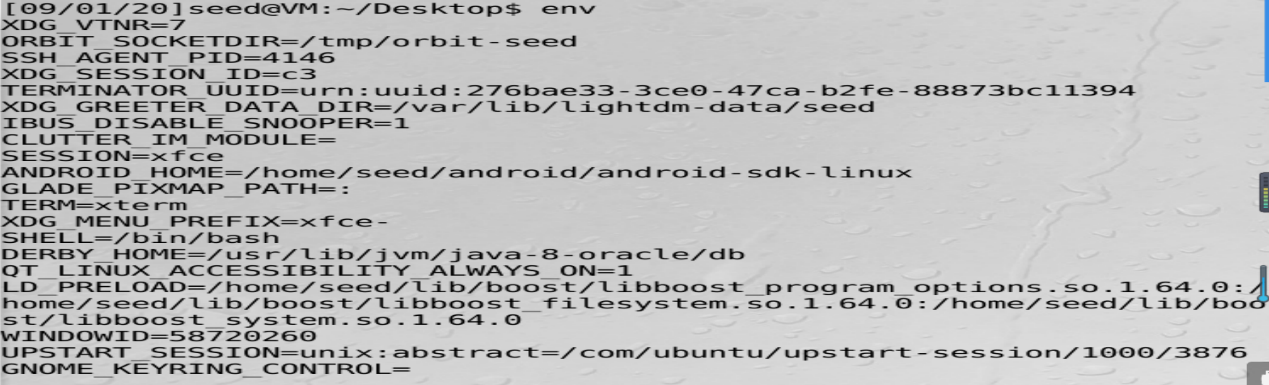
实验报告

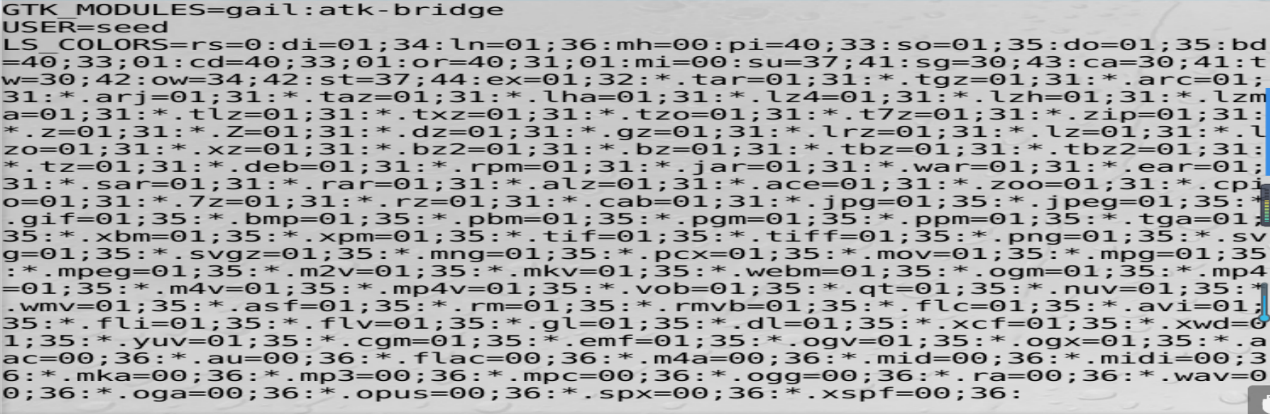
57118102 曹钰

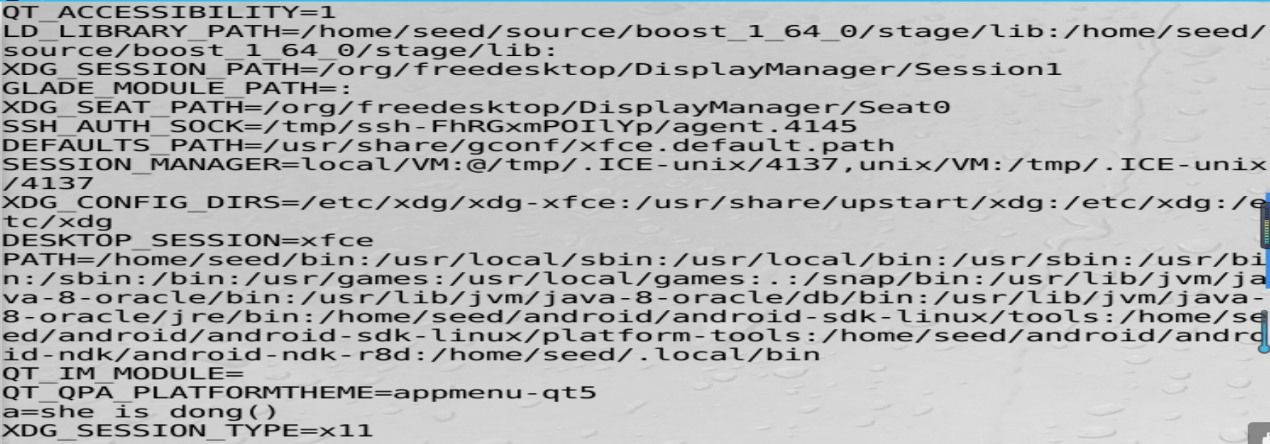
Task1

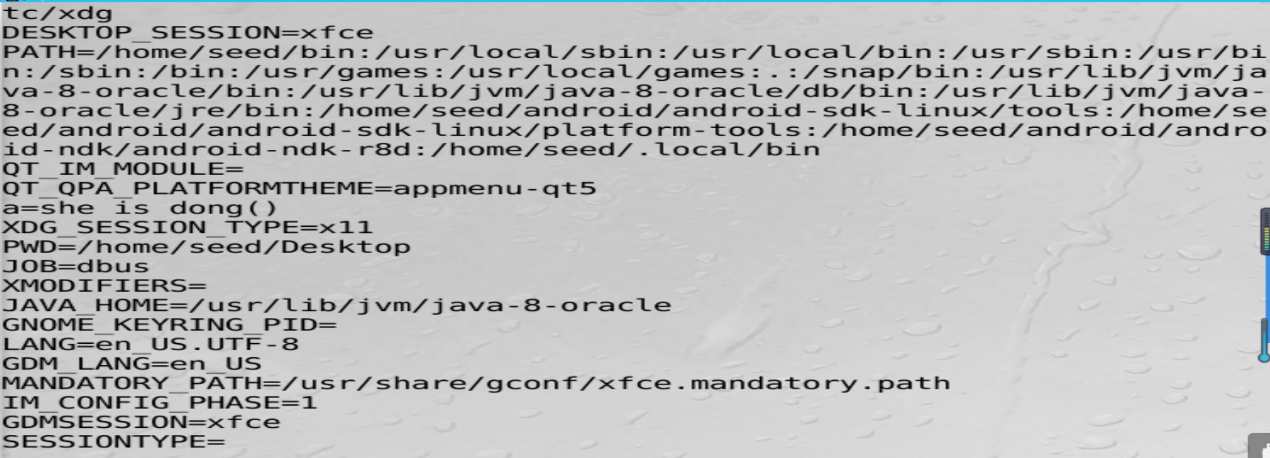
实验过程

1. 使用env指令，列出所有环境变量

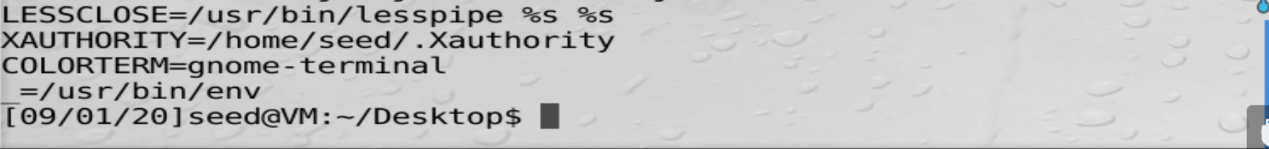




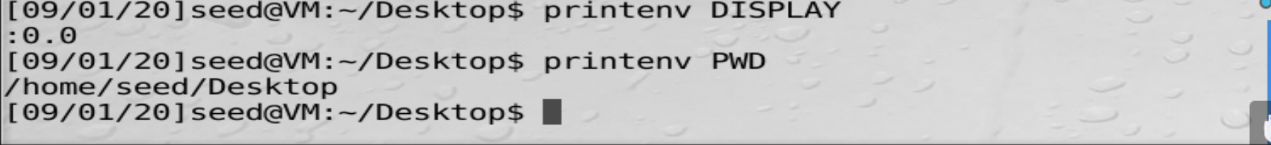




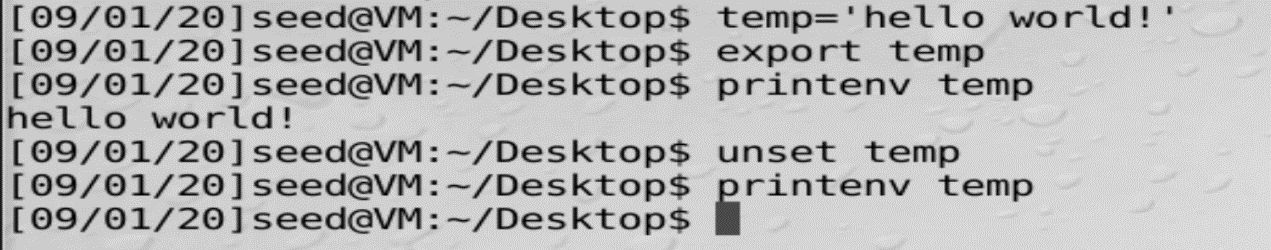




2．显示特定的环境变量，由于env不能达到这个目的，所以使用printenv指令



3．增添一个新的环境变量然后删掉它



Task2

实验过程

1. 编译所给程序并把输出保存在一个文件里



输出为环境变量，与env指令相同

文件中保存的内容为：

XDG\_VTNR=7

ORBIT\_SOCKETDIR=/tmp/orbit-seed

SSH\_AGENT\_PID=1722

XDG\_SESSION\_ID=c1

TERMINATOR\_UUID=urn:uuid:efe40ca3-38ea-4ebf-89fa-43a45e6631ef

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

IBUS\_DISABLE\_SNOOPER=1

CLUTTER\_IM\_MODULE=

SESSION=xfce

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

GLADE\_PIXMAP\_PATH=:

TERM=xterm

XDG\_MENU\_PREFIX=xfce-

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=58720260

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1448

GNOME\_KEYRING\_CONTROL=

GTK\_MODULES=gail:atk-bridge

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

GLADE\_MODULE\_PATH=:

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

SSH\_AUTH\_SOCK=/tmp/ssh-G1shziEYxQ7c/agent.1721

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

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1685,unix/VM:/tmp/.ICE-unix/1685

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

DESKTOP\_SESSION=xfce

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=

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed/programs

JOB=dbus

XMODIFIERS=

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/xfce.mandatory.path

IM\_CONFIG\_PHASE=1

GDMSESSION=xfce

SESSIONTYPE=

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=en\_US

UPSTART\_INSTANCE=

XDG\_SESSION\_DESKTOP=xfce

UPSTART\_EVENTS=started xsession

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-n23tlBhZ58

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

XDG\_DATA\_DIRS=/usr/share/xfce:/usr/share/xfce4:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop:/usr/share

QT4\_IM\_MODULE=

LESSOPEN=| /usr/bin/lesspipe %s

INSTANCE=

UPSTART\_JOB=startxfce4

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

DISPLAY=:0.0

GLADE\_CATALOG\_PATH=:

XDG\_CURRENT\_DESKTOP=XFCE

GTK\_IM\_MODULE=

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

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

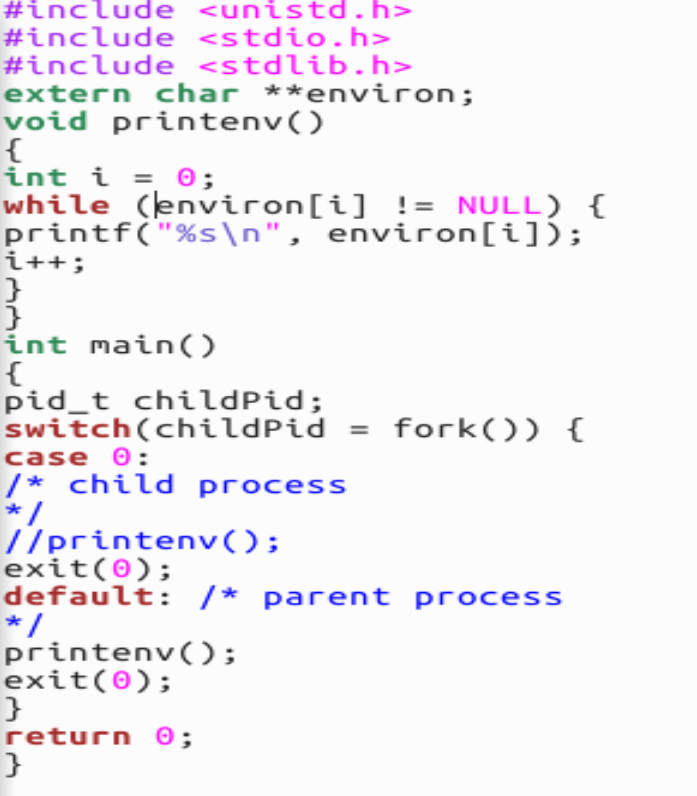
XAUTHORITY=/home/seed/.Xauthority

COLORTERM=gnome-terminal

\_=./a.out

OLDPWD=/home/seed/Desktop

1. 注释掉子进程中的printenv()，在父进程中添加printenv()指令，重新编译并将结果保存在另一个文件中





文件中的内容为：

XDG\_VTNR=7

ORBIT\_SOCKETDIR=/tmp/orbit-seed

SSH\_AGENT\_PID=1722

XDG\_SESSION\_ID=c1

TERMINATOR\_UUID=urn:uuid:efe40ca3-38ea-4ebf-89fa-43a45e6631ef

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

IBUS\_DISABLE\_SNOOPER=1

CLUTTER\_IM\_MODULE=

SESSION=xfce

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

GLADE\_PIXMAP\_PATH=:

TERM=xterm

XDG\_MENU\_PREFIX=xfce-

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=58720260

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1448

GNOME\_KEYRING\_CONTROL=

GTK\_MODULES=gail:atk-bridge

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

GLADE\_MODULE\_PATH=:

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

SSH\_AUTH\_SOCK=/tmp/ssh-G1shziEYxQ7c/agent.1721

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

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1685,unix/VM:/tmp/.ICE-unix/1685

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

DESKTOP\_SESSION=xfce

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=

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed/programs

JOB=dbus

XMODIFIERS=

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/xfce.mandatory.path

IM\_CONFIG\_PHASE=1

GDMSESSION=xfce

SESSIONTYPE=

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=en\_US

UPSTART\_INSTANCE=

XDG\_SESSION\_DESKTOP=xfce

UPSTART\_EVENTS=started xsession

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-n23tlBhZ58

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

XDG\_DATA\_DIRS=/usr/share/xfce:/usr/share/xfce4:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop:/usr/share

QT4\_IM\_MODULE=

LESSOPEN=| /usr/bin/lesspipe %s

INSTANCE=

UPSTART\_JOB=startxfce4

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

DISPLAY=:0.0

GLADE\_CATALOG\_PATH=:

XDG\_CURRENT\_DESKTOP=XFCE

GTK\_IM\_MODULE=

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

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

XAUTHORITY=/home/seed/.Xauthority

COLORTERM=gnome-terminal

\_=./task22

OLDPWD=/home/seed/Desktop

1. 用diff比较两个输出文件的内容



结论：两个文件中除了\_这个环境变量外其他的环境变量都相同，这是因为我把修改前后的两版代码保存到不两个不同的可执行文件里了。而因为环境变量近似于全局变量，所以父进程和子进程可以共享环境变量，所以其他都相同。

**Task3**

实验过程

1. 编译并执行所给的程序



没有输出

1. 将所给代码中的execve函数的参数NULL用environ替换，重新编译并执行



输出为

XDG\_VTNR=7

ORBIT\_SOCKETDIR=/tmp/orbit-seed

SSH\_AGENT\_PID=3753

XDG\_SESSION\_ID=c5

TERMINATOR\_UUID=urn:uuid:d5f43843-265e-4005-b805-f68ee32ebda4

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

IBUS\_DISABLE\_SNOOPER=1

CLUTTER\_IM\_MODULE=

SESSION=xfce

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

GLADE\_PIXMAP\_PATH=:

TERM=xterm

XDG\_MENU\_PREFIX=xfce-

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=58720260

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/3483

GNOME\_KEYRING\_CONTROL=

GTK\_MODULES=gail:atk-bridge

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/Session2

GLADE\_MODULE\_PATH=:

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

SSH\_AUTH\_SOCK=/tmp/ssh-gy9l91aK8LCH/agent.3752

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

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/3744,unix/VM:/tmp/.ICE-unix/3744

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

DESKTOP\_SESSION=xfce

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=

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed/programs/task3

JOB=dbus

XMODIFIERS=

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/xfce.mandatory.path

IM\_CONFIG\_PHASE=1

GDMSESSION=xfce

SESSIONTYPE=

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=en\_US

UPSTART\_INSTANCE=

XDG\_SESSION\_DESKTOP=xfce

UPSTART\_EVENTS=started xsession

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-hzMwi9SH90

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

XDG\_DATA\_DIRS=/usr/share/xfce:/usr/share/xfce4:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop:/usr/share

QT4\_IM\_MODULE=

LESSOPEN=| /usr/bin/lesspipe %s

INSTANCE=

UPSTART\_JOB=startxfce4

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

DISPLAY=:0.0

GLADE\_CATALOG\_PATH=:

XDG\_CURRENT\_DESKTOP=XFCE

GTK\_IM\_MODULE=

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

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

XAUTHORITY=/home/seed/.Xauthority

COLORTERM=gnome-terminal

\_=./task32

OLDPWD=/home/seed/programs/task2

是列出了环境变量

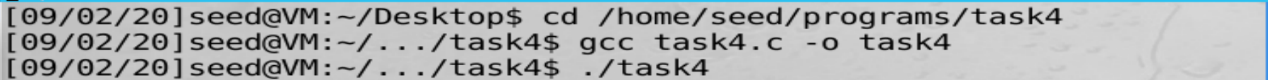
结论

execve()函数是重新开一个新的程序，这个新的程序的运行于原来的程序已经没有关系了，而原来函数的环境变量并不能由新程序直接继承，需要通过execve()函数的第三个参数传递。

**Task4**

实验过程

编译并执行所给程序



输出为环境变量

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

SSH\_AGENT\_PID=1726

SESSION=xfce

XDG\_SESSION\_TYPE=x11

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=

OLDPWD=/home/seed/Desktop

DESKTOP\_SESSION=xfce

QT\_LINUX\_ACCESSIBILITY\_ALWAYS\_ON=1

GTK\_MODULES=gail:atk-bridge

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

INSTANCE=

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-VysWbn81vY

GLADE\_MODULE\_PATH=:

COLORTERM=gnome-terminal

GNOME\_KEYRING\_CONTROL=

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

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

IM\_CONFIG\_PHASE=1

SESSIONTYPE=

UPSTART\_JOB=startxfce4

LOGNAME=seed

GTK\_IM\_MODULE=

WINDOWID=60817412

\_=./task4

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

XDG\_SESSION\_ID=c1

TERM=xterm

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

GLADE\_PIXMAP\_PATH=:

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

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1689,unix/VM:/tmp/.ICE-unix/1689

GDM\_LANG=en\_US

XDG\_MENU\_PREFIX=xfce-

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

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

DISPLAY=:0.0

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=XFCE

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=

XDG\_SESSION\_DESKTOP=xfce

XAUTHORITY=/home/seed/.Xauthority

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

SSH\_AUTH\_SOCK=/tmp/ssh-sddj3CM65IIk/agent.1725

GLADE\_CATALOG\_PATH=:

TERMINATOR\_UUID=urn:uuid:12ee8eed-804f-4998-bdb6-e08d074e04d2

SHELL=/bin/bash

QT\_ACCESSIBILITY=1

GDMSESSION=xfce

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

UPSTART\_EVENTS=started xsession

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1450

XDG\_VTNR=7

QT\_IM\_MODULE=

PWD=/home/seed/programs/task4

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

CLUTTER\_IM\_MODULE=

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

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

XDG\_DATA\_DIRS=/usr/share/xfce:/usr/share/xfce4:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop:/usr/share

JOB=dbus

**Task5**

实验报告

1. 写下所给程序
2. 编译所给程序，并把程序的拥有权交给root，并将程序改为Set-UID程序



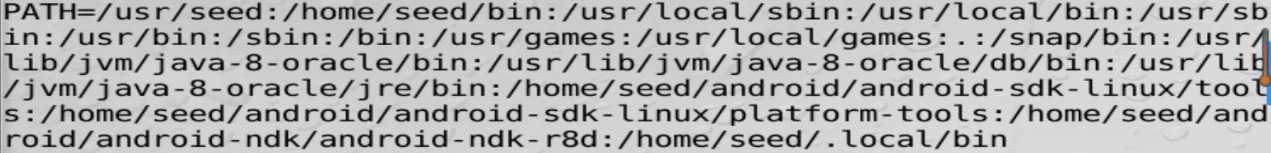


用command指令重新设定环境变量



执行step2中的Set-UID程序







发现：所有之前设置的环境变量都可以在程序中呈现

**Task6**

实验过程

编译所给代码并把程序设置成Set-UID程序



可以获得root权限

先把/bin/sh链接到zsh



再把/bin/sh拷贝到临时文件夹temp里，并且改名为ls



再把环境变量PATH更改为temp的路径



在执行刚才的程序，这时获得root权限

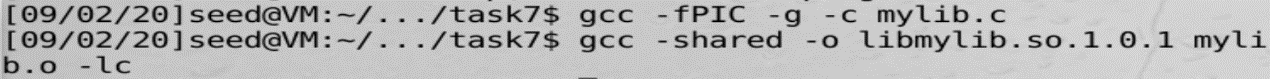


**Task7**

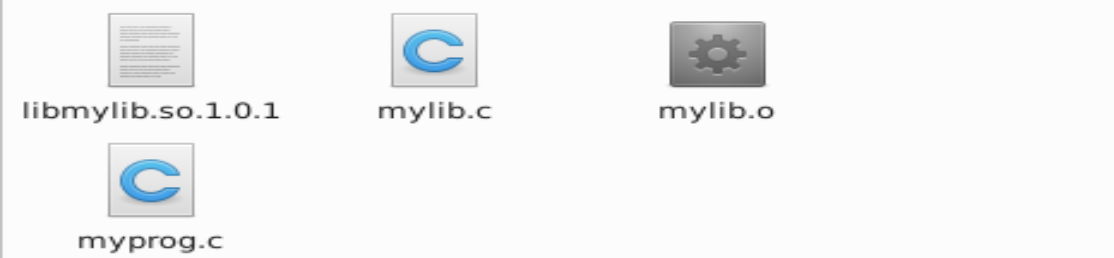
实验过程

1.









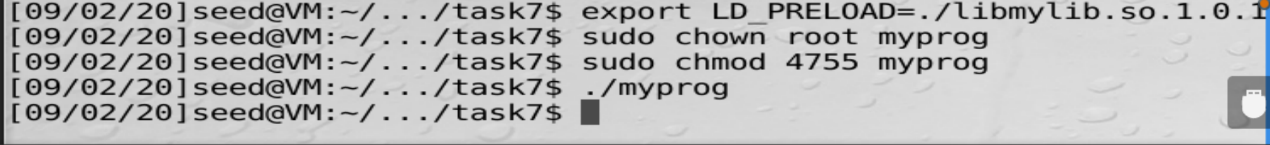


2.

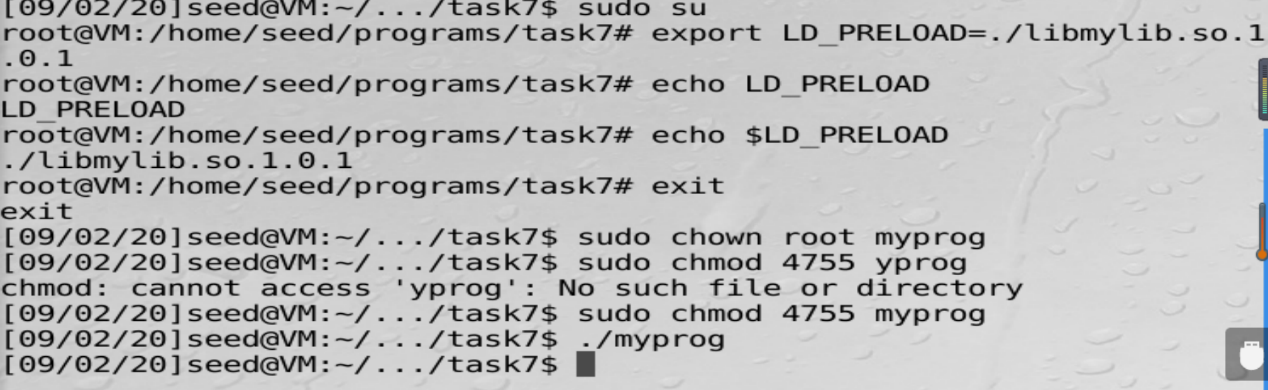
以普通用户的身份运行



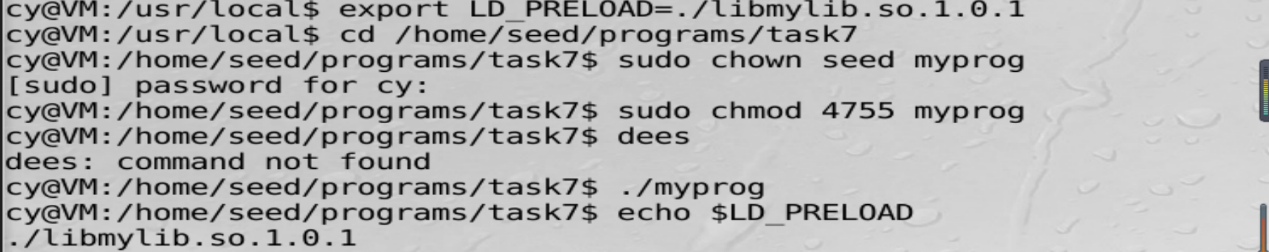
以普通用户运行拥有root权限的myprog



把myprog变成setuid程序，在root用户里修改LD\_PRELOAG



使myprog成为一个Set-UID user1程序，在user2用户（非root用户）中再次设置LD\_PRELOAD环境变量，运行myprog程序



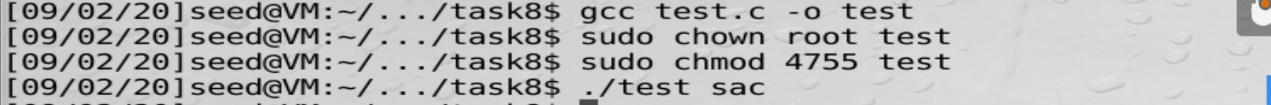
只有自己创建程序自己去运行才会使用LD\_PRELOAD环境变量两个独立程序的环境变量并不相互继承影响

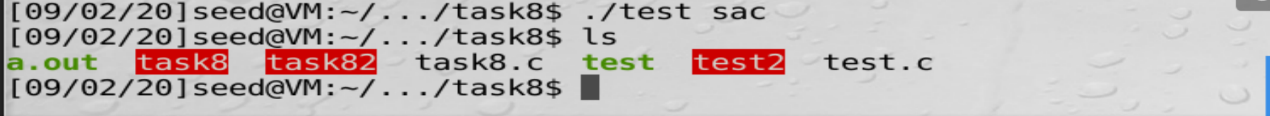
**Task8**

实验步骤

1.

测试删除文件

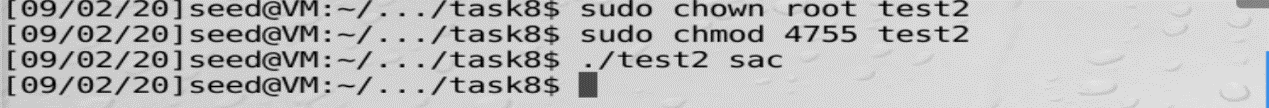


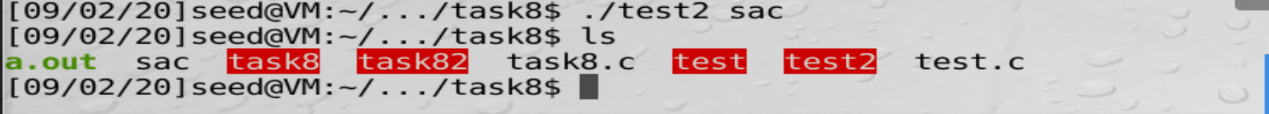


成功删除

2.





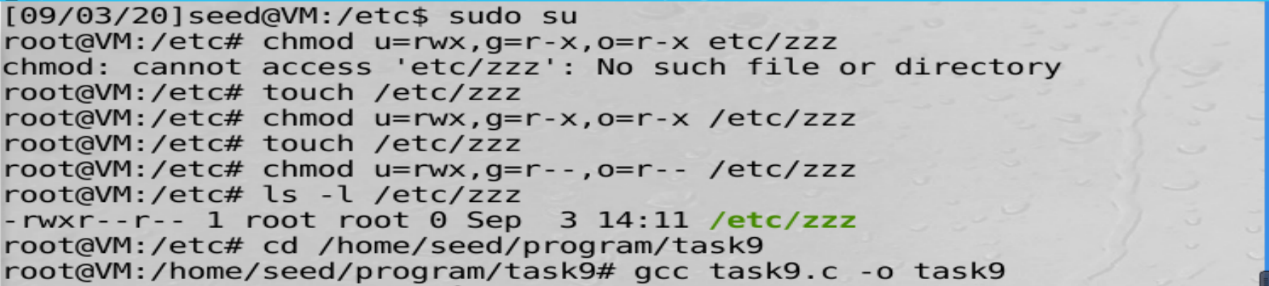


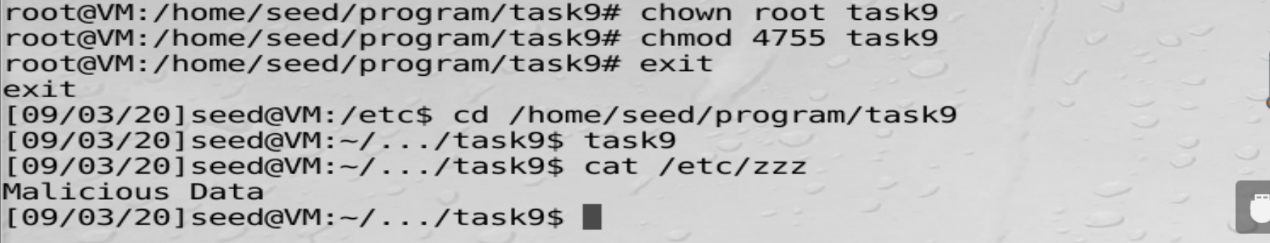
未能成功删除文件

因为system()函数直接链接到bash，出于保护机制会令程序解除setuid

**Task9**

实验过程





文件被改写，分析是因为取消权限后没有关闭文件，导致普通用户依然可以进行root用户才可以进行的操作