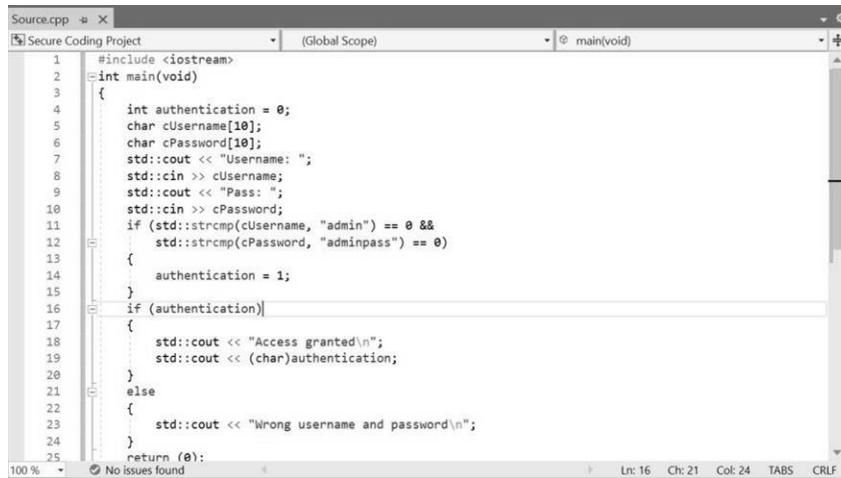


Secure Coding Lab-12

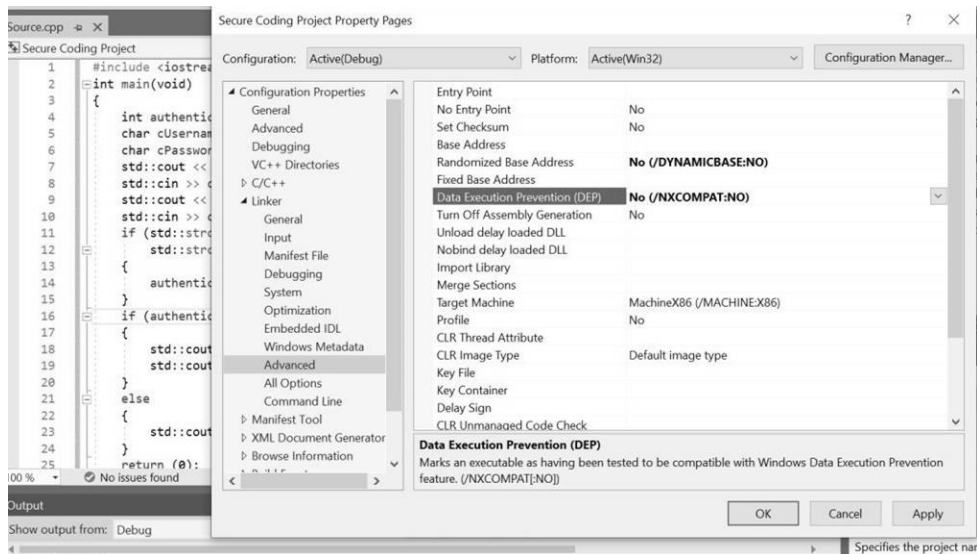
S.Poojith
18BCN7032

Building an executablecode.



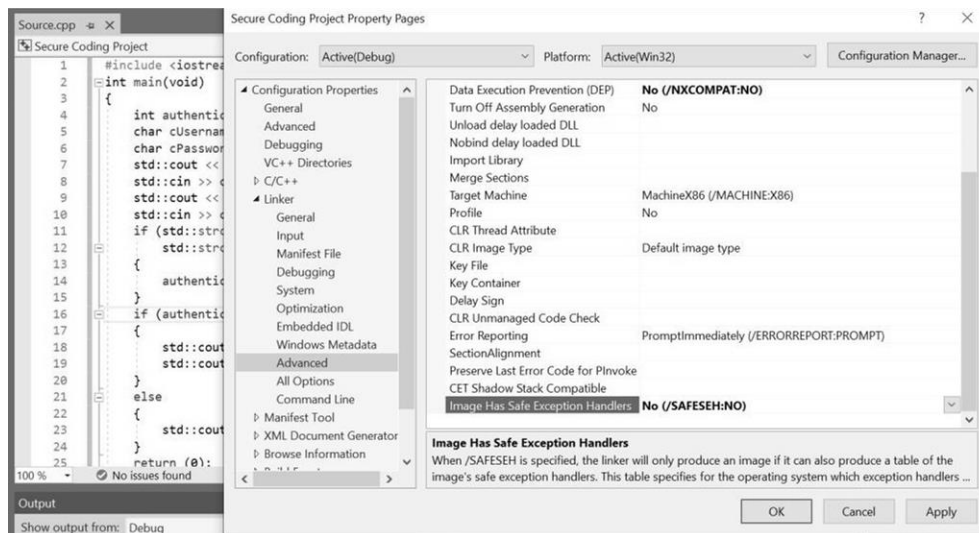
```
1 #include <iostream>
2 int main(void)
3 {
4     int authentication = 0;
5     char cUsername[10];
6     char cPassword[10];
7     std::cout << "Username: ";
8     std::cin >> cUsername;
9     std::cout << "Pass: ";
10    std::cin >> cPassword;
11    if (std::strcmp(cUsername, "admin") == 0 &&
12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

DisableDEP,ASLRand SEH



Secure Coding Lab-12

S.Poojith
18BCN7032



InstallprocessExplorer

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP
Interrupts	0.53	0 K	0 K	n/a	Hardware Interrupts and DPCs		n/a
smss.exe		1,072 K	468 K	592	Windows Session Manager	Microsoft Corporation	Enabled
Memory Compression		1,020 K	36,932 K	2856			Enabled
csrss.exe	< 0.01	2,264 K	3,240 K	760	Client Server Runtime Process	Microsoft Corporation	Enabled
wininit.exe		1,824 K	3,488 K	860	Windows Start-Up Application	Microsoft Corporation	Enabled
services.exe	< 0.01	7,980 K	9,216 K	936	Services and Controller app	Microsoft Corporation	Enabled
svchost.exe	0.12	25,976 K	34,832 K	644	Host Process for Windows S...	Microsoft Corporation	Enabled
dllhost.exe		3,752 K	5,564 K	19052	COM Surrogate	Microsoft Corporation	Enabled
TiWorker.exe		35,184 K	21,772 K	2116	Windows Modules Installer W...	Microsoft Corporation	Enabled
fodhelper.exe		1,408 K	2,244 K	9052	Features On Demand Helper	Microsoft Corporation	Enabled
WmiPvSE.exe		3,900 K	7,996 K	17988	WMI Provider Host	Microsoft Corporation	Enabled
MoUsocoreWorker.exe		14,108 K	19,260 K	15428	MoUSO Core Worker Process	Microsoft Corporation	Enabled
McVulCtr.exe		8,728 K	4,732 K	22492	McAfee Vulnerability Scanner	McAfee, LLC	Enabled
StartMenuExperienceHos...		27,564 K	76,648 K	1892			Enabled
RuntimeBroker.exe		6,688 K	25,852 K	8284	Runtime Broker	Microsoft Corporation	Enabled
SearchApp.exe	0.53	2,07,364 K	2,60,256 K	11268	Search application	Microsoft Corporation	Enabled
SettingSyncHost.exe	< 0.01	11,088 K	31,800 K	23436	Host Process for Setting Syn...	Microsoft Corporation	Enabled
RuntimeBroker.exe		12,940 K	39,656 K	8700	Runtime Broker	Microsoft Corporation	Enabled
YourPhone.exe	Susp...	25,848 K	18,516 K	15972	YourPhone	Microsoft Corporation	Enabled
LockApp.exe	Susp...	13,732 K	46,328 K	16412	LockApp.exe	Microsoft Corporation	Enabled
RuntimeBroker.exe		10,608 K	35,868 K	9888	Runtime Broker	Microsoft Corporation	Enabled
TextInputHost.exe		13,044 K	45,464 K	16860		Microsoft Corporation	Enabled
RuntimeBroker.exe	< 0.01	3,024 K	15,160 K	10628	Runtime Broker	Microsoft Corporation	Enabled
dllhost.exe	0.02	6,624 K	14,396 K	18368	COM Surrogate	Microsoft Corporation	Enabled
RuntimeBroker.exe		7,016 K	25,232 K	20968	Runtime Broker	Microsoft Corporation	Enabled
Cortana.exe	Susp...	31,240 K	58,984 K	19732	Cortana	Microsoft Corporation	Enabled
RuntimeBroker.exe		4,616 K	22,744 K	15980	Runtime Broker	Microsoft Corporation	Enabled
ApplicationFrameHost.exe		24,468 K	40,752 K	3696	Application Frame Host	Microsoft Corporation	Enabled
WinStore.App.exe	Susp...	18,764 K	2,332 K	2124	Store	Microsoft Corporation	Enabled
RuntimeBroker.exe							Enabled

Secure Coding Lab-12

S.Poojith
18BCN7032

EnablingDEPAndASLRin processexplorer.



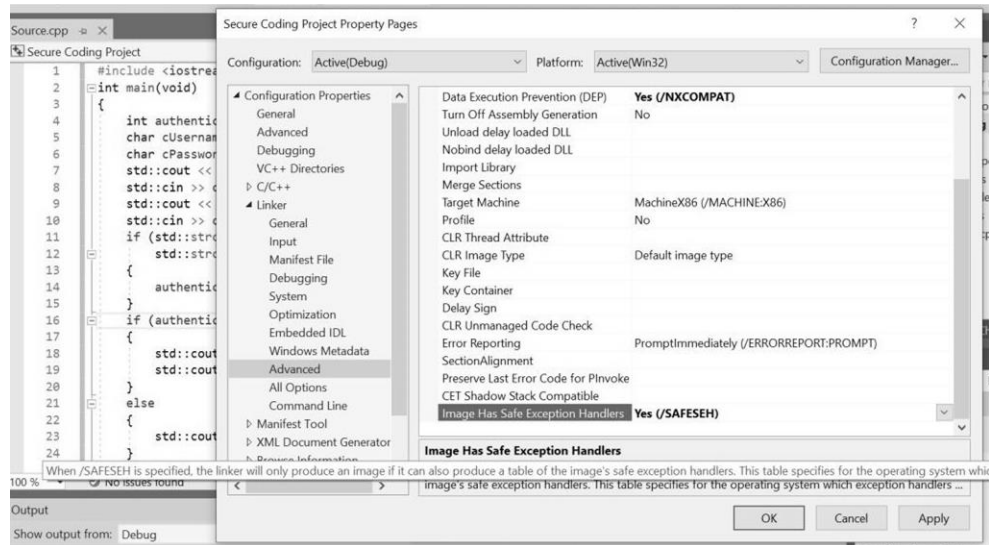
DEPStatusofSecureCodingProject.exeshowsdisabled.



NowenableDEP,ASLRandSEHInVisualStudio.

Secure Coding Lab-12

S.Poojith
18BCN7032



Now, the DEP status of SecureCodingProject.exe shows enabled.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	DEP	ASLR
WINWORD.EXE	0.08	1,31,052 K	1,86,400 K	22912	Microsoft Word	Microsoft Corporation	Enabled (permane...	ASLR
C:\AudioFilterAgent64.exe		1,952 K	9,804 K	20644	Conexant High Definition Aud...	Conexant Systems, Inc.	Enabled (permane...	ASLR
SmartAudio3.exe	< 0.01	56,468 K	48,320 K	15136	SmartAudio 3	Conexant Systems LLC.	Enabled (permane...	ASLR
C:\CratNotify.exe		34,200 K	35,944 K	5796	CratNotify	Conexant Systems, Inc	Enabled (permane...	ASLR
Flow.exe	0.01	58,820 K	49,052 K	13080	Flow	Conexant Systems, Inc	Enabled (permane...	ASLR
McAfeeMcAfee.exe		10,252 K	30,128 K	19300	McAfee	McAfee, LLC	Enabled (permane...	ASLR
Teams.exe	0.02	1,79,344 K	1,26,280 K	16808	Microsoft Teams	Microsoft Corporation	Enabled (permane...	ASLR
Teams.exe	0.25	1,83,580 K	1,41,000 K	9200	Microsoft Teams	Microsoft Corporation	Enabled (permane...	ASLR
Teams.exe	0.01	16,020 K	42,612 K	16604	Microsoft Teams	Microsoft Corporation	Enabled (permane...	ASLR
Teams.exe		33,364 K	38,112 K	18152	Microsoft Teams	Microsoft Corporation	Enabled (permane...	ASLR
Teams.exe	0.29	3,22,544 K	2,78,268 K	17668	Microsoft Teams	Microsoft Corporation	Enabled (permane...	ASLR
Teams.exe		11,496 K	54,552 K	16304	Microsoft Teams	Microsoft Corporation	Enabled (permane...	ASLR
Teams.exe	< 0.01	2,03,020 K	2,08,368 K	7316	Microsoft Teams	Microsoft Corporation	Enabled (permane...	ASLR
Teams.exe	< 0.01	1,36,692 K	1,57,528 K	10292	Microsoft Teams	Microsoft Corporation	Enabled (permane...	ASLR
setup.exe	0.85	1,61,516 K	1,67,416 K	22212	Visual Studio Installer	Microsoft	Enabled (permane...	ASLR
devenv.exe	1.08	3,13,880 K	3,83,588 K	5516	Microsoft Visual Studio 2019	Microsoft Corporation	Enabled (permane...	ASLR
PerfWatson2.exe	< 0.01	47,840 K	56,040 K	12788	PerfWatson2.exe	Microsoft Corporation	Enabled (permane...	ASLR
Microsoft ServiceHub Control...		39,572 K	51,288 K	9408	Microsoft ServiceHub Control...	Microsoft	Enabled (permane...	ASLR
ServiceHub VSDetouredHost...		65,096 K	68,368 K	19872	ServiceHub VSDetouredHost...	Microsoft	Enabled (permane...	ASLR
ServiceHub ThreadedWaitDi...		63,708 K	61,852 K	21964	ServiceHub ThreadedWaitDi...	Microsoft	Enabled (permane...	ASLR
ServiceHub IdentityHost.exe	0.01	54,088 K	58,908 K	4829	ServiceHub IdentityHost.exe	Microsoft	Enabled (permane...	ASLR
ServiceHub SettingsHost.exe		71,144 K	67,164 K	17308	ServiceHub SettingsHost.exe	Microsoft	Enabled (permane...	ASLR
ServiceHub Host CLR x86.exe		48,252 K	49,244 K	16708	ServiceHub Host CLR x86	Microsoft	Enabled (permane...	ASLR
ServiceHub DataWarehouse...	0.53	92,744 K	97,208 K	19060	ServiceHub DataWarehouse...	Microsoft	Enabled (permane...	ASLR
ServiceHub Host CLR x86.exe	< 0.01	78,556 K	79,544 K	15120	ServiceHub Host CLR x86	Microsoft	Enabled (permane...	ASLR
ServiceHub TestWindowSto...		59,536 K	70,172 K	7600	ServiceHub TestWindowStor...	Microsoft	Enabled (permane...	ASLR
MSBuild.exe		34,164 K	55,272 K	17084	MSBuild.exe	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		6,324 K	5,300 K	15912	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
vcpkg.exe	< 0.01	13,684 K	16,824 K	23392	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	ASLR
VsDebugConsole.exe		1,208 K	6,044 K	24696	Visual Studio Debugger Cons...	Microsoft Corporation	Enabled (permane...	ASLR
conhost.exe		7,044 K	16,528 K	23544	Console Window Host	Microsoft Corporation	Enabled (permane...	ASLR
Secure Coding Project.exe		784 K	4,416 K	21480			Enabled (permane...	ASLR
vcpkg.exe	< 0.01	43,108 K	16,588 K	21076	Microsoft (R) Visual C++ Pac...	Microsoft Corporation	Enabled (permane...	ASLR
msvmon.exe		9,812 K	19,724 K	26124	Visual Studio 2019 Remote ...	Microsoft Corporation	Enabled (permane...	ASLR
ScriptedSandbox64.exe	1.15	94,332 K	1,22,972 K	23568	ScriptedSandbox64.exe	Microsoft Corporation	Enabled (permane...	ASLR
processp64.exe	0.77	50,440 K	68,512 K	20980	Sysinternals Process Explorer	Sysinternals - www.sysinter	Enabled (permane...	ASLR

By executing the code at the end, console opens up.



```

}ect
#include <iostream>
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, "admin") == 0)
{
    authentication = 1;
}
if (authentication)
{
    std::cout << "Access granted\n";
    std::cout << (char)authentication;
}
else
{
    std::cout << "Wrong username or password\n";
}
return (0);

```

Username: