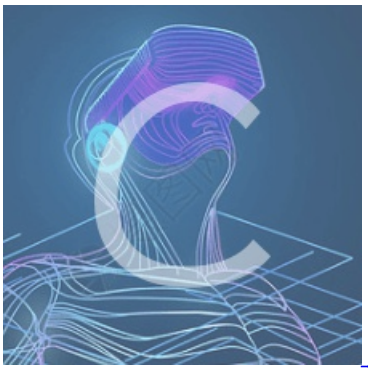
[ACTF新生赛2020]easyre 1

原创

theThreeDay 于 2021-01-24 12:50:01 发布 387 收藏

分类专栏： BU reverse

本文链接：https://blog.csdn.net/weixin_52034946/article/details/113078598



BU reverse 专栏收录该内容

25 篇文章 0 订阅

订阅专栏

查壳,是32位,upx壳,

脱壳就是找的脱壳软件,我也不是很懂,就说下我的具体操作步骤吧

```
C:\Users\handsome>D:\poxiao\reverse\upx\upx\UPX_v3.96_x32\upx-3.96-win32\upx.exe -d D:\QMDownload\problemfile\attachment
\tmp\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.
```


打开cmd,脱upx壳的软件拖进去,空格-d ,空格,有壳文件拖入,解出来了

下面看代码吧

```
  printf("Please input:");
  scanf("%s", &v19);
  if ( (_BYTE)v19 != 'A' || HIBYTE(v19) != 'C' || v20 != 'T' || v21 != 'F' || v22 != '{' || v26 != '}' )
    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;
}
```


然后就挺简单的,就这点代码,下面那个for循环逆着写就行了,注意v4是个数组,

暂时就会c语言,py还没学,用c我实在是不能把那一大串字符串写出来,抄个别人的脚本

```
  db 7Eh                    ; DATA XREF: _main+EC↑r
m db '}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>='
  db '<;:9876543210/.-,+*)(',27h,'&%$# !"',0
  align 40h
```

```
key = '~}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)(\'&%$# !"' #'一定要加\
encrypt = [42,70,39,34,78,44,34,40,73,63,43,64]
x = []
flag = ''
for i in encrypt:
  x.append(key.find(chr(i))+1)
for i in x:
  flag += chr(i)
print(flag)
```

flag{U9X_1S_W6@T?}