**实验一：Environment Variable and Set-UID Program Lab**

57117222 舒卓卓

**任务一**：Manipulating Environment Variables

1. 使用printenv打印环境变量

所得结果如下：[08/31/20]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=60817418

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1467

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/1747,unix/VM:/tmp/.ICE-unix/1747

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-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

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

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-AesBXiWz7X

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

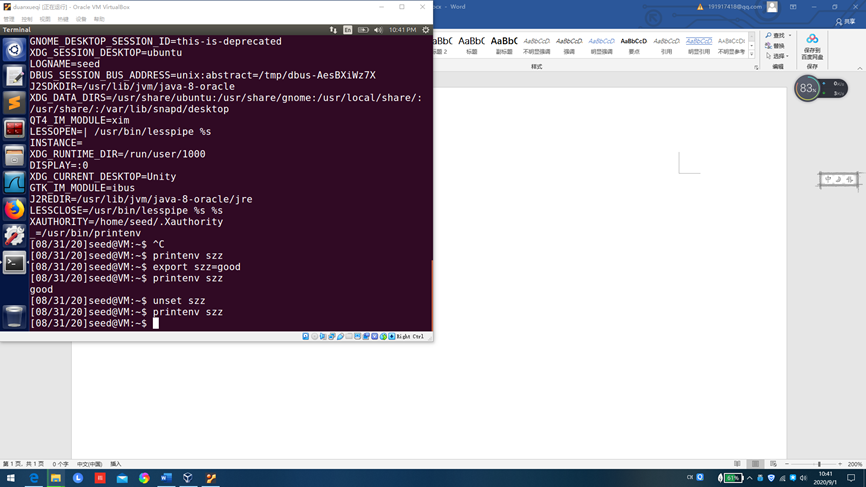
LESSCLOSE=/usr/bin/lesspipe %s %s

XAUTHORITY=/home/seed/.Xauthority

\_=/usr/bin/printenv

2.使用export和unset设置和取消环境变量

如图所示printenv szz为空，之后将其设置为good，再次print为good，unset之后print又变为空



**任务二**：Task2: Passing Environment Variables from Parent Process to Child Process

1.注释掉default分支的printenv，保留case 0分支的printenv，打印子进程的环境变量，结果与task1完全一致，将其保留在child1中

2. 注释掉case 0分支的printenv，保留default分支的printenv，打印子进程的环境变量，结果与task1完全一致，将其保留在child2中

3.使用diff child1 child2 查看两个文件差异，输出为空，两次输出没有区别。

结论：通过比较这两个文件，可以发现，这两个文件输出的环境变量完全相同。说明原环境变量被子进程完全继承。通过man fork，对fork函数做了进一步了解。fork函数通过系统调用创建一个与原来进程几乎完全相同的进程，子进程自父进程继承了进程的资格，环境，堆栈与内存根目录等；但是子进程没有继承父进程的某些特性，比如父进程号，文件描述符，在tms结构中的系统时间，资源使用等。

**任务三**：Environment Variables and execve()

1. 将NULL作为第三个参数传给execve，编译后输出运行为空
2. 将外部变量environ作为第三个参数传给execve，运行后输出与task1一样，除了环境变量为可执行程序task3
3. 结论：使用execve创建的子进程，环境变量取决于execve的第三个参数，第三个参数为字符串数组其中元素是char型字符串，表示当前环境变量

**任务四**：Environment Variables and system()

1. 使用命令system(“ /usr/bin/env”)后，除了环境变量变为可执行程序task4其他输出结果与task1完全一致。
2. 说明system()创建子进程会继承父进程的所有环境变量。

**任务五**：Task 5: Environment Variable and Set-UID Programs

1.运行对应程序可得结果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=60817418

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1467

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/1747,unix/VM:/tmp/.ICE-unix/1747

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-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

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

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-AesBXiWz7X

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

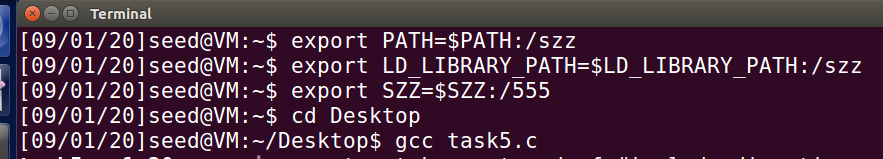
J2REDIR=/usr/lib/jvm/java-8-oracle/jre

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

XAUTHORITY=/home/seed/.Xauthority

OLDPWD=/home/seed

\_=./a.out

1. 进入shell运行命令 sudo chown root task5.c sudo chmod task5.c
2. 设置对应的环境变量

5.运行对应程序所得结果如图所示

[09/01/20]seed@VM:~/Desktop$ /a.out

bash: /a.out: No such file or directory

[09/01/20]seed@VM:~/Desktop$ ./a.out

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=60817418

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1467

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::/szz

SZZ=:/555

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/1747,unix/VM:/tmp/.ICE-unix/1747

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:/szz

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-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

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

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-AesBXiWz7X

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

OLDPWD=/home/seed

\_=./a.out

以上三个被定义的环境变量全部被包括在shell中

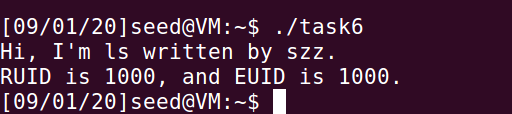
**任务六**： The PATH Environment Variable and SetUID Programs

1. 编写对应程序

#include <stdio.h> #include <sys/types.h> #include <unistd.h>

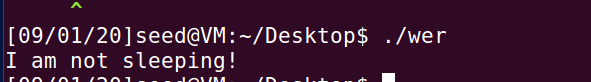
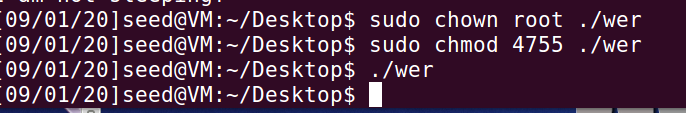
int main() { printf("Hi, I'm ls written by szz.\nRUID is %d, and EUID is %d.\n", getuid(), geteuid()); return 0; }

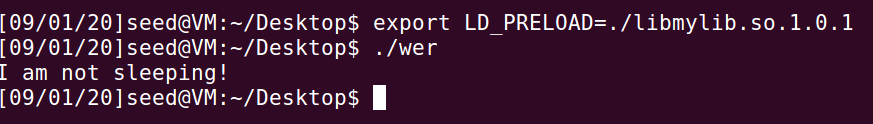
1. 所得结果为：



1. seed的uid为1000.root的uid为1000
2. 调用task6时会自动继承当前环境变量，此时path包含了/home/seed，同时优先级更高，使用相对路径是调用ls时候，会在path中寻找得到一个/home/seed/ls，因此调用我们的程序

**任务七**： The LD\_PRELOAD Environment Variable and Set-UID Programs

1. 
2. 

3. 

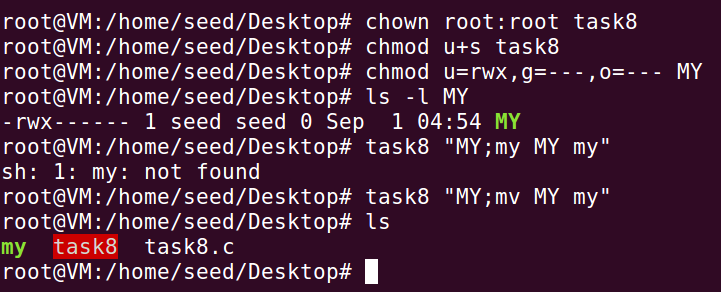
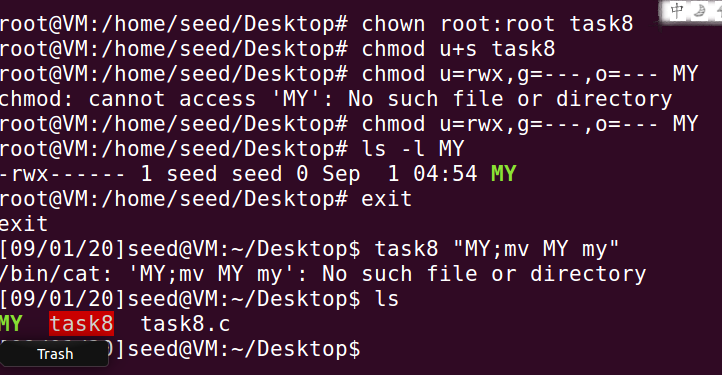
4.结论：以普通用户的身份运行myprog程序时，输出：I am not sleeping!

以普通用户运行拥有root权限的myprog程序时，无输出。

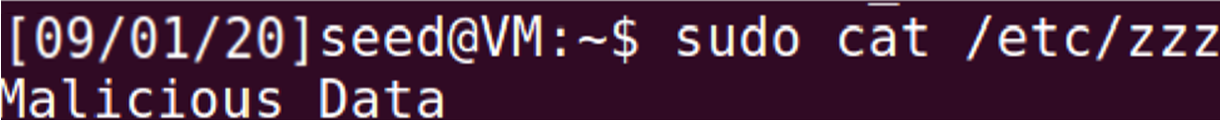
在user2用户中再次设置LD\_PRELOAD环境变量并运行myprog程序时，输出：I am not sleeping!

导致他们不同的原因就在于LD\_PRELOAD环境变量。LD\_PRELOAD环境变量是Unix动态链接库的世界中的一个环境变量，它可以影响程序的运行时的链接，它允许你定义在程序运行前优先加载的动态链接库。这个功能主要是用来有选择性的载入不同动态链接库中的相同函数。在该实验中，mylib.c通过sleep函数，生成了一个libmylib.so.1.0.1链接库。然后将该链接库添加到LD\_PRELOAD环境变量上。比较这三次实验，第一次和第三次实验myprog程序均具有seed用户权限，而在seed用户的LD\_PRELOAD环境变量中也添加了该链接库

**任务八**：Invoking External Programs Using system() versus execve()

1. 保存代码为task8.c文件，切换为root用户，将其编译为task8，并设置其所有者为root，赋予SUID特殊权限。
2. 新建一个名为MY的文件，并设置其权限为仅root用户可读、写、执行
3. 执行task8，发现原本只有root用户才具有读、写、执行的MY文件，已经更名为my
4. 
5. 重新编译task8文件，并设置其所有者为root，赋予SUID特殊权限。新建一个名为MY的文件，并设置其权限为仅root用户可读、写、执行
6. 执行task8，发现上述攻击已经失效
7. 
8. 分析其原因，是因为execve()函数会把file; mv file file\_new 看成是一个文件名，系统会提示不存在这个文件，system()则不会。

**任务9** ：Capability Leaking

1. 

2. 先切换为root用户，创建/etc/zzz，设置其为只有root用户可以写入。保存代码为task.c文件，将其编译为task，并赋予SUID特殊权限。

3. 执行task，查看内容，发现被写入信息

4. 分析其原因是因为其在取消权限前并没有关闭文件，导致seed用户任然可以进行root用户才可以执行的写入操作。