ctf 抓捕赵德汉_2017年网络空间安全技术大赛部分writeup

原创

weixin_39610724 于 2020-12-30 06:06:13 发布 30 收藏
文章标签： ctf抓捕赵德汉

作为一个bin小子，这次一个bin都没做出来,我很羞愧。

0x00 拯救鲁班七号

具体操作不多说，直接进入反编译源码阶段

可以看到，只要2处的str等于a就可以了，而str是由1处的checkPass返回，于是进入checkPass函数。

从代码看，这是调用了so库里的函数，并且我们知道so库的名字叫humen

于是找到so库,拖进ida静态分析

找到checkPass函数，直接F5,通过分析，2中的代码最为关键

这段代码把我们输入的密码做了非常复杂的变换，变换后得到的字符串为S!@#@1FD23154A34

于是我找了16张纸，将flag变换出来了。。。。。

0x01 取证密码

反编译

进入encrypt函数

找到XTU.so拖进ida静态分析。

这段代码很简单，脚本如下

1 dest = [0x39,0x20,7,0xA,0x20,0x29,0x13,2,0x3A,0xC,0x11,0x31,0x3B,0xB,7]2 str = 'Welc0meT0XTUCTF'

3 str1 = 'ylnS567!bcNOUV8vwCDefXYZadoPQRGx13ghTpqrsHklm2EFtuJKLzMijAB094W'

4 a =len(str)5 b = ''

6 for i inrange(a):7 b +=str1[dest[i]]8 print b

运行，得到flag.

0x02 人民的名义-抓捕赵德汉1

是个jar文件，直接反编译。

分析逻辑，直接进入checkPassword分析

很明显只要MD5解密就行

0x03人民的名义-抓捕赵德汉2

是个jar文件，直接反编译

好多乱码，很方，但还是继续分析，进入这个不知名的函数

看到两个关键函数，先进入第一个函数分析，一路追踪

复现这段代码

得到字符串JsnatterrtJuaththovacke

然后进入开始的第二个函数

代码逻辑很简单，下面是脚本

1 #-*- coding: utf-8 -*-

2 deff1(a,b):3 return f2(a) %len(b)4 deff2(b):5 if b > 2:6 return f2(b - 1) + f2(b - 2)7 else:8 return 1

9 x = 'JsnatterrtJuaththovacke'

10 b = ''

11 z =012 for i in range(0,4):13 for j in range(0,4):14 b += x[f1(z +j,x)]15 z += 5

16 print b

运行得到flag.注意格式flag{xxxx-xxxx-xxxx-xxxx}

.