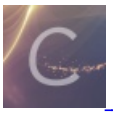
新人的reverse学习(5) xCTF maze

原创

faying 于 2021-04-23 23:47:41 发布 36 收藏 1

分类专栏： CTF Reverse 笔记

本文链接：https://blog.csdn.net/faying/article/details/116075401



题目

逆向新手，刚开始学些写WP，废话较多，还请各位多多包含

1.用exeinfo查看一下，没有壳的ELF，所以直接IDA看看。

2.Shift+F12看看字符串，有这些个字符串，所以肯定有东西，x交叉引用直接会找到目标函数，看看伪代码。

LOAD:000000...	0000000F	C	__gmon_start__
LOAD:000000...	0000000C	C	GLIBC_2.2.5
.rodata:00000...	0000000C	C	Input flag:
.rodata:00000...	0000000C	C	Wrong flag!
.rodata:00000...	00000006	C	nctf{
.rodata:00000...	00000011	C	Congratulations!

3.先看第一段关键代码，意思是s1(也就是flag)开头必须是 “nctf{” ,结尾是 “}”,而且长度是24

```
scanf( "%s", &s1);                              // s1: nctf{
if ( strlen(&s1) != 24 || strncmp(&s1, "nctf{", 5uLL) || *(&byte_6010BF + 24) != 125 )// 最后一位是}
{
ABEL_22:
```

在这里插入图片描述](https://img-blog.csdnimg.cn/2021042323253089.png)

4.然后又是一个while循环，主要是是判断s1元素中的值，有4个，‘O’，’.’ , '0’这四个值的判断。

```
{
  if ( (unsigned __int8)v4 == 'O' )
  {
    v6 = sub_400650(v10);
    goto LABEL_14;
  }
  if ( (unsigned __int8)v4 == 'o' )
  {
    v6 = sub_400660(v10);
    goto LABEL_14;
  }
}
else
{
  if ( (unsigned __int8)v4 == '.' )
  {
    v6 = sub_400670(&v9);
    goto LABEL_14;
  }

  if ( (unsigned __int8)v4 == '0' )
  {
    v6 = sub_400680(&v9);
14:
```


然后看到有两个关键参数v9和v10。
直接进入内存看看两个数

```
028 var_28
024 var_24
```

5.
这一段可以看到v10是var_24 ， v9是var_28，然后猜测，v10算是一个2维数组，
v10第一行就是v10
v10第二行就是v9
因此对于sub_400650到sub_400680这几个函数的分析就可以知道了

```
if ( v4 > 'N' )
{
  if ( (unsigned __int8)v4 == 'O' )
  {
    v6 = sub_400650(v10);                // 左
    goto LABEL_14;
  }
  if ( (unsigned __int8)v4 == 'o' )
  {
    v6 = sub_400660(v10);                // 右
    goto LABEL_14;
  }
}
else
{
  if ( (unsigned __int8)v4 == '.' )
  {
    v6 = sub_400670(&v9);                // 上
    goto LABEL_14;
  }

  if ( (unsigned __int8)v4 == '0' )
  {
    v6 = sub_400680(&v9);                // 下
```


6.然后还看到了一个奇怪的判断，就是这个

```
60                                      //
61LABEL_15:
62      if ( !(unsigned __int8)sub_400690((__int64)asc_601060, v10[0], v9) )// asc:  *******   *  **** * ****  * ***  *#  *** *** ***     *********
```

```
  }
  if ( asc_601060[8 * v9 + v10[0]] != '#' )
    goto LABEL_20;
  v7 = "Congratulations!";
```

通过理性分析，然后还有题目的名字，~~以及对于大佬的借鉴~~，我们可以知道，这是一个迷宫状的图形，当走到了'#'的时候输出正确。

用0表示空格，1表示*

```
00111111
10001001
11101011
11001011
1001#001
11011101
11000001
11111111
```

然后就是走迷宫，就可以得到我们需要的flag了。

```
nctf{o0oo00O000ooo..OO}
```

参考了这位大佬的文章：

https://blog.csdn.net/qq_42967398/article/details/94576708