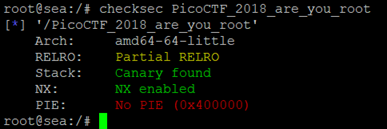
原文链接：<https://blog.csdn.net/seaaseesa/article/details/105588350>

PicoCTF\_2018\_are\_you\_root

首先，检查一下程序的保护机制



然后，我们用IDA分析一下，只要符合条件就可以显示flag，但是按照正常的逻辑是不能的。



Login时，会malloc一个堆，大小为0x10，并且偏移8处就是auth的验证码。但是login时，并没有初始化\*(v7+8)处的值，使得它的值是前面的操作影响。而strdup函数，内部会malloc一个与字符串长度一样的堆，并把字符串拷贝进去。



Reset的时候，释放的是strdup生成的堆。因此，如果strdup生成的堆为0x20，下一次login时第一个malloc就会取出这个堆，而便宜8处的值就是之前用户输入的name的偏移8处的值，因此auth验证码可以任意控制。



