**环境变量与Set-UID程序**

姓名：钱煜 学号：57118105

1. 实验目的

了解环境变量是如何变量影响Set UID程序的行为。

1. 实验内容

1.操作环境变量；

2.将环境变量从父进程传递到子进程；

3.Execve()函数与环境变量；

4.环境变量与System（）；

5.环境变量与Set-UID程序；

6.PATH环境变量和Set-UID程序；

7.LD\_PRELOAD环境变量和Set-UID程序；

8.使用system()和execve()调用外部程序；

9.权能泄露。

1. 实验环境

VMware workstation 15.0x，Seed Ubuntu 16.04

1. 实验

**Task 1.操作环境变量**

使用printenv语句得到结果：

**[09/02/20]seed@VM:~$ printenv**

**XDG\_VTNR=7**

**XDG\_SESSION\_ID=c1**

**XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed**

**CLUTTER\_IM\_MODULE=xim**

**SESSION=ubuntu**

**ANDROID\_HOME=/home/seed/android/android-sdk-linux**

**GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1**

**TERM=xterm-256color**

**VTE\_VERSION=4205**

**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=31457290**

**UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1169**

**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=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:**

**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**

**SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh**

**DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path**

**SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/2439,unix/VM:/tmp/.ICE-unix/2439**

**XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg**

**DESKTOP\_SESSION=ubuntu**

**PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin**

**QT\_IM\_MODULE=ibus**

**QT\_QPA\_PLATFORMTHEME=appmenu-qt5**

**XDG\_SESSION\_TYPE=x11**

**PWD=/home/seed**

**JOB=dbus**

**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**

**IM\_CONFIG\_PHASE=1**

**GDMSESSION=ubuntu**

**SESSIONTYPE=gnome-session**

**GTK2\_MODULES=overlay-scrollbar**

**SHLVL=1**

**HOME=/home/seed**

**XDG\_SEAT=seat0**

**LANGUAGE=en\_US**

**GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated**

**XDG\_SESSION\_DESKTOP=ubuntu**

**LOGNAME=seed**

**DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-gzd4BHLijS**

**J2SDKDIR=/usr/lib/jvm/java-8-oracle**

**XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop**

**QT4\_IM\_MODULE=xim**

**LESSOPEN=| /usr/bin/lesspipe %s**

**INSTANCE=**

**XDG\_RUNTIME\_DIR=/run/user/1000**

**DISPLAY=:0**

**XDG\_CURRENT\_DESKTOP=Unity**

**GTK\_IM\_MODULE=ibus**

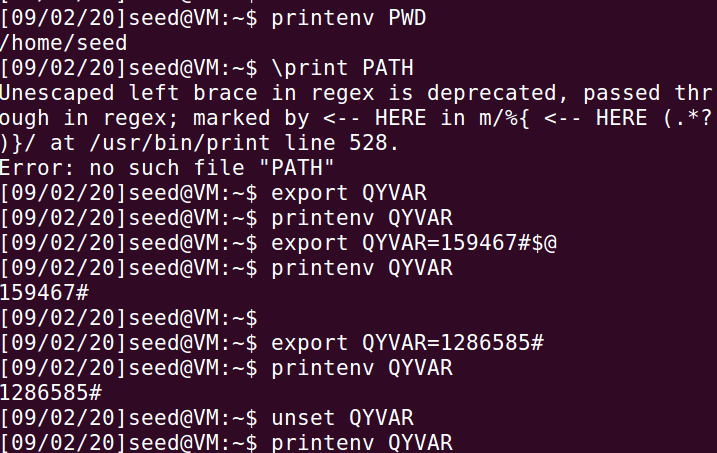
**J2REDIR=/usr/lib/jvm/java-8-oracle/jre**

**LESSCLOSE=/usr/bin/lesspipe %s %s**

**XAUTHORITY=/home/seed/.Xauthority**

**\_=/usr/bin/printenv**

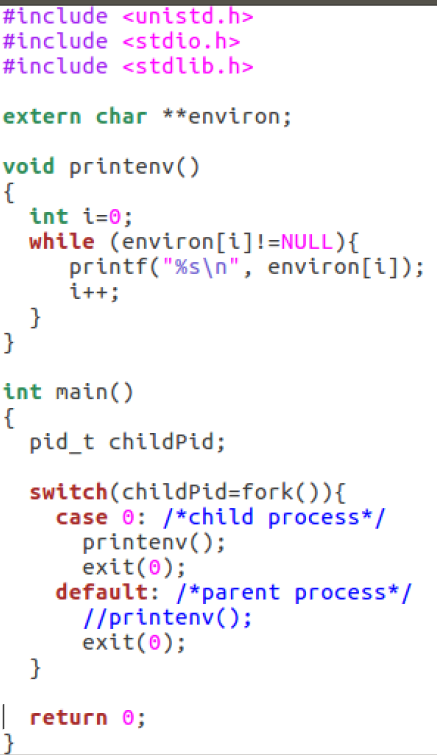
使用特定Printenv语句和set/unset得到结果：



其中，export为设定一个自定义环境变量，unset为消除自定义变量。

**Task 2.将环境变量从父进程传递到子进程**

将要求中给出的代码输入test2.cpp文件：



得到结果：

**[09/02/20]seed@VM:~$ g++ test2.cpp**

**[09/02/20]seed@VM:~$ g++ test2.cpp -o test2.out**

**[09/02/20]seed@VM:~$ ./test2.out**

**XDG\_VTNR=7**

**ORBIT\_SOCKETDIR=/tmp/orbit-seed**

**XDG\_SESSION\_ID=c1**

**XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed**

**TERMINATOR\_UUID=urn:uuid:f58599e7-ff6a-4314-8f9b-0f16a2fa5401**

**IBUS\_DISABLE\_SNOOPER=1**

**CLUTTER\_IM\_MODULE=xim**

**ANDROID\_HOME=/home/seed/android/android-sdk-linux**

**GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1**

**TERM=xterm**

**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=60817412**

**UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1169**

**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=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:**

**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**

**SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh**

**DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path**

**XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg**

**DESKTOP\_SESSION=ubuntu**

**PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin**

**QT\_IM\_MODULE=ibus**

**QT\_QPA\_PLATFORMTHEME=appmenu-qt5**

**XDG\_SESSION\_TYPE=x11**

**PWD=/home/seed**

**JOB=gnome-session**

**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**

**IM\_CONFIG\_PHASE=1**

**GDMSESSION=ubuntu**

**SESSIONTYPE=gnome-session**

**GTK2\_MODULES=overlay-scrollbar**

**SHLVL=1**

**HOME=/home/seed**

**XDG\_SEAT=seat0**

**LANGUAGE=en\_US**

**GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated**

**UPSTART\_INSTANCE=**

**XDG\_SESSION\_DESKTOP=ubuntu**

**UPSTART\_EVENTS=started starting**

**LOGNAME=seed**

**DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-gzd4BHLijS**

**J2SDKDIR=/usr/lib/jvm/java-8-oracle**

**XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop**

**QT4\_IM\_MODULE=xim**

**LESSOPEN=| /usr/bin/lesspipe %s**

**INSTANCE=Unity**

**UPSTART\_JOB=unity-settings-daemon**

**XDG\_RUNTIME\_DIR=/run/user/1000**

**DISPLAY=:0**

**XDG\_CURRENT\_DESKTOP=Unity**

**GTK\_IM\_MODULE=ibus**

**J2REDIR=/usr/lib/jvm/java-8-oracle/jre**

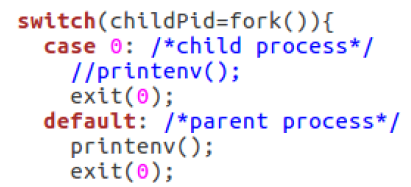
**LESSCLOSE=/usr/bin/lesspipe %s %s**

**XAUTHORITY=/home/seed/.Xauthority**

**COLORTERM=gnome-terminal**

**\_=./test2.out**

随后按照要求注释掉第一个printenv函数，取消注释第二个printenv函数：



得到结果：

**[09/02/20]seed@VM:~$ g++ test2.cpp**

**[09/02/20]seed@VM:~$ g++ test2.cpp -o task2.out**

**[09/02/20]seed@VM:~$ ./task2.out**

**XDG\_VTNR=7**

**ORBIT\_SOCKETDIR=/tmp/orbit-seed**

**XDG\_SESSION\_ID=c1**

**XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed**

**TERMINATOR\_UUID=urn:uuid:d1cfc63d-9e98-4979-adc9-0b679a51aace**

**IBUS\_DISABLE\_SNOOPER=1**

**CLUTTER\_IM\_MODULE=xim**

**ANDROID\_HOME=/home/seed/android/android-sdk-linux**

**GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1**

**TERM=xterm**

**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=60817412**

**UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1169**

**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=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:**

**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**

**SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh**

**DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path**

**XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg**

**DESKTOP\_SESSION=ubuntu**

**PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin**

**QT\_IM\_MODULE=ibus**

**QT\_QPA\_PLATFORMTHEME=appmenu-qt5**

**XDG\_SESSION\_TYPE=x11**

**PWD=/home/seed**

**JOB=gnome-session**

**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**

**IM\_CONFIG\_PHASE=1**

**GDMSESSION=ubuntu**

**SESSIONTYPE=gnome-session**

**GTK2\_MODULES=overlay-scrollbar**

**SHLVL=1**

**HOME=/home/seed**

**XDG\_SEAT=seat0**

**LANGUAGE=en\_US**

**GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated**

**UPSTART\_INSTANCE=**

**XDG\_SESSION\_DESKTOP=ubuntu**

**UPSTART\_EVENTS=started starting**

**LOGNAME=seed**

**DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-gzd4BHLijS**

**J2SDKDIR=/usr/lib/jvm/java-8-oracle**

**XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop**

**QT4\_IM\_MODULE=xim**

**LESSOPEN=| /usr/bin/lesspipe %s**

**INSTANCE=Unity**

**UPSTART\_JOB=unity-settings-daemon**

**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**

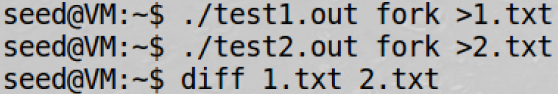
**COLORTERM=gnome-terminal**

**\_=./task2.out**

若直接比较较输出文件，则：

IMG_256

对输出进行重定向并用diff比较：

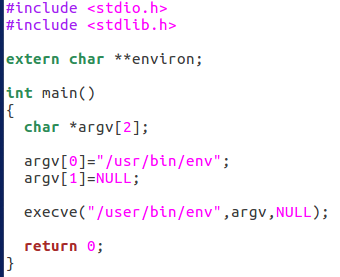


无输出显示，证明两者环境变量相同。

**分析：**fork()函数创建的子进程，继承了父进程包括环境变量在内的大部分设置，但并不继承进程id等环境变量。

**Task 3.环境变量与execve()函数**

根据要求编写cpp文件：



在终端中运行/usr/bin/env命令，得到结果：

**[09/02/20]seed@VM:~$ /usr/bin/env**

**XDG\_VTNR=7**

**ORBIT\_SOCKETDIR=/tmp/orbit-seed**

**XDG\_SESSION\_ID=c1**

**XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed**

**TERMINATOR\_UUID=urn:uuid:7f36a0da-d35c-479a-b494-1049a62a9525**

**IBUS\_DISABLE\_SNOOPER=1**

**CLUTTER\_IM\_MODULE=xim**

**SESSION=ubuntu**

**GIO\_LAUNCHED\_DESKTOP\_FILE\_PID=10265**

**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=54525956**

**UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1169**

**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=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:**

**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**

**SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh**

**DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path**

**GIO\_LAUNCHED\_DESKTOP\_FILE=/usr/share/applications/terminator.desktop**

**XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg**

**DESKTOP\_SESSION=ubuntu**

**PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin**

**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**

**IM\_CONFIG\_PHASE=1**

**GDMSESSION=ubuntu**

**SESSIONTYPE=gnome-session**

**GTK2\_MODULES=overlay-scrollbar**

**SHLVL=1**

**HOME=/home/seed**

**XDG\_SEAT=seat0**

**LANGUAGE=en\_US**

**GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated**

**UPSTART\_INSTANCE=**

**XDG\_SESSION\_DESKTOP=ubuntu**

**UPSTART\_EVENTS=xsession started**

**LOGNAME=seed**

**COMPIZ\_BIN\_PATH=/usr/bin/**

**DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-gzd4BHLijS**

**J2SDKDIR=/usr/lib/jvm/java-8-oracle**

**XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop**

**QT4\_IM\_MODULE=xim**

**LESSOPEN=| /usr/bin/lesspipe %s**

**INSTANCE=**

**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**

**\_=/usr/bin/env**

改写cpp文件中的内容：

task3

再次输出进程流程：

**[09/02/20]seed@VM:~$ /usr/bin/env**

**XDG\_VTNR=7**

**ORBIT\_SOCKETDIR=/tmp/orbit-seed**

**XDG\_SESSION\_ID=c1**

**XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed**

**TERMINATOR\_UUID=urn:uuid:7f36a0da-d35c-479a-b494-1049a62a9525**

**IBUS\_DISABLE\_SNOOPER=1**

**CLUTTER\_IM\_MODULE=xim**

**SESSION=ubuntu**

**GIO\_LAUNCHED\_DESKTOP\_FILE\_PID=10265**

**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=54525956**

**UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1169**

**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=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:**

**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**

**SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh**

**DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path**

**GIO\_LAUNCHED\_DESKTOP\_FILE=/usr/share/applications/terminator.desktop**

**XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg**

**DESKTOP\_SESSION=ubuntu**

**PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin**

**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**

**IM\_CONFIG\_PHASE=1**

**GDMSESSION=ubuntu**

**SESSIONTYPE=gnome-session**

**GTK2\_MODULES=overlay-scrollbar**

**SHLVL=1**

**HOME=/home/seed**

**XDG\_SEAT=seat0**

**LANGUAGE=en\_US**

**GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated**

**UPSTART\_INSTANCE=**

**XDG\_SESSION\_DESKTOP=ubuntu**

**UPSTART\_EVENTS=xsession started**

**LOGNAME=seed**

**COMPIZ\_BIN\_PATH=/usr/bin/**

**DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-gzd4BHLijS**

**J2SDKDIR=/usr/lib/jvm/java-8-oracle**

**XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop**

**QT4\_IM\_MODULE=xim**

**LESSOPEN=| /usr/bin/lesspipe %s**

**INSTANCE=**

**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**

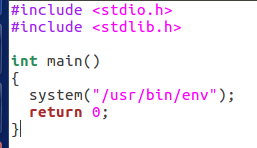
**\_=/usr/bin/env**

对比两次结果，代码中唯一变换的是execve函数中第三个参数。

execve函数主要作用为在原有进程环境下执行新的程序，覆盖原有的内存代码区、数据段和栈，三个参数分别为文件路径，参数数组和新程序的环境变量字符串数组。可见新进程继承环境变量的方法是通过参数传递，而并不会主动继承。

**Task 4.环境变量与System（）**

编写cpp文件：



得到结果：

**[09/02/20]seed@VM:~$ g++ task4.cpp**

**[09/02/20]seed@VM:~$ g++ task4.cpp -o taskf.out**

**[09/02/20]seed@VM:~$ ./taskf.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**

**ORBIT\_SOCKETDIR=/tmp/orbit-seed**

**LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:**

**SHLVL=1**

**J2REDIR=/usr/lib/jvm/java-8-oracle/jre**

**HOME=/home/seed**

**QT4\_IM\_MODULE=xim**

**DESKTOP\_SESSION=ubuntu**

**GIO\_LAUNCHED\_DESKTOP\_FILE=/usr/share/applications/terminator.desktop**

**QT\_LINUX\_ACCESSIBILITY\_ALWAYS\_ON=1**

**GTK\_MODULES=gail:atk-bridge:unity-gtk-module**

**XDG\_SEAT\_PATH=/org/freedesktop/DisplayManager/Seat0**

**INSTANCE=**

**DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-gzd4BHLijS**

**GIO\_LAUNCHED\_DESKTOP\_FILE\_PID=10665**

**COLORTERM=gnome-terminal**

**GNOME\_KEYRING\_CONTROL=**

**QT\_QPA\_PLATFORMTHEME=appmenu-qt5**

**MANDATORY\_PATH=/usr/share/gconf/ubuntu.mandatory.path**

**IM\_CONFIG\_PHASE=1**

**SESSIONTYPE=gnome-session**

**UPSTART\_JOB=unity7**

**LOGNAME=seed**

**GTK\_IM\_MODULE=ibus**

**WINDOWID=31457284**

**\_=./taskf.out**

**DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path**

**XDG\_SESSION\_ID=c1**

**TERM=xterm**

**GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated**

**GTK2\_MODULES=overlay-scrollbar**

**PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin**

**DERBY\_HOME=/usr/lib/jvm/java-8-oracle/db**

**GDM\_LANG=en\_US**

**XDG\_MENU\_PREFIX=gnome-**

**XDG\_SESSION\_PATH=/org/freedesktop/DisplayManager/Session0**

**XDG\_RUNTIME\_DIR=/run/user/1000**

**COMPIZ\_BIN\_PATH=/usr/bin/**

**DISPLAY=:0**

**IBUS\_DISABLE\_SNOOPER=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**

**LANG=en\_US.UTF-8**

**XDG\_CURRENT\_DESKTOP=Unity**

**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=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:**

**XMODIFIERS=@im=ibus**

**XDG\_SESSION\_DESKTOP=ubuntu**

**XAUTHORITY=/home/seed/.Xauthority**

**XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed**

**SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh**

**TERMINATOR\_UUID=urn:uuid:4851eb51-7d10-4e0f-978f-7d71e5d92b88**

**SHELL=/bin/bash**

**QT\_ACCESSIBILITY=1**

**GDMSESSION=ubuntu**

**LESSCLOSE=/usr/bin/lesspipe %s %s**

**UPSTART\_EVENTS=xsession started**

**GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1**

**UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1169**

**XDG\_VTNR=7**

**QT\_IM\_MODULE=ibus**

**PWD=/home/seed**

**JAVA\_HOME=/usr/lib/jvm/java-8-oracle**

**CLUTTER\_IM\_MODULE=xim**

**ANDROID\_HOME=/home/seed/android/android-sdk-linux**

**XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg**

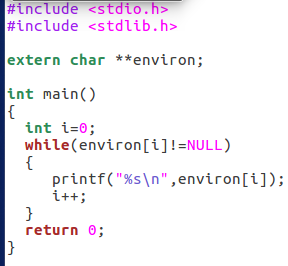
**XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop**

**JOB=unity-settings-daemon**

验证：System（）函数通过调用Excel调用Shell，并在此过程中会将环境变量自动转换给子进程。

**Task 5.环境变量和Set-UID程序**

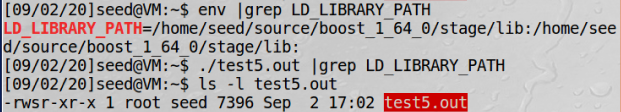
按照要求编写c文件：



编译文件，使其成为Set-UID程序：



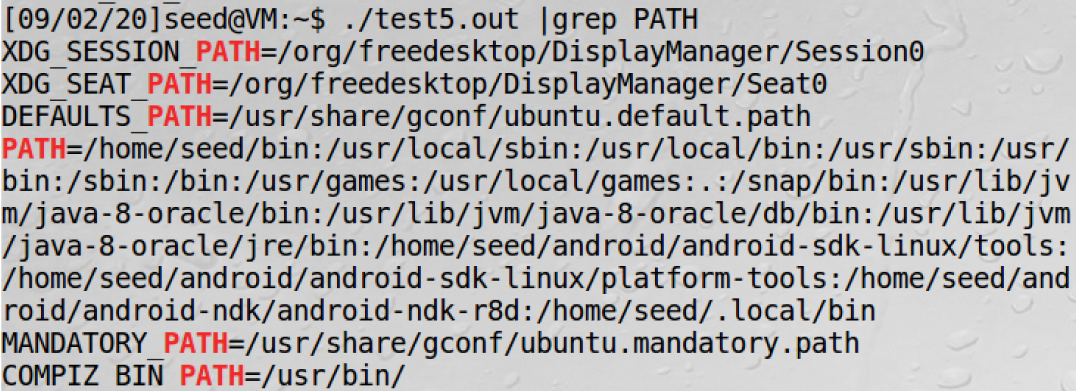
比较两者的LD\_LIBRARY\_PATH：



子进程并没有继承父进程的LD\_LIBRARY\_PATH环境变量。

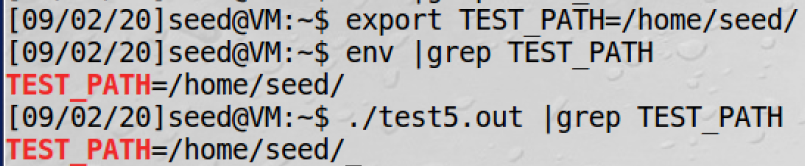
比较两者的PATH变量：





子进程继承了父进程的PATH环境变量。

自主设定自定义变量，比较两者的该自定义变量：

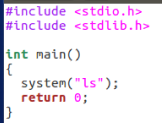


可见子进程继承了父进程的自定义环境变量TEST\_PATH。

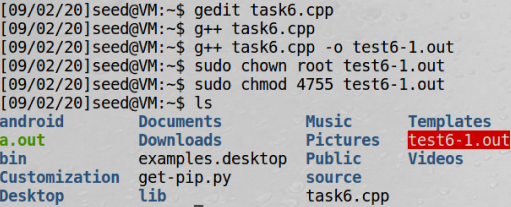
**分析：**Set-UID程序与拥有者拥有一样的权限，普通用户可以执行拥有root权限的程序来完成限定的任务。此外，用户可能通过环境变量影响Set-UID程序的执行逻辑。

**Task 6.PATH环境变量和Set-UID程序**

按照要求编写task6.cpp文件：



将之设置为Set-UID程序并查看：

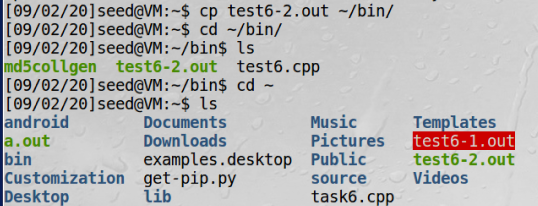


编写自己的ls文件并且编译：

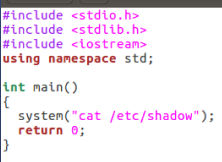


IMG_256

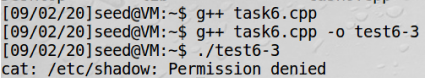
将test6-2.out copy到bin目录下：



尝试启用root权限：



则被拒绝调用：

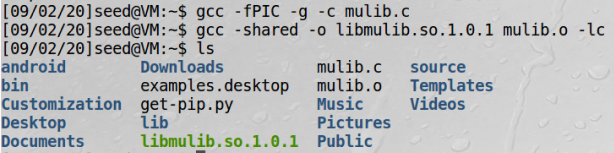


**Task 7.环境变量LD\_PRELOAD和Set-UID程序**

根据要求编写文件mulib.c：



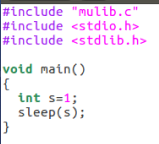
编译成动态链接库文件：

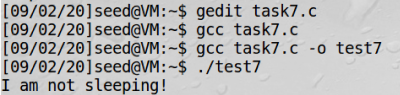


设置LD\_PRELOAD环境：

IMG_256

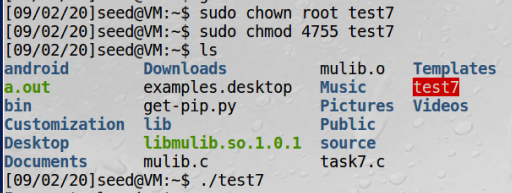
编写task7.c并编译可执行文件：





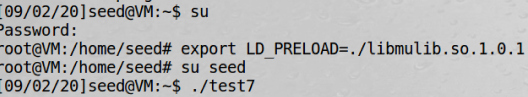
加载的是自定义的sleep库，此时shell定义的环境变量export LD\_PRELOAD传递给了子进程test7。

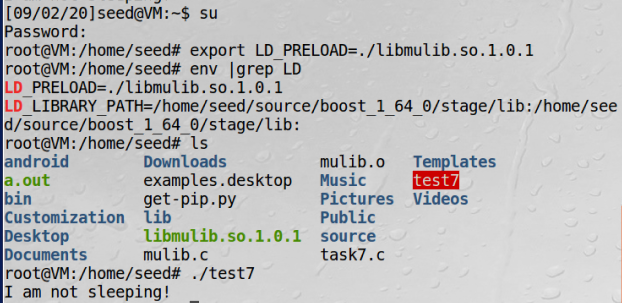
提升test7为Set-UID程序，再次执行：



执行的是系统自带的库，是因为动态链接器的防御措施：特权程序类型的子进程不继承父进程的动态链接库LD\_\*环境变量。

切换用户为root后再次执行：

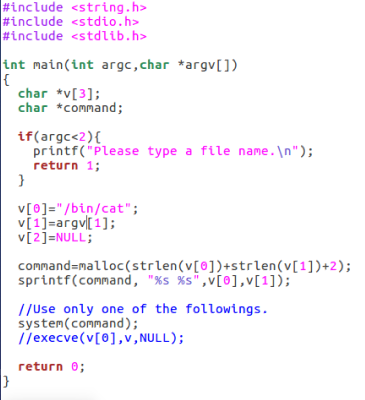




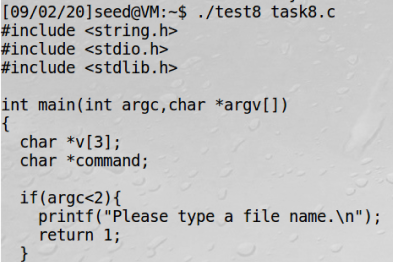
可以执行自定义的动态链接库。shell通过root执行特权提升程序执行，传递了LD\_PRELOAD。

**Task 8.使用system()和execve()调用外部程序**

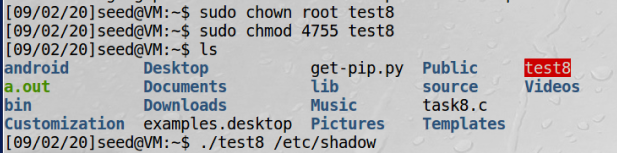
按照要求编写task8.c：



正常编译运行：



提升为ROOT权限后编译运行：



**[09/02/20]seed@VM:~$ ./test8 /etc/shadow**

**root:$6$IHB7yPjy$MvwFOiEtDMupi3uKFIjVQdLJHIX5UqeAFJvI4.570M8.QGKwh1KQYZ9D1aahnphLpoioLjtXtbEU44Fuf7U0l/:18507:0:99999:7:::**

**daemon:\*:17212:0:99999:7:::**

**bin:\*:17212:0:99999:7:::**

**sys:\*:17212:0:99999:7:::**

**sync:\*:17212:0:99999:7:::**

**games:\*:17212:0:99999:7:::**

**man:\*:17212:0:99999:7:::**

**lp:\*:17212:0:99999:7:::**

**mail:\*:17212:0:99999:7:::**

**news:\*:17212:0:99999:7:::**

**uucp:\*:17212:0:99999:7:::**

**proxy:\*:17212:0:99999:7:::**

**www-data:\*:17212:0:99999:7:::**

**backup:\*:17212:0:99999:7:::**

**list:\*:17212:0:99999:7:::**

**irc:\*:17212:0:99999:7:::**

**gnats:\*:17212:0:99999:7:::**

**nobody:\*:17212:0:99999:7:::**

**systemd-timesync:\*:17212:0:99999:7:::**

**systemd-network:\*:17212:0:99999:7:::**

**systemd-resolve:\*:17212:0:99999:7:::**

**systemd-bus-proxy:\*:17212:0:99999:7:::**

**syslog:\*:17212:0:99999:7:::**

**\_apt:\*:17212:0:99999:7:::**

**messagebus:\*:17212:0:99999:7:::**

**uuidd:\*:17212:0:99999:7:::**

**lightdm:\*:17212:0:99999:7:::**

**whoopsie:\*:17212:0:99999:7:::**

**avahi-autoipd:\*:17212:0:99999:7:::**

**avahi:\*:17212:0:99999:7:::**

**dnsmasq:\*:17212:0:99999:7:::**

**colord:\*:17212:0:99999:7:::**

**speech-dispatcher:!:17212:0:99999:7:::**

**hplip:\*:17212:0:99999:7:::**

**kernoops:\*:17212:0:99999:7:::**

**pulse:\*:17212:0:99999:7:::**

**rtkit:\*:17212:0:99999:7:::**

**saned:\*:17212:0:99999:7:::**

**usbmux:\*:17212:0:99999:7:::**

**seed:$6$wDRrWCQz$IsBXp9.9wz9SGrF.nbihpoN5w.zQx02sht4cTY8qI7YKh00wN/sfYvDeCAcEo2QYzCfpZoaEVJ8sbCT7hkxXY/:17372:0:99999:7:::**

**vboxadd:!:17372::::::**

**telnetd:\*:17372:0:99999:7:::**

**sshd:\*:17372:0:99999:7:::**

**ftp:\*:17372:0:99999:7:::**

**bind:\*:17372:0:99999:7:::**

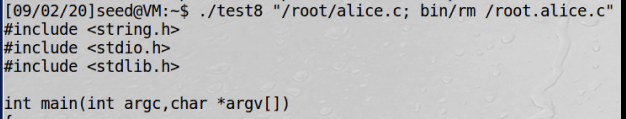
**mysql:!:17372:0:99999:7:::**

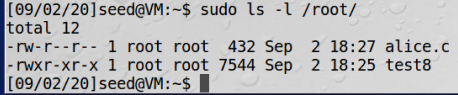
特权查看密码文件。

随后将文件拷贝到root目录下，然后回到seed，运行特权提升程序：

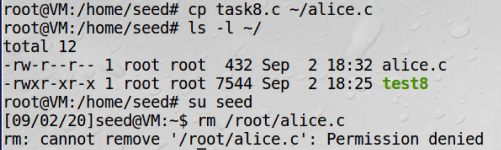


也可以rm文件：



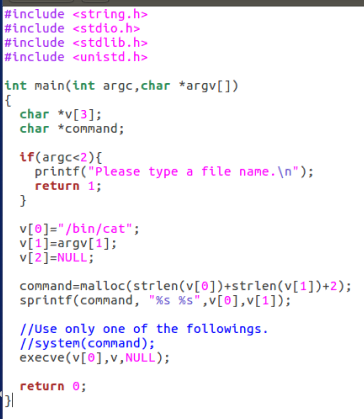


未曾超出rm限制，权限不曾泄露。

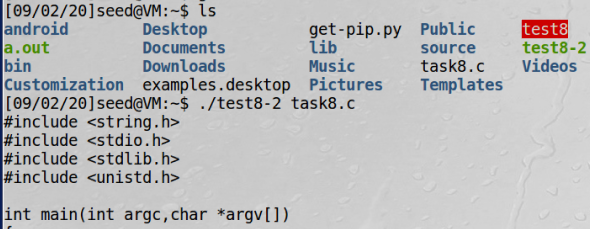


正常情况下，普通用户不可以删除root目录下的文件，但可以强制删除seed用户下由root创建的文件。

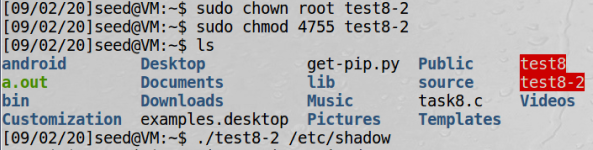
注释掉原代码中的system，取消注释exceve，增加函数库unistd.h：



普通编译：



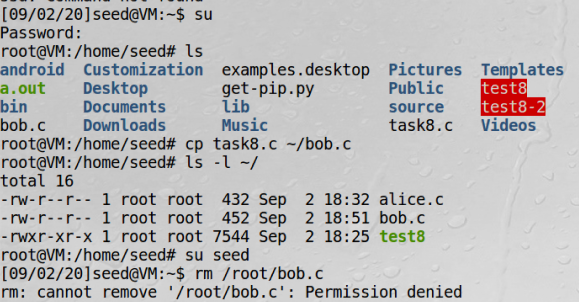
特权提升后编译：



**[09/02/20]seed@VM:~$ ./test8-2 /etc/shadow  
root:$6$IHB7yPjy$MvwFOiEtDMupi3uKFIjVQdLJHIX5UqeAFJvI4.570M8.QGKwh1KQYZ9D1aahnphLpoioLjtXtbEU44Fuf7U0l/:18507:0:99999:7:::  
daemon:\*:17212:0:99999:7:::  
bin:\*:17212:0:99999:7:::  
sys:\*:17212:0:99999:7:::  
sync:\*:17212:0:99999:7:::  
games:\*:17212:0:99999:7:::  
man:\*:17212:0:99999:7:::  
lp:\*:17212:0:99999:7:::  
mail:\*:17212:0:99999:7:::  
news:\*:17212:0:99999:7:::  
uucp:\*:17212:0:99999:7:::  
proxy:\*:17212:0:99999:7:::  
www-data:\*:17212:0:99999:7:::  
backup:\*:17212:0:99999:7:::  
list:\*:17212:0:99999:7:::  
irc:\*:17212:0:99999:7:::  
gnats:\*:17212:0:99999:7:::  
nobody:\*:17212:0:99999:7:::  
systemd-timesync:\*:17212:0:99999:7:::  
systemd-network:\*:17212:0:99999:7:::  
systemd-resolve:\*:17212:0:99999:7:::  
systemd-bus-proxy:\*:17212:0:99999:7:::  
syslog:\*:17212:0:99999:7:::  
\_apt:\*:17212:0:99999:7:::  
messagebus:\*:17212:0:99999:7:::  
uuidd:\*:17212:0:99999:7:::  
lightdm:\*:17212:0:99999:7:::  
whoopsie:\*:17212:0:99999:7:::  
avahi-autoipd:\*:17212:0:99999:7:::  
avahi:\*:17212:0:99999:7:::  
dnsmasq:\*:17212:0:99999:7:::  
colord:\*:17212:0:99999:7:::  
speech-dispatcher:!:17212:0:99999:7:::  
hplip:\*:17212:0:99999:7:::  
kernoops:\*:17212:0:99999:7:::  
pulse:\*:17212:0:99999:7:::  
rtkit:\*:17212:0:99999:7:::  
saned:\*:17212:0:99999:7:::  
usbmux:\*:17212:0:99999:7:::  
seed:$6$wDRrWCQz$IsBXp9.9wz9SGrF.nbihpoN5w.zQx02sht4cTY8qI7YKh00wN/sfYvDeCAcEo2QYzCfpZoaEVJ8sbCT7hkxXY/:17372:0:99999:7:::  
vboxadd:!:17372::::::  
telnetd:\*:17372:0:99999:7:::  
sshd:\*:17372:0:99999:7:::  
ftp:\*:17372:0:99999:7:::  
bind:\*:17372:0:99999:7:::  
mysql:!:17372:0:99999:7:::**

把文件拷贝到root目录下：





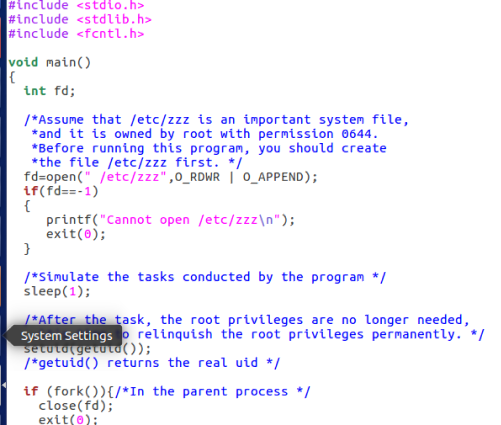
Exceve避免设置参数，以防泄露权限。

**分析：**特权提升通过root实现。

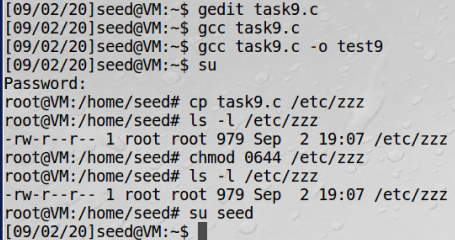
System相对而言比较危险，容易受到环境变量的影响。实验中通过改变PATH，System改为调用自己的ls程序。而Execve不存在这个问题，它不通过shell执行程序。

**Task 9.权能泄露**

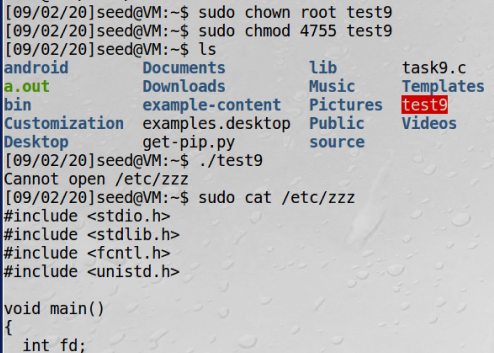
编写task9.c：



编译task9.c，创建 /etc/zzz，退出root：

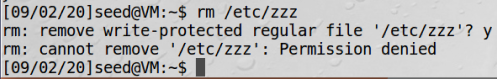


设置特权程序并运行：



可见文件已被修改。

删除 /etc/zzz：



请求被拒绝，普通权限不可以删除 /etc/zzz文件。

分析：Set-UID程序遵循最小特权原则，在不需要的时候永远放弃root特权，即当特权程序交给用户控制的时候，Set-UID程序可以通过setuid（）系统调用来放弃特权。

Set-UID改变调用进程的有效用户，根据保存的设置用户，设置有效用户，但有效用户可以通过setuid（）调用修改，修改后还可以通过保存的设置用户复原。

如果是root进行的Setuid调用，会同时修改实际用户，有效用户和保存的设置用户。