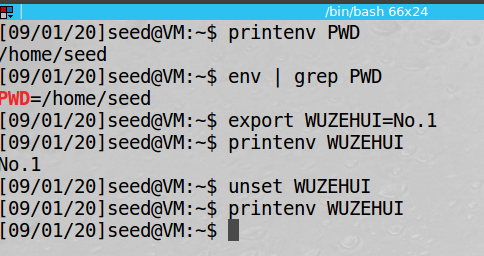
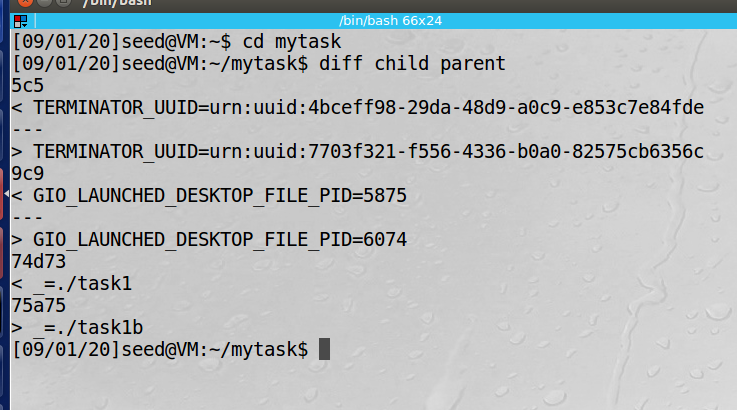
**Lab1**

57117112 吴泽辉

**Task 1**



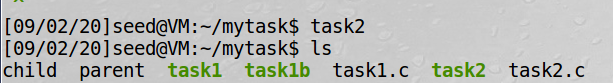
**Task 2**



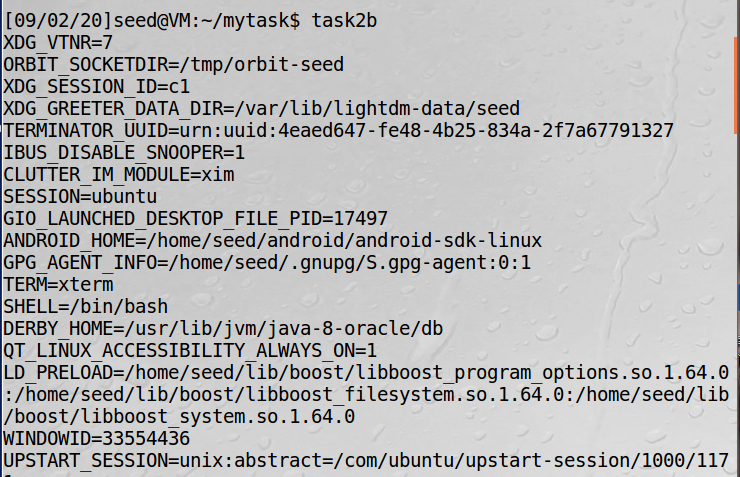
可以看出，父进程与子进程的环境变量基本完全相同，说明子进程复制了父进程的环境变量，只有些进程的id、路径不相同。

**Task 3**

第一个程序的运行结果：

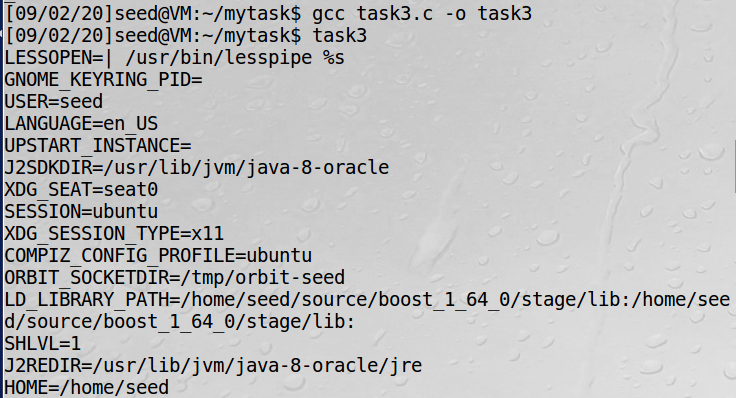


第二个程序的运行结果：

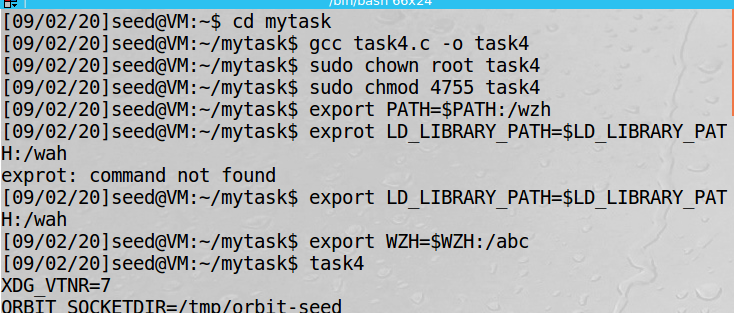


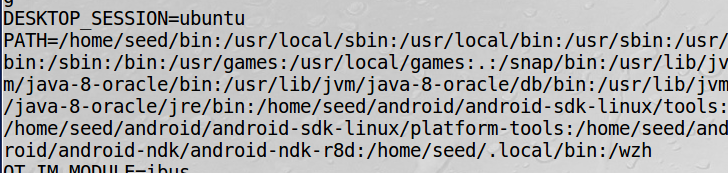
通过观察可以看出execve()函数通过第三个参数environ来获得环境变量。

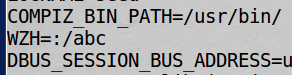
**Task 4**



**Task 5**

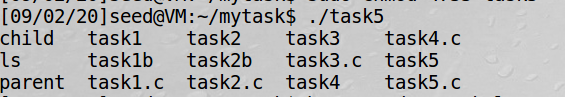






可以看出设置的环境变量PATH和WZH都出现在shell中。

**Task 6：**

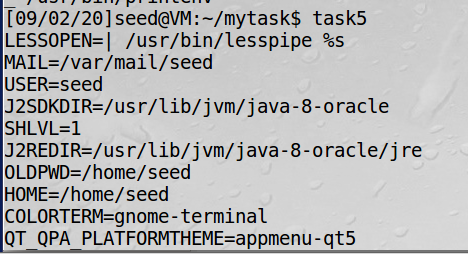


直接运行的结果是ls



将输出环境变量的task4程序复制成ls，然后把task5设成setuid，添加环境变量

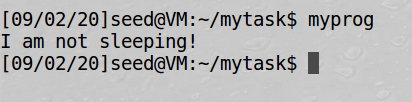




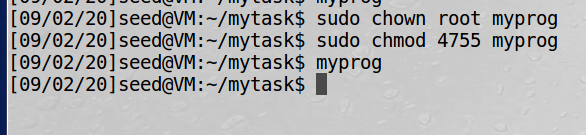
再执行task5可以看到，输出的不是ls命令，而是task4输出环境变量。

**Task 7**

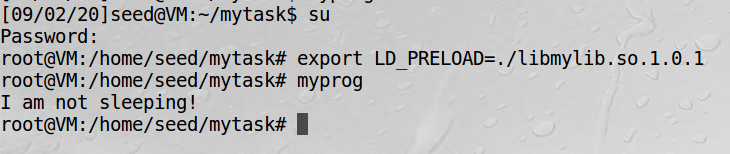
在第一种情况下输出



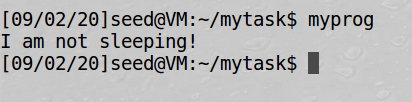
第二种情况下暂停了一秒



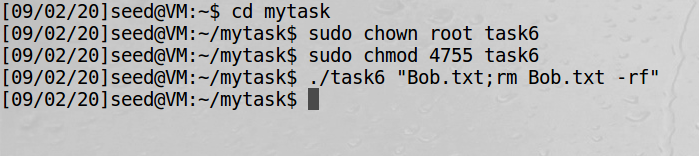
第三种情况下输出



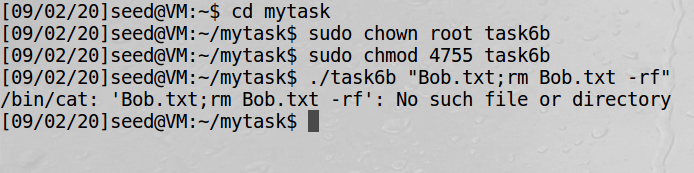
第四种情况下输出



**Task 8**

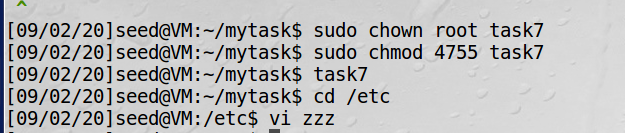


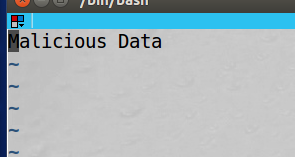
通过./task6 “Bob.txt;rm Bob.txt -rf”命令可以将文件删除



而通过exevce函数显示找不到该文件

**Task 9**





成功写入zzz文件。