

SECURE CODING LAB 10

SUKHMANI SANDHU 18BCE7155

DATE: 26-04-2021

First we work on building an executable on Visual Studio. (C++)
(for this we write the script, build the console application and run it)

```
securecode.cpp  x
securecode (Global Scope)
1 // securecode.cpp : This file contains the 'main' functi
2 //
3
4 #include <iostream>
5 #include <string>
6
7 int main()
8 {
9     std::string biass;
10    std::cout << "Welcome to this thing!\n";
11    std::cout << "Enter your bias:\n ";
12    std::cin >> biass;
13 }
14
15 // ...
```

Below, is the script when run from the IDE

```
Microsoft Visual Studio Debug Console
Welcome to this thing!
Enter your bias:
JK
D:\VSCode\securecode\Debug\securecode.exe (process 9844) exited with code 0.
Press any key to close this window . . .
```

For the purpose of this analysis, we have also dowloaded and installed Process Explorer.
Here, we enable the DEP(Data Execution Prevention) and ASLR (Address Space Layout Randomization) columns.

Process	CPU	Privat...	Working ...	PID	Description	DEP	ASLR
Registry		15,540 K	44,384 K	124		n/a	n/a
System Idle Process	86.93	60 K	8 K	0		Enabled (permane...	n/a
System	1.08	196 K	120 K	4		n/a	n/a
Interrupts	0.44	0 K	0 K	n/a	Hardware Int...	n/a	n/a
smss.exe		1,088 K	1,040 K	572		n/a	n/a
Memory Compression	< 0.01	804 K	80,600 K	2920		n/a	n/a
csrss.exe	< 0.01	2,288 K	5,440 K	788		n/a	n/a
wininit.exe		1,412 K	5,096 K	904		n/a	n/a
services.exe	< 0.01	6,756 K	11,064 K	976		n/a	n/a
svchost.exe	0.10	14,988 K	34,840 K	660	Host Process...	n/a	ASLR
unsecapp.exe		1,524 K	6,112 K	5480		n/a	n/a
WmiPrvSE.exe		33,412 K	43,044 K	5556		n/a	n/a
dllhost.exe		1,732 K	6,696 K	9160	COM Surroga...	Enabled (permane...	ASLR
StartMenuExperienceHo...		36,776 K	84,656 K	9220		Enabled (permane...	ASLR
RuntimeBroker.exe		6,836 K	26,024 K	9316	Runtime Brok...	Enabled (permane...	ASLR
SearchApp.exe	Susp...	2,60,15...	1,05,584 K	9468	Search appli...	Enabled (permane...	ASLR
RuntimeBroker.exe		15,764 K	45,872 K	9672	Runtime Brok...	Enabled (permane...	ASLR

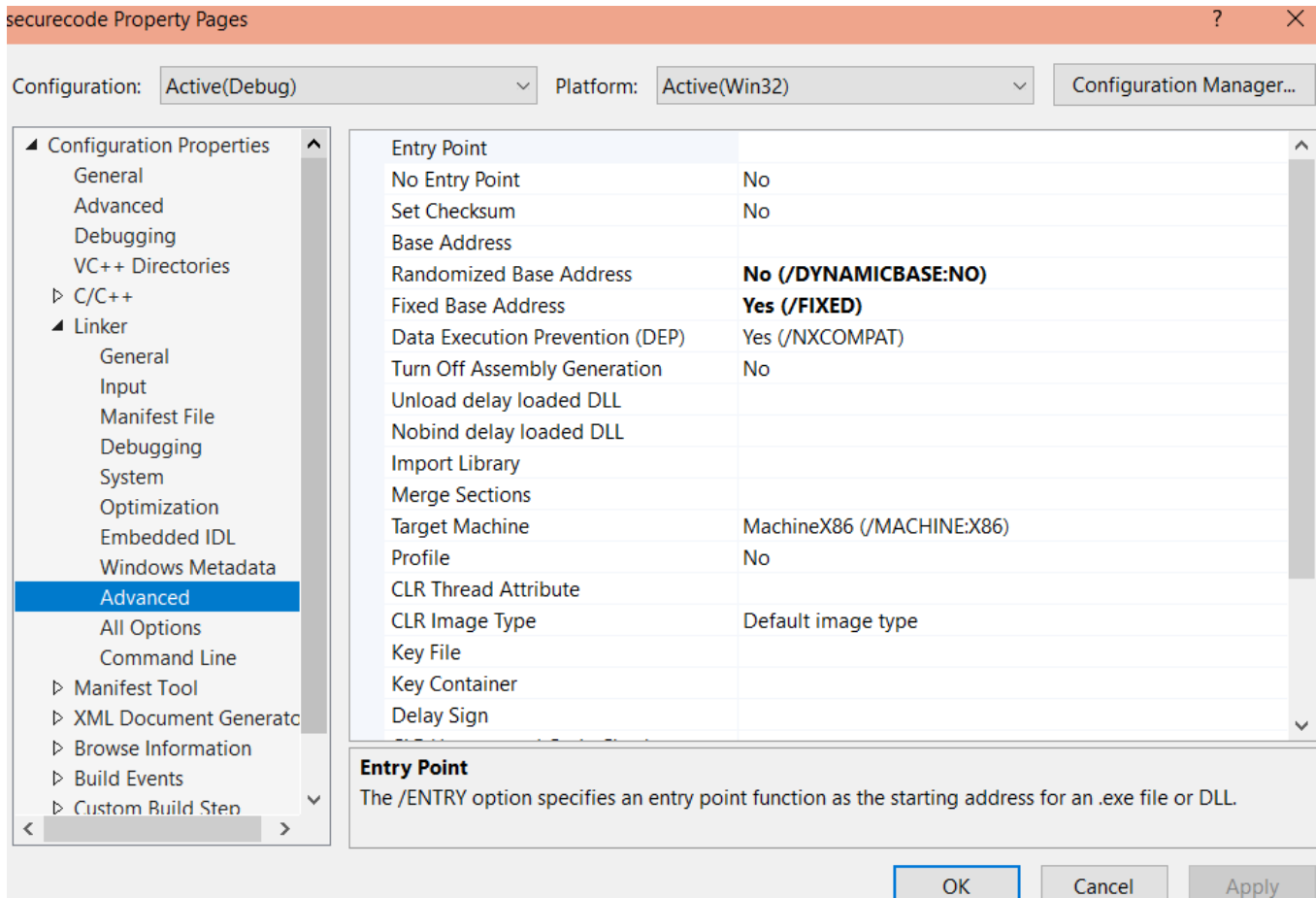
```
D:\>cd D:\VSCode\securecode\Debug

D:\VSCode\securecode\Debug>securecode.exe
Welcome to this thing!
Enter your bias:
    OT7 honestly

D:\VSCode\securecode\Debug>_
```

Additionally, we find the executable for our application and run it on the command prompt.

Going back to Visual Studio, we will enable Randomized Base Address and DEP options in the project properties like so.



We again build and run the application.

Process	CPU	Privat...	Working ...	PID	Description	DEP	ASLR
chrome.exe		49,256 K	86,996 K	11316	Google Chro...	Enabled (permane...	ASLR
chrome.exe		17,868 K	24,440 K	3528	Google Chro...	Enabled (permane...	ASLR
rundll32.exe		2,424 K	9,408 K	6240	Windows hos...	Enabled (permane...	ASLR
securecode.exe		1,252 K	4,864 K	10268		Enabled (permane...	
conhost.exe		8,644 K	17,036 K	15500	Console Win...	Enabled (permane...	ASLR

securecode.exe:10268 Properties

GPU GraphThreadsTCP/IPSecurityEnvironmentJobStrings

ImagePerformancePerformance GraphDisk and Network

Image File

Version: n/a

Build Time: Thu Apr 29 21:06:42 2021

Path (Image is probably packed):

D:\VSCode\securecode\Debug\securecode.exe

Explore

Command line:

"D:\VSCode\securecode\Debug\securecode.exe"

Current directory:

D:\VSCode\securecode\Debug\

Autostart Location:

n/a

Explore

Parent: explorer.exe(11200)

User: DESKTOP-IKR7L1A\sukhm

Started: 21:27:24 29-04-2021 Image: 32-bit

Comment

VirusTotal:

Submit

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

Address Space Load Randomization: Enabled (permanent)Disabled

Control Flow Guard: Disabled

Verify

Bring to Front

Kill Process

Path
C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\KernelBase.d
C:\Program Files (x86)\Common Files\K
C:\Windows\System32\locale.nls