# [BUUCTF]REVERSE------[ACTF新生赛2020]easyre

原创

HAIANAWEI 于 2021-02-03 15:43:41 发布 105 收藏

分类专栏： REVERSE



本文链接：https://blog.csdn.net/BangSen1/article/details/113602275



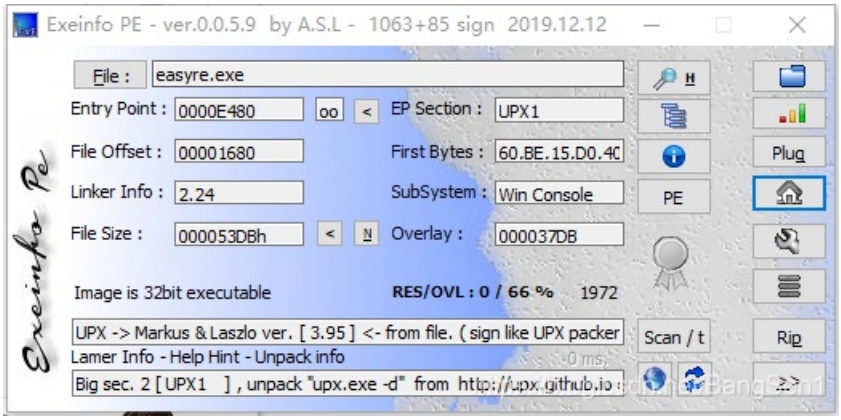

REVERSE 专栏收录该内容

30 篇文章 0 订阅

订阅专栏

## [ACTF新生赛2020]easyre

查壳，32bit，有壳





去壳

用32位IDA打开。

第16行让我们输入 ACTF{}， 也就是flag

第21行可以看出 { }内的长度为12 且v4内的字符要和byte_402000【输入的数组的每一位值-1】

```
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]
```

```
  int v8; // [esp+33h] [ebp-Dh]
  int v9; // [esp+37h] [ebp-9h]
  char v10; // [esp+3Bh] [ebp-5h]
  int i; // [esp+3Ch] [ebp-4h]

  sub_401A10();
  qmemcpy(v4, "*F'\"N,\"(I?+@", sizeof(v4));
  printf("Please input:");
  scanf("%s", v6);
  if ( v6[0] != 'A' || v6[1] != 'C' || v6[2] != 'T' || v6[3] != 'F' || v6[4] != '{' || v10 != '}' )
    return 0;
  v5[0] = v7;
  v5[1] = v8;
  v5[2] = v9;
  for ( i = 0; i <= 11; ++i )
  {
    if ( v4[i] != byte_402000[*((char *)v5 + i) - 1] )
      return 0;
  }
  printf("You are correct!");
  return 0;
}
```



byte_402000的值也已经给我们了

```
UPX0:00401D48                 dd 0
UPX0:00401D4C                 dd 0FFFFFFFFh
UPX0:00401D50 dword_401D50    dd 0ACh dup(0)          ; DATA XREF: UPX0:off_402088↓o
UPX0:00402000 ; char byte_402000[]
UPX0:00402000 byte_402000     db 7Eh                  ; DATA XREF: _main+EC↑r
UPX0:00402001 aZyxwvutsrqponm db '}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>='
UPX0:00402001                 db '<;:9876543210/.-,+*)(',27h,'&%$# !"',0
UPX0:00402060                 align 40h
UPX0:00402080 dword_402080    dd 0FFFFFFFFh           ; DATA XREF: sub_401000+4A↑r
UPX0:00402084 dword_402084    dd 4000h                ; DATA XREF: sub_401000+86↑w
UPX0:00402084                                         ; sub_401000+C7↑r
UPX0:00402088 off_402088      dd offset dword_401D50  ; DATA XREF: sub_401990↑r
UPX0:00402088                                         ; sub_401990+12↑r ...
UPX0:0040208C dword_40208C    dd 0                    ; DATA XREF: sub_4012E0↑r
UPX0:0040208C                                         ; sub_4012E0+40↑o
UPX0:00402090                 align 1000h
UPX0:00403000 ; CHAR ModuleName[]
UPX0:00403000 ModuleName      db 'libgcj-13.dll',0    ; DATA XREF: sub_4012E0+F↑o
UPX0:0040300E ; CHAR ProcName[]
UPX0:0040300E ProcName        db '_Jv_RegisterClasses',0
UPX0:0040300E                                         ; DATA XREF: sub_4012E0+27↑o
UPX0:00403022                 align 4
UPX0:00403024 ; char Format[]
UPX0:00403024 Format          db 'Please input:',0    ; DATA XREF: _main+4A↑o
UPX0:00403032 ; char aS[]
UPX0:00403032 aS              db '%s',0               ; DATA XREF: _main+5E↑o
UPX0:00403035 ; char aYouAreCorrect[]
UPX0:00403035 aYouAreCorrect  db 'You are correct!',0 ; DATA XREF: _main+10A↑o
UPX0:00403046                 align 4
UPX0:00403048 off_403048      dd offset sub_4014B0    ; DATA XREF: sub_401000+4↑r
UPX0:0040304C aMingwRuntimeFa db 'Mingw runtime failure:',0Ah,0
UPX0:0040304C                                         ; DATA XREF: sub_401640+25↑o
UPX0:00403064 ; char aVirtualqueryFa[]
UPX0:00403064 aVirtualqueryFa db '  VirtualQuery failed for %d bytes at address %p',0
UPX0:00403064                                         ; DATA XREF: sub_4016A0+102↑o
UPX0:00403095                 align 4
UPX0:00403098 ; char aUnknownPseudoR_0[]
UPX0:00403098 aUnknownPseudoR_0 db '  Unknown pseudo relocation protocol version %d.',0Ah,0
UPX0:00403098                                         ; DATA XREF: sub_4017B0+1C8↑o
UPX0:004030CA                 align 4
UPX0:004030CC ; char aUnknownPseudoR[]
UPX0:004030CC aUnknownPseudoR db '  Unknown pseudo relocation bit size %d.',0Ah,0
UPX0:004030CC                                         ; DATA XREF: sub_4017B0+C0↑o
UPX0:004030F6                 align 4
```



根据这个算法逆向一下就能得到我们输入的字符串，也就是flag

```
v4 = [42, 70, 39, 34, 78, 44, 34, 40, 73, 63, 43, 64]
string = chr(0x7E)+"}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCB
flag=""

for i in v4:
```

```
for i in v4:
    for j in range(1,len(string)):
        if i == ord(string[j]):
            flag+=chr(j+1)

print ("flag{"+flag+"}")
```