

Kanxue看雪KCTF2019-Q1第六题【Repwn】Writeup

原创

iqiqiya 于 2019-03-26 21:16:26 发布 391 收藏

分类专栏: [我的逆向之路](#) [我的CTF之路](#) -----[看雪KCTF2019-Q1](#) [我的CTF进阶之路](#) 文章标签: [Repwn KCTF2019-Q1](#)

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/xiangshangbashaonian/article/details/88830451>

版权



[我的逆向之路](#) 同时被 3 个专栏收录

108 篇文章 10 订阅

订阅专栏



[我的CTF之路](#)

92 篇文章 5 订阅

订阅专栏



-----[看雪KCTF2019-Q1](#)

4 篇文章 0 订阅

订阅专栏

第六题: Repwn

PEiD查壳, 无壳 直接载入IDA shift+f12分析字符串

Address	Length	Type	String
.data:00...	0000001C	C	Sta`anmXHc[VgXQ:~_caK?RNG-RF
.rdata:0...	00000005	C	@` \a/
.rdata:0...	00000005	C	@80(
.rdata:0...	00000005	C	\b91)!
.rdata:0...	00000005	C	;3#\x1B
.rdata:0...	00000007	C	\a\b\t\b\t\n\v
.rdata:0...	00000005	C	\v\n\r\a\b
.rdata:0...	0000000F	C	(3-!0,1'8\"5.*2\$
.rdata:0...	00000005	C	;3#\x1B
.rdata:0...	00000008	C	<4,\$??/'
.rdata:0...	00000005	C	\a>6.&
.rdata:0...	00000021	C	Key_Is_Wrong,Please_Input_Again!
.rdata:0...	00000017	C	String_Length_is_Wrong
.rdata:0...	0000001C	C	Please Input Your Key_ Now!
.rdata:0...	00000006	C	pause
.rdata:0...	0000000B	C	[mjj] [14^ty

sub_4014C0()分析如下:

```

ion Instruction Data Unexplored External symbol
IDA View-A Pseudocode-A Strings window Hex View-1 Structures
Se ^ 8 int v7; // [esp+28h] [ebp-40h]
.ti 9 int v8; // [esp+2Ch] [ebp-3Ch]
.ti 10 int v9; // [esp+30h] [ebp-38h]
.ti 11 int v10; // [esp+34h] [ebp-34h]
.ti 12 int v11; // [esp+38h] [ebp-30h]
.ti 13 int v12; // [esp+3Ch] [ebp-2Ch]
.ti 14 char mystr; // [esp+40h] [ebp-28h]
.ti 15
.ti 16 sub_404930(0x10u, (int)this, (int)Str);
.ti 17 sub_4044B0();
.ti 18 v1 = 0;
.ti 19 v5 = 'yt^';
.ti 20 v6 = '+pLc';
.ti 21 v7 = 'a+SG';
.ti 22 v8 = 'G-QG';
.ti 23 v9 = 'G1(V';
.ti 24 v10 = ')y}J';
.ti 25 v11 = 'SGA';
.ti 26 v12 = 'ea+';
.ti 27 strcpy(v4, "Ansome_Is_Wrong");
.ti 28 while ( v1 < strlen((const char *)&v5) )
.ti 29     *((_BYTE *)&v5 + v1++) ^= 0x18u; // 这里可以解出 Flag{Th3_K3y_I5_N0t_Rea11Y_K3y}
.ti 30 puts("Please Input Your Key_ Now!");
.ti 31 scanf("%s", &mystr);
.ti 32 if ( sub_4012F0((int)&mystr) ) // flag的第8-19位是X1Y0uN3tG00d, 第20位是H
.ti 33 {
.ti 34     sub_401460(&mystr); // flag长度等于24
.ti 35     system("pause");
.ti 36 }
.ti 37 else
.ti 38 {
.ti 39     puts(v4);
.ti 40 }
.ti 41 return 0;
.ti 42 }

```

<https://blog.csdn.net/xiangshangbashaonian>

sub_4012F0()可以得到flag的第8-19位是X1Y0uN3tG00d, 第20位是H

双击进入sub_401460()

```

Instruction Data Unexplored External symbol
IDA View-A Pseudocode-A Stack of sub_401460 Strings window Hex View-1 Structures
Se ^ 1 int __cdecl sub_401460(char *Str)
.ti 2 {
.ti 3     char Dest; // [esp+8h] [ebp-10h]
.ti 4
.ti 5     if ( strlen(Str) == 24 )
.ti 6     {
.ti 7         if ( sub_4013B0((int)Str) ) // flag长度等于24 最后四位分别减去 X F 3 k
.ti 8         {
.ti 9             Str[20] -= 'X';
.ti 10            Str[21] -= 'F';
.ti 11            Str[22] -= 3;
.ti 12            Str[23] -= 'k';
.ti 13            strcpy(&Dest, Str);
.ti 14        }
.ti 15    }
.ti 16    else
.ti 17    {
.ti 18        printf("String Length is Wrong");
.ti 19    }
.ti 20    return 0;
.ti 21 }

```

<https://blog.csdn.net/xiangshangbashaonian>

可以先分析sub_4013B0

```

1 signed int __cdecl sub_4013B0(int a1)
2 {
3     int v1; // ebx
4     int v2; // ecx
5     int v3; // esi
6     signed int result; // eax
7
8     sub_401380(a1);
9     v1 = dword_40802C + 1000 * dword_408020[0] + 100 * dword_408024 + 10 * dword_408028;
10    v2 = dword_408034 + 10 * dword_408030;
11    v3 = dword_40803C + 10 * dword_408038;
12    if ( 2 * (v1 + v2) != 4040 || 3 * v2 / 2 + 100 * v3 != 115 )
13        goto LABEL_2;
14    result = 1;
15    if ( v1 - 110 * v3 != 1900 )
16    {
17        printf("Key_Is_Wrong,Please_Input_Again!");
18    LABEL_2:
19        result = 0;
20    }
21    return result;
22 }

```

<https://blog.csdn.net/xiangshangbashaonian>

sub_4013B0取输入第一部分前8个字符按aaaabbcc转为整数, 校验是否满足方程组 $(aaaa + bb) * 2 == 4040$ && $(3 * bb / 2) + (100 * cc) == 115$ && $aaaa - 110 * cc == 1900$

这里可以用z3求解

```

from z3 import *
aaaa = Int('aaaa')
bb = Int('bb')
cc = Int('cc')
s = Solver()
s.add(aaaa>0,aaaa<10000)
s.add(bb>0,bb<100)
s.add(cc>0,cc<100)
s.add((aaaa + bb) * 2 == 4040)
s.add((3 * bb / 2) + (100 * cc) == 115)
s.add(aaaa - 110 * cc == 1900)
m = s.model()
print(m[aaaa].as_long())
print(m[bb].as_long())
print(m[cc].as_long())

```

求得20101001

这里如果不明白 可以结合sub_401380()进行理解

```

IDA Vie... Pseudocod... Strings win...
1 int __cdecl sub_401380(int a1)
2 {
3     signed int v1; // edx
4     int result; // eax
5
6     v1 = 0;
7     do
8     {
9         result = *(char *)(v1 + a1) - '0';
10        dword_408020[v1++] = result;
11    }
12    while ( v1 <= 7 );
13    return result;
14}

```

<https://blog.csdn.net/xiangshangbashaonian>

实现了atoi函数 将前8位 作为字符串转换为整型

所以可以用如下脚本:

```

for one in xrange(0,10):
    for two in xrange(0,10):
        for three in xrange(0,10):
            for four in xrange(0,10):
                for five in xrange(0,10):
                    for six in xrange(0,10):
                        for seven in xrange(0,10):
                            for eight in xrange(0,10):
                                v1 = 1000 * one + 100 * two + 10 * three + four
                                v2 = 10 * five + six
                                v3 = 10 * seven + eight
                                if v1 + v2 == 2020 and 100 * v3 + 3 * v2 / 2 == 115 and v1 - 110 * v3 == 19
                                    print one,two,three,four,five,six,seven,eight

#2 0 1 0 1 0 0 1

```

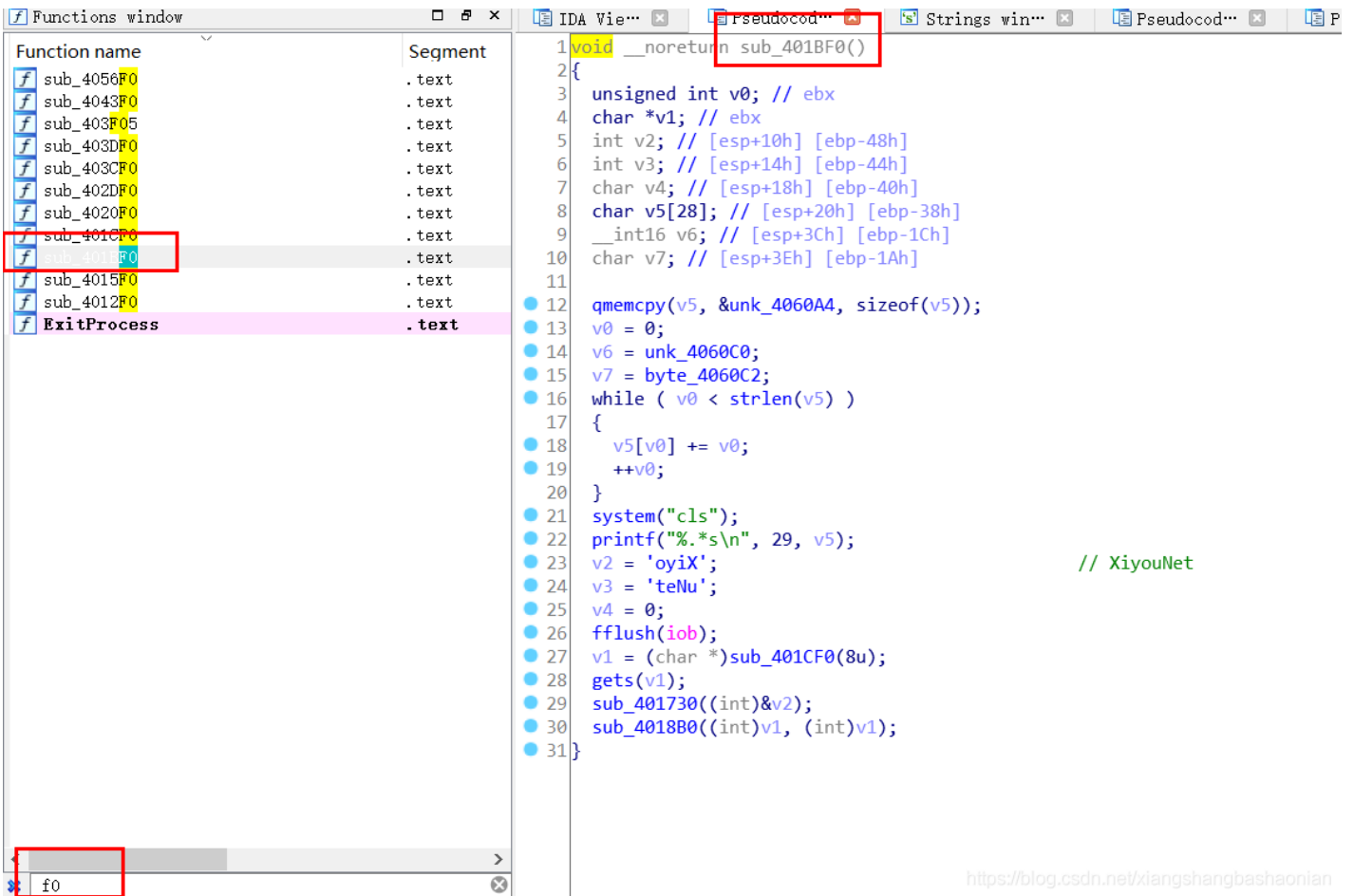
OD进行动态调试 输入20101001X1Y0uN3tG00dHF3k

00401475	74 19	je short Repwn.00401490	
00401477	C70424 9D734	mov dword ptr ss:[esp],Repwn.0040739D	String Length is Wrong
0040147E	E8 35430000	call <imp.&msvcrt.printf>	printf
00401483	> 83C4 14	add esp,0x14	
00401486	31C0	xor eax,eax	
00401488	5B	pop ebx	Repwn.004000F0
00401489	5D	pop ebp	Repwn.004000F0
0040148A	C3	retn	
0040148B	90	nop	
0040148C	8D7426 00	lea esi,dword ptr ds:[esi]	https://blog.csdn.net/xiangshangbashaonian

局部变量buf长度为0x14, 因此会造成栈溢出, 恰好flag后四位会覆盖返回地址

由于flag[20]='H', flag[20]-'X'=0xf0, 考虑到小端序, 所以只能选地址对齐0xf0的函数

这里还可以根据查找字符串引用来确定



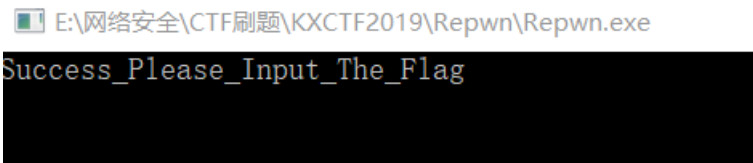
也可以用所有的进行验证 要注意字节溢出 高位舍去

```

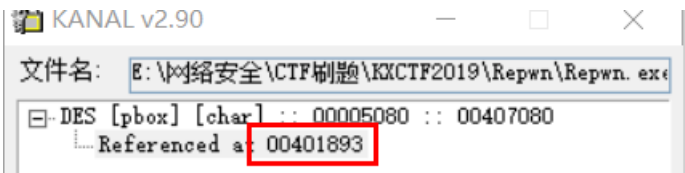
F0 1B 40 00
+ 58 46 03 6B
-----
48 61 43 6B
H a C k

```

得到20101001X1Y0uN3tG00dHaCk



接着就是再次获取输入 sub_401730()与sub_4018b0() 将XiyouNet作为key值把我们的输入进行DES加密



最后与给定的密文进行比较 验证是否一致

```

109 v20 = 2,
110 v29 = 8;
111 while ( 1 )
112 {
113     if ( Dst[v8] != v12[v8] )
114         v9 = 1;
115     if ( ++v8 > 31 )
116     {
117         if ( !v9 )
118             printf(Format);
119         putchar(10);
120         system("pause");
121         ExitProcess(0);
122     }
123 }
124 }

```

<https://blog.csdn.net/xiangshangbashaonian>

我们可以直接使用IDC脚本提取密文

```

.text:00401B6C mov     [ebp+var_28], 5
.text:00401B73 mov     [ebp+var_24], 0Ah
.text:00401B7A mov     [ebp+var_20], 2
.text:00401B81 mov     [ebp+var_1C], 8
.text:00401B88 nop
.text:00401B89 lea    esi, [esi+0]
.text:00401B90
.text:00401B90 loc_401B90:                                ; CODE XREF
EIP .text:00401B90 mov     eax, [ebp+ecx*4+var_138]
.text:00401B97 cmp     [ebp+ecx*4+var_98], eax
.text:00401B9E jz     short loc_401BAB
.text:00401BA0 mov     edi, 1
.text:00401BA5 mov     [ebp+var_16C], edi
.text:00401BAB
.text:00401BAB loc_401BAB:                                ; CODE XREF
.text:00401BAB inc     ecx
.text:00401BAC cmp     ecx, 1Fh
--- .text:00401BAF jle     short loc_401B90
00000F90 00401B90: sub_4018B0:loc_401B90 (Synchronized with EIP)

```

Hex View-1

Execute script

Snippet list

Name
Default snippet

Please enter script body

```

auto from1 = 0x60FD24;
auto from2 = 0x60FD60;
auto i, x, m;
m = from2 - from1;
for(;from1<=from2;from1=from1+4)
{
    x = Byte(from1);
    Message("%x", x);
}

```

Line:8 Column:22

Scripting language IDC Tab size 4

Run Export Import

0034

9db084ac97041e30

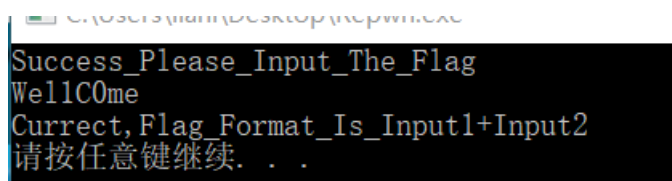
IDC

最后编写python脚本进行DES解密或者使用PYG密码学工具即可：

```
from Crypto.Cipher import DES
des = DES.new('XiyouNet')
s = '9db084ac97041e30'.decode('hex')
print(des.decrypt(s))
#WellC0me
```

最后的flag是input1+input2

也就是20101001X1Y0uN3tG00dHaCkWel1C0me



```
C:\Users\qian\Desktop>python.exe
Success_Please_Input_The_Flag
WellC0me
Currect, Flag_Format_Is_Input1+Input2
请按任意键继续. . .
```

参考链接:

<https://bbs.pediy.com/thread-250242.htm>

<https://bbs.pediy.com/thread-250229.htm>