Details:

Author: **Yossef Zidan (@yossefzidann)**
Challenge Overview: The challenge goal is find the correct input which is the flag.

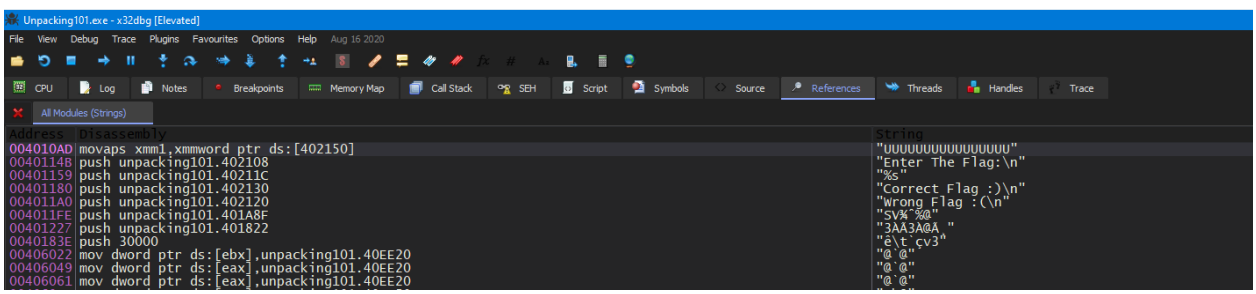
Step 1: Discovery

```
C:\Users\joezid\Desktop\Unpacking 101-Easy\Challenge
λ file Unpacking101.exe
Unpacking101.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

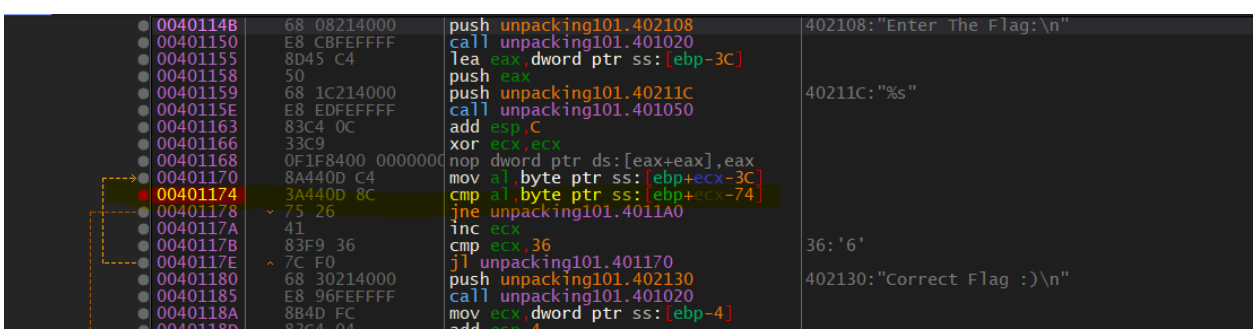
In this challenge, we are given one file which is an x86 PE file.

Step 2: Binary Analysis

If we checked the PE file in IDA we can notice that the pe file is packed so the easiest way to bypass the unpacking process and go directly to the flag check part is to run the PE and attach it to the process using any debugger.



We can see some references to the strings we saw earlier enter the flag ...etc.



If we moved to the reference of the strings we can see that the input is being compared to the flag at 0x401174 we can put a breakpoint there and continue the execution.

```
0040114B   68 08214000    push unpacking101.402108          402108:"Enter The Flag:\n"
00401150   E8 CBFEFFFF    call unpacking101.401020
00401155   8D45 C4        lea eax,dword ptr ss:[ebp-3C]
00401158   50             push eax
00401159   68 1C214000    push unpacking101.40211C          40211C:"%s"
0040115E   E8 EDFEFFFF    call unpacking101.401050
00401163   83C4 0C        add esp,C
00401166   33C9           xor ecx,ecx
00401168   0F1F8400 0000000 nop dword ptr ds:[eax+eax],eax
00401170   8A440D C4      mov al,byte ptr ss:[ebp+ecx-3C]
00401174   3A440D 8C      cmp al,byte ptr ss:[ebp+ecx-74]
00401178   75 26          jne unpacking101.4011A0
0040117A   41             inc ecx
0040117B   83F9 36        cmp ecx,36                        36:'6'
0040117E   7C F0          jl unpacking101.401170
00401180   68 30214000    push unpacking101.402130          402130:"Correct Flag :)\n"
00401185   E8 96FEFFFF    call unpacking101.401020
0040118A   8B4D FC        mov ecx,dword ptr ss:[ebp-4]
0040118D   83C4 04        add esp,4
00401190   33CD           xor ecx,ebp
00401192   B8 01000000    mov eax,1
00401197   E8 1A000000    call unpacking101.401186
0040119C   8BE5           mov esp,ebp
0040119E   5D             pop ebp
```

```
Hide FPU
EAX   00000061   'a'
EBX   0020E000
ECX   00000000
EDX   00000001
EBP   0063FF28
ESP   0063FEB4   "ASCWG{M4y_1_cL34r_y0ur_sL4t3_4nd_w1p3_y0ur_c0nsc13nc3}"
ESI   009957A0   &"C:\\Users\\joezid\\Desktop\\Unpacking 101-Easy\\Challenge
EDI   00996158   &"ALLUSERSPROFILE=C:\\ProgramData"

EIP   00401174   unpacking101.00401174

EFLAGS   00000344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C00700BB

GS 002B  FS 0053
ES 002B  DS 002B
```

Flag: **ASCWG{M4y_1_cL34r_y0ur_sL4t3_4nd_w1p3_y0ur_c0nsc13nc3}**