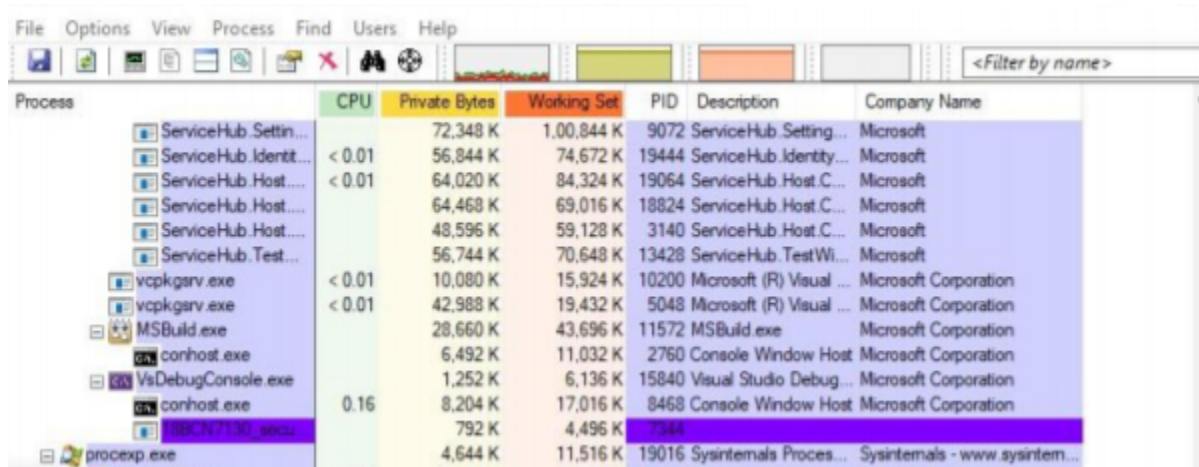


I have Enabled DEP, ASLR, SEH again

The Visual Studio will not respond after enabling the ASLR :



Verifying the status of DEP & ASLR in Process Explorer after Enabling



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
ServiceHub.Settin...		72,348 K	1,00,844 K	9072	ServiceHub.Setting...	Microsoft
ServiceHub.Identi...	< 0.01	56,844 K	74,672 K	19444	ServiceHub.Identity...	Microsoft
ServiceHub.Host...	< 0.01	64,020 K	84,324 K	19064	ServiceHub.Host.C...	Microsoft
ServiceHub.Host...		64,468 K	69,016 K	18824	ServiceHub.Host.C...	Microsoft
ServiceHub.Host...		48,596 K	59,128 K	3140	ServiceHub.Host.C...	Microsoft
ServiceHub.Test...		56,744 K	70,648 K	13428	ServiceHub.TestWi...	Microsoft
vcpkgarv.exe	< 0.01	10,080 K	15,924 K	10200	Microsoft (R) Visual ...	Microsoft Corporation
vcpkgarv.exe	< 0.01	42,988 K	19,432 K	5048	Microsoft (R) Visual ...	Microsoft Corporation
MSBuild.exe		28,660 K	43,696 K	11572	MSBuild.exe	Microsoft Corporation
conhost.exe		6,492 K	11,032 K	2760	Console Window Host	Microsoft Corporation
VsDebugConsole.exe		1,252 K	6,136 K	15840	Visual Studio Debug...	Microsoft Corporation
conhost.exe	0.16	8,204 K	17,016 K	8468	Console Window Host	Microsoft Corporation
procexp.exe		792 K	4,496 K	7548		
procexp.exe		4,644 K	11,516 K	19016	Sysinternals Proces...	Sysinternals - www.sysintern...

chrome.exe		22,200 K	44,564 K	17136	Google Chrome	Google LLC	Enabled (permane... ASLR
chrome.exe		17,856 K	23,164 K	2152	Google Chrome	Google LLC	Enabled (permane... ASLR
devenv.exe	1.30	2,46,852 K	3,68,992 K	10096	Microsoft Visual Studio 2019	Microsoft Corporation	Enabled (permane... ASLR
PerfWatson2.exe	< 0.01	48,792 K	69,516 K	11916	PerfWatson2.exe	Microsoft Corporation	Enabled (permane... ASLR
Microsoft ServiceHub Contr		35,140 K	50,676 K	13156	Microsoft ServiceHub Control	Microsoft	Enabled (permane... ASLR