ez_brainfuzz

没活嗯整，乱出的（（

首先就是brainfuck，最简单的理解方法输出ASCII。

然后是fuzz。没啥说的贴个exp吧（

```
from pwn import *

# context.log_level = "debug"
#   20001
p = connect("47.76.71.50", "20001")

alphabet = "abcdefghijklmnopqrstuvwxyz1234567890"
dis = lambda x, y: ord(x) - ord(y)


def getfuckstr(str):
    if len(str) == 0:
        return ""
    base = "+++++++++[->+++++++++<]>+++++++++++++++++"
    cad = [dis(str[0], "a")]
    for i in range(1, len(str)):
        cad.append(dis(str[i], str[i - 1]))
    finalstr = ""
    for t in cad:
        if t > 0:
            finalstr += t * "+" + "."
        else:
            finalstr += (-t) * "-" + "."
    return base + finalstr


base_str = ""
cur_sim = 0
sendcmd = lambda cmd: p.sendlineafter(">>> ", cmd.encode()).decode().split("\n")
[-1]
while True:
    for i in alphabet:
        sendcmd(getfuckstr(base_str + i))
        res = p.recvline().decode()
        if res.find("SBCTF") != -1:
            print(res, base_str)
            exit(0)
        now_sim = int(res.replace("Now similarity: ", "").replace("%", ""))
        if now_sim > cur_sim:
            print(res)
            cur_sim = now_sim
            base_str += i
```

qrazy_pic_encode

两次dct与一次dct之间可以通过自己做几组测试数据发现差别，可以应用很多种算法将其区分开来

not_pic_encode

zlib流被再次zlib加密了，解密下放回去即可