BUUCTF_[ACTF新生赛2020]easyre 1

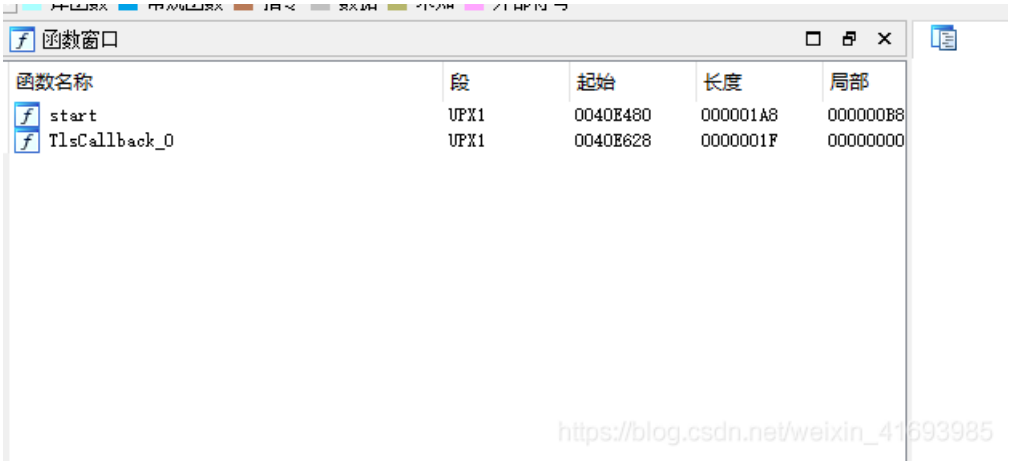
原创

一夜通宵程序员 于 2021-06-14 11:20:14 发布 355 收藏

分类专栏： 反调试学习 文章标签： python c语言

本文链接：https://blog.csdn.net/weixin_41693985/article/details/117899098

拿到程序拖入ida中，发现有UPX壳



所以脱壳然后再拖入ida进入主函数

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char v4; // [esp+12h] [ebp-2Eh]
  char v5; // [esp+13h] [ebp-2Dh]
  char v6; // [esp+14h] [ebp-2Ch]
  char v7; // [esp+15h] [ebp-2Bh]
  char v8; // [esp+16h] [ebp-2Ah]
  char v9; // [esp+17h] [ebp-29h]
  char v10; // [esp+18h] [ebp-28h]
  char v11; // [esp+19h] [ebp-27h]
  char v12; // [esp+1Ah] [ebp-26h]
  char v13; // [esp+1Bh] [ebp-25h]
  char v14; // [esp+1Ch] [ebp-24h]
  char v15; // [esp+1Dh] [ebp-23h]
  int v16; // [esp+1Eh] [ebp-22h]
  int v17; // [esp+22h] [ebp-1Eh]
  int v18; // [esp+26h] [ebp-1Ah]
  __int16 v19; // [esp+2Ah] [ebp-16h]
  char v20; // [esp+2Ch] [ebp-14h]
  char v21; // [esp+2Dh] [ebp-13h]
  char v22; // [esp+2Eh] [ebp-12h]
  int v23; // [esp+2Fh] [ebp-11h]
  int v24; // [esp+33h] [ebp-Dh]
  int v25; // [esp+37h] [ebp-9h]
  char v26; // [esp+3Bh] [ebp-5h]
  int i; // [esp+3Ch] [ebp-4h]

  __main();
  v4 = 42;
  v5 = 70;
  v6 = 39;
  v7 = 34;
  v8 = 78;
  v9 = 44;
  v10 = 34;
  v11 = 40;
  v12 = 73;
  v13 = 63;
  v14 = 43;
  v15 = 64;
  printf("Please input:");
  scanf("%s", &v19);
  if ( (_BYTE)v19 != 65 || HIBYTE(v19) != 67 || v20 != 84 || v21 != 70 || v22 != 123 || v26 != 125 )
    return 0;
  v16 = v23;
  v17 = v24;
  v18 = v25;
  for ( i = 0; i <= 11; ++i )
  {
    if ( *(&v4 + i) != _data_start__[*((char *)&v16 + i) - 1] )
      return 0;
  }
  printf("You are correct!");
  return 0;
}
```

其中for循环是关键函数，其中意思是在_data_start__函数中找到v4—>v15的字符

```
.data:00402000 __data_start__  db 7Eh                 ; DATA XREF: _main+EC↑r
.data:00402001 aZyxwvutsrqponm db '}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>='
.data:00402001                 db '<;:9876543210/.-,+*)(',27h,'&%$# !"',0
```

所以上脚本

```
v4 = [42,70,39,34,78,44,34,40,73,63,43,64]
#r：防特殊字符转义
str = r'~}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)('+chr(0x27)+r'&%$
# !"'
s=[]
flag1 = ''
for i in v4:
    print(i)
    s.append(str.find(chr(i))+1)
for i in s:
    flag1 += chr(i)
print(flag1)
```

最后输出得到flag