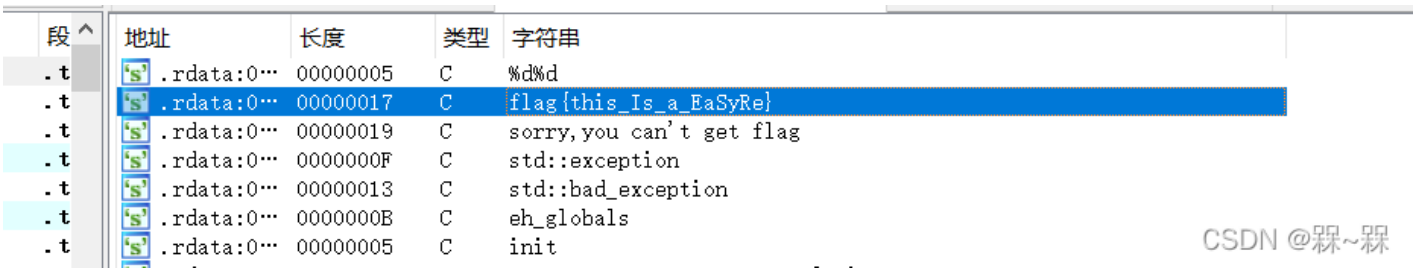
BUUCTF解析

原创

羖~羖 于 2022-02-21 14:42:00 发布 39 收藏
文章标签： p2p linq gnu 开发语言

easyre 1

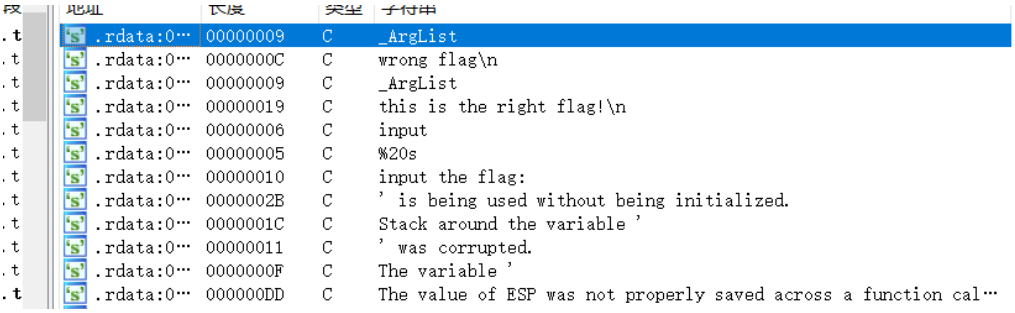
这个在IDI中打开用 SHIFT+F12 查看字符串窗口发现flag



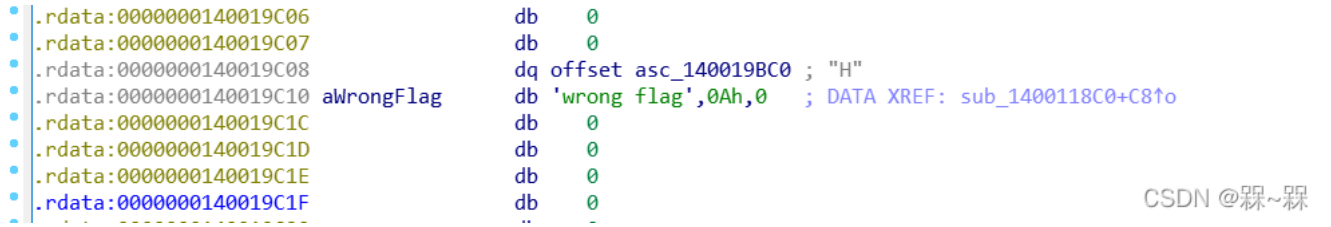
reverse1

下好后是一个压缩包的形式于是解压后查看是一个exe文件倒是不能用

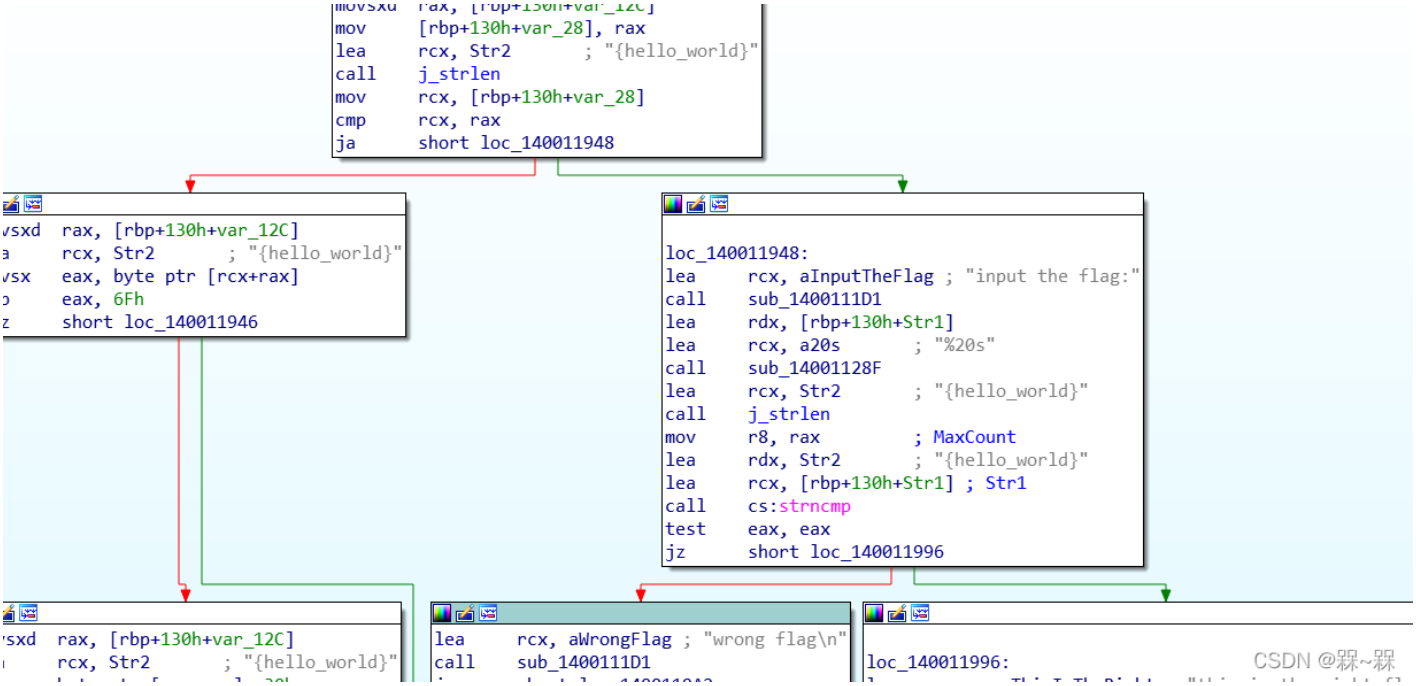
接着用IDI打开并SHIFT+F12 查看字符串窗口



发现flag进行跟进



再次跟进



发现flag 提示是hello_world 并且与Str2函数有关F5查看

```
  7  char v5; // [rsp+0h] [rbp-20h]
  8  int j; // [rsp+24h] [rbp+4h]
  9  char Str1; // [rsp+48h] [rbp+28h]
 10  unsigned __int64 v8; // [rsp+128h] [rbp+108h]
 11
 12  v0 = &v5;
 13  for ( i = 82i64; i; --i )
 14  {
 15    *(_DWORD *)v0 = -858993460;
 16    v0 += 4;
 17  }
 18  for ( j = 0; ; ++j )
 19  {
 20    v8 = j;
 21    v2 = j_strlen(Str2);
 22    if ( v8 > v2 )
 23      break;
 24    if ( Str2[j] == 111 )
 25      Str2[j] = 48;
 26  }
 27  sub_1400111D1("input the flag:");
 28  sub_14001128F("%20s", &Str1);
 29  v3 = j_strlen(Str2);
 30  if ( !strncmp(&Str1, Str2, v3) )
 31    sub_1400111D1("this is the right flag!\n");
 32  else
 33    sub_1400111D1("wrong flag\n");
 34  sub_14001113B(&v5, &unk_140019D00);
```


发现有一个for循环并包含一个if比较 字符与数字选中数字+R进行转义

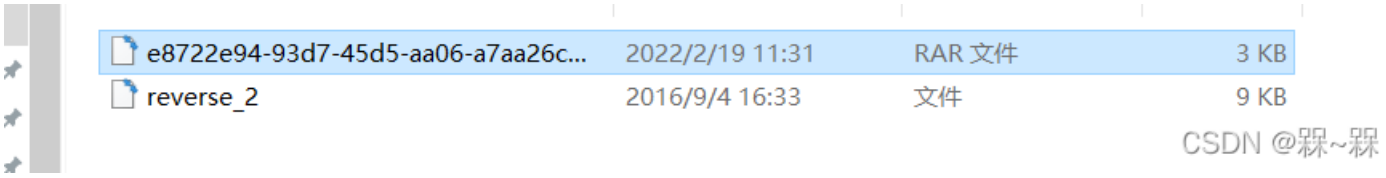
```
if ( Str2[j] == 'o' )
  Str2[j] = '0';
}
sub_1400111D1("input the flag:");
```

及意思是将o变成0

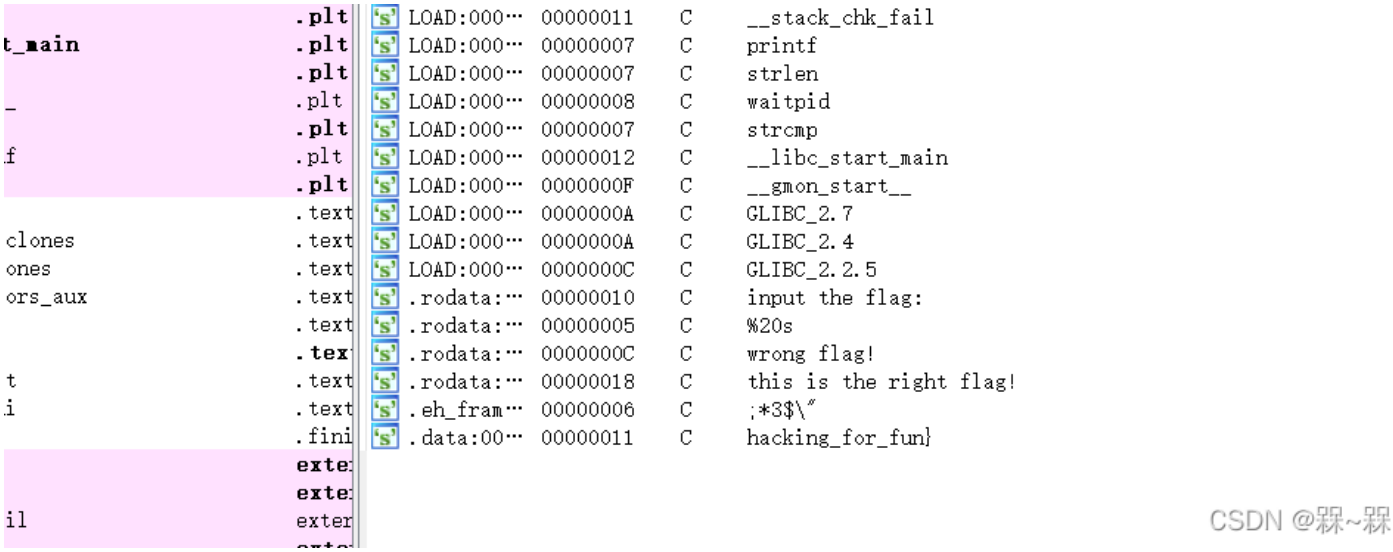
得到flag{hell0_w0rld}

reverse2

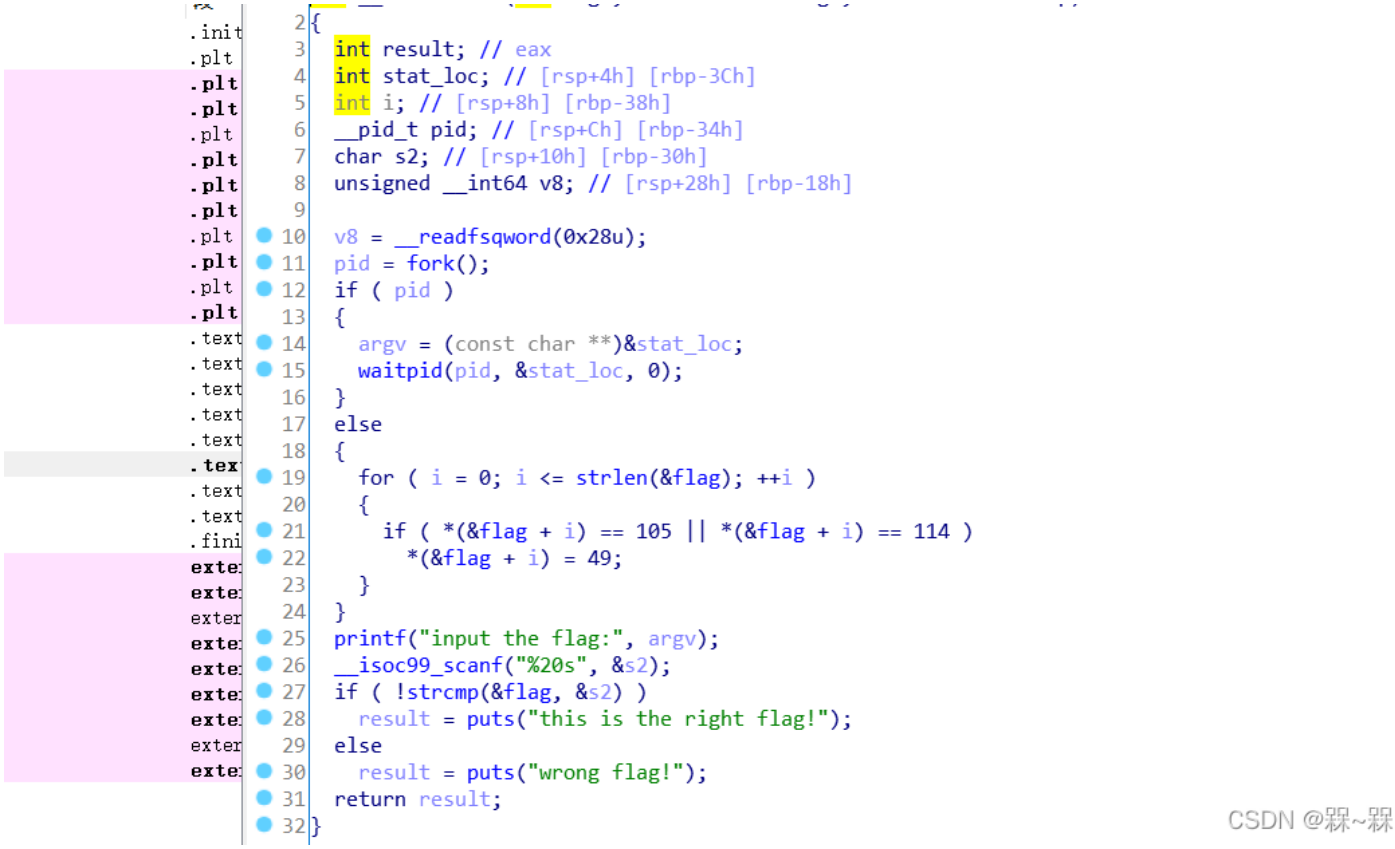
一个没有提示的压缩包解压后是一个



用神IDI进行反汇编



发现有flag提示还有个比较特殊的{hacking_for_fun}不鸟他打开flag



也是和上一题一致是一个字符替换转换后

```
  }
  else
  {
    for ( i = 0; i <= strlen(&flag); ++i )
    {
      if ( *(&flag + i) == 'i' || *(&flag + i) == 'r' )
        *(&flag + i) = '1';
    }
  }
```

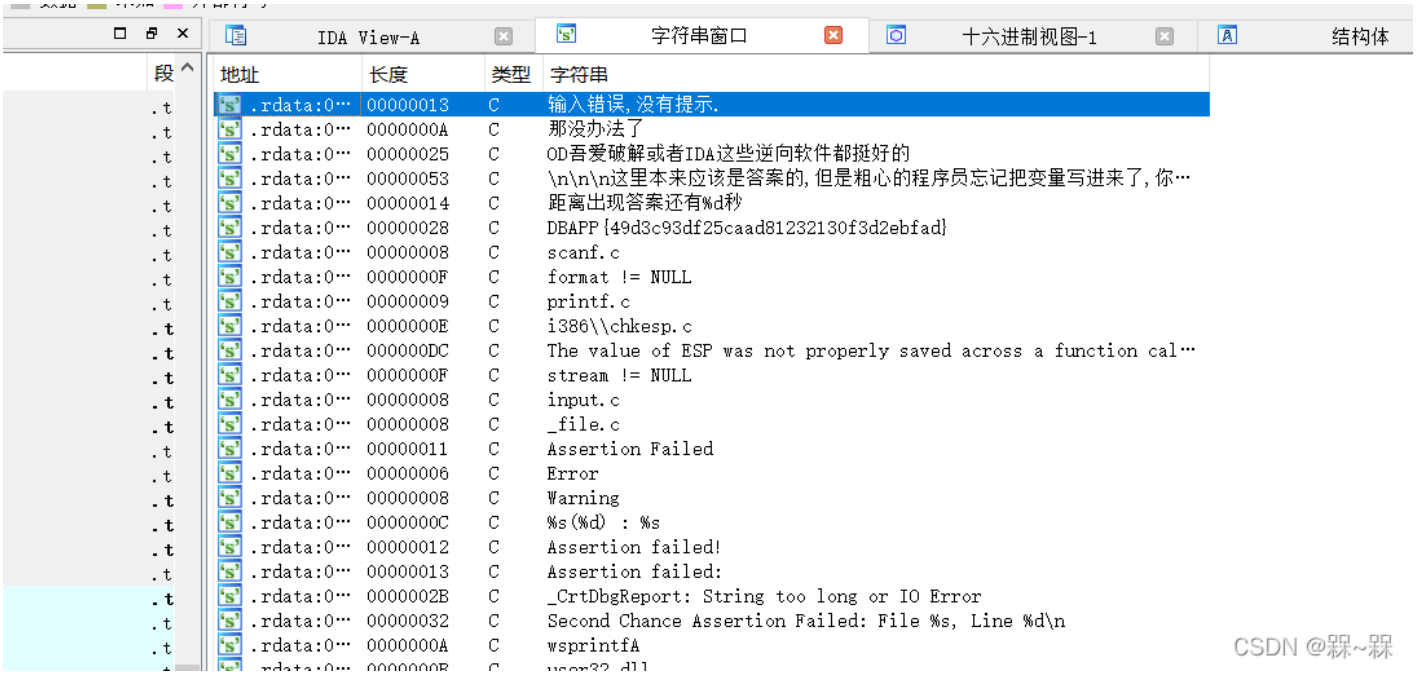

但没有对比文本于是想到这个特殊的{hacking_for_fun}进行替换后即得到

flag{{hack1ng_fo1_fun}

内涵的软件

这个是一个exe文件打开后是这样的

有点被耍的感觉有IDI打开



直接得到flag别想多千万别想多这就是flag