BABYRE 攻防世界

原创

北风~ 于 2020-04-29 22:23:57 发布 1137 收藏 1

分类专栏： 逆向与保护

本文链接：https://blog.csdn.net/weixin_45055269/article/details/105850121

版权

逆向与保护 专栏收录该内容

65 篇文章 4 订阅

订阅专栏

工具

IDA动调

思路展开

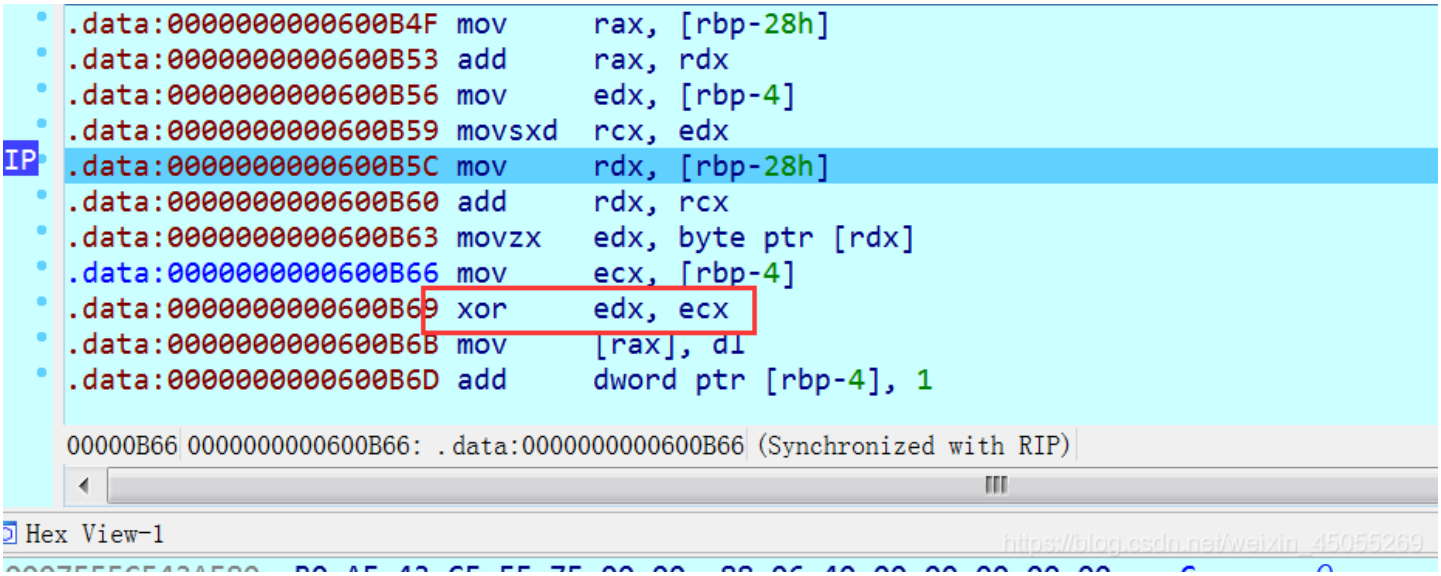
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s; // [rsp+0h] [rbp-20h]
  int v5; // [rsp+18h] [rbp-8h]
  int i; // [rsp+1Ch] [rbp-4h]

  for ( i = 0; i <= 181; ++i )
  {
    envp = (const char **)(*((unsigned __int8 *)judge + i) ^ 0xCu);
    *((_BYTE *)judge + i) ^= 0xCu;
  }
  printf("Please input flag:", argv, envp);
  __isoc99_scanf("%20s", &s);
  v5 = strlen(&s);
  if ( v5 == 14 && (unsigned int)judge(&s) ) #输入长度14
    puts("Right!");
  else
    puts("Wrong!");
  return 0;
}
```

judge函数F5没用，猜测judge函数动态生成，下断点动调。

```
B04 mov     [rbp-28h], rdi
B08 mov     byte ptr [rbp-20h], 66h
B08 judge endp ; sp-analysis failed
B08
B0C mov     byte ptr [rbp-1Fh], 6Dh
B10 mov     byte ptr [rbp-1Eh], 63h
B14 mov     byte ptr [rbp-1Dh], 64h
B18 mov     byte ptr [rbp-1Ch], 7Fh
B1C mov     byte ptr [rbp-1Bh], 6Bh
B20 mov     byte ptr [rbp-1Ah], 37h
B24 mov     byte ptr [rbp-19h], 64h
```


发现14个赋值语句，猜测与flag有关。接着跟进去找到关键算法'异或'（下图）



查看ecx的值发现是0x0到0xe，正好14个，与前面赋值语句异或就是flag。

```
cipher=[0x66,0x6d,0x63,0x64,0x7f,0x6b,0x37,0x64,0x3b,0x56,0x60,0x3b,0x6e,0x70]
flag=""
for i in range(0x0,0xe):
 flag+=chr(cipher[i]^i)
print(flag)
```

flag{n1c3_j0b}