攻防世界 Reverse高手进阶区 3分题 babymips

原创

思源湖的鱼 于 2021-01-20 18:58:31 发布 192 收藏

分类专栏： ctf 文章标签： ctf reverse 攻防世界

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112907491

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的3分题

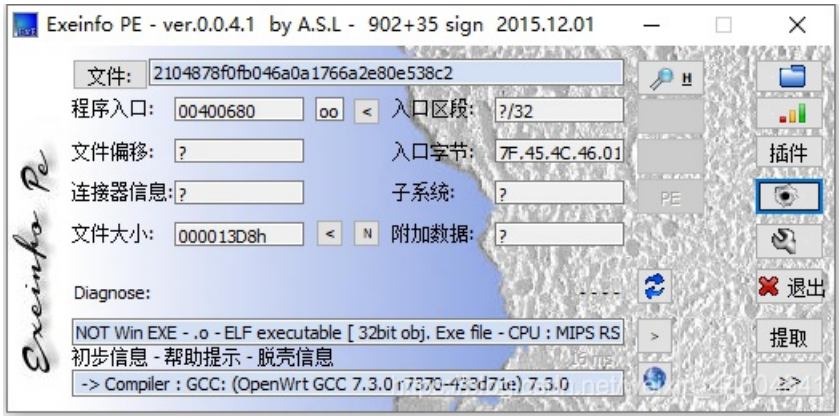
本篇是babymips的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

PE查壳



扔进ida无法反编译

查了查

因为用的是mips架构

需要插件

然后用ghidra可以反编译

```
1 void FUN_004009a8(void)
2
3 {
4   int iVar1;
5   int i;
6   byte input [36];
7
8   setbuf(stdout,(char *)0x0);
9   setbuf(stdin,(char *)0x0);
10  printf("Give me your flag:");
11  scanf("%32s",input);
12  i = 0;
13  while (i < 0x20) {
14    input[i] = input[i] ^ 0x20U - (char)i;    //这里将输入进行异或 (0x20-i)
15    i = i + 1;
16  }
17  iVar1 = strncmp((char *)input,_fdata,5);    //前5字节输入转换后为 "Q|j{g"
18 if (iVar1 == 0) {
19    f_5-end_004007f0((char *)input);          //转换后的结果进行下一步处理
20  }
21 else {
22    puts("Wrong");
23  }
24 return;
25 }
```



```
1 void f_5-end_004007f0(char *op_str)
2
3 {
4   size_t lens;
5   int iVar1;
6   uint i;
7
8   i = 5;
9   while (lens = strlen(op_str), i < lens) {
10    if ((i & 1) == 0) {    //偶数时
11      op_str[i] = (byte)((uint)((int)op_str[i] << 0x1a) >> 0x18) | op_str[i] >> 6;//高2位右移6位成为低2位，低6位左移2位成为高6位  相当于一字节循环左移2位
12    }
13    else {//奇数时
14      op_str[i] = op_str[i] >> 2 | (byte)((uint)((int)op_str[i] << 0x1e) >> 0x18);//高6位右移2位成为低6位，低2位左移6位成为高2位  相当于循环右移2位
15    }
16    i = i + 1;
17  }
18  iVar1 = strncmp(op_str + 5,PTR_ARRAY_00410d04,0x1b);
19  if (iVar1 == 0) {
20    puts("Right!");
21  }
22  else {
23    puts("Wrong!");
24  }
25  return;
26 }
```


逻辑清晰

直接逆向

```
    flag = "qctf{"
    keys = [0x52, 0xFD, 0x16, 0xA4, 0x89, 0xBD, 0x92, 0x80, 0x13, 0x41, 0x54, 0xA0, 0x8D, 0x45, 0x18, 0x81,  0xD
E, 0xFC, 0x95, 0xF0, 0x16, 0x79, 0x1A, 0x15, 0x5B, 0x75, 0x1F]
    print len(keys)
    for i in xrange(5,0x20):
     for c in xrange(0,0x100):
      fst = (c ^ ((0x20-i)))
      if (i % 2) == 0:
       res = ((fst << 2) % 0x100) | (fst >> 6)
      else:
       res = (fst >> 2) | ((fst << 6) % 0x100)
      if (res == keys[i-5]):
       flag += chr(c)
    print flag
```

```
flag = "qctf{"
keys = [0x52, 0xFD, 0x16, 0xA4, 0x89, 0xBD, 0x92, 0x80, 0x13, 0x41, 0x54, 0xA0, 0x8D,
print len(keys)
for i in xrange(5,0x20):
    for c in xrange(0,0x100):
        fst = (c ^ ((0x20-i)))
        if (i % 2) == 0:
            res = ((fst << 2) % 0x100) | (fst >> 6)
        else:
            res = (fst >> 2) | ((fst << 6) % 0x100)
        if (res == keys[i-5]):
            flag += chr(c)
print flag
```

```
27
qctf{ReA11y_4_B@89_mlp5_4_XmAn_}
```


得到flag

结语

反编译