

这道题还是比较简单的

## 去壳

```
PowerShell 7-preview (x64)
>>
>> ^C
PS C:\Users\wsxk\Desktop\ctf\BUUCTF> cd .\ACTF新生赛2020_easyre\
PS C:\Users\wsxk\Desktop\ctf\BUUCTF\ACTF新生赛2020_easyre> ls

Directory: C:\Users\wsxk\Desktop\ctf\BUUCTF\ACTF新生赛2020_easyre

Mode                LastWriteTime         Length Name
----                -
-a-----          2021/5/17   14:48           25600 attachment.tar
-a-----          2020/3/5    18:02           21467 easyre.exe

PS C:\Users\wsxk\Desktop\ctf\BUUCTF\ACTF新生赛2020_easyre> .\easyre.exe
Please input:safsadf
PS C:\Users\wsxk\Desktop\ctf\BUUCTF\ACTF新生赛2020_easyre> .\upx.exe -d .\easyre.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

File size      Ratio      Format      Name
-----
28123 <-      21467      76.33%      win32/pe      easyre.exe

Unpacked 1 file.
PS C:\Users\wsxk\Desktop\ctf\BUUCTF\ACTF新生赛2020_easyre> .\easyre.exe
Please input:safsadf
PS C:\Users\wsxk\Desktop\ctf\BUUCTF\ACTF新生赛2020_easyre> _
```

## ida查看

```
IDA - easyre.exe C:\Users\wsxk\Desktop\ctf\BUUCTF\ACTF新生赛2020_easyre\easyre.exe
File Edit Jump Search View Debugger Lumina Options Windows Help
[Icons] [No debugger]
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions window:
  Function name
  [?] __mingw_CRTStartup
  [?] _gnu_exception_handler@4
  [?] _mainCRTStartup
  [?] _WinMainCRTStartup
  [?] _atexit
  [?] _onexit
  [?] _gcc_register_frame
  [?] _gcc_deregister_frame
  [?] _main
  [?] __dyn_tls_dtor@12
  [?] __dyn_tls_init@12
  [?] __tlregdtor
  [?] __cpu_features_init
  [?] _fpreset
  [?] _report_error
  [?] _write_memory_part_0
  [?] _pei386_runtime_relocator
  [?] __do_global_dtors
  [?] __do_global_ctors
  <
  Line 9 of 51
  Output window
  [96]
  [85, 57, 88, 95, 49, 83, 95, 87, 54, 64, 84, 63]
  [85, 57, 88, 95, 49, 83, 95, 87, 54, 64, 84, 63]
  Python>str(flag)
  '[85, 57, 88, 95, 49, 83, 95, 87, 54, 64, 84, 63]'
  09X_1S_W6@17
  Python
  AU: idle Down Disk: 91GB

IDA View-A:
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     _BYTE v4[12]; // [esp+12h] [ebp-2Eh] BYREF
4     _DWORD v5[3]; // [esp+1Eh] [ebp-22h]
5     _BYTE v6[5]; // [esp+2Ah] [ebp-16h] BYREF
6     int v7; // [esp+2Fh] [ebp-11h]
7     int v8; // [esp+33h] [ebp-Dh]
8     int v9; // [esp+37h] [ebp-9h]
9     char v10; // [esp+3Bh] [ebp-5h]
10    int i; // [esp+3Ch] [ebp-4h]
11
12    __main();
13    qmemcpy(v4, "F'\\N,\\(I?+@", sizeof(v4));
14    printf("Please input:");
15    scanf("%s", v6);
16    if ( v6[0] != 'A' || v6[1] != 'C' || v6[2] != 'T' || v6[3] != 'F' || v6[4] != '{' || v10 != '}' )
17        return 0;
18    v5[0] = v7;
19    v5[1] = v8;
20    v5[2] = v9;
21    for ( i = 0; i <= 11; ++i )
22    {
23        if ( v4[i] != _data_start_1[*(char *)v5 + i - 1] )
24            return 0;
25    }
26    printf("You are correct!");
27    return 0;
28}
```

可以看出v4是比较字符串，flag格式为ACTF{}，中间的输入值，每个-1作为索引在data——start数组中找到字符，来和v4进行比较

## 解决办法

爆破，找到v4的每个字符在data——start中的位置，然后每个加1就能得到输入

## 知识点

主要是利用了scanf的溢出，因为局部变量存在栈中，scanf时覆盖了v8，v9，v10的值。