Week3

黑给

没有pie，没有栈溢出保护，但是栈溢出的长度只能覆盖到返回地址，然后另一个read能写到一个固定的地址，于是先send一个paSswOrd然后覆盖返回地址为main函数开头，并在这里构造rop链，然后两次send并覆盖返回地址，同时覆盖栈基地址，第一次之后rbp=0x6010a0，第二次之后rbp=0x6010a，rsp=0x6010b0。第二次的返回地址为找到的gadget，我用的是_libc_csu_init()里的，调用了write，输出了gets、read、setbuf、write、strcmp的真实地址，因为动态加载不会变动地址后三位，所以对照这个用libc-database去找，确定了版本，然后用onegadgets轻松获得权限。