-We have a ELF x86 file

-Decompile it with a disassembly (gdb or IDA)



-It uses malloc and memset to allocate a memory area 0x18 bit long.

Then use move to write into this area our flag

→ static analysis, we get the flag is : FLAG-4092849uio2jfklsj4kl

—> dynamic analysis, set a breakpoint before the last call \_puts

note that the address of flag is at [esp+2ch] = 0x804b1a0

RUN, it breaks, display this then get the FLAG

