

## Task 1 : Manipulating Environment Variables

Output when the command **env** is used to print all the environment variables:

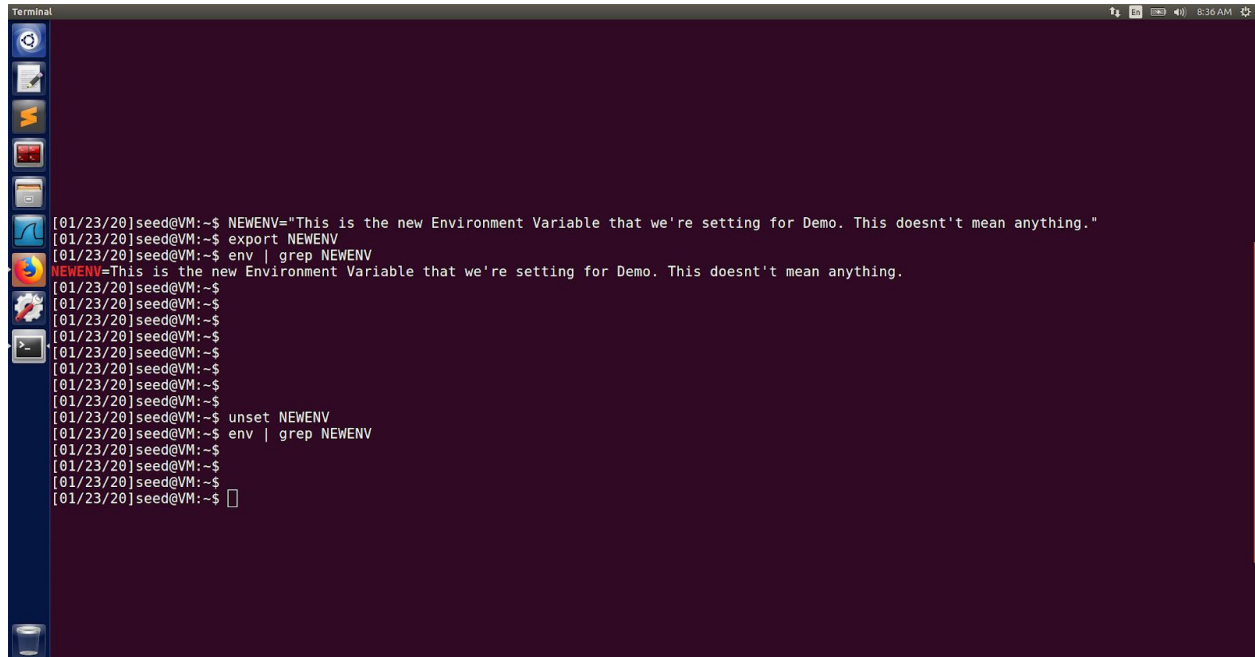
```
Terminal
JOB=unity-settings-daemon
XMODIFIERS=@im=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
COM_LANG=en_US
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
SHLVL=1
HOME=/home/seed
XDG_SEAT=seat0
LANGUAGE=en_US
LIBGL_ALWAYS_SOFTWARE=1
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
UPSTART_INSTANCE=
UPSTART_EVENTS=xsession started
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-1LUCxh5Yc0
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
=/usr/bin/env
[01/23/20]seed@VM:~$
```

Output when we execute grep command to search for a particular command containing the relevant search keyword:

```
Terminal
[01/23/20]seed@VM:~$ env | grep UPSTART
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1575
UPSTART_INSTANCE=
UPSTART_EVENTS=xsession started
UPSTART_JOB=unity7
[01/23/20]seed@VM:~$
```

***Setting and Unsetting an Environment Variable.***

Here, we're setting a new environment variable using the export command and unsetting the same using the unset command. It is cross verified using the grep command on env with the variable name we've set.

A terminal window with a dark purple background and a blue sidebar on the left containing various application icons. The terminal shows a series of commands and their outputs. The user sets an environment variable 'NEWENV' to a specific string, exports it, and then uses 'env | grep NEWENV' to verify its presence. After several empty prompts, the user unsets the variable and runs the same grep command again, which returns no output.

```
[01/23/20]seed@VM:~$ NEWENV="This is the new Environment Variable that we're setting for Demo. This doesn't mean anything."
[01/23/20]seed@VM:~$ export NEWENV
[01/23/20]seed@VM:~$ env | grep NEWENV
NEWENV=This is the new Environment Variable that we're setting for Demo. This doesn't mean anything.
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ unset NEWENV
[01/23/20]seed@VM:~$ env | grep NEWENV
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$ 
[01/23/20]seed@VM:~$
```

## Task 2: Passing Environment Variables from Parent Process to Child Process

- Step 1:** We execute the given code and the output is the list of all the environment variables.

```

/home/seed/ENV_SET_UID/childProcessOutput - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
1 ANDROID_HOME=/home/seed/android/android-sdk-linux
2 SHELL=/bin/bash
3 TEMP=/tmp/.X56color
4 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
5 USER=root
6 LS_COLORS=di=01:34:ln=01:36:mh=00:pi=40:33:so=01:35:do=01:35:bd=40:33:cd=40:33: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:*
7 LD_LIBRARY_PATH=/home/seed/source/boost_1.64.0/stage/lib:/home/seed/source/boost_1.64.0/stage/lib
8 SUDO_UID=1000
9 SUDO_USER=root
10 PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d
11 MAIL=/var/mail/root
12 PWD=/home/seed/ENV_SET_UID
13 JAVA_HOME=/usr/lib/jvm/java-8-oracle
14 HOME=/root
15 SUDO_COMMAND=/bin/bash
16 SHLVL=2
17 LANG=en_US.UTF-8
18 LOGNAME=root
19 LESSOPEN=| /usr/bin/lesspipe %s
20 DISPLAY=:0
21 SUDO_UID=1000
22 LESSCLOSE=| /usr/bin/lesspipe %s %s
23 XAUTHORITY=/home/seed/.Xauthority
24 OLDPWD=/home/seed

```

- Step 2:** Here we execute the parent process and from the output it is evident that the child process inherits the environment variables from the parent process.

```

/home/seed/ENV_SET_UID/parentProcessOutput - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
1 ANDROID_HOME=/home/seed/android/android-sdk-linux
2 SHELL=/bin/bash
3 TEMP=/tmp/.X56color
4 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
5 USER=root
6 LS_COLORS=di=01:34:ln=01:36:mh=00:pi=40:33:so=01:35:do=01:35:bd=40:33:cd=40:33: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:*
7 LD_LIBRARY_PATH=/home/seed/source/boost_1.64.0/stage/lib:/home/seed/source/boost_1.64.0/stage/lib
8 SUDO_UID=1000
9 SUDO_USER=root
10 PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d
11 MAIL=/var/mail/root
12 PWD=/home/seed/ENV_SET_UID
13 JAVA_HOME=/usr/lib/jvm/java-8-oracle
14 HOME=/root
15 SUDO_COMMAND=/bin/bash
16 SHLVL=2
17 LANG=en_US.UTF-8
18 LOGNAME=root
19 LESSOPEN=| /usr/bin/lesspipe %s
20 DISPLAY=:0
21 SUDO_UID=1000
22 LESSCLOSE=| /usr/bin/lesspipe %s %s
23 XAUTHORITY=/home/seed/.Xauthority
24 OLDPWD=/home/seed

```

The diff command on both the files returns null. This proves that both the files are the same.

```

root@VM: /home/seed/ENV_SET_UID# gcc task2 2.c
root@VM: /home/seed/ENV_SET_UID# ./a.out > childProcessOutput
root@VM: /home/seed/ENV_SET_UID# gcc task2 2.c
root@VM: /home/seed/ENV_SET_UID# ./a.out > parentProcessOutput
root@VM: /home/seed/ENV_SET_UID# diff parentProcessOutput childProcessOutput
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#

```

### Task 3: Environment Variables and execve() :

- **Step 1:** Since the third argument passed to the execve() function is null, we cannot see any output.

```

root@VM: /home/seed/ENV_SET_UID# gcc task3.c
task3.c: In function 'main':
task3.c:9:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve("/usr/bin/env", argv, NULL);
  ~~~~~^
root@VM: /home/seed/ENV_SET_UID# ./a.out
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#

```

- **Step 2:** With the environ string passed to the execve() function as **execve("/usr/bin/env",argv,environ)** the name of the executable file after compilation is added to the environment variables list at the end. It's **a.out** in our case.

```

root@VM: /home/seed/ENV_SET_UID#
SHELL=/bin/bash
TERM=xterm-256color
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
USER=root
LS_COLORS=rs=0:di=01:34:ln=01:36:mh=00:pi=40:33:so=01:35:do=01:35:bd=40:33:cd=40:33: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:
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
SUDO_USER=seed
SUDO_UID=1000
USERNAME=root
PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d
MAIL=/var/mail/root
PWD=/home/seed/ENV_SET_UID
JAVA_HOME=/usr/lib/jvm/java-8-oracle
LANG=en_US.UTF-8
HOME=/root
SUDO_COMMAND=/bin/bash
SHLVL=2
LANGUAGE=en_US
LOGNAME=root
LESSOPEN=| /usr/bin/lesspipe %s
DISPLAY=:0
SUDO_GID=1000
LESSCLOSE=/usr/bin/lesspipe %s %s
XAUTHORITY=/home/seed/.Xauthority
./a.out
OLDPWD=/home/seed
root@VM: /home/seed/ENV_SET_UID#

```



## Task 4: Environment Variables and system()

On execution of the system(), it first spawns the bash and bash executes a command that prints all the environment variables.

```

root@VM: /home/seed/ENV_SET_UID# subl task4.c
root@VM: /home/seed/ENV_SET_UID# gcc task4.c
root@VM: /home/seed/ENV_SET_UID# ./a.out
ANDROID_HOME=/home/seed/android/android-sdk-linux
SHELL=/bin/bash
TERM=xterm-256color
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
USER=root
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:*lzh=01:31:*lzm=01:31:*tlz=01:31:*txz=01:31:*tzo=01:31:*t7z=01:31:*zip=01:31:*z=01:31:*Z=01:31:*d2=01:31:*gz=01:31:*lrz=01:31:*lz=01:31:*lzo=01:31:*xz=01:31:*b2=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:
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
SUDO_USER=seed
SUDO_UID=1000
USERNAME=root
PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d
MAIL=/var/mail/root
PWD=/home/seed/ENV_SET_UID
JAVA_HOME=/usr/lib/jvm/java-8-oracle
LANG=en_US.UTF-8
HOME=/root
SUDO_COMMAND=/bin/bash
SHLVL=2
LANGUAGE=en_US
LOGNAME=root
LESSOPEN=| /usr/bin/lesspipe %s
DISPLAY=:0
SUDO_GID=1000
LESSCLOSE=/usr/bin/lesspipe %s %s

```

## Task 5: Environment Variable and Set-UID Programs

- **Step 1:** On execution of the output file after compilation, the program prints all the environment variables.

```

root@VM: /home/seed/ENV_SET_UID# gcc task5_1.c
root@VM: /home/seed/ENV_SET_UID# ./a.out
ANDROID_HOME=/home/seed/android/android-sdk-linux
SHELL=/bin/bash
TERM=xterm-256color
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
USER=root
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:*lzh=01:31:*lzm=01:31:*tlz=01:31:*txz=01:31:*tzo=01:31:*t7z=01:31:*zip=01:31:*z=01:31:*Z=01:31:*d2=01:31:*gz=01:31:*lrz=01:31:*lz=01:31:*lzo=01:31:*xz=01:31:*b2=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:
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
SUDO_USER=seed
SUDO_UID=1000
USERNAME=root
PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d
MAIL=/var/mail/root
PWD=/home/seed/ENV_SET_UID
JAVA_HOME=/usr/lib/jvm/java-8-oracle
LANG=en_US.UTF-8
HOME=/root
SUDO_COMMAND=/bin/bash
SHLVL=2
LANGUAGE=en_US
LOGNAME=root
LESSOPEN=| /usr/bin/lesspipe %s
DISPLAY=:0
SUDO_GID=1000
LESSCLOSE=/usr/bin/lesspipe %s %s

```

- **Step 2:** The output after changing the ownership of the executable and changing the permissions. We can see the owner is now the **root**, and it's permission also being changed.

[illegible]

- **Step 3:** After setting the environment variables using the export command and re-running the code we can see all the environment variables we set. All the environment variables set in the parent process(shell) got into the set-uid chile process. The output shows the environment variables we set previously.

```
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID# export LD_LIBRARY_PATH=/home/source/seed
root@VM: /home/seed/ENV_SET_UID# export PATH=/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin
root@VM: /home/seed/ENV_SET_UID# export My_Name=Darshan Kodipalli
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID# gcc task5_1.c
root@VM: /home/seed/ENV_SET_UID# ./a.out
ANDROID_HOME=/home/seed/android/android-sdk-linux
SHELL=/bin/bash
TERM=xterm-256color
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
OLDPWD=/home/seed
USER=root
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;* t1z=01;31;* txz=01;31;* tzo=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;* fl1=01;35;* flv=01;35;* gl=01;35;* d=01;35;* xc=01;35;* xwd=01;35;* yuv=01;35;* cgm=01;35;* emf=01;35;* ovg=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;* mp=00;36;* ogg=00;36;* ra=00;36;* wav=00;36;* oga=00;36;* opus=00;36;* spx=00;36;* xspf=00;36;
LD_LIBRARY_PATH=/home/source/seed
SUDO_USER=seed
SUDO_UID=1000
USERNAME=root
PATH=/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin
MAIL=/var/mail/root
PWD=/home/seed/ENV_SET_UID
JAVA_HOME=/usr/lib/jvm/java-8-oracle
My_Name=Darshan Kodipalli
LANG=en_US.UTF-8
HOME=/root
SUDO_COMMAND=/bin/bash
```



## **Task 6: The PATH Environment Variable and Set-UID programs.**

Can you let this Set-UID program run your code instead of `/bin/ls`? If you can, is your code running with the root privilege? Describe and explain your observations.

→ We can let this Set-UID program run seamlessly but as the system can be exploited, it is risky. Since there are some privileges changed to the program, the code is now running with the root privilege. Since the `system()` spawns the shell which in turn executes the command that we run, it can easily be exploited and misused.

```

root@VM: /home/seed/ENV_SET_UID# gcc task6.c
task6.c: In function 'main':
task6.c:3:1: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
  system("ls");
  ^
root@VM: /home/seed/ENV_SET_UID# sudo chown root a.out
root@VM: /home/seed/ENV_SET_UID# sudo chmod 4755 a.out
root@VM: /home/seed/ENV_SET_UID# ./a.out
a.out childProcessOutput parentProcessOutput task2_2.c task3.c task4.c task5_1.c task6.c
root@VM: /home/seed/ENV_SET_UID#

```

## **Task 7: The LD\_PRELOAD Environment Variable and Set-UID Programs**

- **Step 1:** Run it as a regular program as a normal user.

```

root@VM: /home/seed/ENV_SET_UID# gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
root@VM: /home/seed/ENV_SET_UID# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM: /home/seed/ENV_SET_UID# subl myprog.c
a.out libmylib.so.1.0.1 mylib.o parentProcessOutput task3.c task5_1.c
childProcessOutput mylib.c myprog.c task2_2.c task4.c task6.c
root@VM: /home/seed/ENV_SET_UID# ./a.out
I am not sleeping!
root@VM: /home/seed/ENV_SET_UID#

```

- **Step 2:** Make it a Set-UID Program and run it as a normal user.

```

root@VM: /home/seed/ENV_SET_UID# sudo chown root task2_2.c task3.c task4.c task5_1.c task6.c
root@VM: /home/seed/ENV_SET_UID# sudo chown root myprog.c
root@VM: /home/seed/ENV_SET_UID# sudo chmod 4755 myprog.c
root@VM: /home/seed/ENV_SET_UID# gcc myprog.c
myprog.c: In function 'main':
myprog.c:3:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
root@VM: /home/seed/ENV_SET_UID# ./a.out
I am not sleeping!
root@VM: /home/seed/ENV_SET_UID#

```

- **Step 3:** Changing the program as a Set-UID program, running it as a root, Exporting the LD\_PRELOAD environment variable to the root and rerunning it.

```

root@VM: /home/seed/ENV_SET_UID# subl myprog.c
root@VM: /home/seed/ENV_SET_UID# gcc myprog.c
root@VM: /home/seed/ENV_SET_UID# ./a.out
root@VM: /home/seed/ENV_SET_UID#

```

- **Step 4:** With another user account userB, changing myprog to a Set-UID userB program, export the LD\_PRELOAD variable to userB's account and re-running it.

```
root@VM: /home/seed/ENV_SET_UID# subl myprog.c
root@VM: /home/seed/ENV_SET_UID# gcc myprog.c
root@VM: /home/seed/ENV_SET_UID# ./a.out
root@VM: /home/seed/ENV_SET_UID#
```

## Task 8: Invoking External Programs using system() versus execve()

- **Step 1:** If you were Bob, can you compromise the integrity of the system? For example, can you remove a file that is not writable to you?  
→ Since we're making use of a system() which calls the shell to execute the command and shell has root privileges so we will be able to remove a file. Therefore we can compromise the integrity of the system.
- **Step 2:** Do your attacks in Step 1 still work? Please describe and explain your observations.  
→ No, the attack will not be successful, since we're making use of execv() which does not create a new process, instead it replaces bash with command to be executed. Since the cat command is used, we get a similar output when run both the versions. More exploitation can be done with the system() than with the execve().

```
root@VM: /home/seed/ENV_SET_UID# gcc task8.c
root@VM: /home/seed/ENV_SET_UID# ./a.out
System and Network Security, ~ CSP 544
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID#
root@VM: /home/seed/ENV_SET_UID# gcc task8_1.c
task8_1.c: In function 'main':
task8_1.c:17:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
execve(v[0], v, NULL);
^
root@VM: /home/seed/ENV_SET_UID# ./a.out
System and Network Security, ~ CSP 544
root@VM: /home/seed/ENV_SET_UID#
```



## Task 9: Capability Leaking

Run the program as a normal user, and describe what you have observed. Will the file `/etc/zzz` be modified?

→ Since the file `/etc/zzz` is open even before the Set-UID, we can see the file has been modified. To avoid this, we can move `Set-UID(setuid(getuid()))` above the `open()`.

```
root@VM: /home/seed/ENV_SET_UID# gcc task9.c
task9.c: In function 'main':
task9.c:12:2: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  sleep(1);
  ^
task9.c:13:2: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
  setuid(getuid());
  ^
task9.c:13:9: warning: implicit declaration of function 'getuid' [-Wimplicit-function-declaration]
  setuid(getuid());
  ^
task9.c:14:6: warning: implicit declaration of function 'fork' [-Wimplicit-function-declaration]
  if (fork()) {
  ^
task9.c:15:3: warning: implicit declaration of function 'close' [-Wimplicit-function-declaration]
  close (fd);
  ^
task9.c:18:3: warning: implicit declaration of function 'write' [-Wimplicit-function-declaration]
  write (fd, "Malicious Data\n", 15);
  ^
root@VM: /home/seed/ENV_SET_UID# sudo chown root a.out
root@VM: /home/seed/ENV_SET_UID# sudo chmod 4755 a.out
root@VM: /home/seed/ENV_SET_UID# ./a.out
Cannot open /etc/zzz
root@VM: /home/seed/ENV_SET_UID#
```

```
root@VM: /home/seed/ENV_SET_UID# sudo chown root a.out
root@VM: /home/seed/ENV_SET_UID# sudo chmod 4755 a.out
root@VM: /home/seed/ENV_SET_UID# ./a.out
I am not sleeping!
root@VM: /home/seed/ENV_SET_UID#
```