buuctf luck_guy

原创

菜逼的ctf之路 于 2020-10-10 16:53:22 发布 569 收藏 2

buuctf 逆向luck_guy

文件无壳，ida打开
找到主函数

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v4; // [rsp+14h] [rbp-Ch]
  unsigned __int64 v5; // [rsp+18h] [rbp-8h]

  v5 = __readfsqword(0x28u);
  welcome();
  puts("__________________");
  puts("try to patch me and find flag");
  v4 = 0;
  puts("please input a lucky number");
  __isoc99_scanf("%d", &v4);
  patch_me(v4);
  puts("OK,see you again");
  return 0;
}
```

函数内容很简单，进入patch_me()函数看看
也很简单，进入get_flag()函数瞅瞅，发现不寻常的地方

```
unsigned __int64 get_flag()
{
  unsigned int v0; // eax
  char v1; // al
  signed int i; // [rsp+4h] [rbp-3Ch]
  signed int j; // [rsp+8h] [rbp-38h]
  __int64 s; // [rsp+10h] [rbp-30h]
  char v6; // [rsp+18h] [rbp-28h]
  unsigned __int64 v7; // [rsp+38h] [rbp-8h]

  v7 = __readfsqword(0x28u);
  v0 = time(0LL);
  srand(v0);
  for ( i = 0; i <= 4; ++i )
  {
    switch ( rand() % 200 )
    {
      case 1:
        puts("OK, it's flag:");
        memset(&s, 0, 0x28uLL);
        strcat((char *)&s, f1);
        strcat((char *)&s, &f2);
        printf("%s", &s);
        break;
      case 2:
        printf("Solar not like you");
        break;
      case 3:
        printf("Solar want a girlfriend");
        break;
      case 4:
        v6 = 0;
        s = 91801473502846247 45LL;
        strcat(&f2, (const char *)&s);
        break;
      case 5:
        for ( j = 0; j <= 7; ++j )
        {
          if ( j % 2 == 1 )
            v1 = *(&f2 + j) - 2;
          else
            v1 = *(&f2 + j) - 1;
          *(&f2 + j) = v1;
        }
        break;
      default:
        puts("emmm,you can't find flag 23333");
        break;
    }
  }
  return __readfsqword(0x28u) ^ v7;
}
```

利用time()函数生成随机数, 然后和200求余，却发现只有5种结果是有用的，这概率。。。。

找代码逻辑，case1中是剪切，f1的内容是”GXY{do_not_“这。。。

f2是空，但是看后面case4，case5发现给f2赋值，大胆猜逻辑，先case4赋值，然后case5，进行加密操作，最后case1，进行剪切(别问为什么，问就是猜的),最后写脚本

```
f2=[0x69,0x63,0x75,0x67,0x60,0x6f,0x66,0x7f]
for i in range(8):
    if ( i % 2 == 1 ):
        v1 = f2[i] - 2
    else:
       v1 = f2 [i] - 1
    f2[i] = v1
str=''
for i in f2:
    str+=chr(i)
print('GXY{do_not_'+str)
```