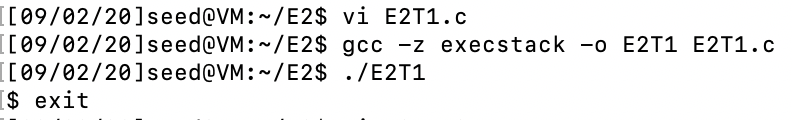
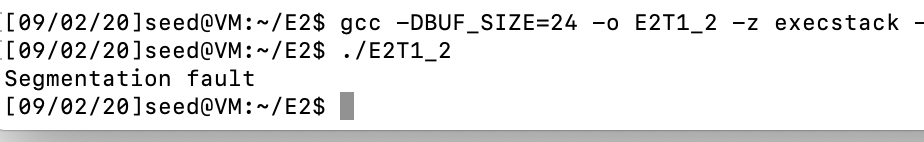
**Enviroment Report**

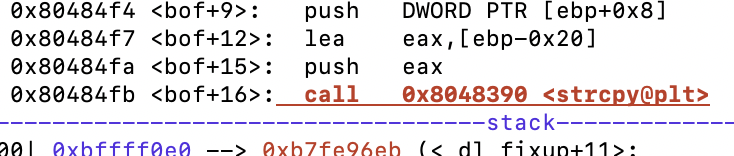
**57117139吴星灿**

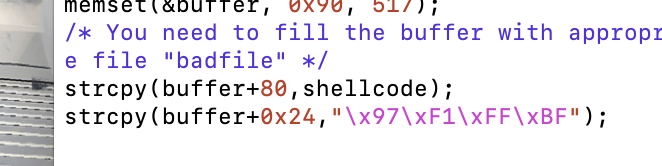
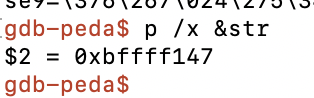
**Task 1**

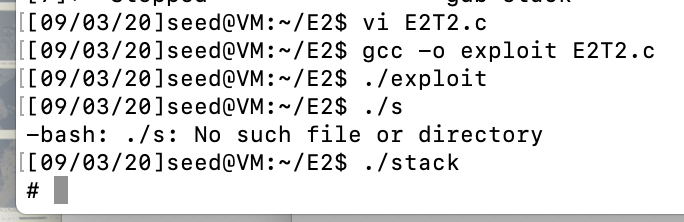




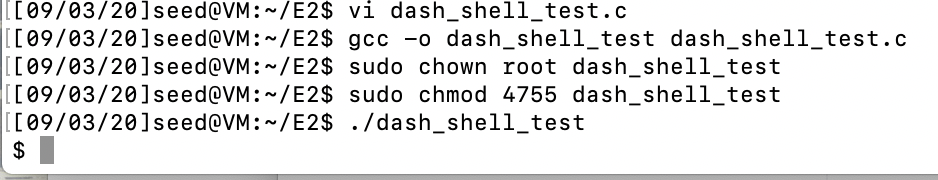
**Task2**

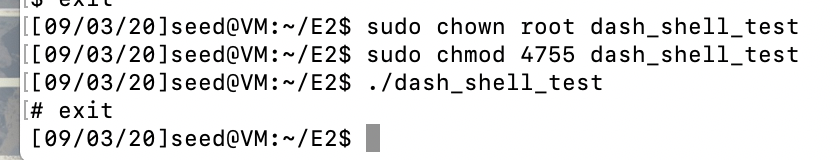


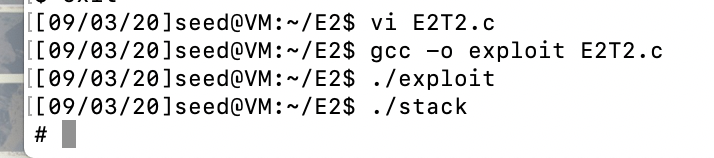




**Task3**

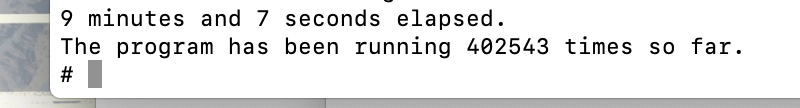






按照实验步骤添上setuid(0)，获得root权限的shell

**Task4**



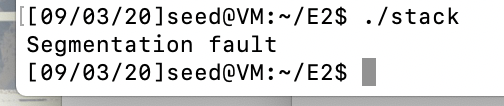
运行脚本 得到root权限的shell

**Task5**



因为内存保护机制所以运行代码被直接中断

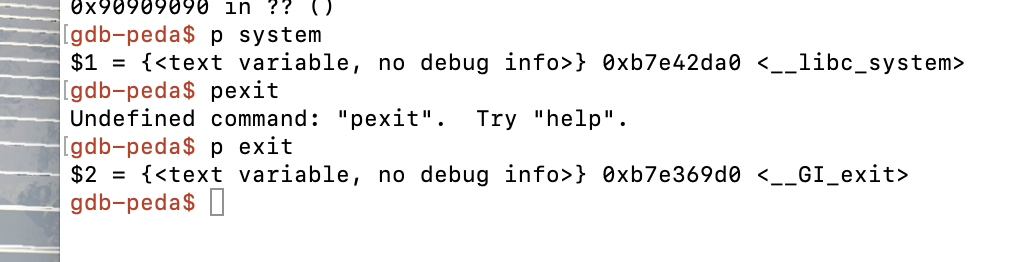
**Task6**



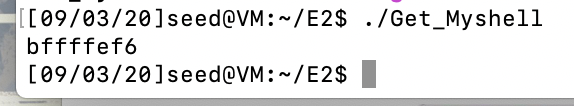
因为随机地址所以得到分页错误

**Lab2**

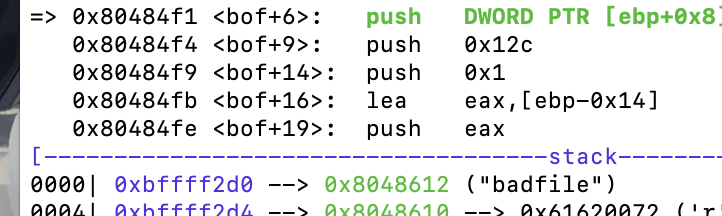
**Task1**

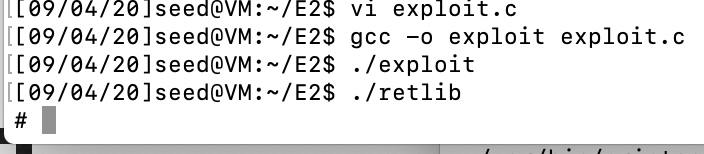


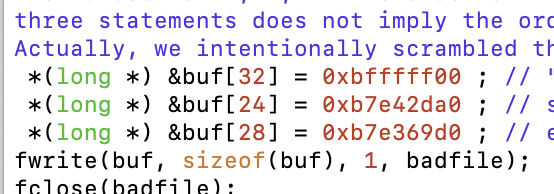
**Task2**



**Task3**



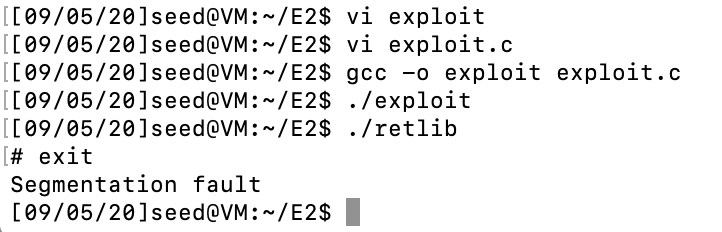




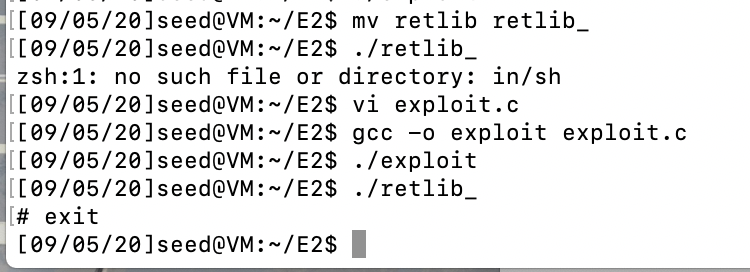
通过多次尝试MYSHELL的地址，成功打开root权限的shell

附加问题

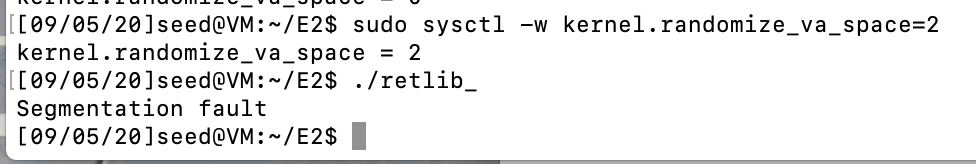
exit()不是必须的，注释掉exit复刻实验依旧可以提取，但是无法正常退出shell，但是可能崩溃。



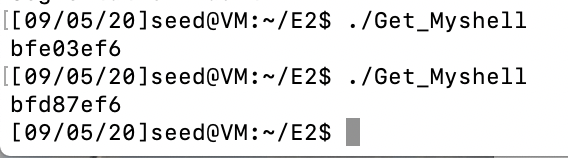
更改文件名会影响环境变量的值，需要改变在原环境变量的地址上做更改才能运行



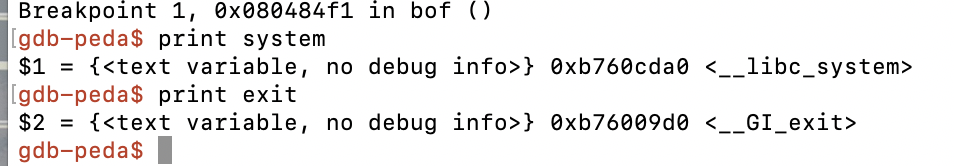
**Task4**

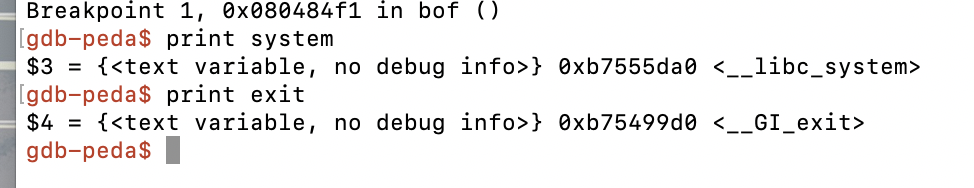


原方法不再适用



环境变量的地址不断改变





两次运行的system和exit的地址不同

**Task5看不懂rop编程**

**Task6**