BugkuCTF-练习题_逆向_入门逆向writeup

原创

Peter·Pan 于 2019-08-29 10:20:56 发布 498 收藏 2

分类专栏： CTF 文章标签： CTF练习题

本文链接：https://blog.csdn.net/PannnJq/article/details/100132438

writeup

题目: baby.zip

- Step1 下载这个压缩包，解压后为baby.exe文件，放入exeinfo中查看信息。
- Step2 在IDA中打开baby.exe
- Step3 找到main函数使用F5键转换，没发现任何信息，view-string查看字符串也没有信息。

```
.text:00401475                call    _printf
.text:0040147A                mov     byte ptr [esp+2Fh], 66h
.text:0040147F                mov     byte ptr [esp+2Eh], 6Ch
.text:00401484                mov     byte ptr [esp+2Dh], 61h
.text:00401489                mov     byte ptr [esp+2Ch], 67h
.text:0040148E                mov     byte ptr [esp+2Bh], 7Bh
.text:00401493                mov     byte ptr [esp+2Ah], 52h
.text:00401498                mov     byte ptr [esp+29h], 65h
.text:0040149D                mov     byte ptr [esp+28h], 5Fh
.text:004014A2                mov     byte ptr [esp+27h], 31h
.text:004014A7                mov     byte ptr [esp+26h], 73h
.text:004014AC                mov     byte ptr [esp+25h], 5Fh
.text:004014B1                mov     byte ptr [esp+24h], 53h
.text:004014B6                mov     byte ptr [esp+23h], 30h
.text:004014BB                mov     byte ptr [esp+22h], 5Fh
.text:004014C0                mov     byte ptr [esp+21h], 43h
.text:004014C5                mov     byte ptr [esp+20h], 30h
.text:004014CA                mov     byte ptr [esp+1Fh], 4Fh
.text:004014CF                mov     byte ptr [esp+1Eh], 4Ch
.text:004014D4                mov     byte ptr [esp+1Dh], 7Dh
.text:004014D9                mov     eax, 0
.text:004014DE                leave
.text:004014DF                retn
.text:004014DF _main          endp
```


- Step4 看到一连串ptr+数字，使用R键将其转化后发现flag

```
.text:00401475                call    _printf
.text:0040147A                mov     byte ptr [esp+2Fh], 'f'
.text:0040147F                mov     byte ptr [esp+2Eh], 'l'
.text:00401484                mov     byte ptr [esp+2Dh], 'a'
.text:00401489                mov     byte ptr [esp+2Ch], 'g'
.text:0040148E                mov     byte ptr [esp+2Bh], '{'
.text:00401493                mov     byte ptr [esp+2Ah], 'R'
.text:00401498                mov     byte ptr [esp+29h], 'e'
.text:0040149D                mov     byte ptr [esp+28h], '_'
.text:004014A2                mov     byte ptr [esp+27h], '1'
.text:004014A7                mov     byte ptr [esp+26h], 's'
.text:004014AC                mov     byte ptr [esp+25h], '_'
.text:004014B1                mov     byte ptr [esp+24h], 'S'
.text:004014B6                mov     byte ptr [esp+23h], '0'
.text:004014BB                mov     byte ptr [esp+22h], '_'
.text:004014C0                mov     byte ptr [esp+21h], 'C'
.text:004014C5                mov     byte ptr [esp+20h], '0'
.text:004014CA                mov     byte ptr [esp+1Fh], 'O'
.text:004014CF                mov     byte ptr [esp+1Eh], 'L'
.text:004014D4                mov     byte ptr [esp+1Dh], '}'
.text:004014D9                mov     eax, 0
.text:004014DE                leave
.text:004014DF                retn
.text:004014DF _main          endp
```


flag： flag{Re_1s_S0_C0OL}