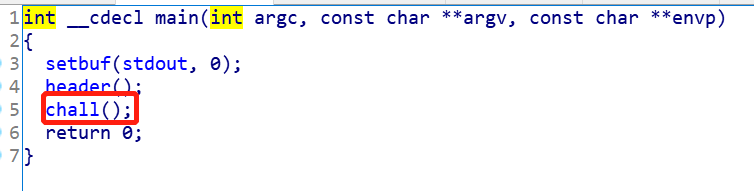
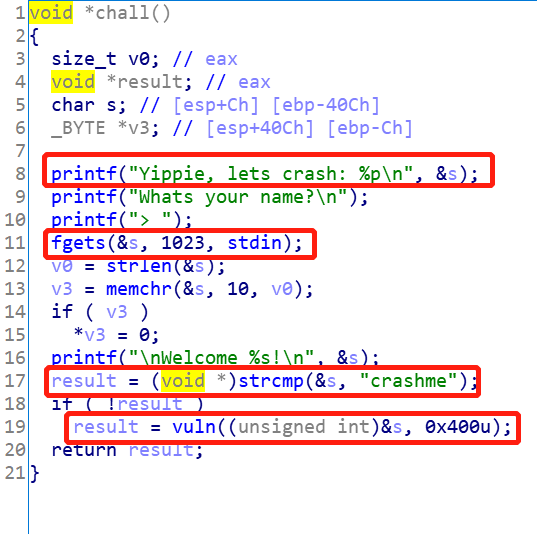


可以看到，NX是关闭的。

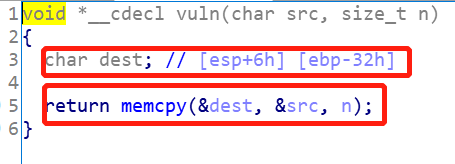
看main函数：





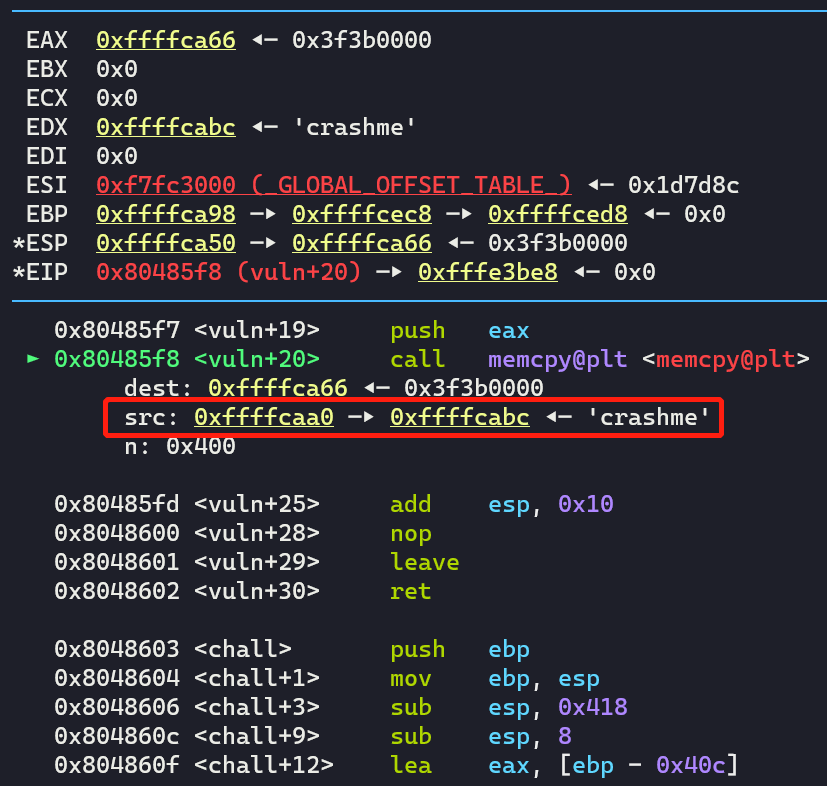
第8行泄露了栈地址，第十一行从标准输入中读取，注意fgets函数，遇到\x00是不会停止的，遇到\n才会。

然后如果与“crashme”比较长度是一样的，那儿走进vuln函数。可以看到，vuln由越界拷贝的情况：



需要注意的是：这里dest的大小和实际拷贝到的大小不一致！！！！！

要在gdb里面调试一下才知道偏移量！！！



这里的src并不是crashme的首地址！！！

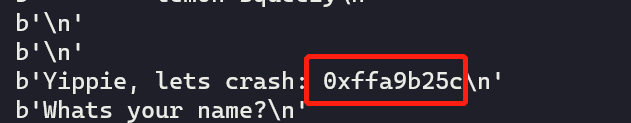
多了0X1C的地址，dest+ebp一共是0X36

剩余要填0x36 – 8(crashme\x00) – 0x1c = 0x12

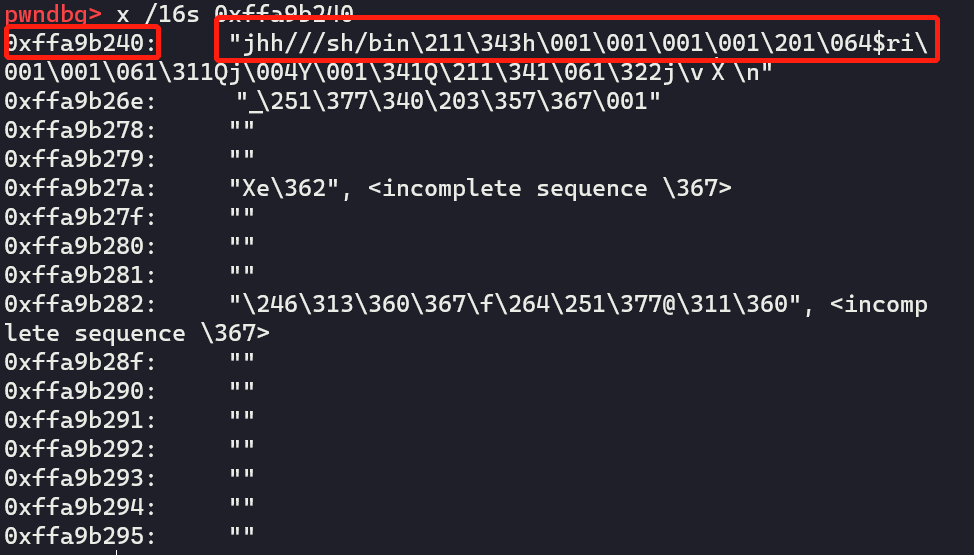
然后填上shellcode的地址

最后的地址呢,也一定要手动去调试一下！！！

泄露的地址是：



找到的shellcode的地址是：



比泄露的地址要低0x1c个字节

所以最终的payload：

Crashme\x00 + 18\*’a’ + (leak\_addr – 0x1c)+ shellcode