

xctf IgniteMe

原创

菜逼的ctf之路 于 2020-10-13 22:23:42 发布 37 收藏 1

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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_45701079/article/details/109062277

版权

xctf IgniteMe

简单题记录一下(本菜鸡也只能记录一下简单题了)

看源代码

```
1 int v4; // edx
2 void *v5; // eax
3 int result; // eax
4 void *v7; // eax
5 void *v8; // eax
6 void *v9; // eax
7 size_t i; // [esp+4Ch] [ebp-8Ch]
8 char v11[4]; // [esp+50h] [ebp-88h]
9 char v12[28]; // [esp+58h] [ebp-80h]
10 char v13; // [esp+74h] [ebp-64h]
11
12 v3 = (void *)sub_402B30((int)&unk_446360, "Give me your flag:");
13 sub_4013F0(v3, (int (__cdecl *)(void *))sub_403670);
14 sub_401440((int)&dword_4463F0, v4, (int)v12, 127);
15 if ( strlen(v12) < 0x1E && strlen(v12) > 4 )
16 {
17     strcpy(v11, "EIS{");
18     for ( i = 0; i < strlen(v11); ++i )
19     {
20         if ( v12[i] != v11[i] )
21         {
22             v7 = (void *)sub_402B30((int)&unk_446360, "Sorry, keep trying! ");
23             sub_4013F0(v7, (int (__cdecl *)(void *))sub_403670);
24             return 0;
25         }
26     }
27     if ( v13 == 125 )
28     {
29         if ( sub_4011C0(v12) )
30             v9 = (void *)sub_402B30((int)&unk_446360, "Congratulations! ");
31         else
32             v9 = (void *)sub_402B30((int)&unk_446360, "Sorry, keep trying! ");
33         sub_4013F0(v9, (int (__cdecl *)(void *))sub_403670);
34         result = 0;
35     }
36 }
```

00001037 _main:24 (401037)

https://blog.csdn.net/weixin_45701079

前面的我也没看懂，直接看判断函数sub_4011c0()

打开函数

```
IDA View-A Pseudocode-A Hex View-1 Structures Enums
3 size_t v2; // eax
4 signed int v3; // [esp+50h] [ebp-80h]
5 char v4[32]; // [esp+54h] [ebp-ACh]
6 int v5; // [esp+74h] [ebp-8Ch]
7 int v6; // [esp+78h] [ebp-88h]
8 size_t i; // [esp+7Ch] [ebp-84h]
9 char v10[32]; // [esp+80h] [ebp-80h]
```

```

9  cnar v8[128]; // [esp+800] [ebp-800]
10
11 if ( strlen(a1) <= 4 )
12     return 0;
13 i = 4;
14 v6 = 0;
15 while ( i < strlen(a1) - 1 )
16     v8[v6++] = a1[i++];
17 v8[v6] = 0;
18 v5 = 0;
19 v3 = 0;
20 memset(v4, 0, 0x20u);
21 for ( i = 0; ; ++i )
22 {
23     v2 = strlen(v8);
24     if ( i >= v2 )
25         break;
26     if ( v8[i] >= 97 && v8[i] <= 122 )
27     {
28         v8[i] -= 32;
29         v3 = 1;
30     }
31     if ( !v3 && v8[i] >= 65 && v8[i] <= 90 )
32         v8[i] += 32;
33     v4[i] = byte_4420B0[i] ^ sub_4013C0(v8[i]);
34     v3 = 0;
35 }
36 return strcmp("GONDPHYGjPEKruv{{pj}X@rF", v4) == 0;
37}

```

000011C0 sub_4011C0:3 (4011C0)

https://blog.csdn.net/waixin_45761079

逻辑简单先把大小写转换一下(大写转小写, 小写转大写), 之后先进入sub_4012c0()函数, 然后数据异或, 看函数

```

1 int __cdecl sub_4013C0(int a1)
2 {
3     return (a1 ^ 0x55) + 72;
4 }

```

简单加密

直接贴出exp

```

a = [
    0x0D, 0x13, 0x17, 0x11, 0x02, 0x01, 0x20, 0x1D, 0x0C, 0x02, 0x19, 0x2F, 0x17, 0x2B, 0x24, 0x1F,
    0x1E, 0x16, 0x09, 0x0F, 0x15, 0x27, 0x13, 0x26, 0x0A, 0x2F, 0x1E, 0x1A, 0x2D, 0x0C, 0x22, 0x4
]
s='GONDPHYGjPEKruv{{pj}X@rF'
flag=''
for i in range(len(s)):
    flag+=chr((((ord(s[i])^a[i])-72)^0x55)^32)
print(flag)

```

最后一个异或32的是大小写转换(看过王爽的汇编的应该懂为啥), 不过因为下划线的存在,异或32之后下划线也变了, 所以得到的数据把空格换成下划线就可以了(加上EIS{})。

最近做题有点少, 因为社团招新和培训和本地环境出错了, 所以书本学习总结可能要向后安排了。