题目:

Daddy, teach me how to use random value in programming!

ssh random@pwnable.kr -p2222 (pw:guest)

连接进去看一下:

```
#include <stdio.h>

int main(){
        unsigned int random;
        random = rand();        // random value!

        unsigned int key=0;
        scanf("%d", &key);

        if( (key ^ random) == 0xdeadbeef ){
                printf("Good!\n");
                system("/bin/cat flag");
                return 0;
        }

        printf("Wrong, maybe you should try 2^32 cases.\n");
        return 0;
}
```

通过随机数验证即可，而该程序缺少随机数种，则随机数为固定

```
#include<stdio.h>

int main(){
        int random=0;
        random=rand();
        printf("%d",random);
        return 0;
}
```

测试一下

```
fish@ubuntu:/mnt/hgfs/share$ ./random
1804289383fish@ubuntu:/mnt/hgfs/share$
```

则写出脚本:

```python
from pwn import  *

target=ssh(user='random',host='pwnable.kr',port=2222,password='guest')

r=target.process('./random')

payload='3039230856'

r.sendline(payload)

print(r.recv())
```

得到 flag:

```
fish@ubuntu:/mnt/hgfs/share$ python fish.py
[+] Connecting to pwnable.kr on port 2222: Done
[*] random@pwnable.kr:
    Distro    Ubuntu 16.04
    OS:       linux
    Arch:     amd64
    Version:  4.4.179
    ASLR:     Enabled
[+] Starting remote process './random' on pwnable.kr: pid 22965
Good!
Mommy, I thought libc random is unpredictable...
```