

Secure Coding (CSE 2010)

LAB Experiment: 11

Done by,

Aadil Mohammed

Reg.No:19BCI7052

SLOT: L23+L24

Lab experiment – Creating secure and safe executable

Download and install visual studio (recent edition)

Write a C++ code of your own to build an executable and run the same.

Download process explorer and verify the DEP & ASLR status

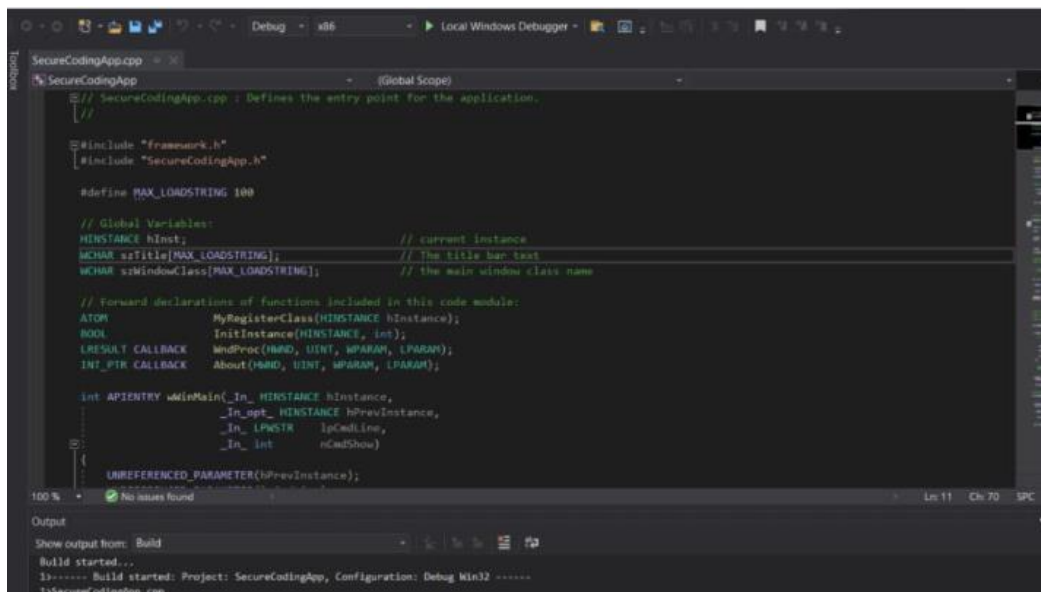
Enable software DEP, ASLR and SEH in the visual studio and rebuild the same executable

Again, verify the DEP & ASLR status in the process explorer

Report the same with separate screenshot - before and after enabling DEP & ASLR.

Happy Learning!!!

- Creating a new executable (.exe) file



```

SecureCodingApp.cpp
SecureCodingApp
(Global Scope)
// SecureCodingApp.cpp : Defines the entry point for the application.
//
#include "framework.h"
#include "SecureCodingApp.h"

#define MAX_LOADSTRING 100

// Global Variables:
HINSTANCE hInst;                                // current instance
WCHAR szTitle[MAX_LOADSTRING];                  // The title bar text
WCHAR szWindowClass[MAX_LOADSTRING];            // the main window class name

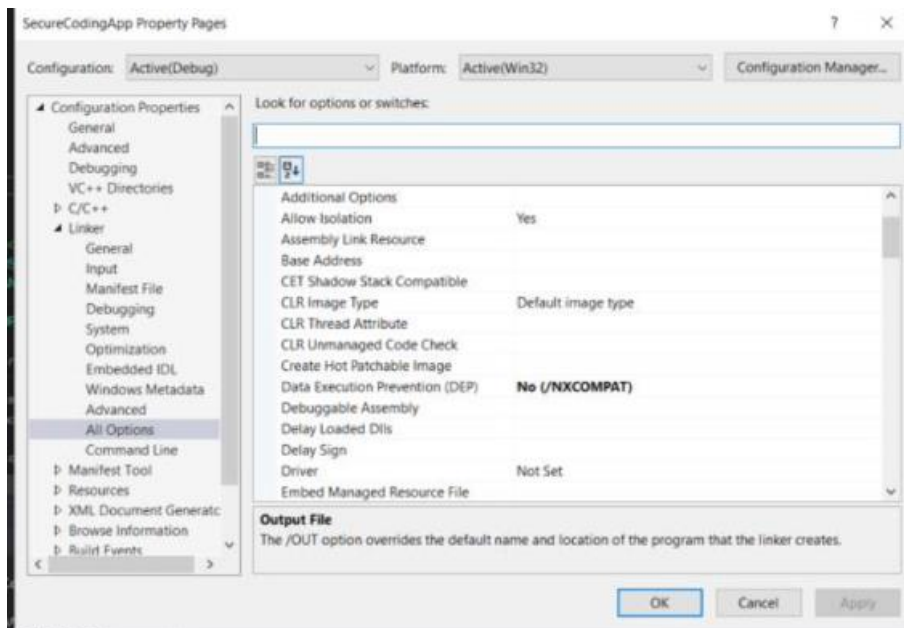
// Forward declarations of functions included in this code module:
ATOM MyRegisterClass(HINSTANCE hInstance);
BOOL InitInstance(HINSTANCE, int);
LRESULT CALLBACK WndProc(HWND, UINT, WPARAM, LPARAM);
INT_PTR CALLBACK About(HWND, UINT, WPARAM, LPARAM);

int APIENTRY wMain(_In_ HINSTANCE hInstance,
                 _In_opt_ HINSTANCE hPrevInstance,
                 _In_ LPWSTR lpCmdLine,
                 _In_ int nCmdShow)
{
    UNREFERENCED_PARAMETER(hPrevInstance);

    // ...
}

```

- Disabling DER and ASLR:



Process Explorer - Systematix: www.systematix.com [LAPTOP-B196QUJ3\Nishit Verma]

File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name | DEP | ASLR |
|-----------------------------|--------|---------------|-------------|-------|----------------------------------|----------------------------|----------------------|------|
| chrome-control.exe | 0.25 | 7,220 K | 9,876 K | 16116 | | | Disabled (permanent) | |
| chrome.exe | < 0.01 | 76,900 K | 1,32,152 K | 7604 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 6,112 K | 6,916 K | 9848 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 3,02,280 K | 2,56,372 K | 20012 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 21,264 K | 33,496 K | 15124 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 13,704 K | 15,748 K | 14324 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 33,604 K | 44,128 K | 16088 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| cmd.exe | | 2,152 K | 3,848 K | 14872 | Windows Command Process... | Microsoft Corporation | Enabled (permanent) | ASLR |
| conhost.exe | | 6,620 K | 7,548 K | 18306 | Console Window Host | Microsoft Corporation | Enabled (permanent) | ASLR |
| browserhost.exe | | 5,416 K | 8,300 K | 12348 | McAfee WebAdvisor | McAfee, LLC | Enabled (permanent) | ASLR |
| cmd.exe | | 2,152 K | 3,864 K | 12292 | Windows Command Process... | Microsoft Corporation | Enabled (permanent) | ASLR |
| conhost.exe | | 6,672 K | 7,536 K | 10444 | Console Window Host | Microsoft Corporation | Enabled (permanent) | ASLR |
| McBrowHost.exe | | 4,744 K | 9,872 K | 18112 | McAfee WDS Shared Brow... | McAfee, LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 13,768 K | 19,080 K | 16332 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | 0.01 | 2,34,016 K | 1,90,168 K | 15532 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 17,960 K | 18,964 K | 11060 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome-control.exe | 0.27 | 6,336 K | 19,900 K | 1400 | | | Disabled (permanent) | |
| devenv.exe | 1.18 | 242,444 K | 3,55,034 K | 5620 | Microsoft Visual Studio 2019 | Microsoft Corporation | Enabled (permanent) | ASLR |
| PerfWatson2.exe | < 0.01 | 46,776 K | 67,000 K | 12776 | PerfWatson2.exe | Microsoft Corporation | Enabled (permanent) | ASLR |
| Microsoft.ServiceHub.Con... | < 0.01 | 41,432 K | 56,372 K | 12132 | Microsoft.ServiceHub.Con... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.IdentityHost... | 0.01 | 60,752 K | 79,528 K | 4704 | ServiceHub.IdentityHost.exe | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.VSDetours... | | 94,908 K | 77,980 K | 4708 | ServiceHub.VSDetoursHost... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.SettingsHost... | 0.01 | 1,00,960 K | 1,02,232 K | 9900 | ServiceHub.SettingsHost.exe | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.Host.CLR.x86... | | 1,24,448 K | 81,928 K | 19144 | ServiceHub.Host.CLR.x86... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.TestWindow... | | 64,544 K | 71,936 K | 13320 | ServiceHub.TestWindowSt... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.Host.CLR.x86... | | 57,488 K | 63,256 K | 19320 | ServiceHub.Host.CLR.x86... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.DataWarehouse... | 0.03 | 87,640 K | 96,992 K | 14048 | ServiceHub.DataWarehouse... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.ThreadedW... | | 72,176 K | 80,884 K | 2344 | ServiceHub.ThreadedWai... | Microsoft | Enabled (permanent) | ASLR |
| vsipgsvc.exe | < 0.01 | 19,216 K | 26,776 K | 18720 | Microsoft (R) Visual C++ Pack... | Microsoft Corporation | Enabled (permanent) | ASLR |
| MSBuild.exe | | 36,368 K | 48,716 K | 14548 | MSBuild.exe | Microsoft Corporation | Enabled (permanent) | ASLR |
| conhost.exe | | 6,396 K | 10,828 K | 2496 | Console Window Host | Microsoft Corporation | Enabled (permanent) | ASLR |
| ScriptedGDI.exe | | 15,220 K | 26,832 K | 4420 | | | Disabled (permanent) | |
| ScriptedGDI.exe | 0.03 | 92,520 K | 1,21,424 K | 21372 | ScriptedGDI.exe | Microsoft Corporation | Enabled (permanent) | ASLR |
| process.exe | | 5,196 K | 11,404 K | 15968 | Systematix Process Explorer | Systematix - www.system... | Enabled (permanent) | ASLR |
| process4.exe | 0.01 | 41,460 K | 60,480 K | 18332 | Systematix Process Explorer | Systematix - www.system... | Enabled (permanent) | ASLR |
| ShippingTool.exe | | 4,516 K | 20,024 K | 12148 | Shipping Tool | Microsoft Corporation | Enabled (permanent) | ASLR |
| GoogleCrashHandler.exe | 0.30 | 1,616 K | 116 K | 11236 | | n/a | n/a | n/a |
| GoogleCrashHandler64.exe | | 1,672 K | 148 K | 11244 | | n/a | n/a | n/a |
| juched.exe | | 4,168 K | 8,732 K | 12536 | Java Update Scheduler | Oracle Corporation | Enabled (permanent) | ASLR |
| juchek.exe | | 3,944 K | 7,460 K | 16672 | Java Update Checker | Oracle Corporation | Enabled (permanent) | ASLR |
| HPSystemEventLibHost.exe | | 69,004 K | 22,380 K | 14428 | HPSystemEventLibHost | HP Inc. | Enabled (permanent) | ASLR |
| McPvTray.exe | | 3,648 K | 784 K | 6456 | McAfee File Lock Monitor | McAfee, LLC | Enabled (permanent) | ASLR |
| McSmfWk.exe | | 2,996 K | 3,416 K | 1212 | | n/a | n/a | n/a |
| Teams.exe | < 0.01 | 2,02,736 K | 1,46,476 K | 10304 | Microsoft Teams | Microsoft Corporation | Enabled (permanent) | ASLR |
| Teams.exe | | 1,09,620 K | 77,196 K | 5216 | Microsoft Teams | Microsoft Corporation | Enabled (permanent) | ASLR |

- When DEP and ASLR status in program explorer when DEP and ASLR has been enabled in visual studio for the executable file.

File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name | DEP | ASLR |
|-----------------------------|--------|---------------|-------------|-------|----------------------------------|----------------------------|----------------------|------|
| chrome.exe | < 0.01 | 76,902 K | 1,31,812 K | 7604 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 6,112 K | 6,904 K | 9848 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 3,02,280 K | 2,51,248 K | 20012 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 21,096 K | 33,204 K | 15124 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 13,704 K | 15,720 K | 14324 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 33,604 K | 42,596 K | 16088 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| cmd.exe | | 2,152 K | 3,816 K | 14872 | Windows Command Process... | Microsoft Corporation | Enabled (permanent) | ASLR |
| conhost.exe | | 6,680 K | 7,464 K | 18396 | Console Window Host | Microsoft Corporation | Enabled (permanent) | ASLR |
| browserhost.exe | | 5,416 K | 8,180 K | 12348 | McAfee WebAdvisor | McAfee, LLC | Enabled (permanent) | ASLR |
| cmd.exe | | 2,152 K | 3,820 K | 12292 | Windows Command Process... | Microsoft Corporation | Enabled (permanent) | ASLR |
| conhost.exe | | 6,672 K | 7,460 K | 10444 | Console Window Host | Microsoft Corporation | Enabled (permanent) | ASLR |
| McBrowHost.exe | | 4,744 K | 9,848 K | 18112 | McAfee WDS Shared Brow... | McAfee, LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 13,820 K | 19,048 K | 16332 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | 0.02 | 2,33,116 K | 1,91,280 K | 15532 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome.exe | | 17,960 K | 18,612 K | 11060 | Google Chrome | Google LLC | Enabled (permanent) | ASLR |
| chrome-control.exe | 0.25 | 6,336 K | 15,440 K | 1400 | | | Disabled (permanent) | |
| devenv.exe | 0.81 | 248,208 K | 3,62,016 K | 5620 | Microsoft Visual Studio 2019 | Microsoft Corporation | Enabled (permanent) | ASLR |
| PerfWatson2.exe | < 0.01 | 48,488 K | 69,004 K | 12776 | PerfWatson2.exe | Microsoft Corporation | Enabled (permanent) | ASLR |
| Microsoft.ServiceHub.Con... | | 41,972 K | 56,920 K | 12132 | Microsoft.ServiceHub.Con... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.IdentityHost... | < 0.01 | 60,756 K | 79,620 K | 4704 | ServiceHub.IdentityHost.exe | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.VSDetours... | | 94,684 K | 77,904 K | 4708 | ServiceHub.VSDetoursHost... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.SettingsHost... | 0.13 | 1,00,812 K | 1,02,132 K | 9900 | ServiceHub.SettingsHost.exe | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.Host.CLR.x86... | | 1,23,520 K | 81,492 K | 19144 | ServiceHub.Host.CLR.x86... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.TestWindow... | | 64,320 K | 71,832 K | 13320 | ServiceHub.TestWindowSt... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.Host.CLR.x86... | < 0.01 | 57,176 K | 63,144 K | 19320 | ServiceHub.Host.CLR.x86... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.DataWarehouse... | 0.66 | 91,060 K | 1,02,588 K | 14048 | ServiceHub.DataWarehouse... | Microsoft | Enabled (permanent) | ASLR |
| ServiceHub.ThreadedW... | | 71,400 K | 80,484 K | 2344 | ServiceHub.ThreadedWai... | Microsoft | Enabled (permanent) | ASLR |
| MSBuild.exe | | 33,612 K | 50,312 K | 14548 | MSBuild.exe | Microsoft Corporation | Enabled (permanent) | ASLR |
| conhost.exe | | 6,340 K | 10,804 K | 2496 | Console Window Host | Microsoft Corporation | Enabled (permanent) | ASLR |
| vsipgsvc.exe | < 0.01 | 19,476 K | 26,864 K | 18720 | Microsoft (R) Visual C++ Pack... | Microsoft Corporation | Enabled (permanent) | ASLR |
| ScriptedGDI.exe | | 15,316 K | 26,968 K | 4420 | | | Enabled (permanent) | ASLR |
| ScriptedGDI.exe | 1.01 | 94,044 K | 1,23,392 K | 21360 | ScriptedGDI.exe | Microsoft Corporation | Enabled (permanent) | ASLR |
| process.exe | | 5,120 K | 11,372 K | 15968 | Systematix Process Explorer | Systematix - www.system... | Enabled (permanent) | ASLR |
| process4.exe | 1.02 | 41,364 K | 60,612 K | 18332 | Systematix Process Explorer | Systematix - www.system... | Enabled (permanent) | ASLR |
| ShippingTool.exe | 0.21 | 4,396 K | 27,852 K | 4768 | Shipping Tool | Microsoft Corporation | Enabled (permanent) | ASLR |
| GoogleCrashHandler.exe | | 1,616 K | 116 K | 11236 | | n/a | n/a | n/a |
| GoogleCrashHandler64.exe | | 1,672 K | 148 K | 11244 | | n/a | n/a | n/a |
| juched.exe | | 4,168 K | 8,680 K | 12536 | Java Update Scheduler | Oracle Corporation | Enabled (permanent) | ASLR |
| juchek.exe | | 3,944 K | 7,400 K | 16672 | Java Update Checker | Oracle Corporation | Enabled (permanent) | ASLR |
| HPSystemEventLibHost.exe | | 69,016 K | 21,980 K | 14428 | HPSystemEventLibHost | HP Inc. | Enabled (permanent) | ASLR |
| McPvTray.exe | | 3,648 K | 784 K | 6456 | McAfee File Lock Monitor | McAfee, LLC | Enabled (permanent) | ASLR |
| McSmfWk.exe | | 2,996 K | 3,388 K | 1212 | | n/a | n/a | n/a |
| Teams.exe | < 0.01 | 2,02,740 K | 1,46,196 K | 10304 | Microsoft Teams | Microsoft Corporation | Enabled (permanent) | ASLR |
| Teams.exe | | 1,09,620 K | 77,072 K | 5216 | Microsoft Teams | Microsoft Corporation | Enabled (permanent) | ASLR |