83：Whitzard OJ逆向-Dont Crack It

原创

S1lenc3 于 2020-03-03 23:08:46 发布 151 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_41858371/article/details/104644139

这道题我也是很懵，不知道怎么拿到flag，也找不到writeup，求大佬指点。

先查壳，UPX，直接-d脱衣服。

```
4
5  scanf((unsigned __int64)&unk_48A6B4);
6  if ( (unsigned __int64)sizeof(&v1, &v1) > 0x13 )
7    return 0LL;
8  if ( (unsigned int)sub_401A78((__int64)&v1) != 0 )
9    sub_408870((unsigned __int64)"WOW! You're so cool!");
0  return 0LL;
1}
```

可以猜出这两个函数。

```
15  v3 = 0LL;
16  v4 = 0LL;
17  v5 = 0;
18  sub_401A29(&dword_400000, 256LL, &v6);
19  for ( i = 0; ; ++i )
20  {
21    v1 = i;
22    if ( v1 >= sizeof(a1, 256LL) )
23      break;
24    *((_BYTE *)&v3 + i) = *((_BYTE *)&v6 + i) ^ *(_BYTE *)(i + a1);
25  }
26  return (unsigned int)cmp(&v3, &unk_48A6A0) == 0;
27}
```


这个是加密函数，刚开始还傻傻的分析了一下sub_401a29,里边超多代码，后果断放弃，后来再看了看，发现这个函数是独立的，不受我们输入的影响，所以直接gdb调试dump内存。

```
命令：
 b *0x??????
   x /16x 0x?????
```

然后异或解密出来根本不是可视字符，我疯了，动态修改内存验证结果没错，可能flag在别的地方会有什么坑吧。。。