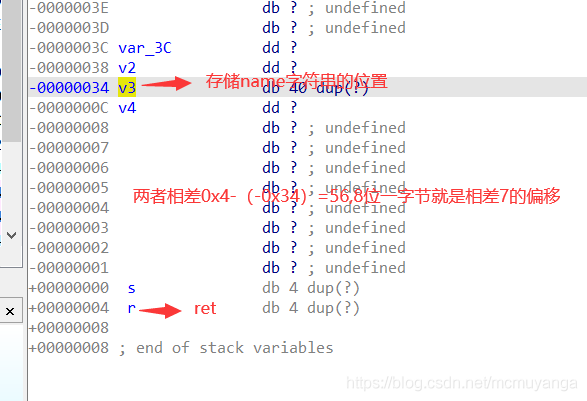
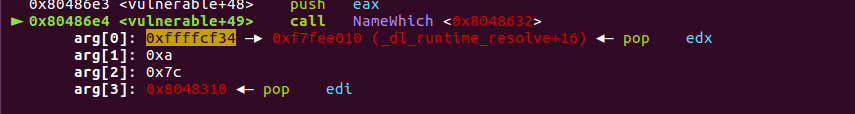
<https://blog.csdn.net/mcmuyanga/article/details/114673240>

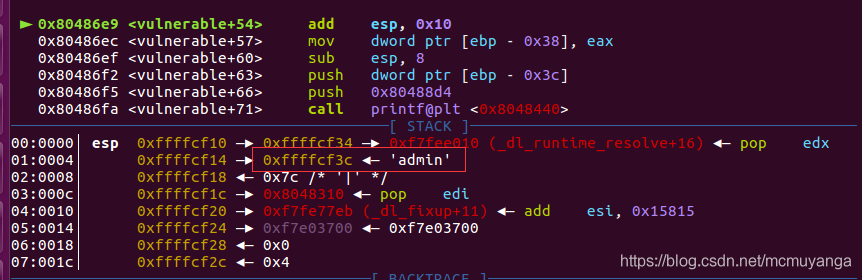
法一：ida看栈布局找偏移  


法二：动态调试

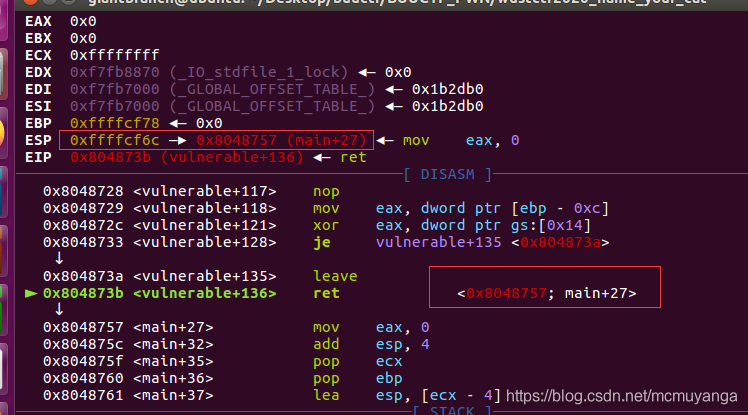
程序进入NameWhich的情况，传入的参数地址是0xffffcf34



传入一个参数后,地址变成了0xffffcf3c



来到返回地址



他们相差cf6c-cf34=56,一个参数占8位，中间相差7个参数

因此我们可以for循环执行到第5次的时候，在输入name for which的时候输入7，让它定位到ret的地址上，覆写成backdoor即可