# Vulnserver

vulnserver程序的功能：

1. 创建socket，等待客户端连接，端口为9999
2. 客户端连接后，会给客户端发送欢迎信息：Welcome to Vulnerable Server! Enter HELP for help
3. 连接后，客户端可以向vulnserver程序发送一系列命令进行交换，命令如下：

HELP

STATS [stat\_value]

RTIME [rtime\_value]

LTIME [ltime\_value]

SRUN [srun\_value]

TRUN [trun\_value]

GMON [gmon\_value]

GDOG [gdog\_value]

KSTET [kstet\_value]

GTER [gter\_value]

HTER [hter\_value]

LTER [lter\_value]

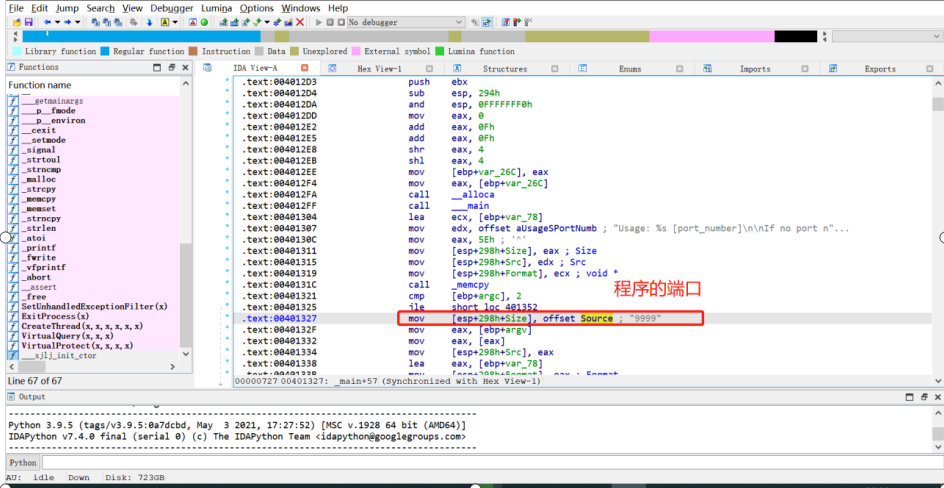
KSTAN [lstan\_value]

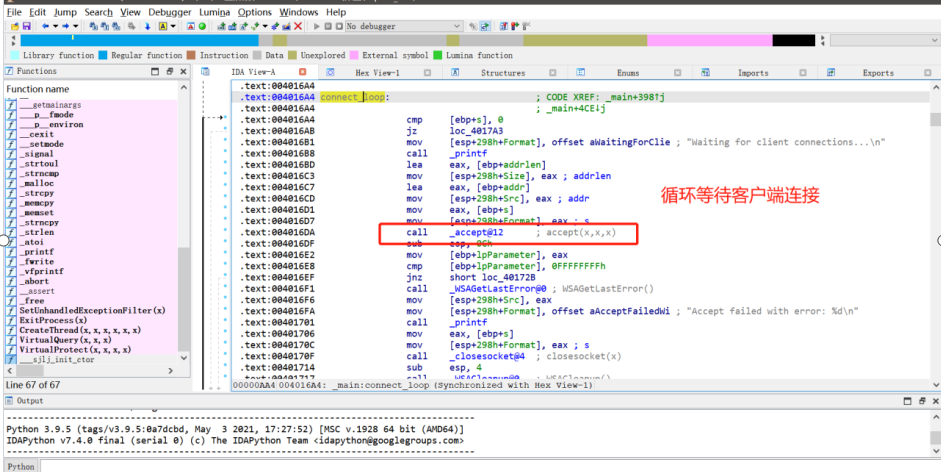
EXIT

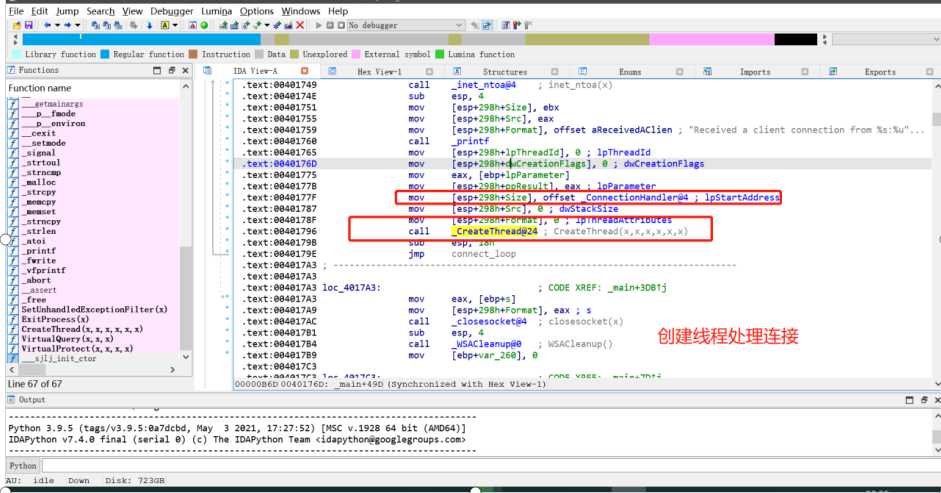
1. vulnserver程序收到命令后，会做对应的处理，并回复客户端

IDA分析：

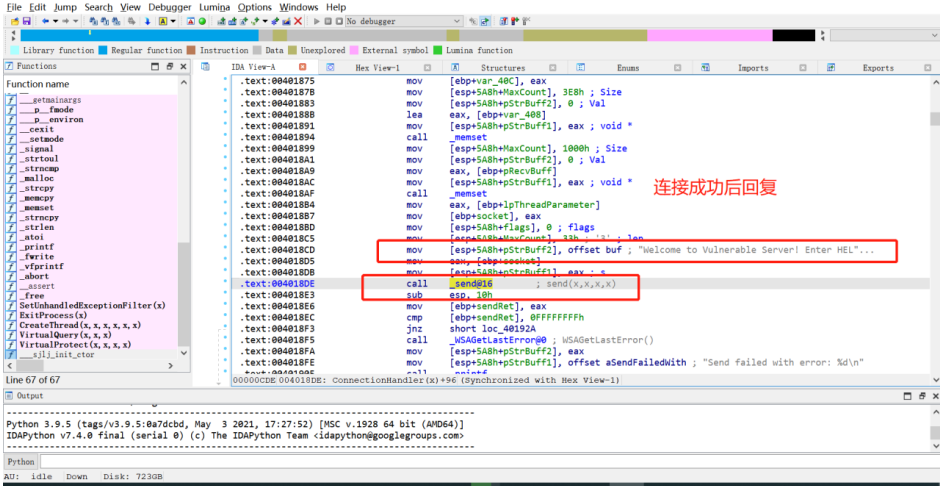
一、主线程

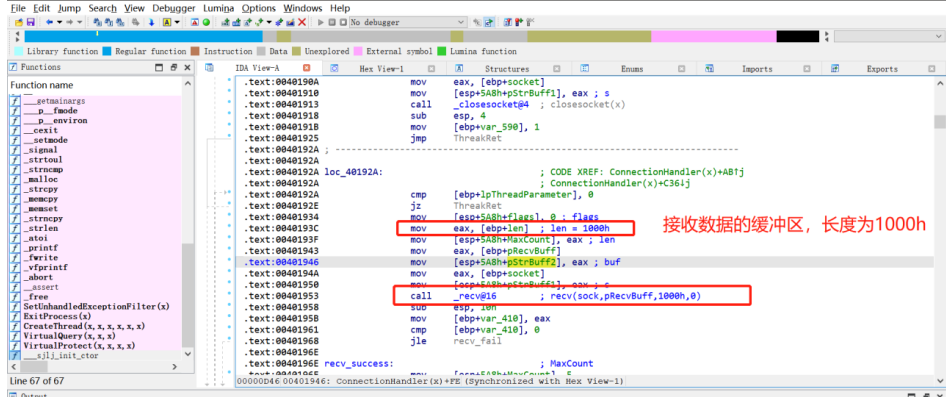


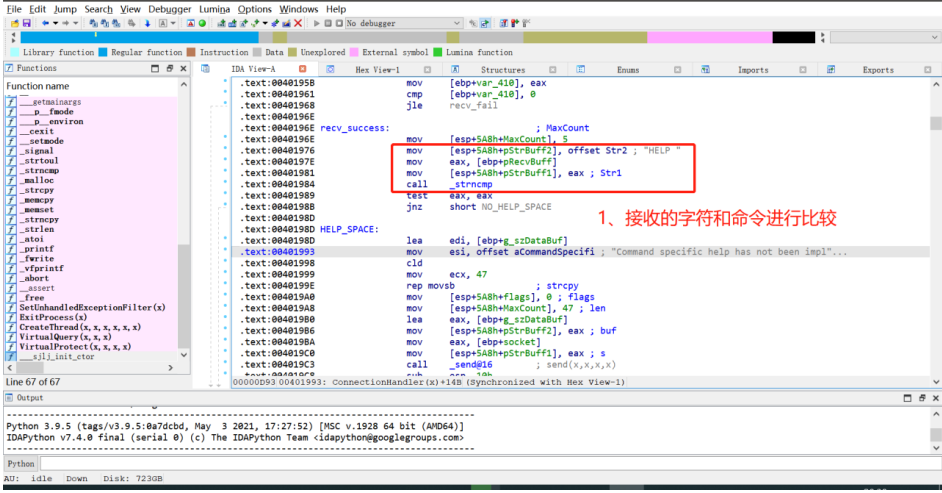


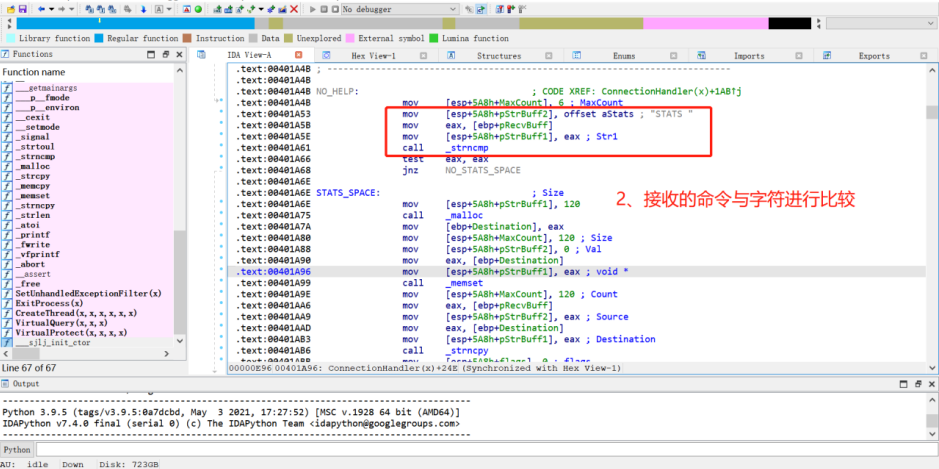


1. 与客户端通信的线程



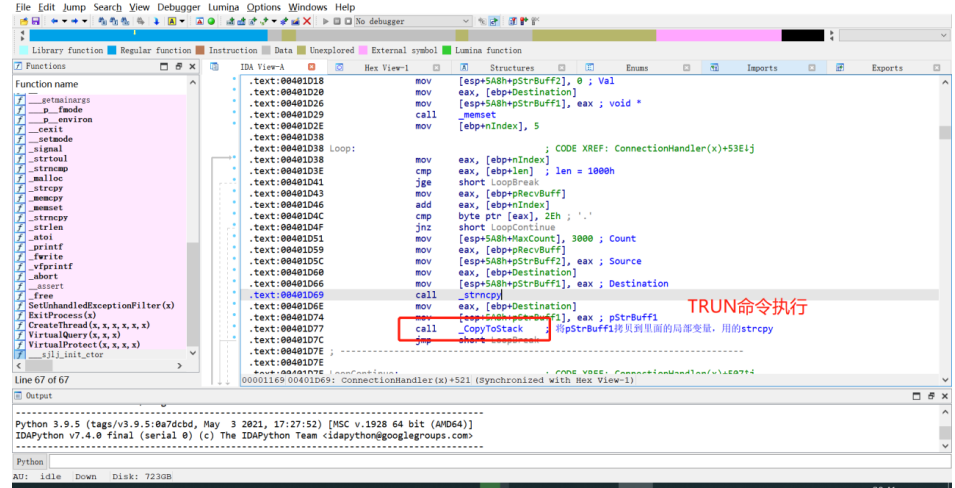




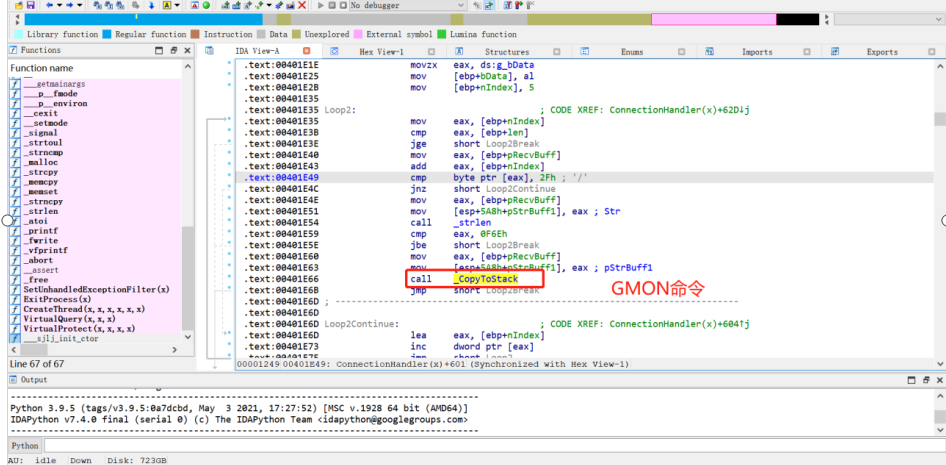


vulnserver程序的栈溢出漏洞：

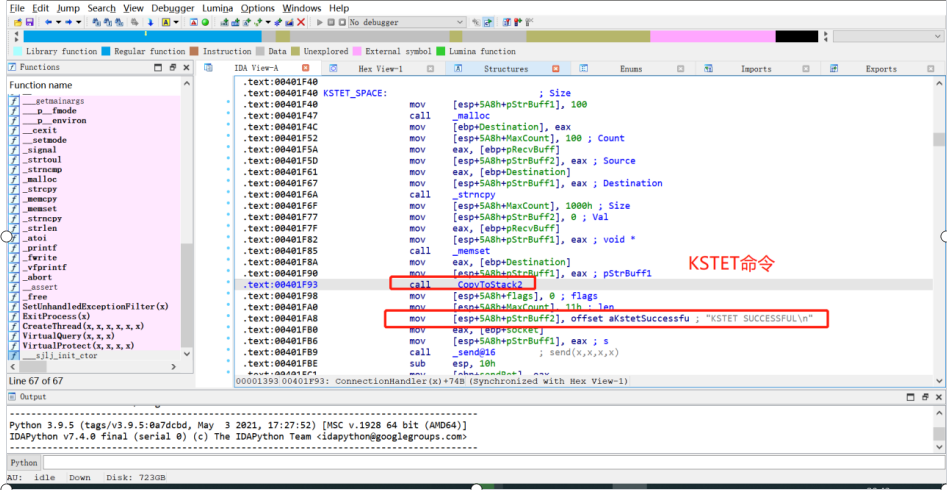
1. 与TRUN命令对比成功后，会调用一个复制函数，里面调用的是strcpy函数，dest的大小为2008，而src的大小为4096（1000h）,导致栈溢出



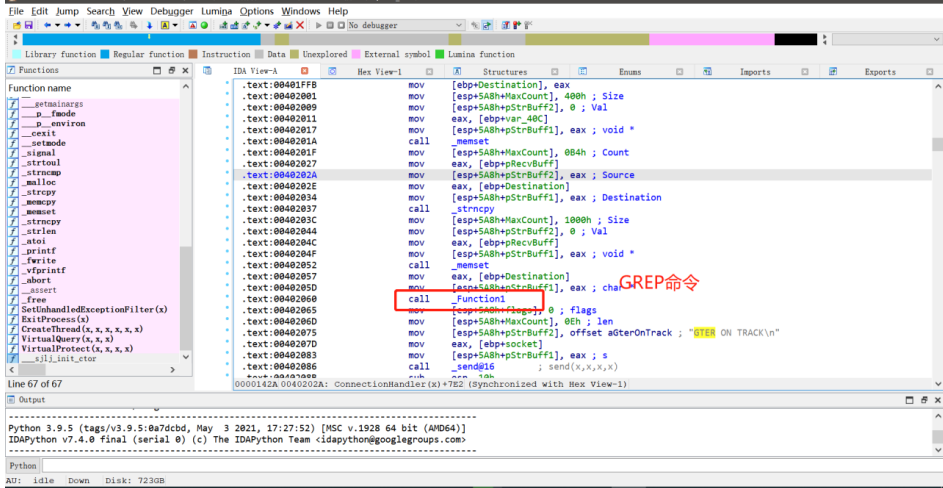
1. 与GMON命令对比成功后，会调用一个复制函数，里面调用的是strcpy函数，dest的大小为2008，而src的大小为4096（1000h）,导致栈溢出



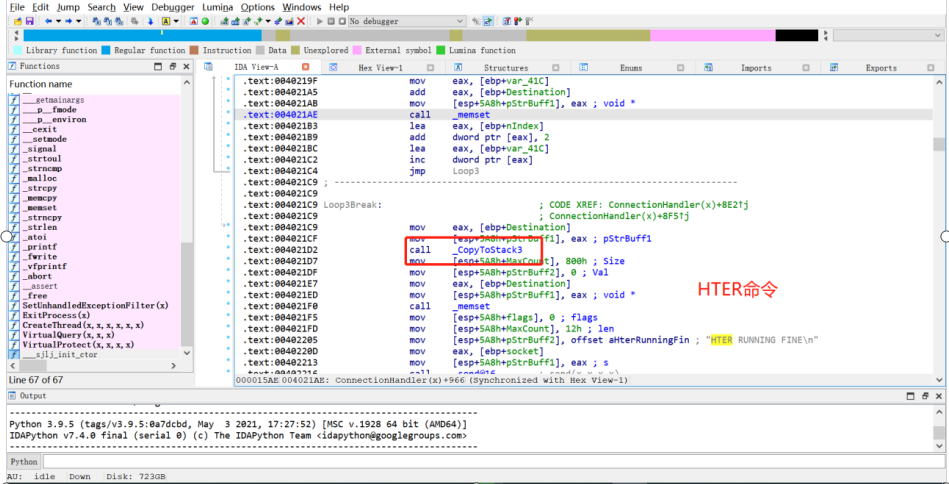
3、与KSTET命令对比成功后，会调用一个复制函数，里面调用的是strcpy函数，dest的大小为72，而src的大小为4096（1000h）,导致栈溢出



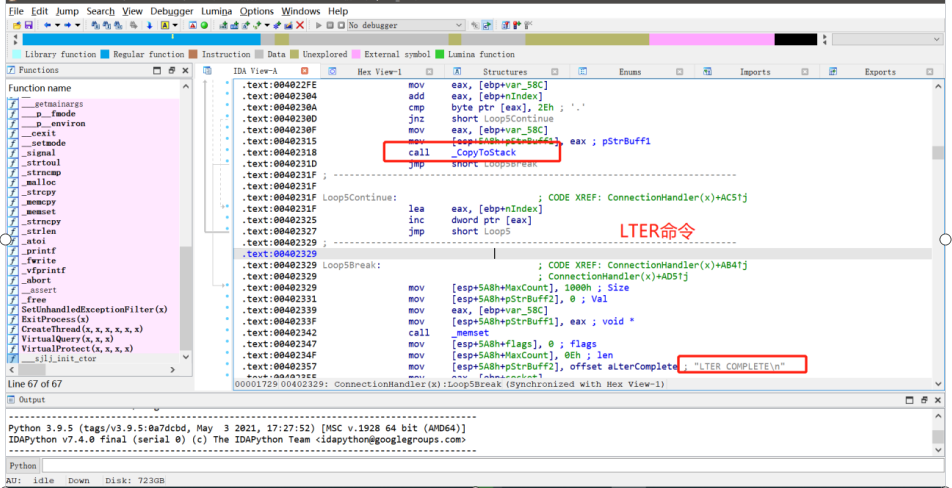
4、与GTER命令对比成功后，会调用一个复制函数，里面调用的是strcpy函数，dest的大小为152，而src的大小为4096（1000h）,导致栈溢出

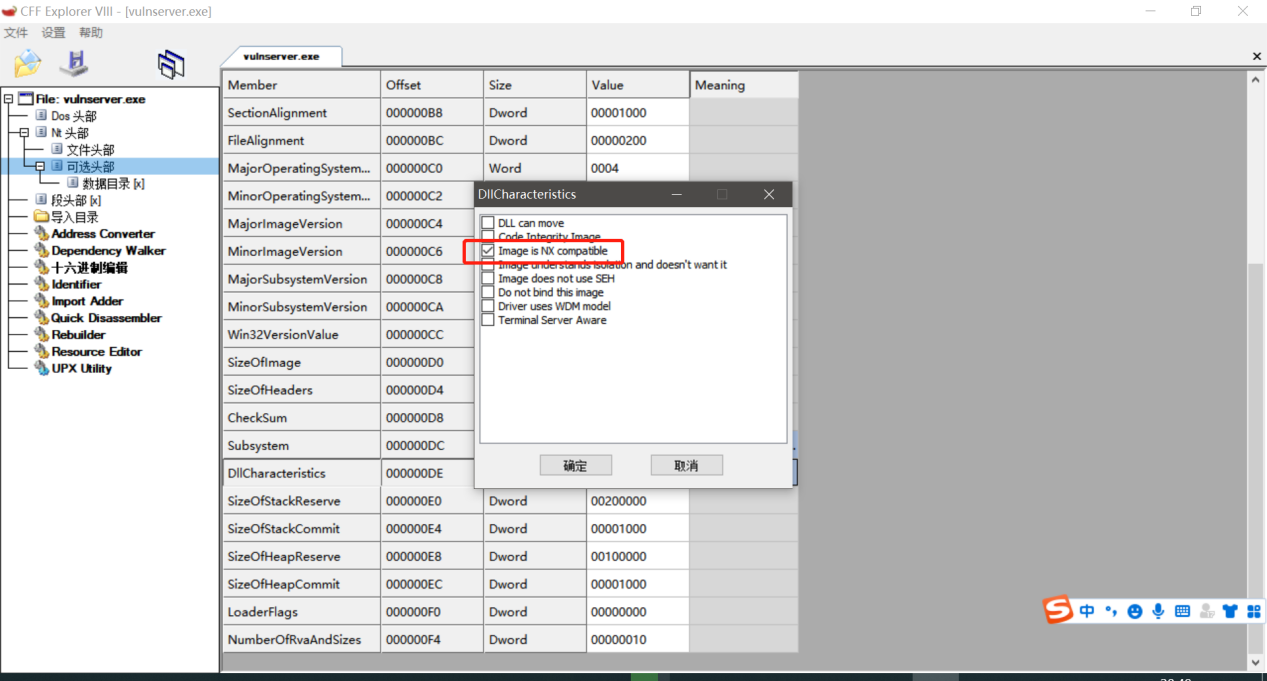


1. 与HTER命令对比成功后，会调用一个复制函数，里面调用的是strcpy函数，dest的大小为1016，而src的大小为4096（1000h）,导致栈溢出



1. 与LTER命令对比成功后，会调用一个复制函数，里面调用的是strcpy函数，dest的大小为2008，而src的大小为4096（1000h）,导致栈溢出





1. 发送带ROP的shellcode，执行成功

