

多看汇编

太坑了

利用gets函数，往bss段写入/bin/sh

写rop链获取shell