



















gcc escalate.c -o escalate -m32 -fno-stack-protector -z execstack

gdb ./escalate

disas main

disas vulnerable

info reg

x/32 $esp

x/32z $esp

run $(python -c 'print("A"\*408+"BCDE")')

run $(python -c 'print("A"\*400)')

run $(python -c 'print("A"\*408)')