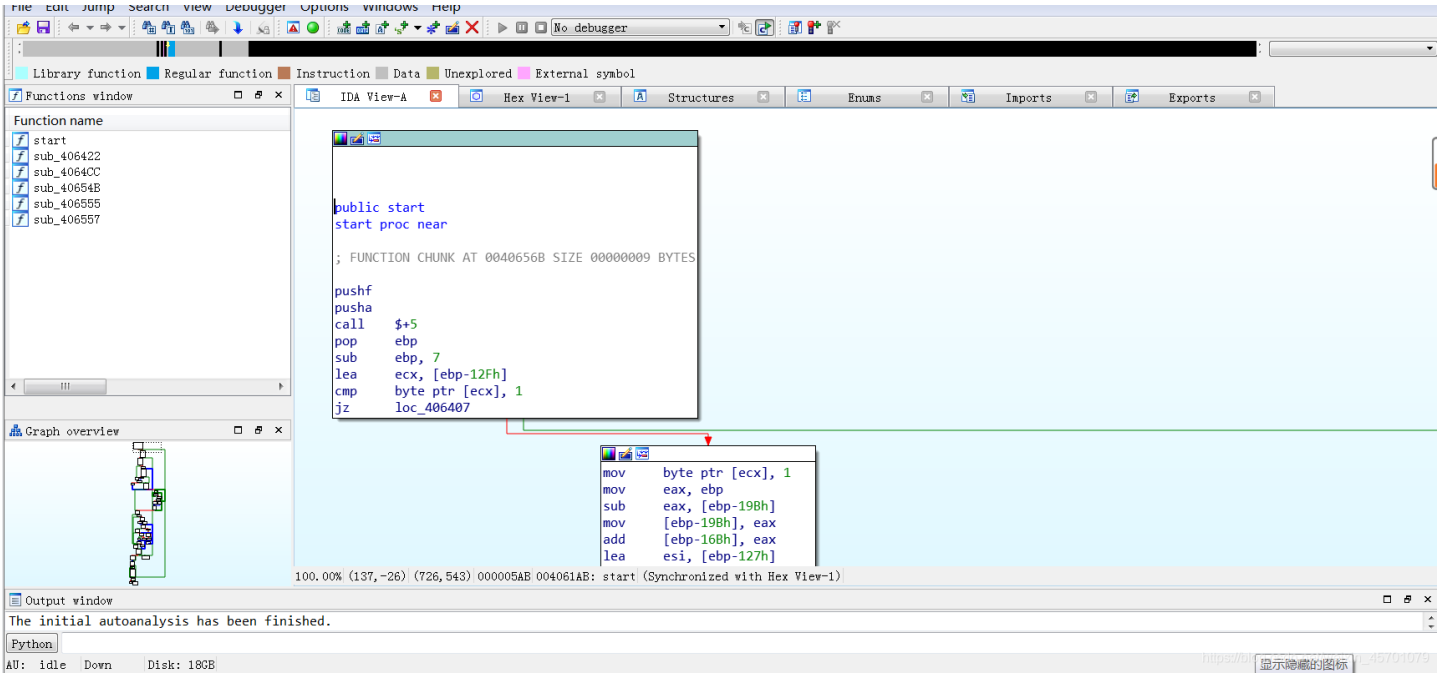
xctf crackme

原创

菜逼的ctf之路 于 2020-10-22 20:17:31 发布 103 收藏

xctf crackme

文件用ida打开



发现有壳，查壳发现nspack壳

我用工具没有成功，没办法只能手脱

脱壳参考这位大佬

脱壳成功

```
_BOOL4 v19; // [rsp+B8h] [rbp-8h]
int i; // [rsp+BCh] [rbp-4h]

sub_407470((__int64)"Give me the password: ", argv, envp, argv);
sub_4075A0((__int64)"%s", v9);
for ( i = 0; v9[i]; ++i )
  ;
v19 = i == 22;
v18 = 10;
do
{
  v7 = sub_406D90((__int64)"%s", (__int64)v9, v3, v4, v5, v6);
  v4 = (unsigned int)(v7 % 22);
  v15 = v7 % 22;
  v17 = 0;
  v14 = byte_6B4270[v7 % 22];
  v13 = v9[v7 % 22];
  v12 = v7 % 22 + 1;
  v16 = 0;
  while ( v16 < v12 )
  {
    ++v16;
    v17 = 1828812941 * v17 + 12345;
  }
  v3 = v17;
  v11 = v17 ^ v13;
  if ( v14 != ((unsigned __int8)v17 ^ v13) )
    v19 = 0;
  --v18;
}
while ( v18 );
if ( v19 )
  v10 = sub_407470((__int64)"Congras\n");
else
```


逻辑简单

最后贴上我的payload

```
a= [
    0x00000012, 0x00000004, 0x00000008, 0x00000014, 0x00000024, 0x0000005C, 0x0000004A, 0x0000003D,
    0x00000056, 0x0000000A, 0x00000010, 0x00000067, 0x00000000, 0x00000041, 0x00000000, 0x00000001,
    0x00000046, 0x0000005A, 0x00000044, 0x00000042, 0x0000006E, 0x0000000C, 0x00000044, 0x00000072,
    0x0000000C, 0x0000000D, 0x00000040, 0x0000003E, 0x0000004B, 0x0000005F, 0x00000002, 0x00000001,
    0x0000004C, 0x0000005E, 0x0000005B, 0x00000017, 0x0000006E, 0x0000000C, 0x00000016, 0x00000068,
    0x0000005B, 0x00000012,0x48,0x0e]
s="this_is_not_flag"
flag=''
for i in range(42):
    flag+=chr(ord(s[i%16])^a[i])
print(flag)
```

总结：这道题逻辑还是比较简单的，主要还是脱壳要成功