**Task1: Manipulating Environment Variables**

1. **Use printenv or env command to print out the environment variables. If you are interested in some particular environment variables, such as PWD, you can use "printenv PWD" or "env | grep PWD".**

[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=29360138

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1420

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/1728,unix/VM:/tmp/.ICE-unix/1728

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

LIBGL\_ALWAYS\_SOFTWARE=1

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

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-WUJdey2FBF

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

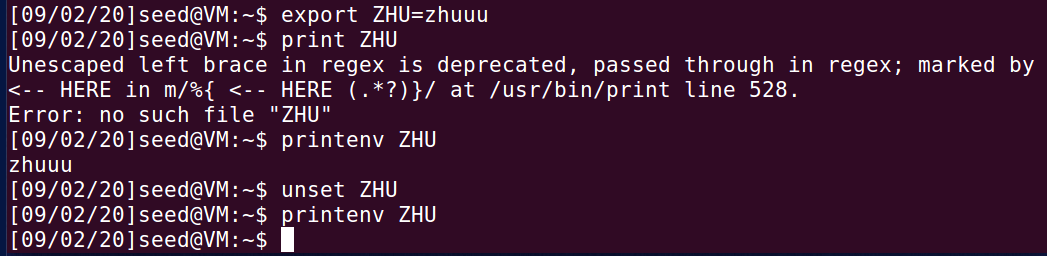
J2REDIR=/usr/lib/jvm/java-8-oracle/jre

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

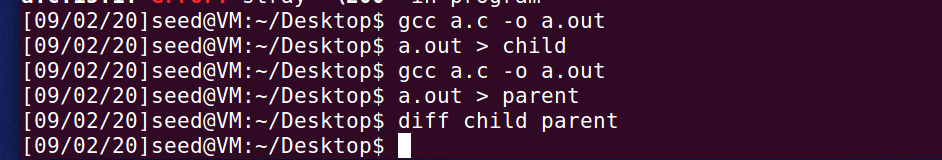
XAUTHORITY=/home/seed/.Xauthority

\_=/usr/bin/printenv

1. **Use export and unset to set or unset environment variables. It should be noted that these two commands are not seperate programs; they are two of the Bash’s internal commands (you will not be able to ﬁnd them outside of Bash).**

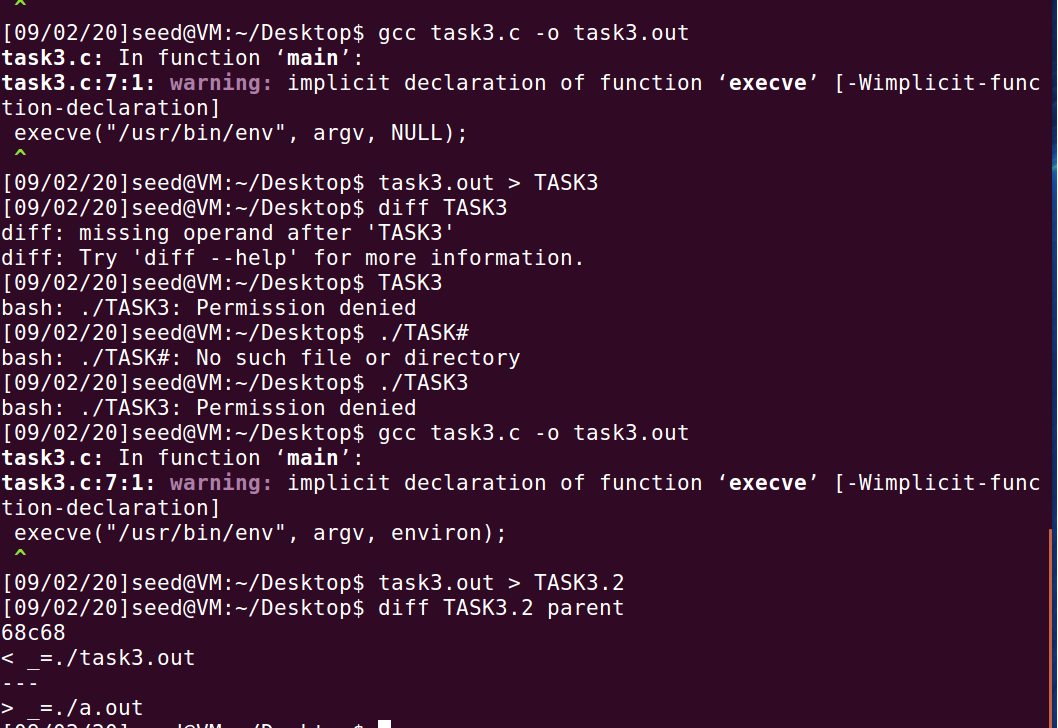
****

**Task2: PassingEnvironmentVariablesfromParentProcesstoChildProcess**

****

**用diff 命令可知，子进程和父进程的环境变量一致。说明环境变量可以被继承。**

**Task3: Environment Variablesand execve()**

****

使用execve("/usr/bin/env", argv, NULL); 命令时，输出的环境变量为空。这时因为NULL 强行更改了环境变量为空。当换成execve ("/usr/bin/env", argv, environ);时, 比较此次输出与上一个task的环境变量进行比较，除了最后的文件命名不一样，内容全部一样。说明此时，environ 参数赋予新程序与系统环境变量相同的环境变量。

**Task4: Environment Variablesand system()**

运行结果：

LESSOPEN=| /usr/bin/lesspipe %s

GNOME\_KEYRING\_PID=

USER=seed

LANGUAGE=en\_US

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

XDG\_SEAT=seat0

SESSION=ubuntu

XDG\_SESSION\_TYPE=x11

COMPIZ\_CONFIG\_PROFILE=ubuntu

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

SHLVL=1

LIBGL\_ALWAYS\_SOFTWARE=1

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

HOME=/home/seed

QT4\_IM\_MODULE=xim

OLDPWD=/home

DESKTOP\_SESSION=ubuntu

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-WUJdey2FBF

GNOME\_KEYRING\_CONTROL=

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

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

IM\_CONFIG\_PHASE=1

SESSIONTYPE=gnome-session

LOGNAME=seed

GTK\_IM\_MODULE=ibus

WINDOWID=29360138

\_=./task4.out

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

XDG\_SESSION\_ID=c1

TERM=xterm-256color

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

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1728,unix/VM:/tmp/.ICE-unix/1728

GDM\_LANG=en\_US

XDG\_MENU\_PREFIX=gnome-

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

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

DISPLAY=:0

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

SHELL=/bin/bash

QT\_ACCESSIBILITY=1

GDMSESSION=ubuntu

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

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

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1420

XDG\_VTNR=7

QT\_IM\_MODULE=ibus

PWD=/home/seed/Desktop

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

VTE\_VERSION=4205

JOB=dbus

**Task5: EnvironmentVariableand Set-UID Programs**

**Step 1 ： 执行结果如下**

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=29360138

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1420

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/1728,unix/VM:/tmp/.ICE-unix/1728

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/Desktop

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

LIBGL\_ALWAYS\_SOFTWARE=1

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

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-WUJdey2FBF

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

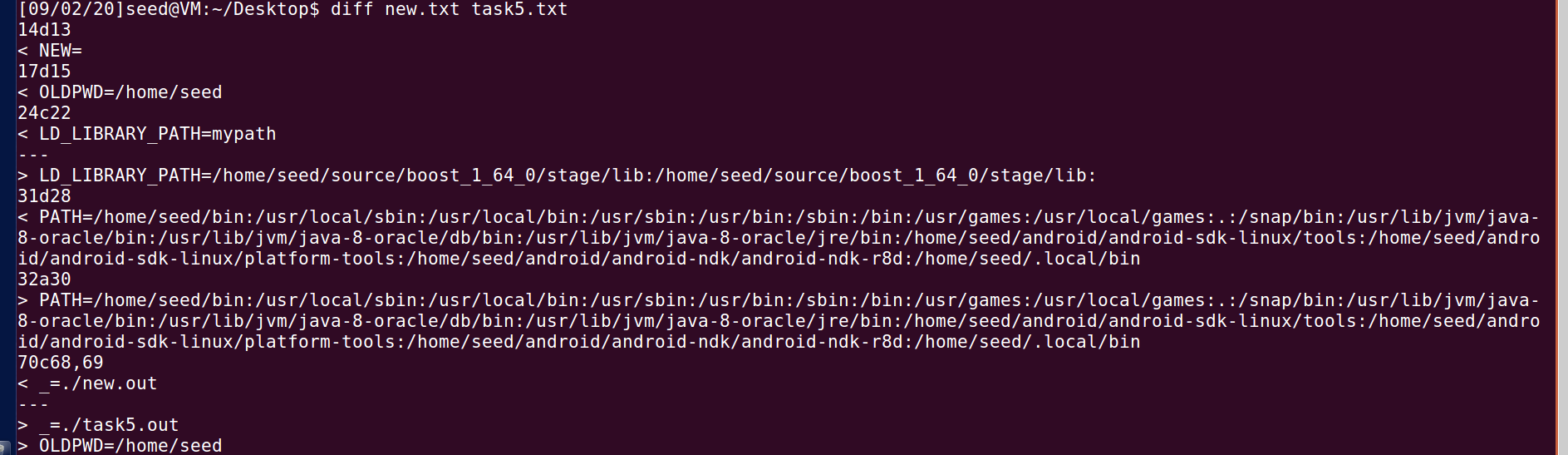
\_=./task5.out

OLDPWD=/home/seed

**Step 2 执行命令**



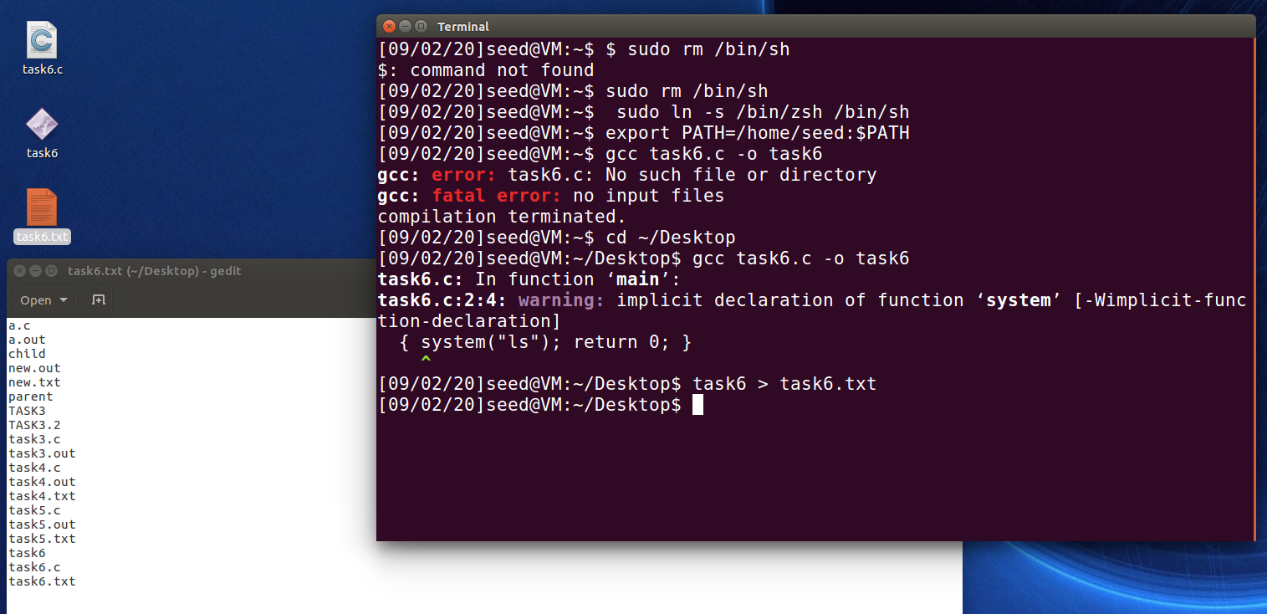
**Step 3：执行结果如下：diff 比较更改前后的区别**



可以看到export 的三个变量都有更改。

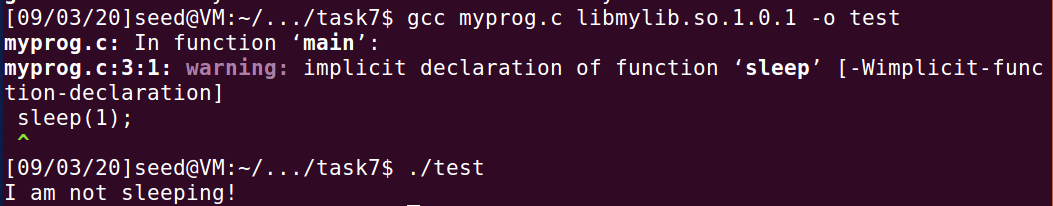
**Task6: The PATH Environmen tVariableand Set-UID Programs**

安装shell用来执行system 函数里的ls命令，改变权限为root 并设置为set-uid程序。可以利用该程序在当前路径下执行ls并输出不必非要使用/bin/ls，结果如下

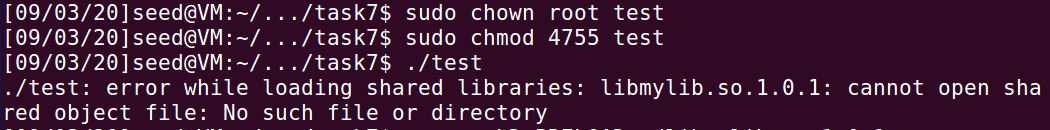
****

**Task7: The LD PRELOAD Environment Variableand Set-UID Programs**

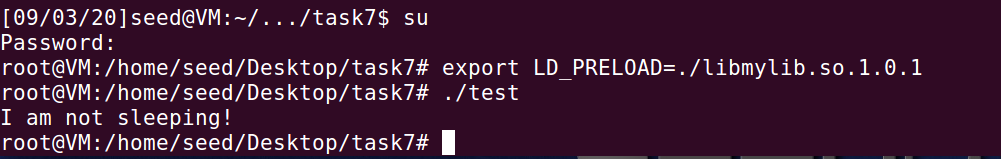
1. **普通用户，链接动态链接库 输出如下**

****

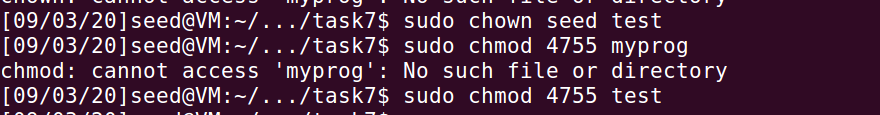
1. **普通用户，将程序设置为set-uid程序，程序报错**

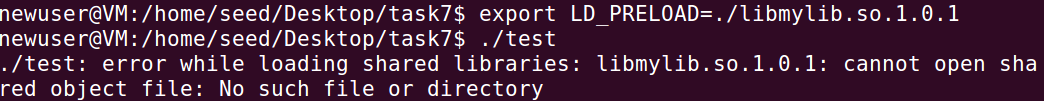
****

1. **在root模式下修改LD\_PRELOAD 环境变量。输出如下：**

****

1. **将可执行文件所有权改为新用户，并在seed下exprot动态库并执行：**



****

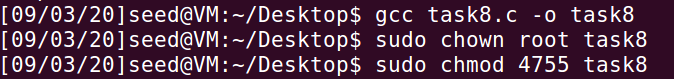
**程序无法执行。程序调用者与程序owner不一致时，ruid与euid不一致时，便不会链接到动态链接库。**

**Task8: Invoking External Programs Using system() versus execve()**

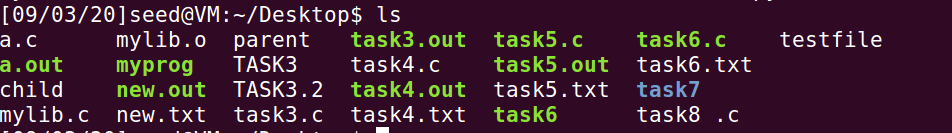
1. **设置文件task8为只读文件**

****

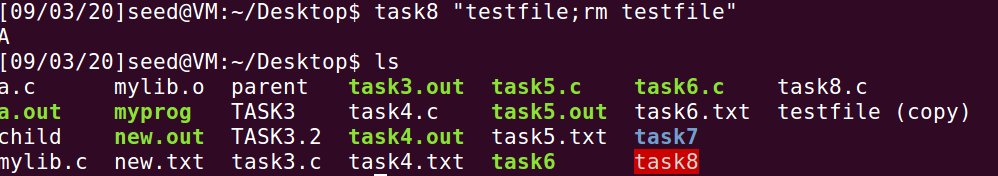
1. **编译task8.c, 并将task8 改为root用户的set uid 程序**

****

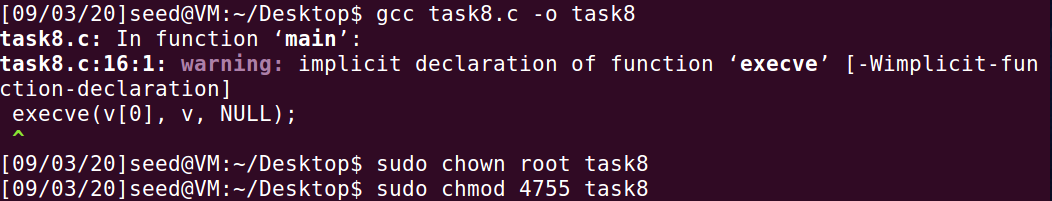
1. **查看此时的文件列表，可以查到有testfile文件的存在**

****

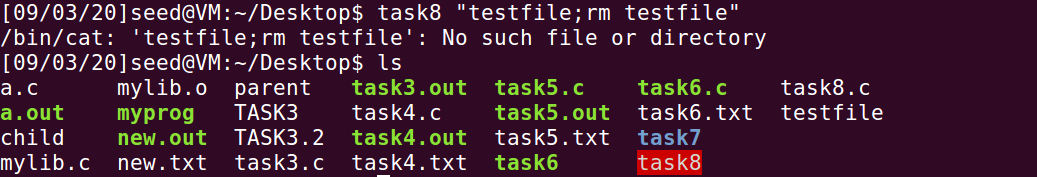
1. **运行task8，发现删除了不可写文件testfile**

****

1. **使用execuve（）函数，重新编译，并设可执行文件为root用户的set uid程序**

****

1. **再次尝试删除文件，提示不存在该文件，删除失败**

****

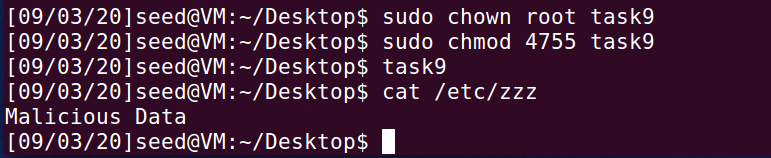
1. **system()由于是调用shell执行cmd，且未对输入进行约束，导致注入攻击能够成功；而execve()不调用shell，所以注入失败。**

**Task9: Capability Leaking**

1. **创建etc/zzz，并设置为root拥有，0644权限**

****

1. **编译test9.c 并把可执行文件设置为root拥有的set uid 程序，执行task9.发现文件被写入了Malicious Data**

****

1. **在此实验中，尽管启动进程的用户不再拥有特权，但是由于该进程是fork出的进程，继承了父进程的特权，所以执行该文件仍然可以对zzz文件进行改写**