Bugku pwn3

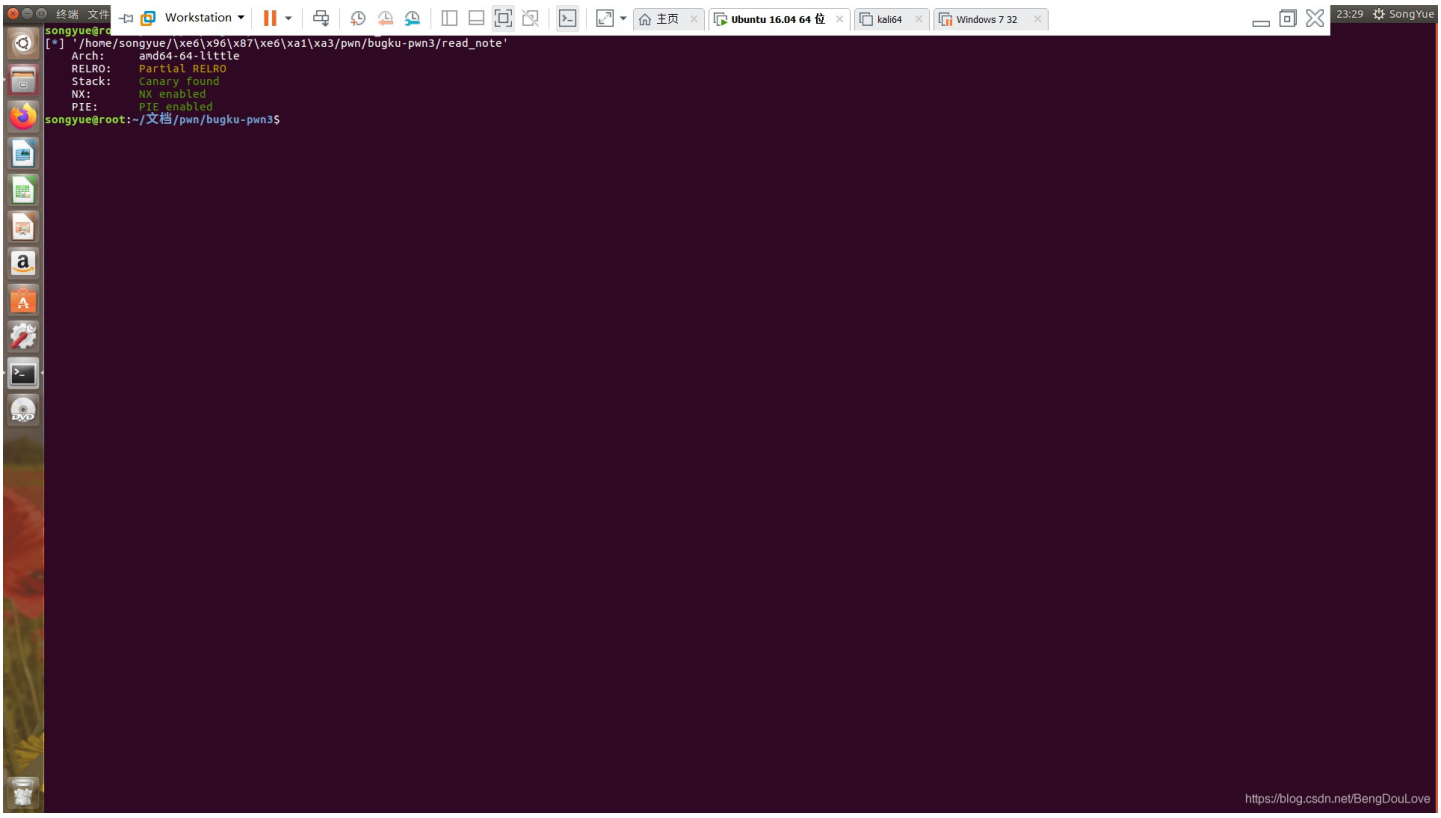
原创

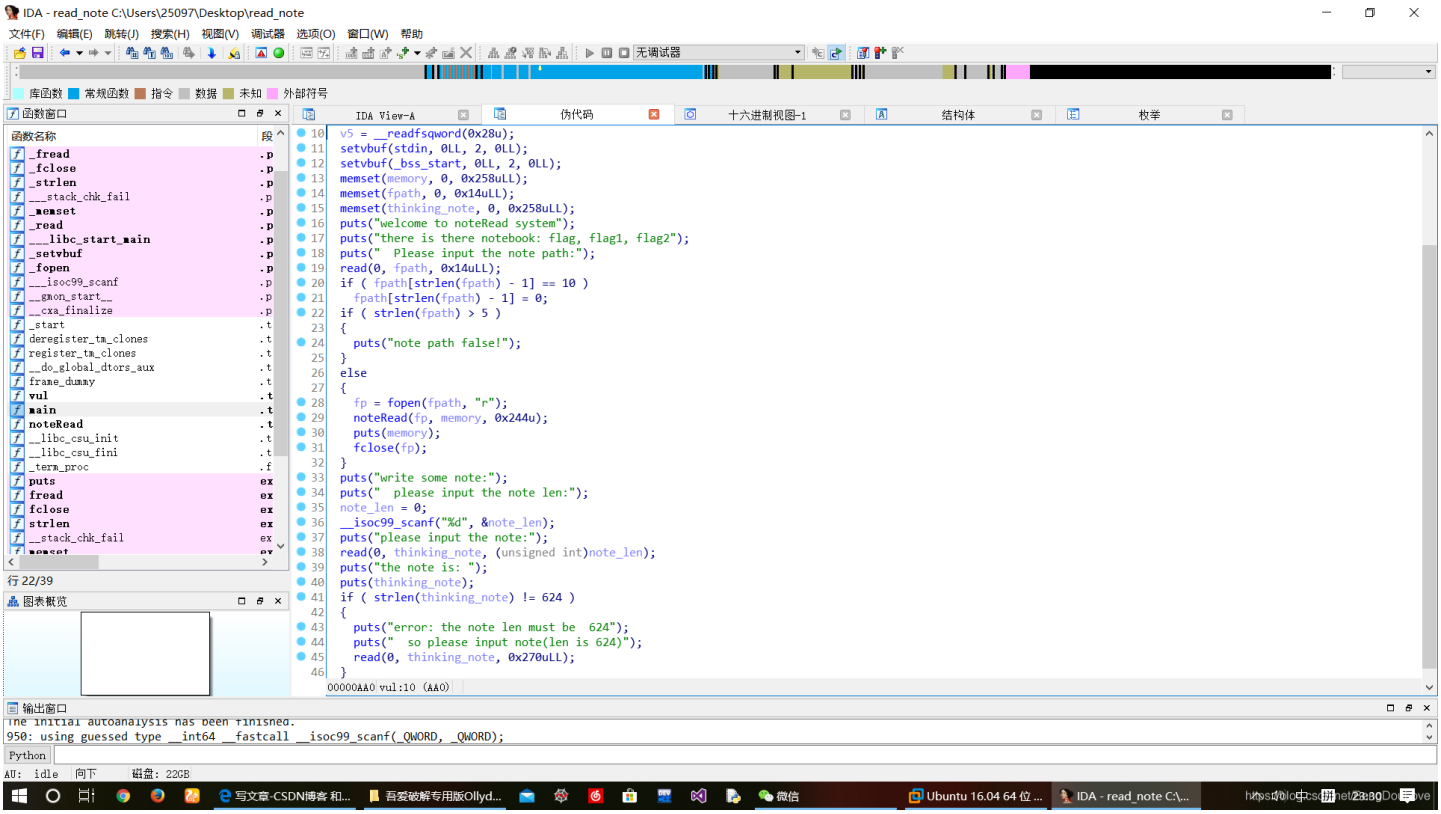
Bengd0u 于 2020-03-09 23:57:49 发布 214 收藏

本文链接：https://blog.csdn.net/BengDouLove/article/details/104764569

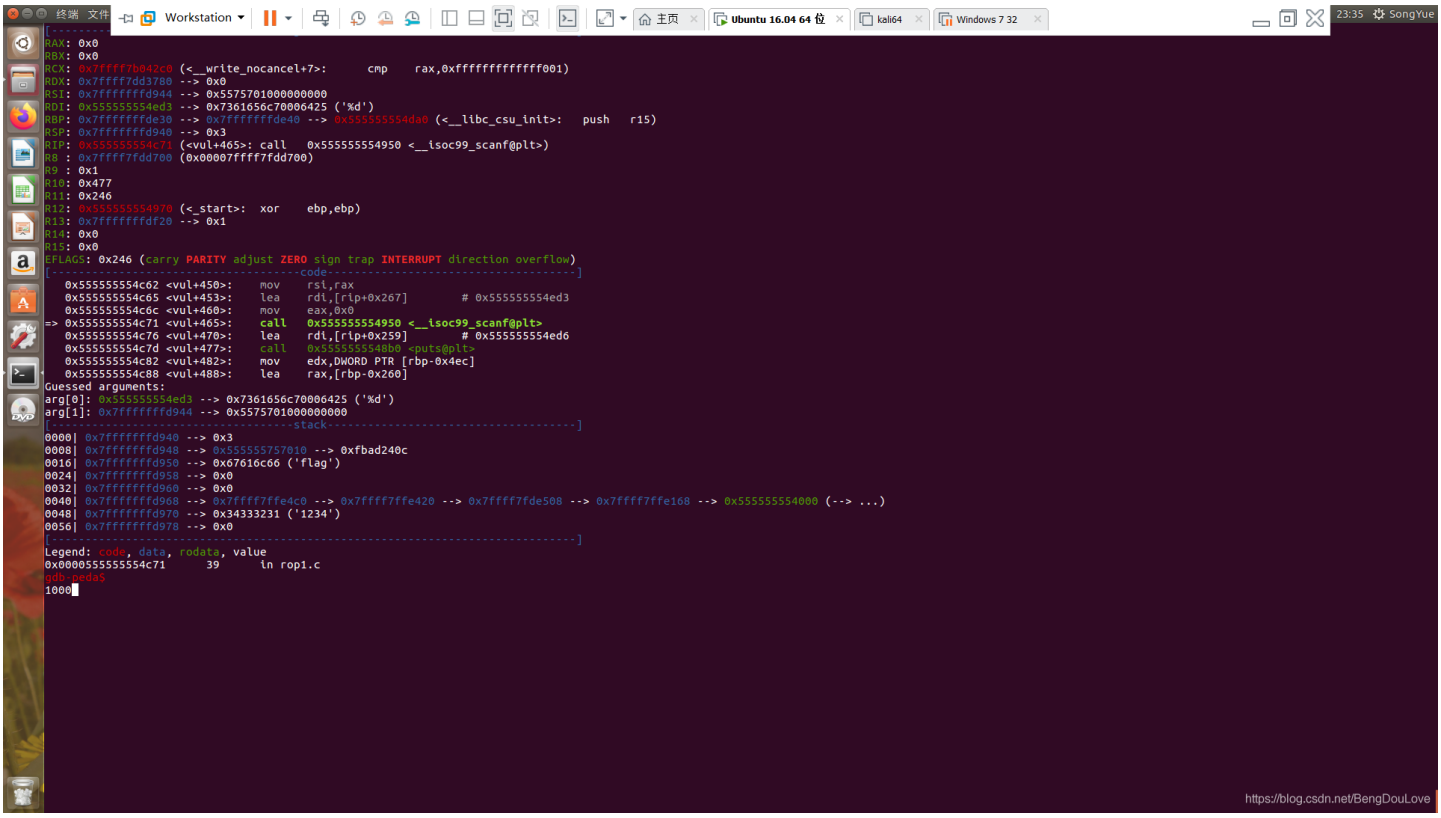
版权

这道题保护机制全都是开启的

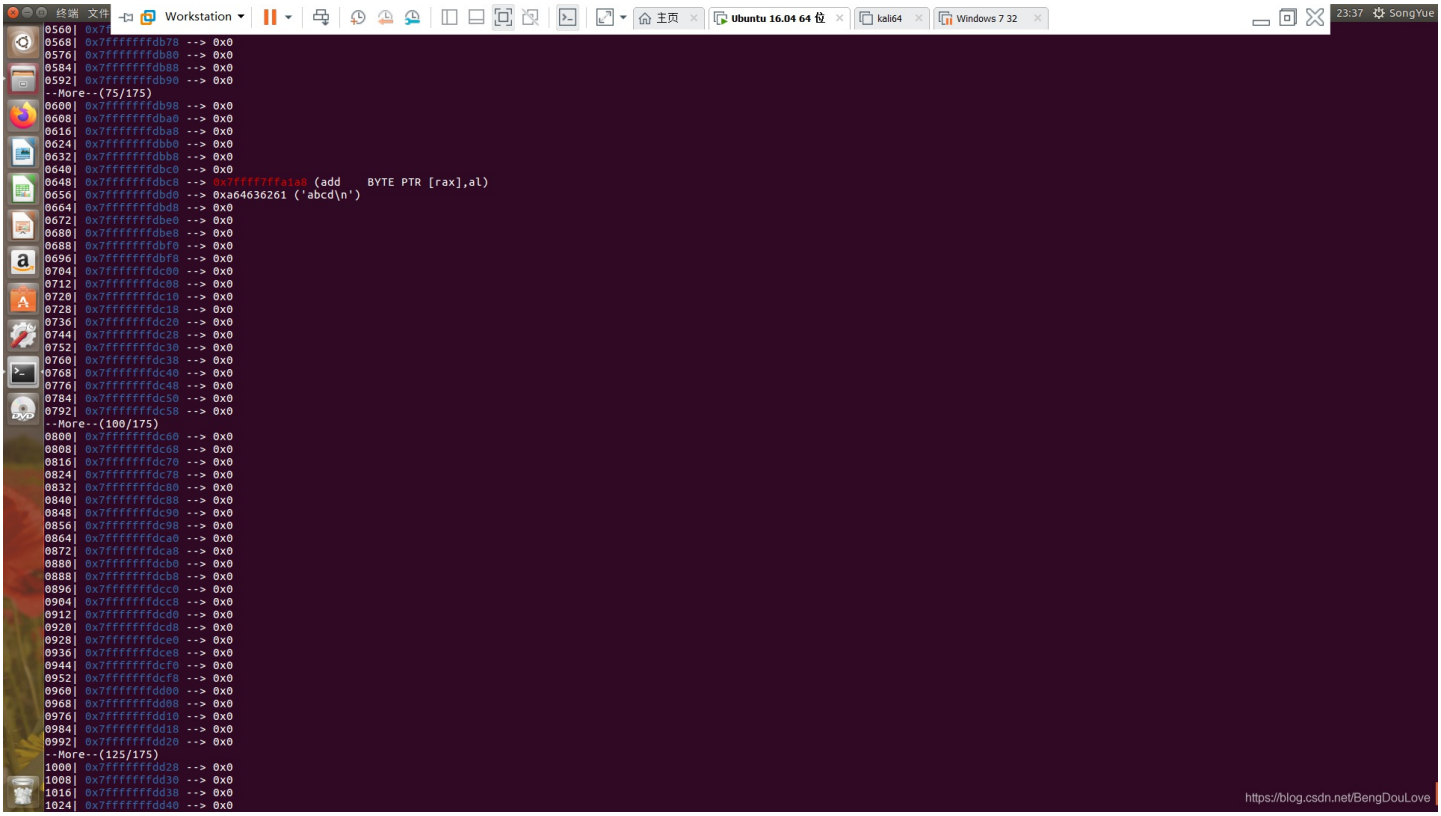


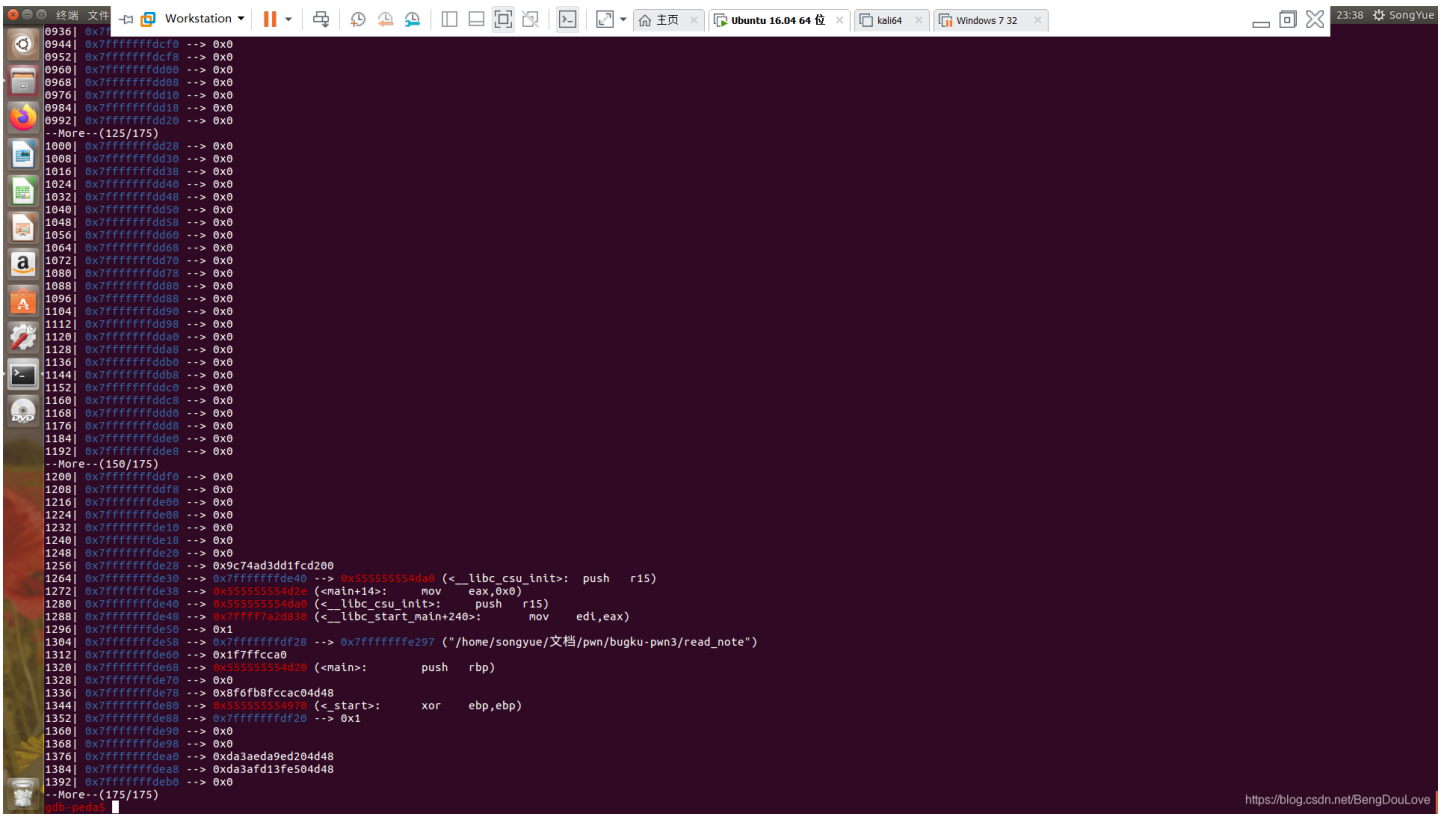


这个程序意思是一开始让你选择一个无关紧要的文件，打开这个文件之后读取文件内容打印，然后就是用户的输入
先输入要输入的内容有多长，之后写入thinking_note，这里thinking_note大小是固定的，所以这里造成栈溢出，
下一步判断是否624个字，也没啥用，好像每次都不对然后进入if，这里又可以读取0x270的内容



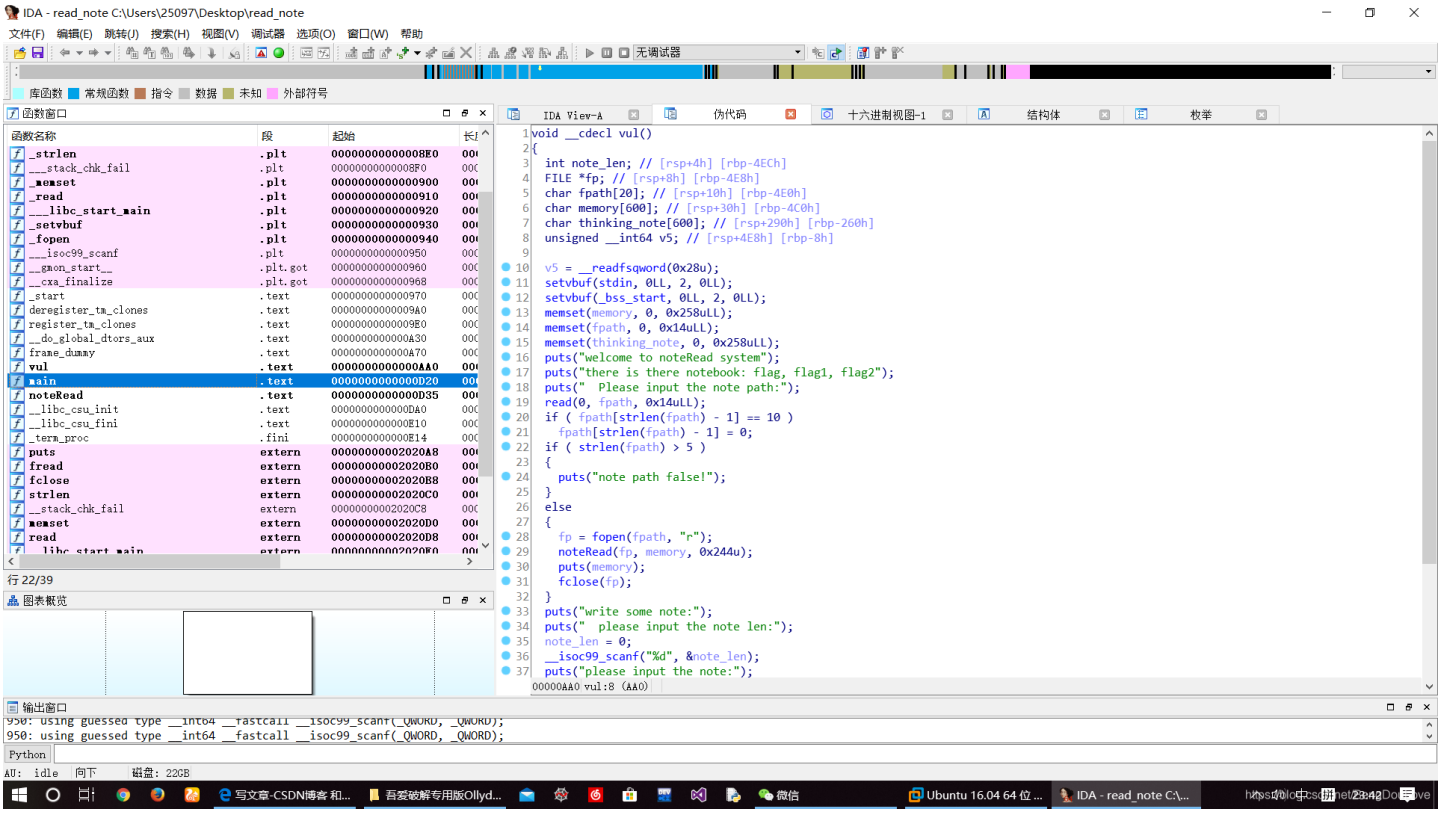
这里读入1000





在第一个read的地方输入了abcd，然后从ida上也看到canary在rbp+8的位置，也就是，序号1256那个位置

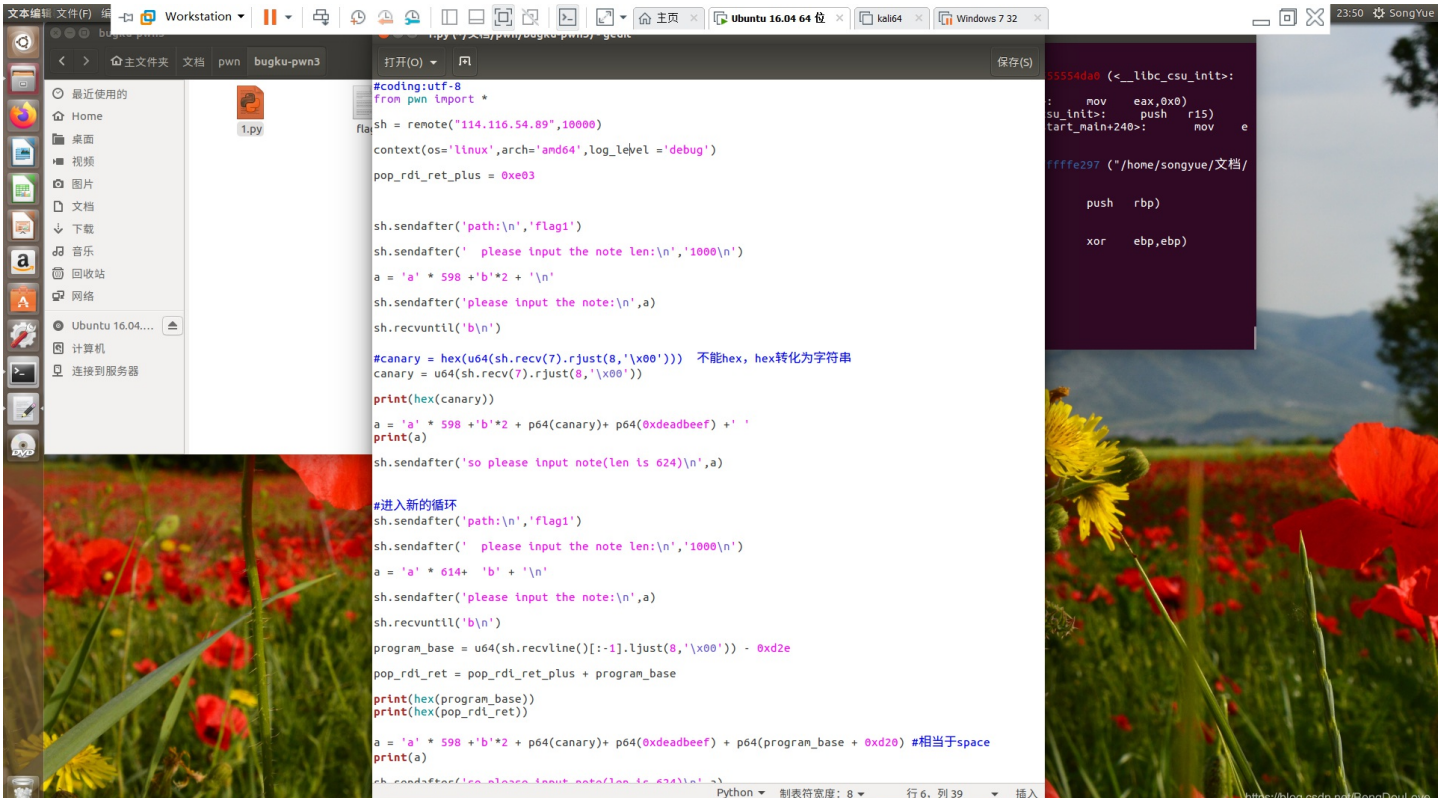
现在有三件事不知道，第一个是canary值，第二个是libc基址，第三个是程序的基址（因为要ROP）

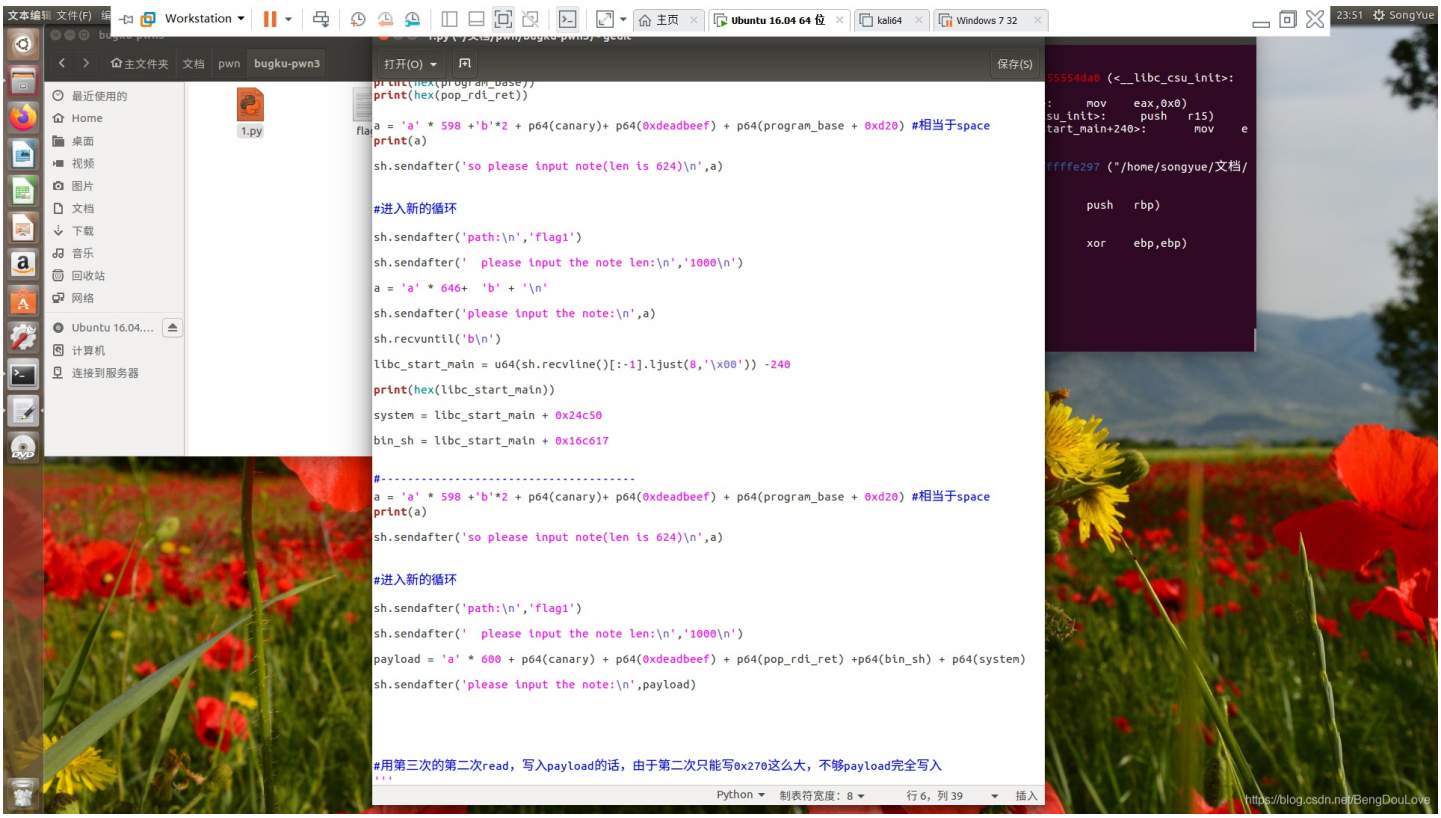


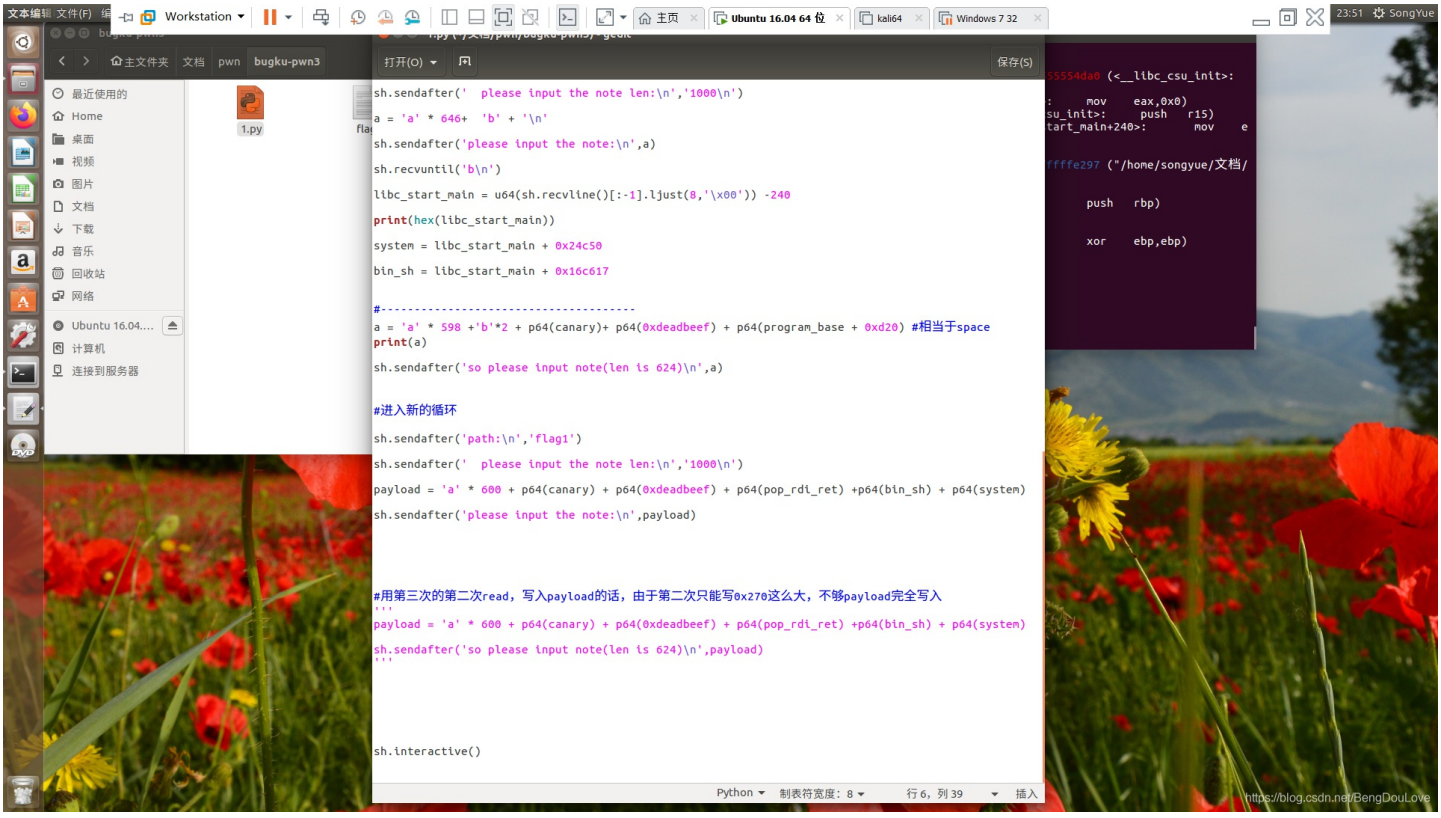
这张图可以看到，main函数位置是d20，而在上个图可以看到，rbp下面的返回main函数的地址是d2e，这俩就差一个字节，所以可以通过栈溢出写入这个返回地址的最后一个字节，2e改为20，这样我们可以不停地进行main函数，一次获取上面说的三个缺少的信息

但是在这个之前，必须知道canary的值，因为通过vul函数返回地址返回main的时候要检查canary，所以第一个获取的肯定是canary，之后通过第二个read来再次回到main

第二次和第三次main用来获取libc基址和程序代码的基址，（应该没有顺序之分吧），每次都用同样的方法返回main







拙劣的代码，我是一遍一遍试的

之前犯一个错误，就是想最后一次在main里的时候，通过第一个read已经获取好了所有信息，就通过第二个read直接过去呗，然后不对，想了半天也不知道为什么。。。后来明白的，第二次read规定输入长度了就只能是0x270，我写着一大堆rop进去根本不够用，所以还得有第四次main的第一次read写入才行。。。

bugku的pwn我都肝完了，虽然很多不是自己想出来的，都是一边看writeup一边学，不过调试了那么多，调了那么多坑应该也涨了不少知识，下一步要肝堆了，，，这个比栈难得多，坚持吧。。。ctf比赛都是堆的题，刚结束的XCTF我还是一道题也没能做。。唉