

新人的reverse学习(3) [GXYCTF2019]luck_guy——WriteUp

原创

fayinq 于 2021-04-02 15:30:44 发布 34 收藏 1

分类专栏: [CTF Reverse 笔记](#)

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/fayinq/article/details/115399791>

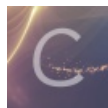
版权



[CTF 同时被 3 个专栏收录](#)

12 篇文章 0 订阅

订阅专栏



[Reverse](#)

7 篇文章 0 订阅

订阅专栏



[笔记](#)

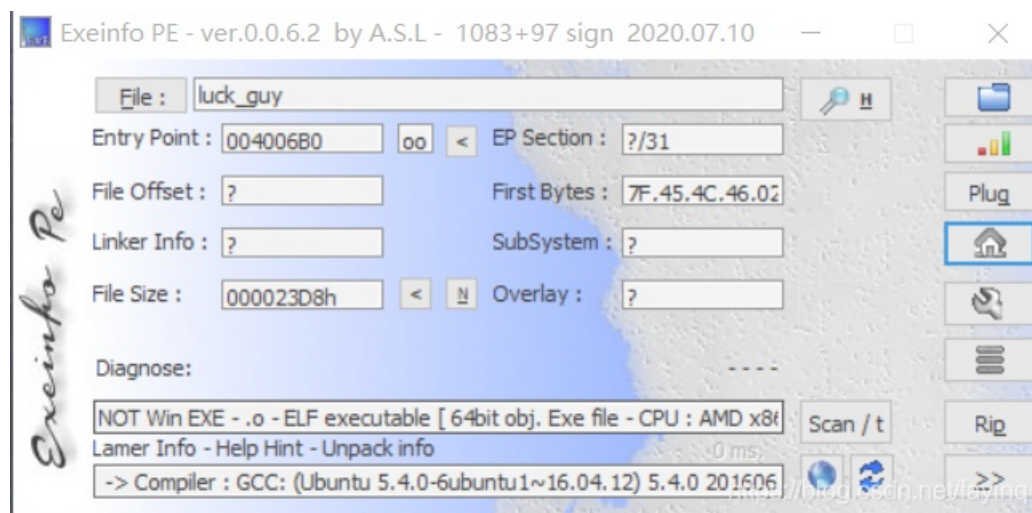
7 篇文章 0 订阅

订阅专栏

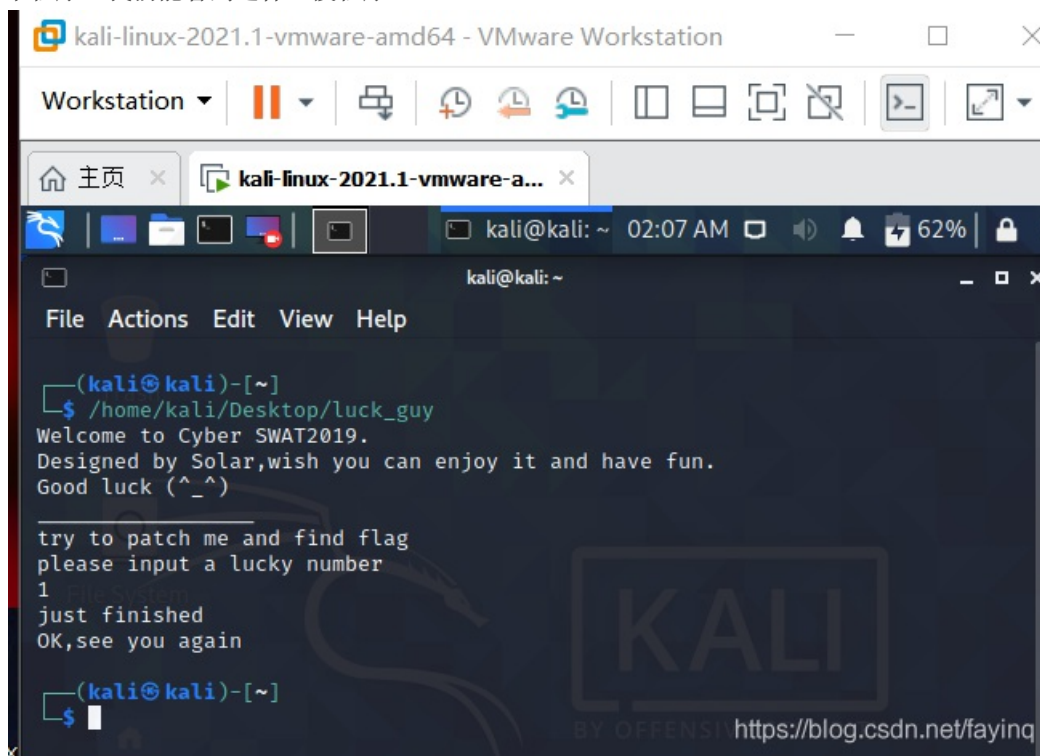
[https://buuoj.cn/challenges#\[GXYCTF2019\]luck_guy](https://buuoj.cn/challenges#[GXYCTF2019]luck_guy)

逆向新手, 刚开始学些写WP, 废话较多, 还请各位多多包含

1.先查壳 拖到exeinfo里 看出来这是一个ELF文件, 所以先拖到Kali里面去看看

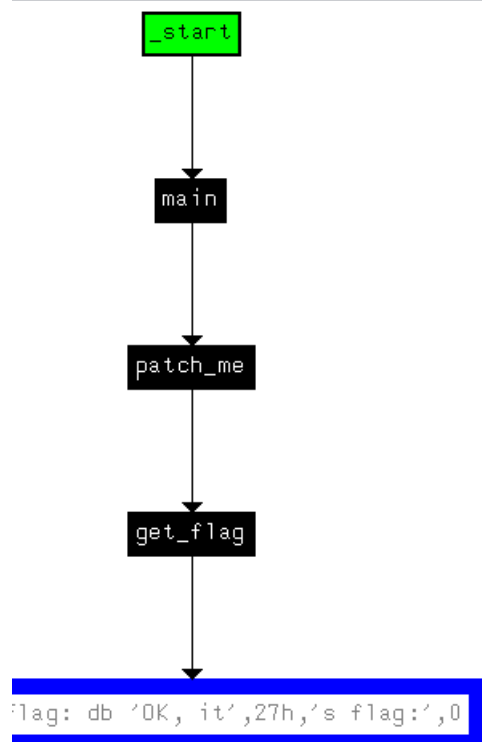


2.打开Kali运行一下程序，我们可以看到这样一段程序



3.所以我们接下来直接用IDA打开，SHIFT+F12打开字符串界面。能看到有一些可以的字符串,直接点进去，然后去找他的交叉引用

```
3400B18 aDesignedBySola db 'Designed by Solar,wish you can enjoy it and have fun
3400B18 ; DATA XREF: welcome+E10
3400B4E ; char aGoodLuck_[]
3400B4E aGoodLuck_ db 'Good luck (^_^)',0 ; DATA XREF: welcome+1810
3400B5E ; char aOkItSFlag[]
3400B5E aOkItSFlag db 'OK, it',27h,'s flag:',0
3400B5E ; DATA XREF: welcome+1810,1810,1810,1810
```



4.由此可知，我们可能需要去分析patch_me函数

5.5查看伪代码，发现有一个get_flag()函数，这可能就是我们flag的所在

```
int __usercall patch_me@eax>(&eax, __int64 a1@<rbp>, int a2@<edi>)  
{  
    int result; // eax@2  
  
    *(_DWORD *)(a1 - 4) = a2;  
    if ( (((unsigned int)((unsigned __int64)*(_DWORD *)(a1 - 4) >> 32) >> 31) + (unsigned  
        - ((unsigned int)((unsigned __int64)*(_DWORD *)(a1 - 4) >> 32) >> 31) == 1 )  
        result = puts("just finished");  
    else  
        result = get_flag();  
    return result;  
}
```

<https://blog.csdn.net/faying>

6.这个函数中，我们首先能看到有V1和V2用到了srand（）和rand（）

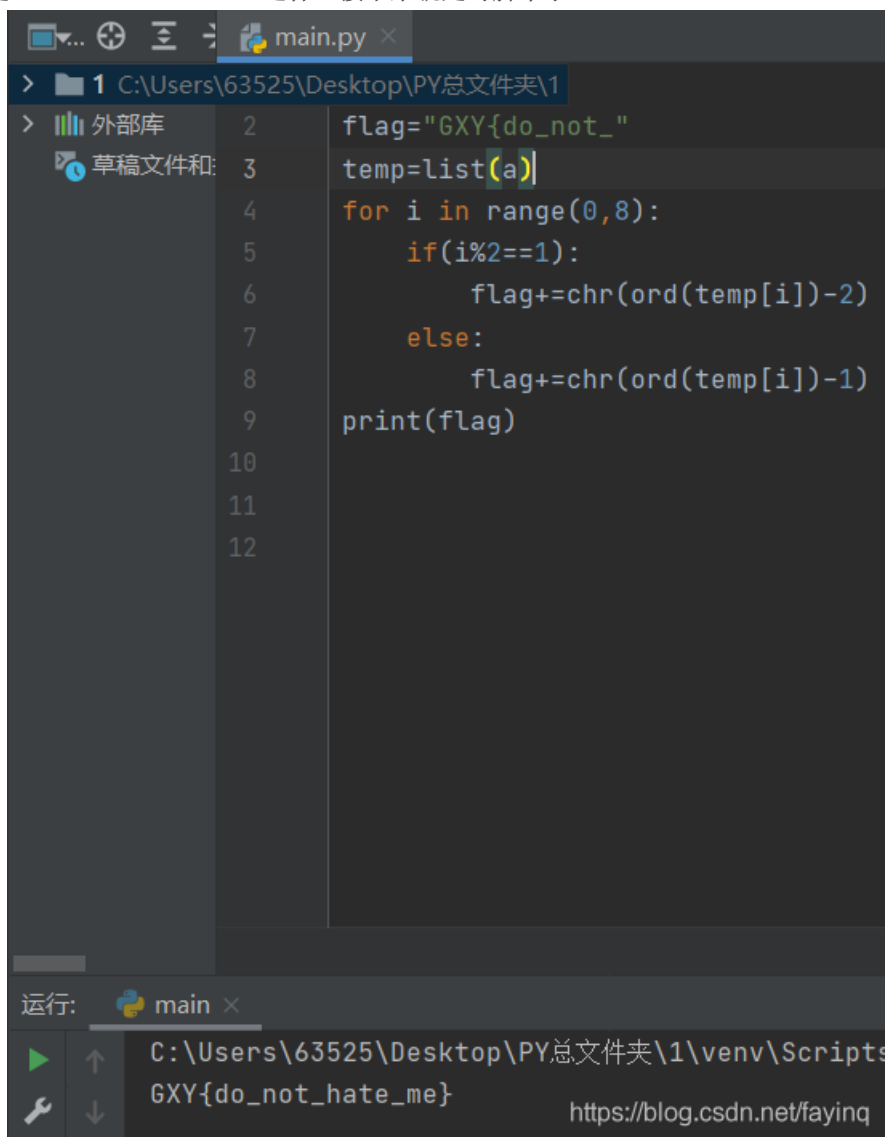
而且在Switch的判断条件中，与v1有关系，所以我猜测，本题是一个伪随机，看看case里面的东西就行。

```
switch ( *(_DWORD *)(a1 - 52) )  
{  
    case 1:  
        puts("OK, it's flag:");  
        memset((void *)(a1 - 48), 0, 0x28uLL);  
        strcat((char *)(a1 - 48), f1);  
        strcat((char *)(a1 - 48), &f2);  
        printf("%s", a1 - 48);  
        break;  
    case 2:  
        printf("Solar not like you");  
        break;  
    case 3:  
        printf("Solar want a girlfriend");  
        break;  
    case 4:  
        *(_QWORD *)(a1 - 48) = '\0';  
        *(_BYTE *)(a1 - 40) = '\0';  
        *(_BYTE *)(a1 - 48) = 'i';  
        *(_BYTE *)(a1 - 47) = 'c';  
        *(_BYTE *)(a1 - 46) = 'u';  
        *(_BYTE *)(a1 - 45) = 'g';  
        *(_BYTE *)(a1 - 44) = '.';  
        *(_BYTE *)(a1 - 43) = 'o';  
        *(_BYTE *)(a1 - 42) = 'f';  
        *(_BYTE *)(a1 - 41) = '■';  
        strcat(&f2, (const char *)(a1 - 48));  
        break;  
    case 5:  
        for ( *(_DWORD *)(a1 - 56) = 0; *(_DWORD *)(a1 - 56) <= 7; ++*(_DWORD *)(a1 - 56) )  
        {  
            if ( (((unsigned int)((unsigned __int64)*(_DWORD *)(a1 - 56) >> 32) >> 31)  
                + (unsigned __int8)*(_DWORD *)(a1 - 56) & 1  
                - ((unsigned int)((unsigned __int64)*(_DWORD *)(a1 - 56) >> 32) >> 31) == 1 )// 判断a1-56是否为奇数  
                *(&f2 + *(_DWORD *)(a1 - 56)) -= 2;  
            else  
                --*(&f2 + *(_DWORD *)(a1 - 56));  
        }  
        break;  
    default:  
        puts("emm,you can't find flag 23333");  
}
```

<https://blog.csdn.net/faying>

7.

然后猜一猜，觉着应该是case4->case5->case1这样，接下来就是写脚本了



```
main.py x
> 1 C:\Users\63525\Desktop\PY总文件夹\1
> 外部库 2 flag="GXY{do_not_"
草稿文件和: 3 temp=list(a)
4 for i in range(0,8):
5     if(i%2==1):
6         flag+=chr(ord(temp[i])-2)
7     else:
8         flag+=chr(ord(temp[i])-1)
9 print(flag)
10
11
12

运行: main x
C:\Users\63525\Desktop\PY总文件夹\1\venv\Scripts
GXY{do_not_hate_me} https://blog.csdn.net/fayingq
```

8. 最后ok了