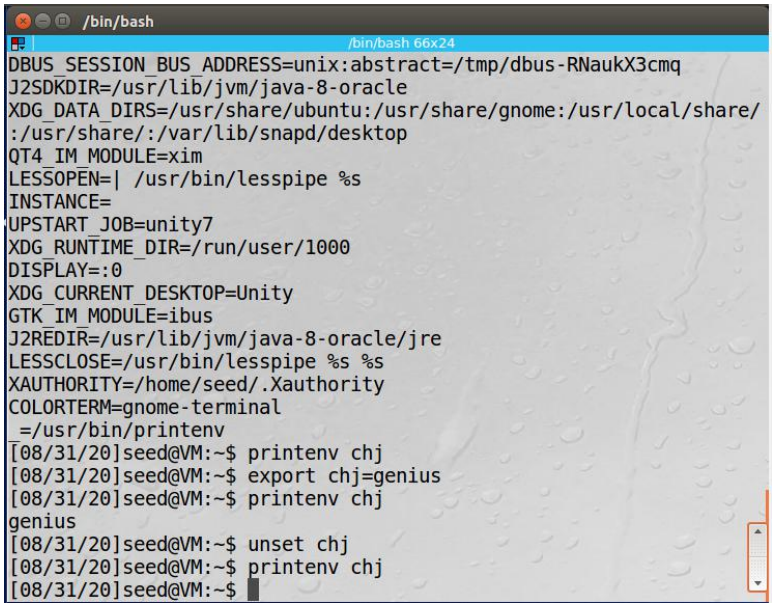
Lab1-report　57117219 尚林灏

Task 1:

使用 printenv 打印环境变量结果为



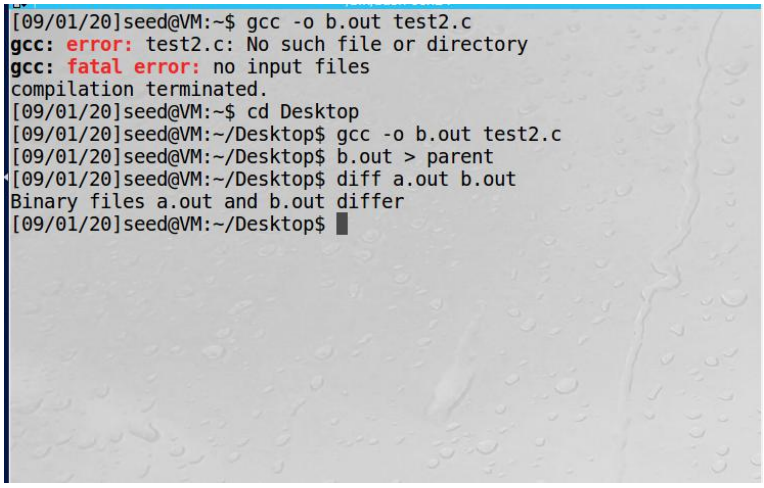
Task2:

执行保存结果的 a.out 文件，查看代码的运行结果

将 child process 中 printenv()注释，将 process 中 parent printenv()取消注释，重新保存编译 C 文件。执行保存结果的 b.out 文件，查看代码的运行结果

```
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:00b0911d-8ba5-4f07-8c2e-505a65d3abff
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2525
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
XDG_MENU_PREFIX=gnome-
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/
lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/
libboost_system.so.1.64.0
WINDOWID=23068676
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1425
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/
boost_1_64_0/stage/lib:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
```

将两次的结果进行比对：将 a.out、b.out 文件的结果分别保存为 child 和 parent 文件，再使用 diff 命令比较，发现两者除了文件名外完全相同。这说明子进程环境变量会继承父环境变量。进一步查阅资料了解到，子进程自父进程继承到进程的资格、环境、堆栈、内存等，但子进程所独有的是不同的父进程号、自己的文件描述符和目录流的拷贝、在 tms 结构中的系统时间、不继承异步输入和输出等



Task3：

编译并运行以下程序。描述观察到的实验结果。该程序简单地调用了/usr/bin/env,该系统调用能够打印出当前进程的环境变量。重新保存和编译文件，发现执行结果为空。

查询函数 execve()的作用，其调用格式如下：int execve(const char * filename，char * const argv[]，char * const envp[])第一个参数为一个可执行的有效的路径名。第二个参数系利用数组指针来传递给执行文件，argv 是要调用的程序执行的参数序列，也就是我们要调用的程序需要传入的参数。envp 则为传递给执行文件的新环境变量数。所以在此处，我们赋予新进程的环境变量为空，自然印出环境变量结果为空。

把 execve()的调用改为以下内容，观察结果.将原语句换为：execve("/usr/bin/env", argv, environ)；重新保存和编译文件，得到结果。

```
[09/01/20]seed@VM:~$ gcc -o b.out test2.c
gcc: error: test2.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[09/01/20]seed@VM:~$ cd Desktop
[09/01/20]seed@VM:~/Desktop$ gcc -o b.out test2.c
[09/01/20]seed@VM:~/Desktop$ b.out > parent
[09/01/20]seed@VM:~/Desktop$ diff a.out b.out
Binary files a.out and b.out differ
[09/01/20]seed@VM:~/Desktop$ gcc test3.c
test3.c: In function 'main':
test3.c:9:1: warning: implicit declaration of function 'execve' [-
Wimplicit-function-declaration]
 execve("/usr/bin/env", argv, NULL);
 ^
[09/01/20]seed@VM:~/Desktop$ gcc test3.c
test3.c: In function 'main':
test3.c:9:1: warning: implicit declaration of function 'execve' [-
Wimplicit-function-declaration]
 execve("/usr/bin/env", argv, environ);
 ^
[09/01/20]seed@VM:~/Desktop$
```

```
QT_IM_MODULE=ibus
QT_QPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed
JOB=unity-settings-daemon
XMODIFIERS=@im=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
GDM_LANG=en_US
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
SHLVL=1
HOME=/home/seed
XDG_SEAT=seat0
LANGUAGE=en_US
LIBGL_ALWAYS_SOFTWARE=1
```

Task4：

重新保存和编译文件得到如下结果（截取部分）：查阅资料得 system（）的调用格式如下：int system（const char * string）.system()会调用 fork()产生子进程，由子进程来调用/bin/sh-c string 来执行参数 string 字符串所代表的命令，此命>令执行完后随即返回原调用的进程。在调用 system()期间 SIGCHLD 信号会被暂时搁置，SIGINT 和 SIGQUIT 信号则会被忽略。

具体个描述为这样三个步骤：调用 fork（）函数新建一个子进程；在子进程中调用 exec 函数去执行 command；在父进程中调用 wait 去等待子进程结束。返回值 =-1:出现错误 =0:调用成功但是没有出现子进程 >0:成功退出的子进程的 id 如果 system()在调用/bin/sh 时失败则返回 127，其他失败原因返回-1。若参数 string 为空指针(NULL)，则返回非零值>。如果 system()调用成功则最后会返回执行 shell 命令后的返回值，但是此返回值也有可能为 system()调用/bin/sh 失败所返回的 127，因此最好能再检查 errno 来确认执行成功。

```
test3.c: In function ‘main’:
test3.c:9:1: warning: implicit declaration of function ‘execve’ [-
Wimplicit-function-declaration]
 execve("/usr/bin/env", argv, environ);
 ^
[09/01/20]seed@VM:~/Desktop$ gcc -o r4.out test4.c
[09/01/20]seed@VM:~/Desktop$ ./r4.out
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
UPSTART_INSTANCE=
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
ORBIT_SOCKETDIR=/tmp/orbit-seed
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/see
d/source/boost_1_64_0/stage/lib:
SHLVL=1
LIBGL_ALWAYS_SOFTWARE=1
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
HOME=/home/seed
```

Task5：

在当前进程中打印出所有的环境变量

重新保存、编译和执行给出的代码，得到如下结果（截取部分），此结果就是当前所有环境变量：

将上述程序的所有权改为 root，并使它成为一个 Set-UID 程序

先切换为 root 账户，使用 chown root:root demo5.c 将此 c 文件权限改为 root 权限

使用一般用户登录终端，使用 export 命令设置如下环境变量：PATH 、LD_LIBRARY_PATH、ANY_NAME

export PATH="$PATH:/usr/local/"

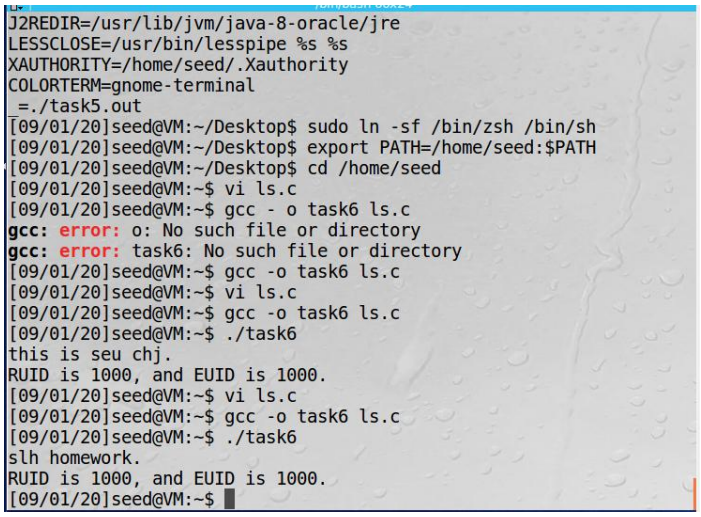
export LD_LIBRARY_PATH="$LD_LIBRARY_PATH:/usr/local/"

export LXJ="/usr/local"

```
root@VM: /home/seed/Desktop 66x24
TH:/usr/local/"
root@VM:/home/seed/Desktop# export CHJ="/usr/local"
root@VM:/home/seed/Desktop# gcc test5.c
root@VM:/home/seed/Desktop# gcc test5.c
root@VM:/home/seed/Desktop# gcc test55.c
root@VM:/home/seed/Desktop# sudo chown root test55.c
root@VM:/home/seed/Desktop# sudo chmod 4755 test55.c
root@VM:/home/seed/Desktop# gcc r5.out test55.c
gcc: error: r5.out: No such file or directory
root@VM:/home/seed/Desktop# gcc -o r5.out test55.c
root@VM:/home/seed/Desktop# ./r5.out
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
CLUTTER_IM_MODULE=xim
TERMINATOR_UUID=urn:uuid:00b0911d-8ba5-4f07-8c2e-505a65d3abff
IBUS_DISABLE_SNOOPER=1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
GIO_LAUNCHED_DESKTOP_FILE_PID=2525
SESSION=ubuntu
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
ANDROID_HOME=/home/seed/android/android-sdk-linux
SHELL=/bin/bash
XDG_MENU_PREFIX=gnome-
```

Task 6：

按照手册进行实验，最后得到结果



Task7：

```
compilation terminated.
[09/01/20]seed@VM:~$ cd Desktop
[09/01/20]seed@VM:~/Desktop$ gcc -fPIC -g -c mylib.c
[09/01/20]seed@VM:~/Desktop$ gcc -shared -o libmylib.so.1.0.1 myli
b.o -lc
[09/01/20]seed@VM:~/Desktop$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~/Desktop$ gcc -o myprog myprog.c
myprog.c: In function ‘main’:
myprog.c:4:1: warning: implicit declaration of function ‘sleep’ [-
Wimplicit-function-declaration]
 sleep(1);
 ^
[09/01/20]seed@VM:~/Desktop$ ./myprog
I am not sleeping!
[09/01/20]seed@VM:~/Desktop$ sudo chown root ./myprog
[09/01/20]seed@VM:~/Desktop$ sudo chmod 4755 ./myprog
[09/01/20]seed@VM:~/Desktop$ ./myprog
[09/01/20]seed@VM:~/Desktop$
```

```
[09/01/20]seed@VM:~/Desktop$ gcc -shared -o libmylib.so.1.0.1 myli
b.o -lc
[09/01/20]seed@VM:~/Desktop$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~/Desktop$ gcc -o myprog myprog.c
myprog.c: In function ‘main’:
myprog.c:4:1: warning: implicit declaration of function ‘sleep’ [-
Wimplicit-function-declaration]
 sleep(1);
 ^
[09/01/20]seed@VM:~/Desktop$ ./myprog
I am not sleeping!
[09/01/20]seed@VM:~/Desktop$ sudo chown root ./myprog
[09/01/20]seed@VM:~/Desktop$ sudo chmod 4755 ./myprog
[09/01/20]seed@VM:~/Desktop$ ./myprog
[09/01/20]seed@VM:~/Desktop$ ^C
[09/01/20]seed@VM:~/Desktop$ su
Password:
su: Authentication failure
[09/01/20]seed@VM:~/Desktop$ su
Password:
root@VM:/home/seed/Desktop# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Desktop# ./myprog
I am not sleeping!
root@VM:/home/seed/Desktop#
```

```
root@VM:/home/seed/Desktop# ^C
root@VM:/home/seed/Desktop# ^C
root@VM:/home/seed/Desktop# exqit
exqit: command not found
root@VM:/home/seed/Desktop# qxit
No command 'qxit' found, did you mean:
 Command 'qgit' from package 'qgit' (universe)
qxit: command not found
root@VM:/home/seed/Desktop# exit
exit
[09/01/20]seed@VM:~/Desktop$ sudo chown chj ./myprog
chown: invalid user: ‘chj’
[09/01/20]seed@VM:~/Desktop$ sudo chown root ./myprog
[09/01/20]seed@VM:~/Desktop$ sudo chmod 4755 ./myprog
[09/01/20]seed@VM:~/Desktop$ ./myprog
[09/01/20]seed@VM:~/Desktop$ gcc -o test7 test7.c
test7.c: In function ‘main’:
test7.c:2:2: warning: implicit declaration of function ‘system’ [-
Wimplicit-function-declaration]
  system("env | grep LD_PRELOAD");
  ^
[09/01/20]seed@VM:~/Desktop$ ./test7
LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~/Desktop$
```

```
UPSTART_JOB=unity7
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
XDG_CURRENT_DESKTOP=Unity
GTK_IM_MODULE=ibus
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
LESSCLOSE=/usr/bin/lesspipe %s %s
XAUTHORITY=/home/seed/.Xauthority
COLORTERM=gnome-terminal
_=./task5.out
[09/01/20]seed@VM:~/Desktop$ sudo ln -sf /bin/zsh /bin/sh
[09/01/20]seed@VM:~/Desktop$ export PATH=/home/seed:$PATH
[09/01/20]seed@VM:~/Desktop$ cd /home/seed
[09/01/20]seed@VM:~$ vi ls.c
[09/01/20]seed@VM:~$ gcc - o task6 ls.c
gcc: error: o: No such file or directory
gcc: error: task6: No such file or directory
[09/01/20]seed@VM:~$ gcc -o task6 ls.c
[09/01/20]seed@VM:~$ vi ls.c
[09/01/20]seed@VM:~$ gcc -o task6 ls.c
[09/01/20]seed@VM:~$ ./task6
this is seu chj.
RUID is 1000, and EUID is 1000.
[09/01/20]seed@VM:~$
```

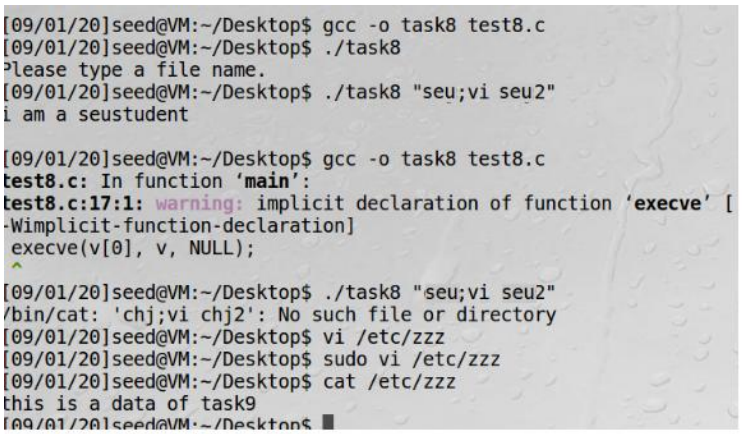
Task8：

```
[09/01/20]seed@VM:~/Desktop$ ./test7
LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~/Desktop$ cat chj
cat: chj: No such file or directory
[09/01/20]seed@VM:~/Desktop$ vi chj
[09/01/20]seed@VM:~/Desktop$ cat chj
i am a seustudent

[09/01/20]seed@VM:~/Desktop$ gcc -o task8 test8.c
[09/01/20]seed@VM:~/Desktop$ ./task8
Please type a file name.
[09/01/20]seed@VM:~/Desktop$ ./task8 "seu;vi seu2"
i am a seustudent

[09/01/20]seed@VM:~/Desktop$ gcc -o task8 test8.c
test8.c: In function 'main':
test8.c:17:1: warning: implicit declaration of function 'execve' [
-Wimplicit-function-declaration]
 execve(v[0], v, NULL);
 ^
[09/01/20]seed@VM:~/Desktop$ ./task8 "seu;vi seu2"
/bin/cat: 'chj;vi chj2': No such file or directory
[09/01/20]seed@VM:~/Desktop$
```

```
~
~
~
~
~
"seu2" [New File]                                0,0-1         All
```

Task9：

首先创建 /etc/zzz 文件。然后，按照题目指令运行相应的程序后，查看 /etc/zzz 文件：写入 data，发现可以写入，查找资料可得，在调用 fork() 之前， fd 并没有被关闭，因此，子进程会复制父进程所有的文件描述符，也 包括 fd 。在父进程中，使用 close(fd) 关闭了 fd ，但是在子进程中由于是复制的，所以 fd 不受父进 程影响，依然存在。此时，尽管子进程的权限已经被降级，但其拥有文件描述符，就可以对其进行修 改，从而对 /etc/zzz 文件进行了写操作。


[09/01/20]seed@VM:~/Desktop$ gcc -o task8 test8.c
[09/01/20]seed@VM:~/Desktop$ ./task8
Please type a file name.
[09/01/20]seed@VM:~/Desktop$ ./task8 "seu;vi seu2"
i am a seustudent
[09/01/20]seed@VM:~/Desktop$ gcc -o task8 test8.c
test8.c: In function 'main':
test8.c:17:1: warning: implicit declaration of function 'execve' [
-Wimplicit-function-declaration]
execve(v[0], v, NULL);
[09/01/20]seed@VM:~/Desktop$ ./task8 "seu;vi seu2"
/bin/cat: 'chj;vi chj2': No such file or directory
[09/01/20]seed@VM:~/Desktop$ vi /etc/zzz
[09/01/20]seed@VM:~/Desktop$ sudo vi /etc/zzz
[09/01/20]seed@VM:~/Desktop$ cat /etc/zzz
this is a data of task9