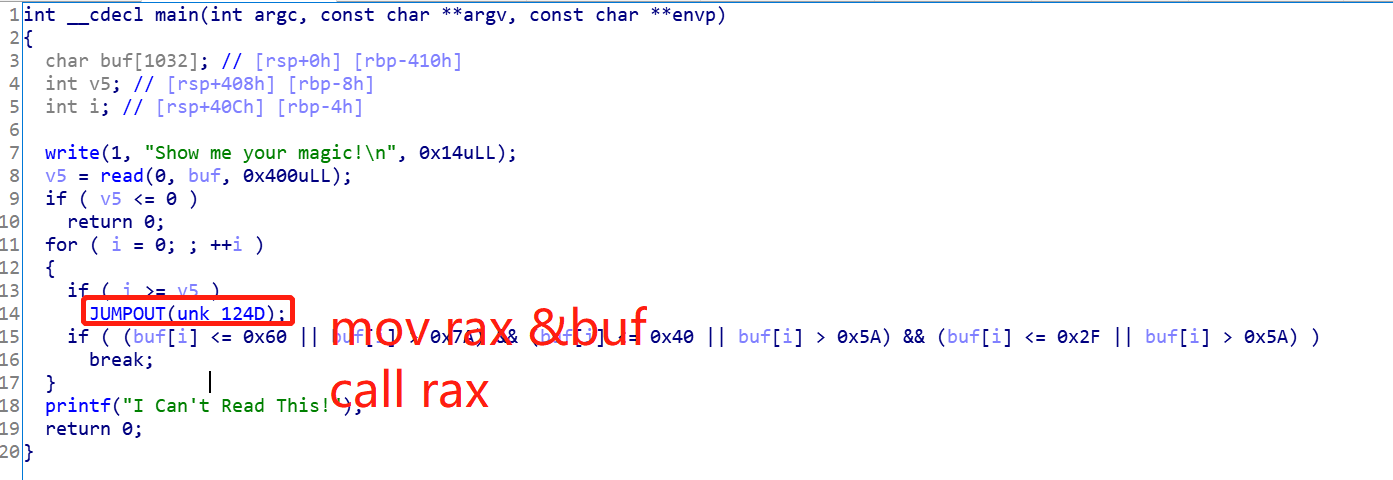
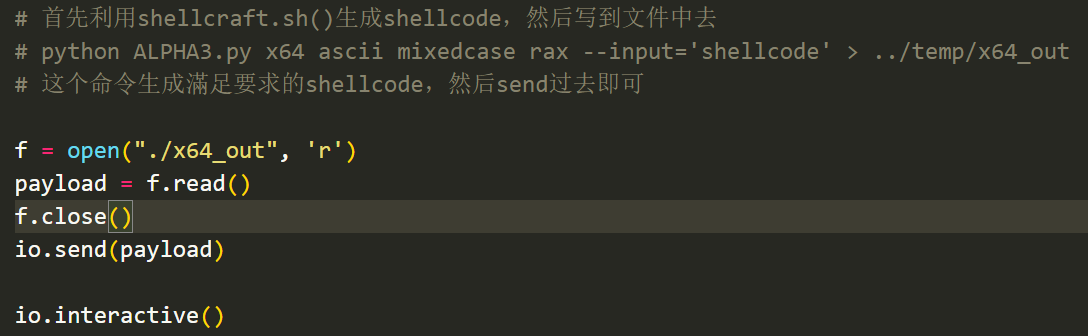


开了PIE，开了FULL RELRO

一开是疯狂报错，然后把call rax改掉就可以反汇编了。



下面直接限制了shelllcode不能包含小于0x30和大于0x7a的字符，这就很尴尬，不会做，一波百度，



涨姿势了！