

Secure Coding Lab-11

Deva Dattu Javvadi
18BCN7081
L39+L40

Lab experiment – Creating secure and safe executable

1) C++ Code & building the Executable

```
#include <iostream>

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

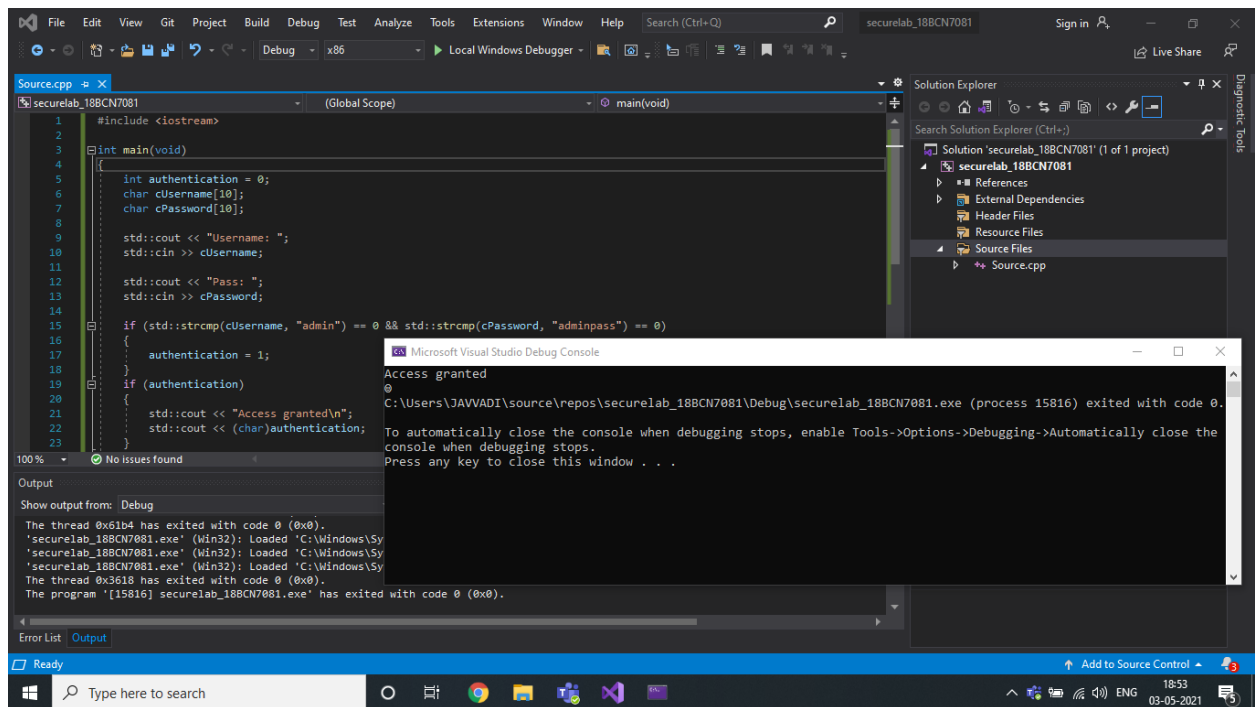
    std::cout << "Username: ";
    std::cin >> cUsername;

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

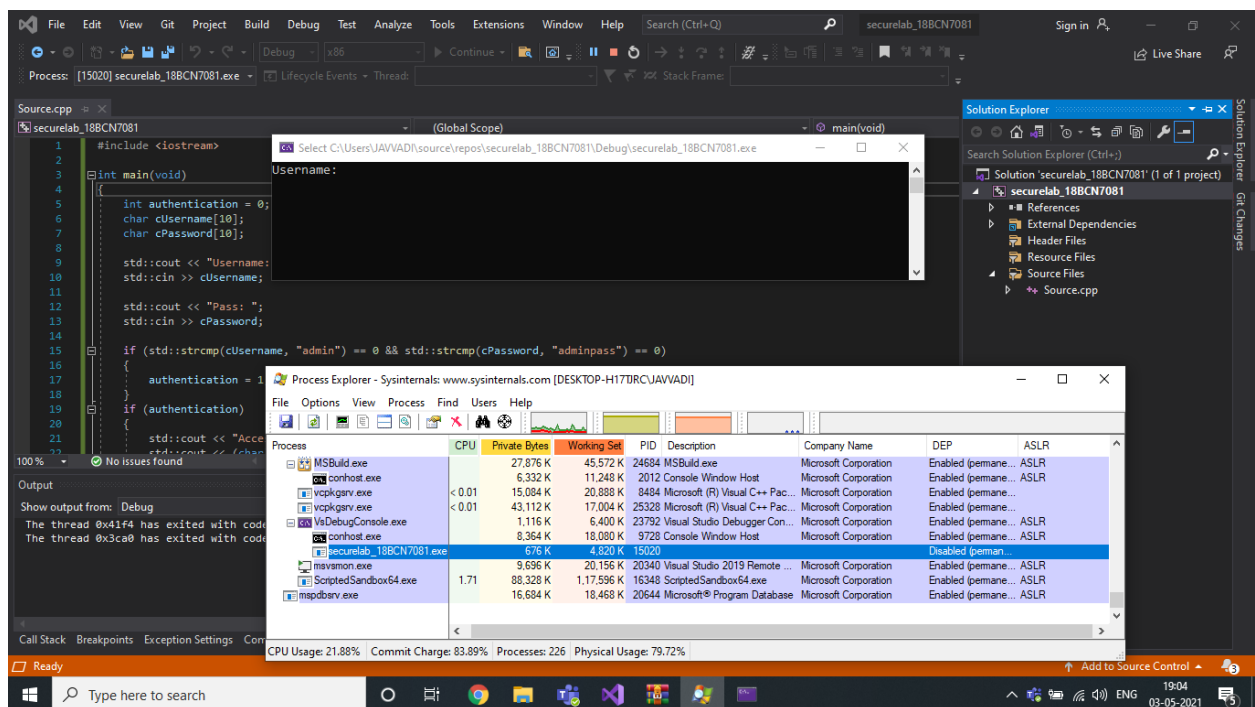
    if (std::strcmp(cUsername, "admin") == 0 &&
std::strcmp(cPassword, "adminpass") == 0)
    {
        authentication = 1;
    }
    if (authentication)
    {
        std::cout << "Access granted\n";
        std::cout << (char)authentication;
    }
    else
    {
        std::cout << "Wrong username and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

    return (0);
}
```

}



2) Verifying the DEP & ASLR status in Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-H17DJRC\JAVVADI]

File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name | DEP | ASLR |
|--------------------------|--------|---------------|-------------|-------|---------------------------------|-----------------------|---------------------|------|
| ServiceHub.TestWindow... | < 0.01 | 57,280 K | 69,780 K | 18220 | ServiceHub.TestWindowSto... | Microsoft | Enabled (permane... | ASLR |
| MSBuild.exe | | 27,728 K | 45,516 K | 24684 | MSBuild.exe | Microsoft Corporation | Enabled (permane... | ASLR |
| conhost.exe | | 6,332 K | 11,248 K | 2012 | Console Window Host | Microsoft Corporation | Enabled (permane... | ASLR |
| vcpgkgsrv.exe | < 0.01 | 15,084 K | 20,888 K | 8484 | Microsoft (R) Visual C++ Pac... | Microsoft Corporation | Enabled (permane... | |
| vcpgkgsrv.exe | < 0.01 | 43,112 K | 17,004 K | 25328 | Microsoft (R) Visual C++ Pac... | Microsoft Corporation | Enabled (permane... | |
| VsDebugConsole.exe | | 1,116 K | 6,400 K | 23792 | Visual Studio Debugger Con... | Microsoft Corporation | Enabled (permane... | ASLR |
| conhost.exe | | 8,332 K | 18,072 K | 9728 | Console Window Host | Microsoft Corporation | Enabled (permane... | ASLR |
| securelab_18BCN7081.exe | | 676 K | 4,820 K | 15020 | | | Disabled (perman... | |
| misysmon.exe | | 9,664 K | 20,144 K | 20340 | Visual Studio 2019 Remote ... | Microsoft Corporation | Enabled (permane... | ASLR |
| ScriptedSandbox64.exe | 1.62 | 88,052 K | 1,17,456 K | 16348 | ScriptedSandbox64.exe | Microsoft Corporation | Enabled (permane... | ASLR |
| mispdbsrv.exe | | 16,212 K | 18,272 K | 20644 | Microsoft® Program Database | Microsoft Corporation | Enabled (permane... | ASLR |

CPU Usage: 24.01% Commit Charge: 84.13% Processes: 226 Physical Usage: 80.30%

You can see DEP disabled & No ASLR.

3) Rebuilding the same executable After enabling DEP & ASLR

Visual Studio IDE showing the source code for `securelab_18BCN7081` and the `securelab_18BCN7081 Property Pages` dialog box.

Source.cpp:

```

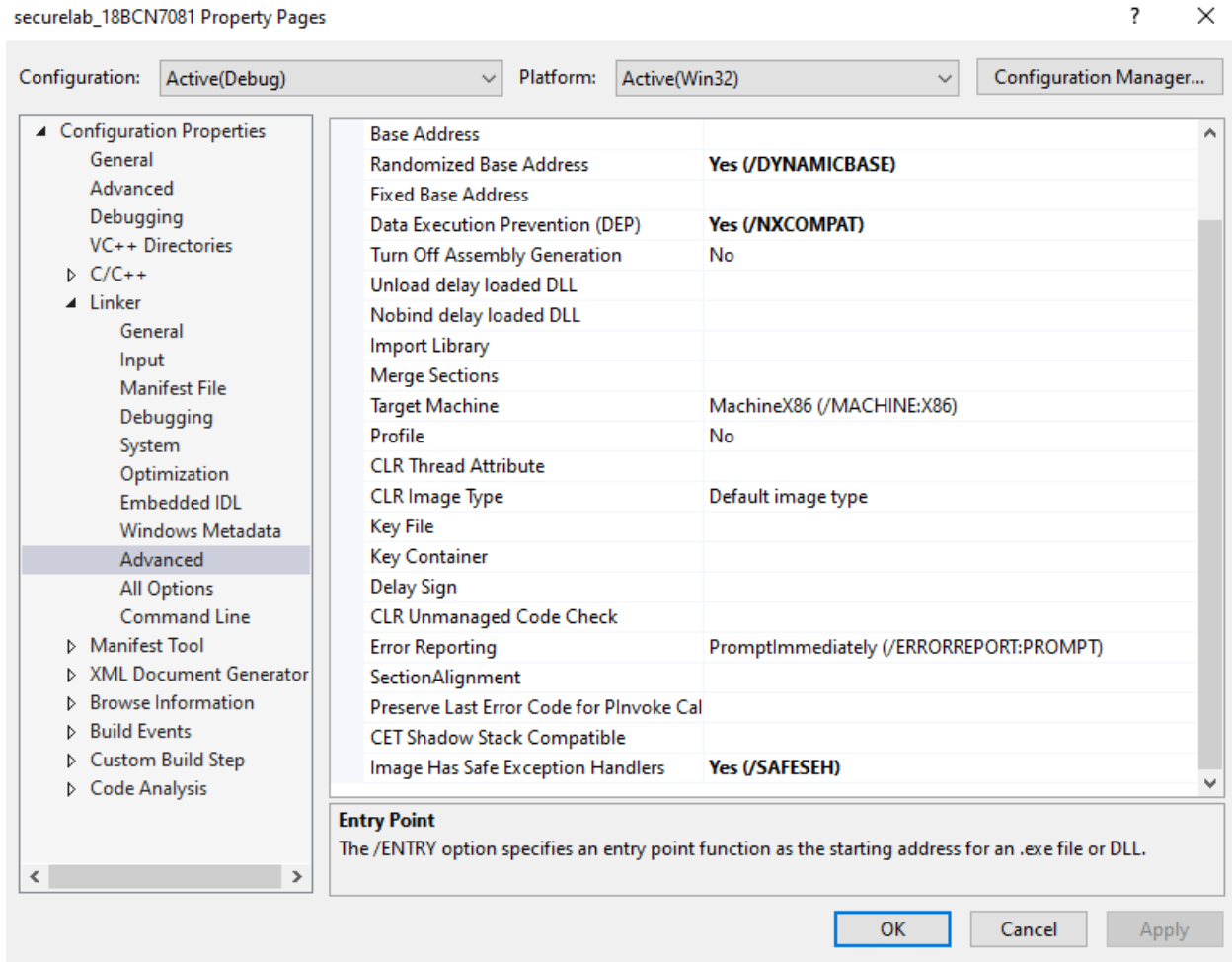
1 #include <iostream>
2
3 int main(void)
4 {
5     int authentication = 0;
6     char cUsername[10];
7     char cPassword[10];
8
9     std::cout << "Username: ";
10    std::cin >> cUsername;
11
12    std::cout << "Pass: ";
13    std::cin >> cPassword;
14
15    if (std::strcmp(cUsername, "admin") == 0 && std::strcmp(cPassword, "1234") == 0)
16    {
17        authentication = 1;
18    }
19    if (authentication)
20    {
21        std::cout << "Access Granted\n";
22        std::cout << (char)cUsername;
23    }
24 }

```

securelab_18BCN7081 Property Pages:

- Configuration: Active(Debug) Platform: Active(Win32)
- Configuration Properties:
 - General: Base Address: Randomized Base Address (Yes /DYNAMICBASE)
 - Advanced: Data Execution Prevention (DEP): Yes (/NXCOMPAT)
 - Linker: Turn Off Assembly Generation: No
 - General: Target Machine: MachineX86 (/MACHINE:X86)
 - Advanced: CLR Image Type: Default image type
 - Advanced: Key File:
 - Advanced: Key Container:
 - Advanced: Delay Sign:
 - Advanced: CLR Unmanaged Code Check: PromptImmediately (/ERRORREPORT:PROMPT)
 - Advanced: Error Reporting:
 - Advanced: SectionAlignment:
 - Advanced: Preserve Last Error Code for PInvoke Calls:
 - Advanced: CET Shadow Stack Compatible:
 - Advanced: Image Has Safe Exception Handlers: Yes (/SAFESEH)
- Entry Point: The /ENTRY option specifies an entry point function as the starting address for an .exe file or DLL.

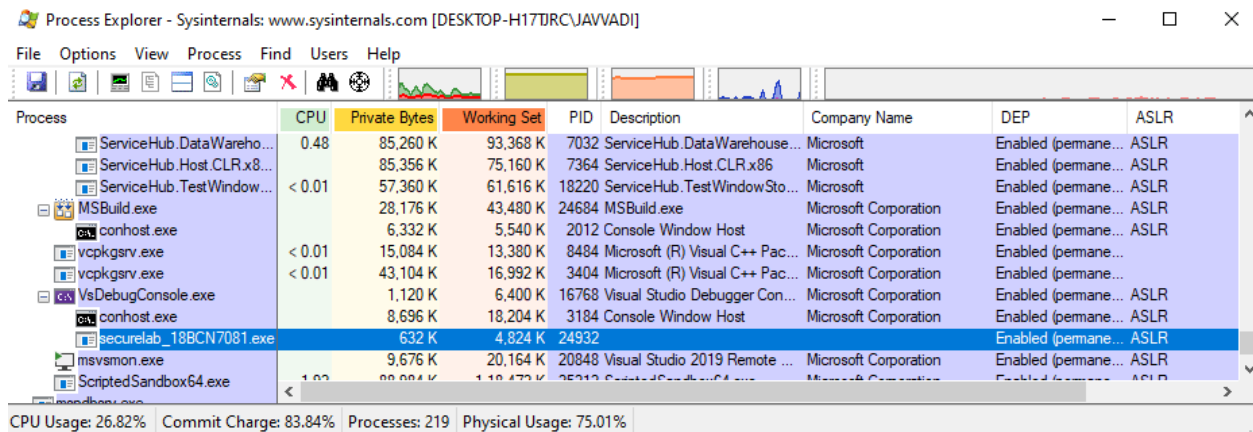
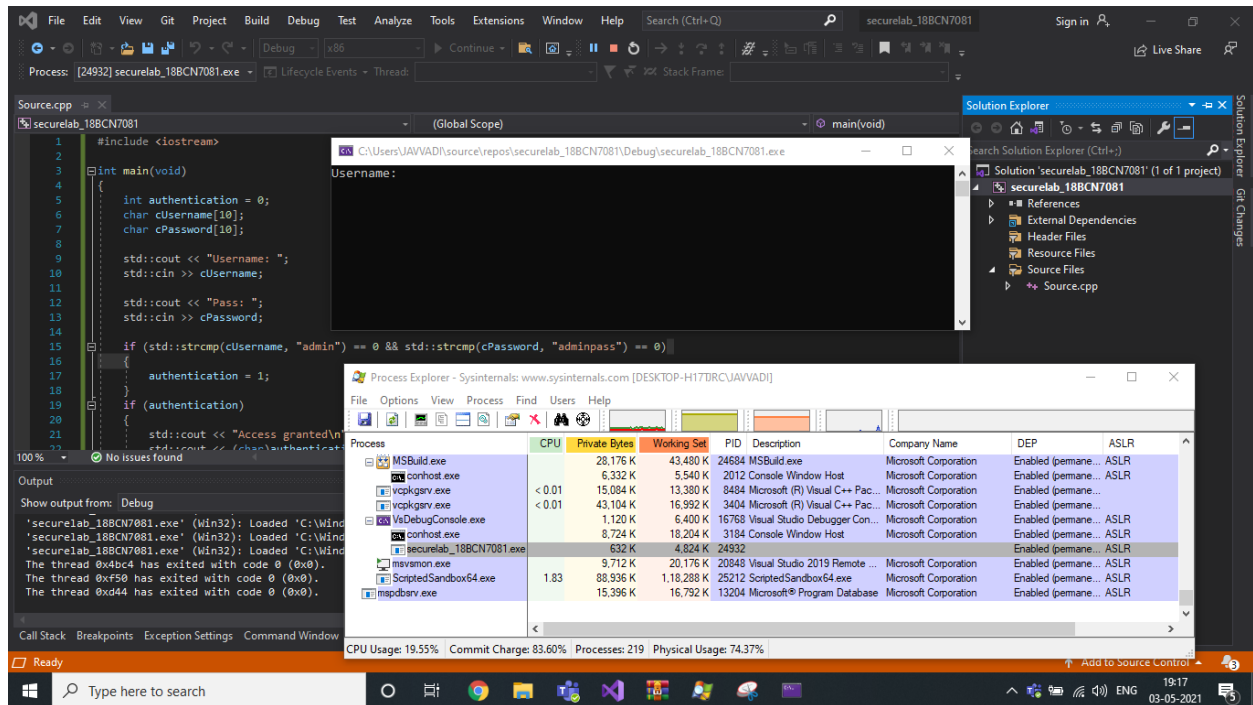
Output: The thread 0x41f4 has exited with code 0. The thread 0x3ca0 has exited with code 0. The thread 0x17d0 has exited with code 0. The program '[15820] securelab_18BCN7081.exe' has exited with code 0.



As you can see, I have enabled DEP, ASLR, SEH above.

I have Rebuilt my project and run the same and we can verify the status of DEP, ASLR, SEH.

4) Verifying the DEP & ASLR status in Process Explorer after enabling



Submitted
Deva Dattu Javadi
18BCN7081
L39+L40