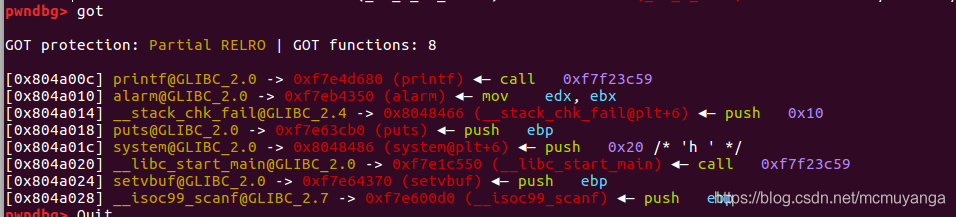
跟cat又有点不一样，cat的参数存储在栈上，可以通过计算buf与ret的偏移来修改ret为后门，这次的buf在bss段，没法获取栈地址。

bss段距离got表不远，这边的想法是将printf@got修改成后门函数，这样在调用printf的时候就能获取shell了。  
但是在计算偏移的时候发现print@got的偏移不是8的整数倍



print@got偏移=（0x804a00c-0x0804A060）/8=–10.5  
看Namewitch函数发现scanf函数也会执行，就转变该scanf@got了  
scanf@got偏移=（0x804a028-0x0804A060）/8=–7