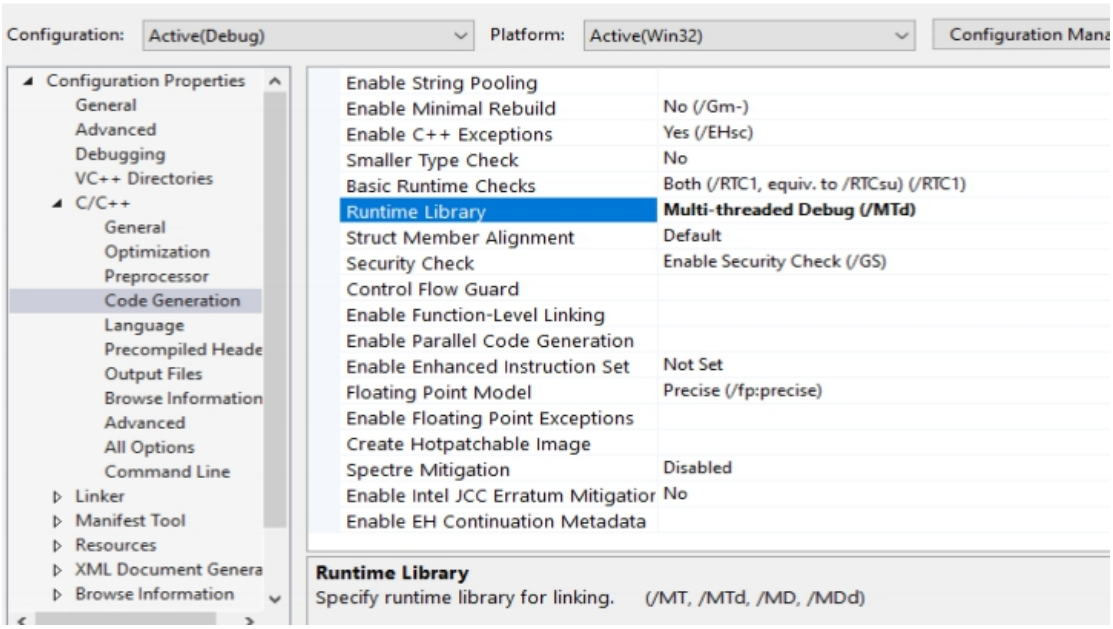
CSE 2010 Secure Coding
WIN 20-21
Lab- 11

NAME:S.BHAVYA SREE
REG.NO:19BCN7257
Topic: Creating secure and safe executable
Lab experiment - Creating secure and safe executable
Task:
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.

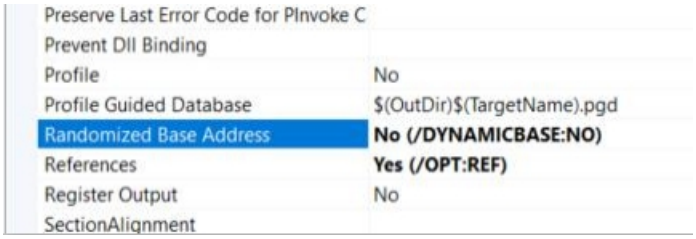
- Building a executable

```
#include "framework.h"
#include "lab11sc.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 wWinMain(_In_ HINSTANCE hInstance,
                      _In_opt_ HINSTANCE hPrevInstance,
                      _In_ LPWSTR    lpCmdLine,
                      _In_ int       nCmdShow)
{
    UNREFERENCED_PARAMETER(hPrevInstance);
    UNREFERENCED_PARAMETER(lpCmdLine);

    // TODO: Place code here.

    // Initialize global strings
    LoadStringW(hInstance, IDS_APP_TITLE, szTitle, MAX_LOADSTRING);
    LoadStringW(hInstance, IDC_LAB11SC, szWindowClass, MAX_LOADSTRING);
    MyRegisterClass(hInstance);

    // Perform application initialization:
    if (!InitInstance (hInstance, nCmdShow))
    {
        return FALSE;
00 %    No issues found
utos
```

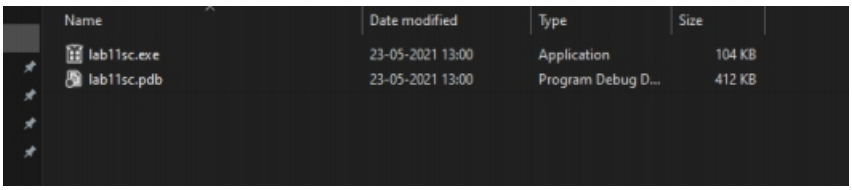
In Visual Studio DEP & ASLR is enabled by default, we have to disable them by going to property pages of the project build



- now disable the DEP & ASLR



- build the exe by setting the project build to release mode and exe is created



- Now install the process explorer and run it, there if we run the process explorer and the exe we created at same time, out exe will be shown in process explorer
- But Even though, we disabled the DEP and ASLR in the project build the process explorer is showing that DEP and ASLR is enabled.
- Conclusion:Windows is programmed to enable the services by default. So even though an exe isn't build enabling the DEP and ASLR windows by default will enable it.