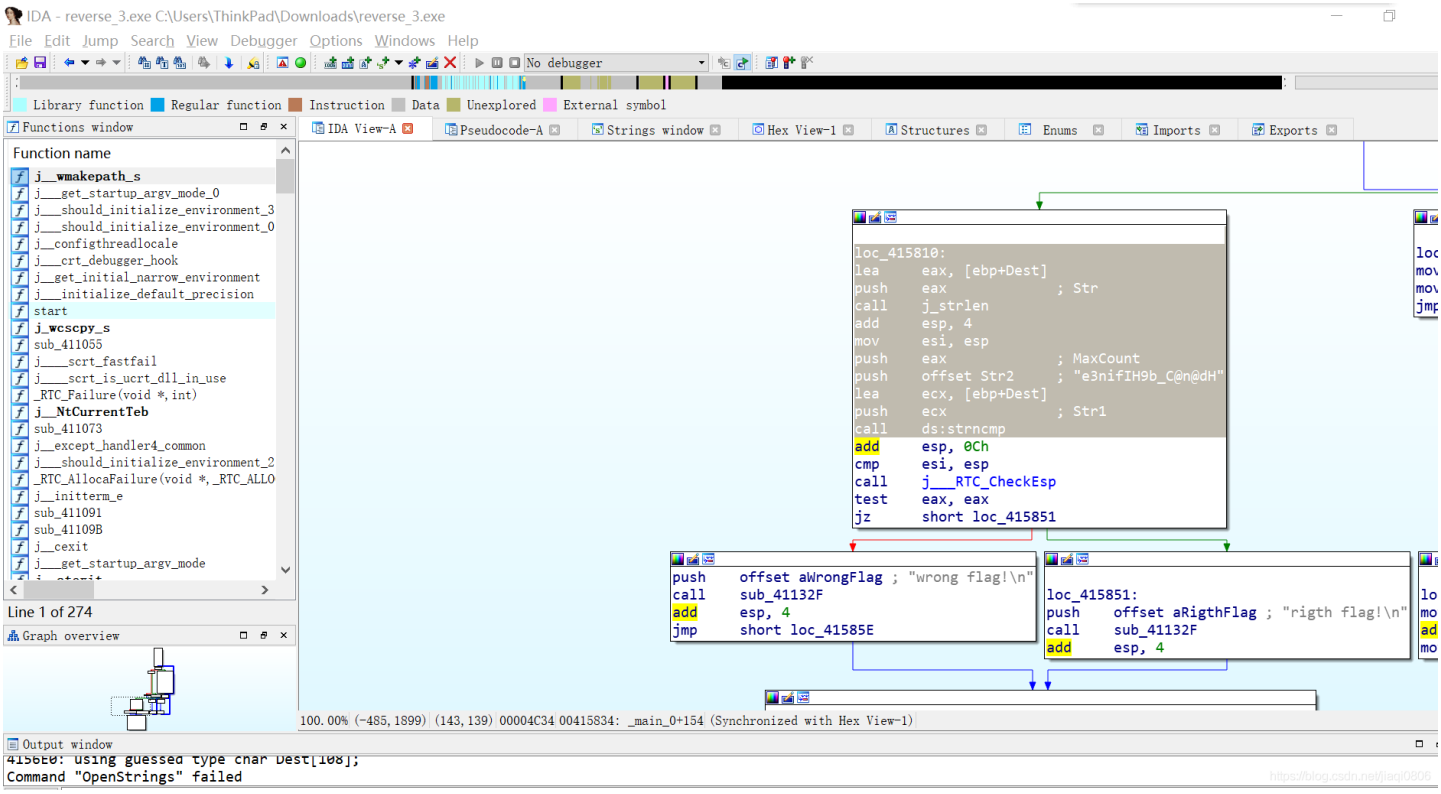
[bugku逆向] love WriteUp

原创

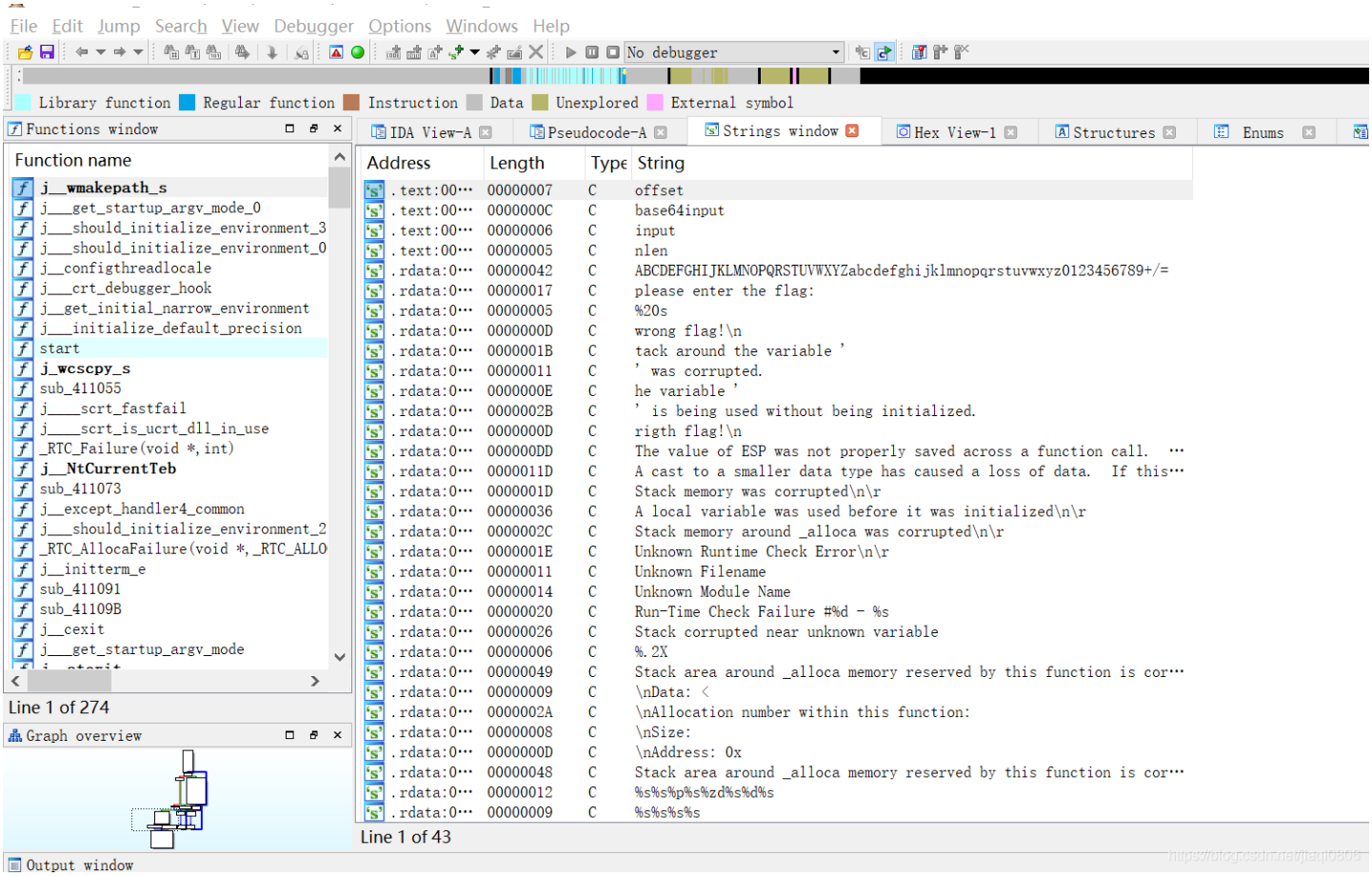
球球球你了 于 2020-02-23 18:16:25 发布 124 收藏

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/jiaqi0806/article/details/104464297
版权

用IDA打开reverse.exe 界面如下



快捷键 shift+F12 打开字符串视图



找到关键词：base64（考虑是否是base64编码？） 以及wrong/right flag的判断

双击wrong flag！ 找到对应函数 ctrlX 后再F5可以打开对应的伪代码

IDA Vie… | Pseudocode-B | Pseudocod… | Strings w

```
  6  int v3; // edx
  7  __int64 v4; // ST08_8
  8  signed int j; // [esp+DCh] [ebp-ACh]
  9  signed int i; // [esp+E8h] [ebp-A0h]
 10  signed int v8; // [esp+E8h] [ebp-A0h]
 11  char Dest[108]; // [esp+F4h] [ebp-94h]
 12  char Str; // [esp+160h] [ebp-28h]
 13  char v11; // [esp+17Ch] [ebp-Ch]
 14
 15  for ( i = 0; i < 100; ++i )
 16  {
 17    if ( (unsigned int)i >= 0x64 )
 18      j____report_rangecheckfailure();
 19    Dest[i] = 0;
 20  }
 21  sub_41132F("please enter the flag:");
 22  sub_411375("%20s", &Str);
 23  v0 = j_strlen(&Str);
 24  v1 = (const char *)sub_4110BE(&Str, v0, &v11);
 25  strncpy(Dest, v1, 0x28u);
 26  v8 = j_strlen(Dest);
 27  for ( j = 0; j < v8; ++j )
 28    Dest[j] += j;
 29  v2 = j_strlen(Dest);
 30  if ( !strncmp(Dest, Str2, v2) )
 31    sub_41132F("rigth flag!\n");
 32  else
 33    sub_41132F("wrong flag!\n");
 34  HIDWORD(v4) = v3;
 35  LODWORD(v4) = 0;
 36  return v4;
 37}
```

https://blog.csdn.net/jiaqi0806

观察代码成分 copy输入到dest并做了个累加 比较和str2的值

这里再根据之前base64的判断 可能是输入的字符base64加密后加上index值，再转化成字符串，与e3niflH9b_C@n@dH（点击str2就会定位到str2的字符串）比较 若一致则输出right flag

可以写一个python脚本进行计算

```python
import base64
s='e3nifIH9b_C@n@dH'
f=''
n=len(s)
for i in range(n):
    f+=chr(ord(s[i])-i)
print(f)
print(base64.b64decode(f))
```

拿到flag

创作打卡挑战赛

赢取流量/现金/CSDN周边激励大奖