<https://hackmd.io/gZRERGwVS5qeqo1Bv_bfAg?both>

Get OOB write

Overwrite function pointer or return address

ROP to call memprotect

Write shellcode

Jump to shellcode