

攻防世界 Reverse高手进阶区 2分题 666

原创

思源湖的鱼 于 2020-12-24 14:00:57 发布 139 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [reverse](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_44604541/article/details/111625382

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

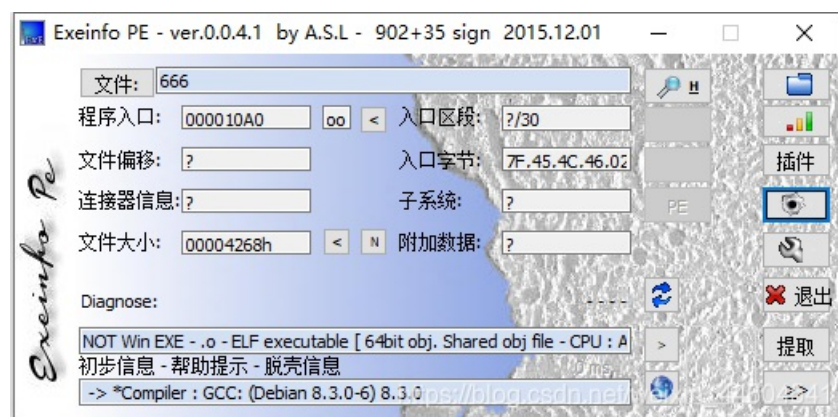
本篇是666的writeup

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

```

1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     char s; // [rsp+0h] [rbp-1E0h]
4     char v5; // [rsp+F0h] [rbp-F0h]
5
6     memset(&s, 0, 0x1EuLL);
7     printf("Please Input Key: ", 0LL);
8     __isoc99_scanf("%s", &v5);
9     encode(&v5, &s);
10    if ( strlen(&v5) == key )
11    {
12        if ( !strcmp(&s, enflag) )
13            puts("You are Right");
14        else
15            puts("flag{This_1s_f4cker_flag}");
16    }
17    return 0;

```

https://blog.csdn.net/weixin_44604541

```

1 int __fastcall encode(const char *a1, __int64 a2)
2 {
3     char v3[32]; // [rsp+10h] [rbp-70h]
4     char v4[32]; // [rsp+30h] [rbp-50h]
5     char v5[40]; // [rsp+50h] [rbp-30h]
6     int v6; // [rsp+78h] [rbp-8h]
7     int i; // [rsp+7Ch] [rbp-4h]
8
9     i = 0;
10    v6 = 0;
11    if ( strlen(a1) != key )
12        return puts("Your Length is Wrong");
13    for ( i = 0; i < key; i += 3 )
14    {
15        v5[i] = key ^ (a1[i] + 6);
16        v4[i + 1] = (a1[i + 1] - 6) ^ key;
17        v3[i + 2] = a1[i + 2] ^ 6 ^ key;
18        *(_BYTE *)(a2 + i) = v5[i];
19        *(_BYTE *)(a2 + i + 1LL) = v4[i + 1];
20        *(_BYTE *)(a2 + i + 2LL) = v3[i + 2];
21    }
22    return a2;
23 }

```

https://blog.csdn.net/weixin_44604541

```

.data:0000000000004060 enflag          db 'izwhroz""w"v.K".Ni',0
.data:0000000000004073                align 20h
.data:0000000000004080                public key
.data:0000000000004080 key          dd 12h
.data:0000000000004080                ; DATA XREF: encode+2Dtr
                ; encode+5Ftr ...

```

转换下enflag

ASCII转换到 ASCII (例: a b c)

```
i z w h r o z " " w " v . K " . N i
```

添加空格 删除空格 将空白字符转换

十六进制转换到16进制(例:0x61或61或61/62) 删除 0x

```
0x69 0x7a 0x77 0x68 0x72 0x6f 0x7a 0x22 0x22 0x77  
0x22 0x76 0x2e 0x4b 0x22 0x2e 0x4e 0x69
```

十进制转换到 10进制 (例: 97 98 99)

```
105 122 119 104 114 111 122 34 34 119 34 118 46 75  
34 46 78 105
```

二进制转换到 2进制(例:01100001 01100010 01100011)

```
01101001 01111010 01110111 01101000 01110010  
01101111 01111010 00100010 00100010 01110111  
00100010 01110110 00101110 01001011 00100010  
00101110 01001110 01101001
```

根据逻辑

写脚本

```
enflag=[105, 122, 119, 104, 114, 111, 122, 34, 34, 119, 34, 118, 46, 75, 34, 46, 78, 105, 0]  
flag=''  
for i in range(0,18,3):  
    flag+=chr((18^enflag[i])-6)  
    flag+=chr((18^enflag[i+1])+6)  
    flag+=chr(18^enflag[i+2]^6)  
print(flag)
```

得到flag: `unctf{b66_6b6_66b}`

结语

简单题