XCTF BABYRE

原创

酸酸菜鱼 于 2020-08-04 18:46:53 发布 237 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/lhk124/article/details/107790921

1. 用exeinfo查出是个elf文件，把后缀去了丢linux系统里
2. 看汇编代码和F5（在judge函数里）
3. 方法1：直接写脚本
4. 方法2：运行至运算结束部分，直接查看寄存器。

```
v2 = 0x66;
v3 = 0x6D;
v4 = 0x63;
v5 = 0x64;
v6 = 0x7F;
v7 = 0x6B;
v8 = 0x37;
v9 = 0x64;
v10 = 0x3B;
v11 = 0x56;
v12 = 0x60;
v13 = 0x3B;
v14 = 0x6E;
v15 = 0x70;
for ( i = 0; i <= 13; ++i )
  *(_BYTE *)(i + a1) ^= i;                      // a1是输入，输入进行异或操作后
for ( i = 0; i <= 13 && *(_BYTE *)(i + a1) == *(&v2 + i); ++i )// 异或后的与v2-v15逐位比较
  ;
```



```
"""
正向思路:
    1.判断长度
    2.逐位与i进行异或运算
逆向思路:
    1.逐位异或回去
"""


str_list =[0x66, 0x6D, 0x63, 0x64, 0x7F, 0x6B, 0x37, 0x64, 0x3B, 0x56, 0x60, 0x3B, 0x6E, 0x70]
flag = list('01234567891234')
for i in range(len(str_list)):
    flag[i] = chr(str_list[i] ^ i)
print(''.join(flag))
```