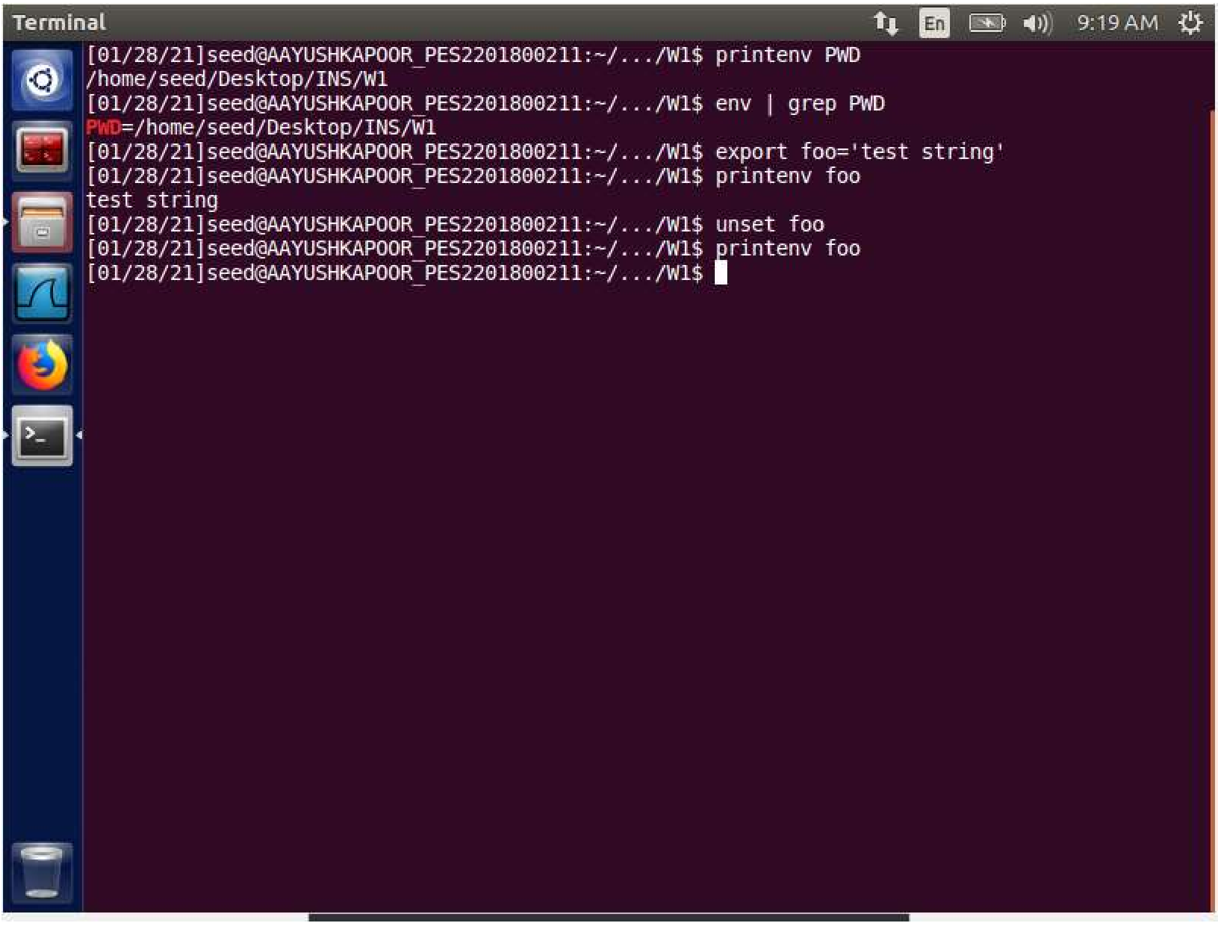
PES UNIVERSITY
INFORMATION SECURITY
WEEK 1 LAB

AAYUSH KAPOOR PES2201800211

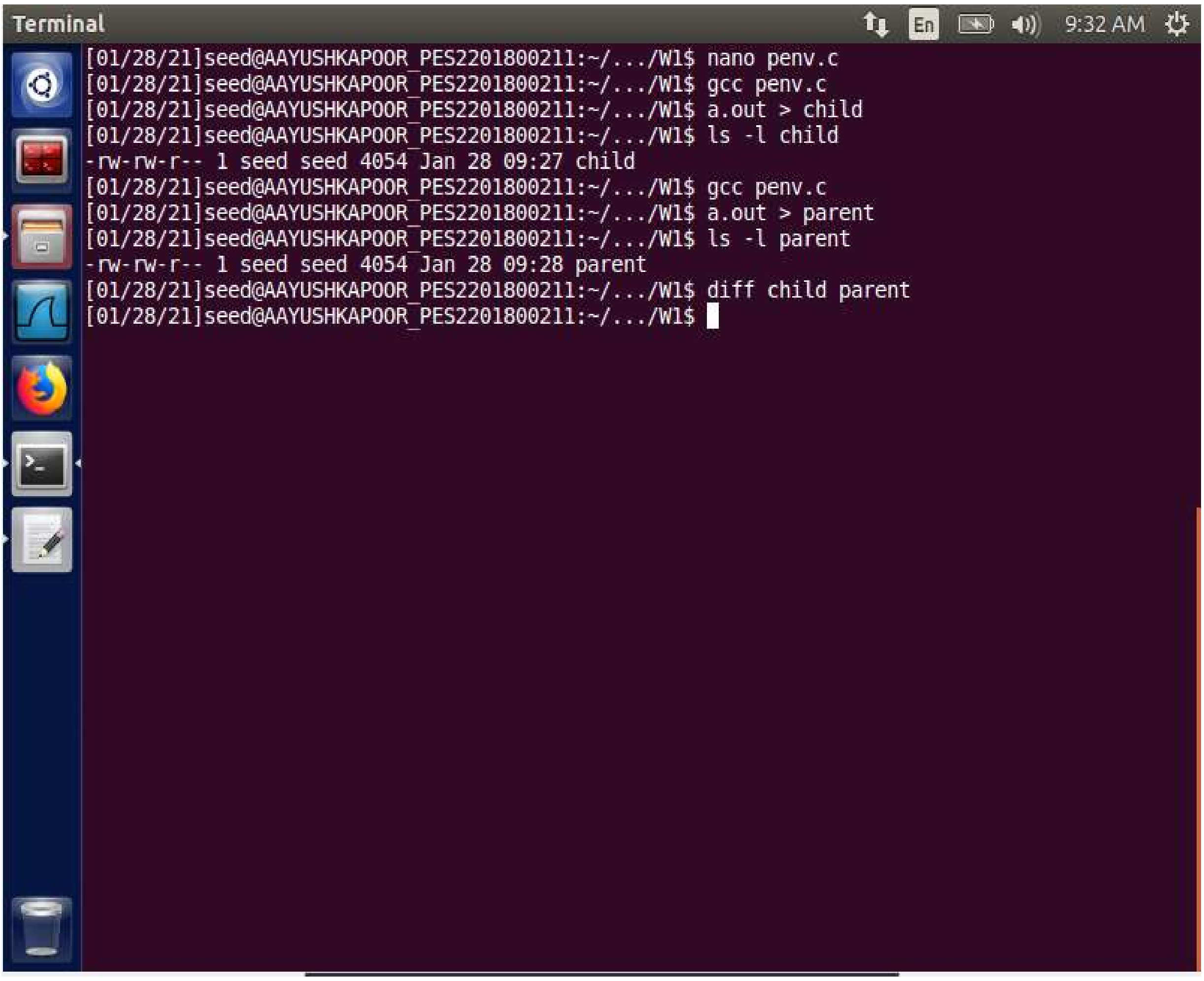
TASK 1:



```
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv PWD
/home/seed/Desktop/INS/W1
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ env | grep PWD
PWD=/home/seed/Desktop/INS/W1
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ export foo='test string'
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv foo
test string
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ unset foo
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv foo
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$
```

This task displays the working directory and later create a foo variable with some value and unsetting/deleting the foo variable, hence does not display any value when printenv is given second time.

TASK 2:

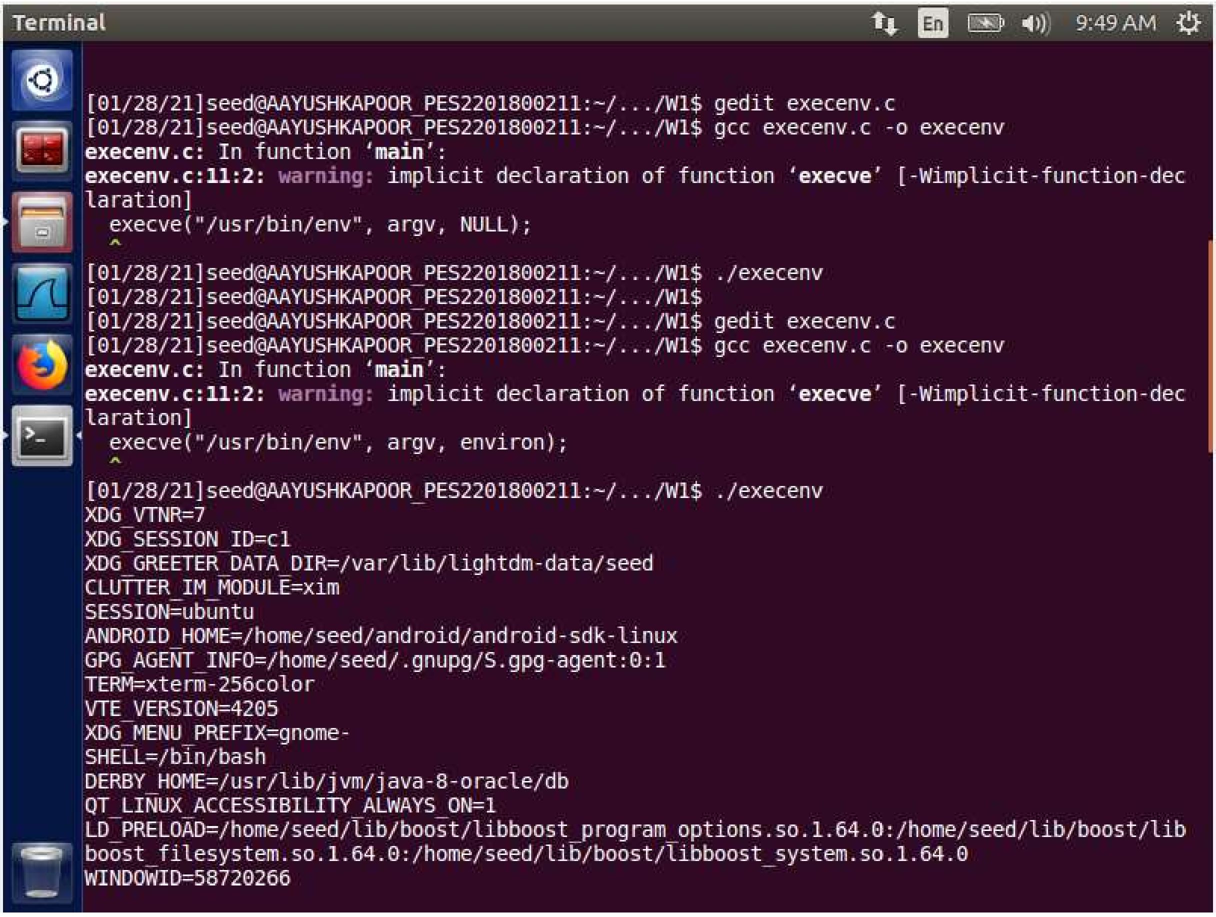


```
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ nano penv.c
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc penv.c
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ a.out > child
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l child
-rw-rw-r-- 1 seed seed 4054 Jan 28 09:27 child
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc penv.c
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ a.out > parent
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l parent
-rw-rw-r-- 1 seed seed 4054 Jan 28 09:28 parent
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ diff child parent
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$
```

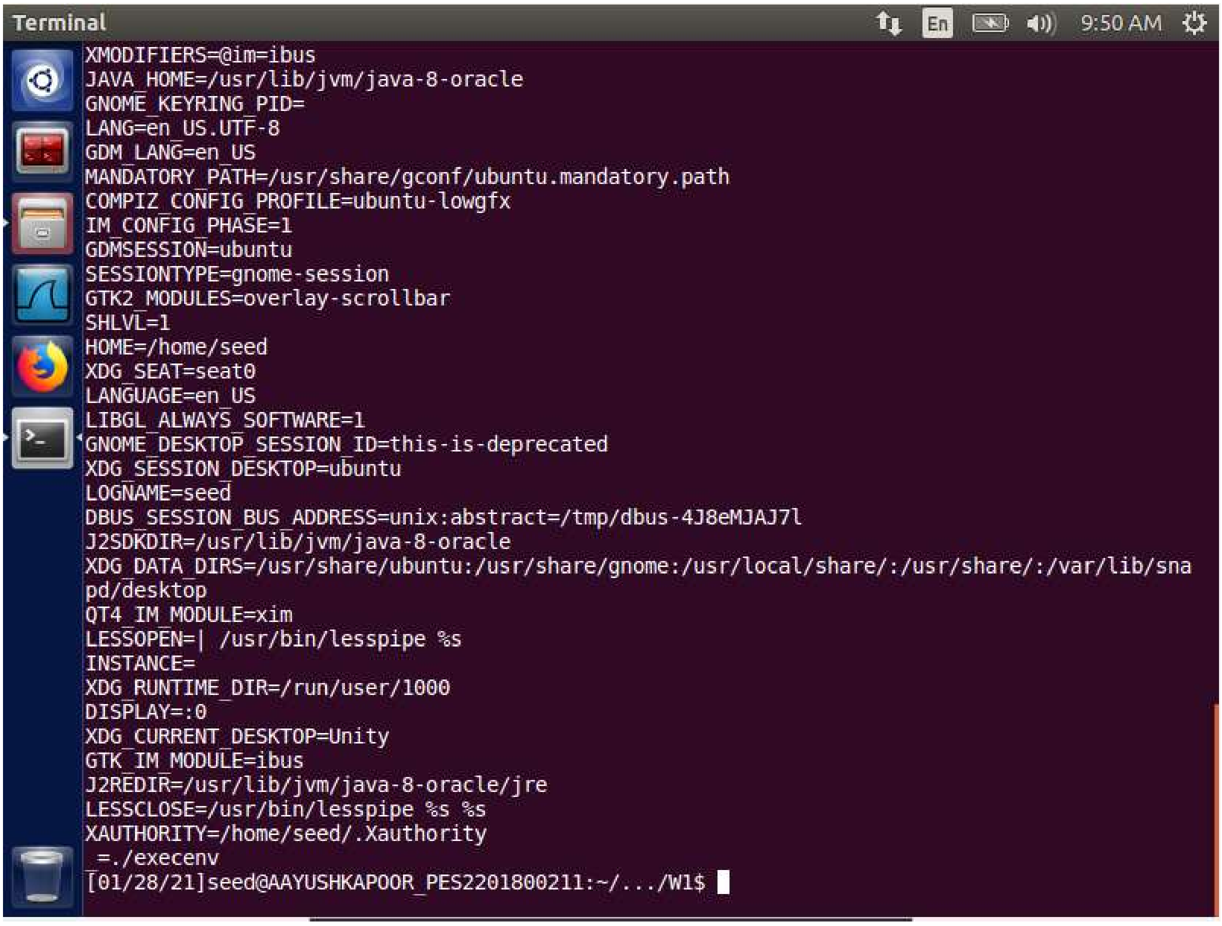
In this task we are checking whether a child inherits the environment variables from the parent, and the answer to that is **Yes** because the difference between child and parent output is **0**.
The string of output after ls command is 664 :

- rw - 6 => Readable and writable by owner
- rw - 6 => Readable and writable by group
- r - 4 => Only readable by others(neither user nor belonging to group)

TASK 3:



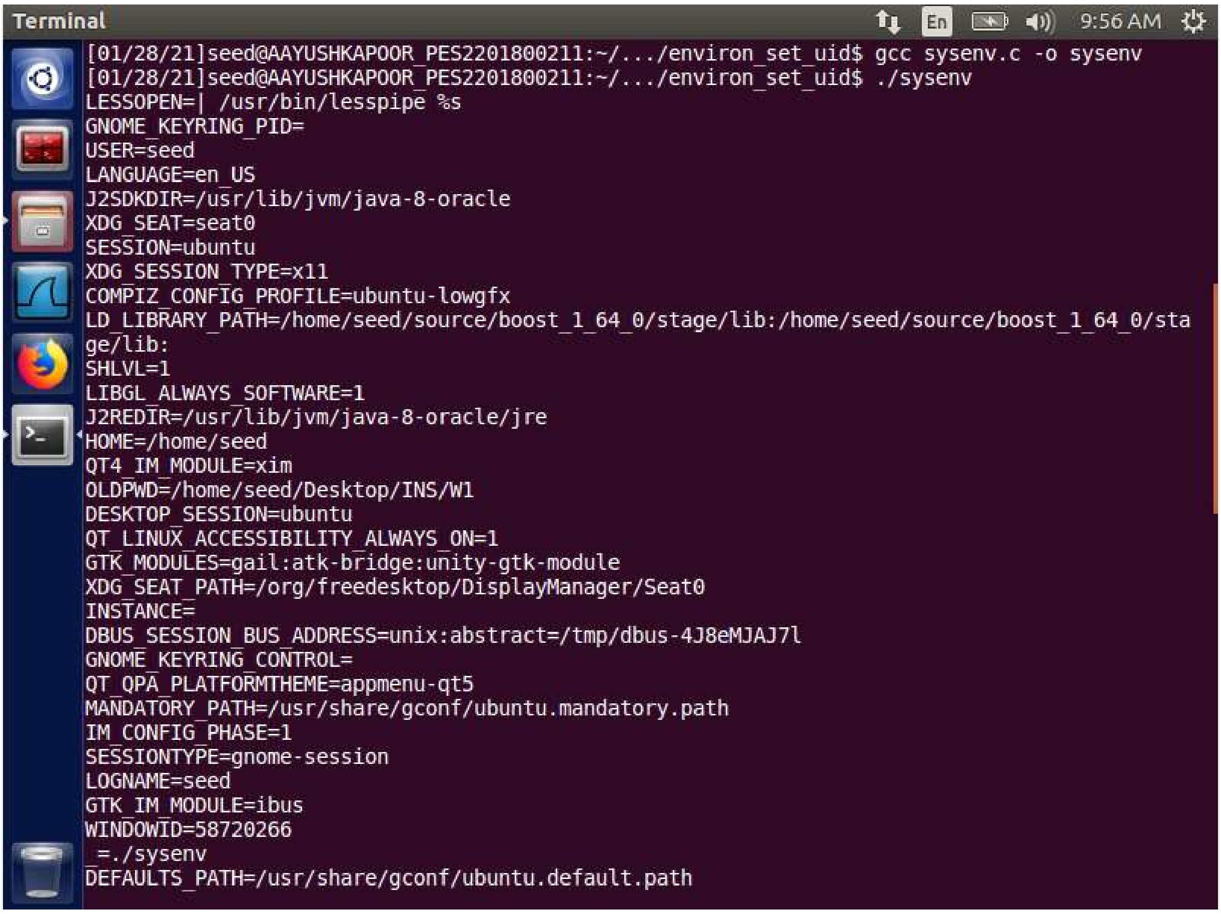
```
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gedit execenv.c
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc execenv.c -o execenv
execenv.c: In function ‘main’:
execenv.c:11:2: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-dec
laration]
  execve("/usr/bin/env", argv, NULL);
  ^
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ./execenv
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gedit execenv.c
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc execenv.c -o execenv
execenv.c: In function ‘main’:
execenv.c:11:2: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-dec
laration]
  execve("/usr/bin/env", argv, environ);
  ^
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ./execenv
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/lib
boost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
WINDOWID=58720266
```



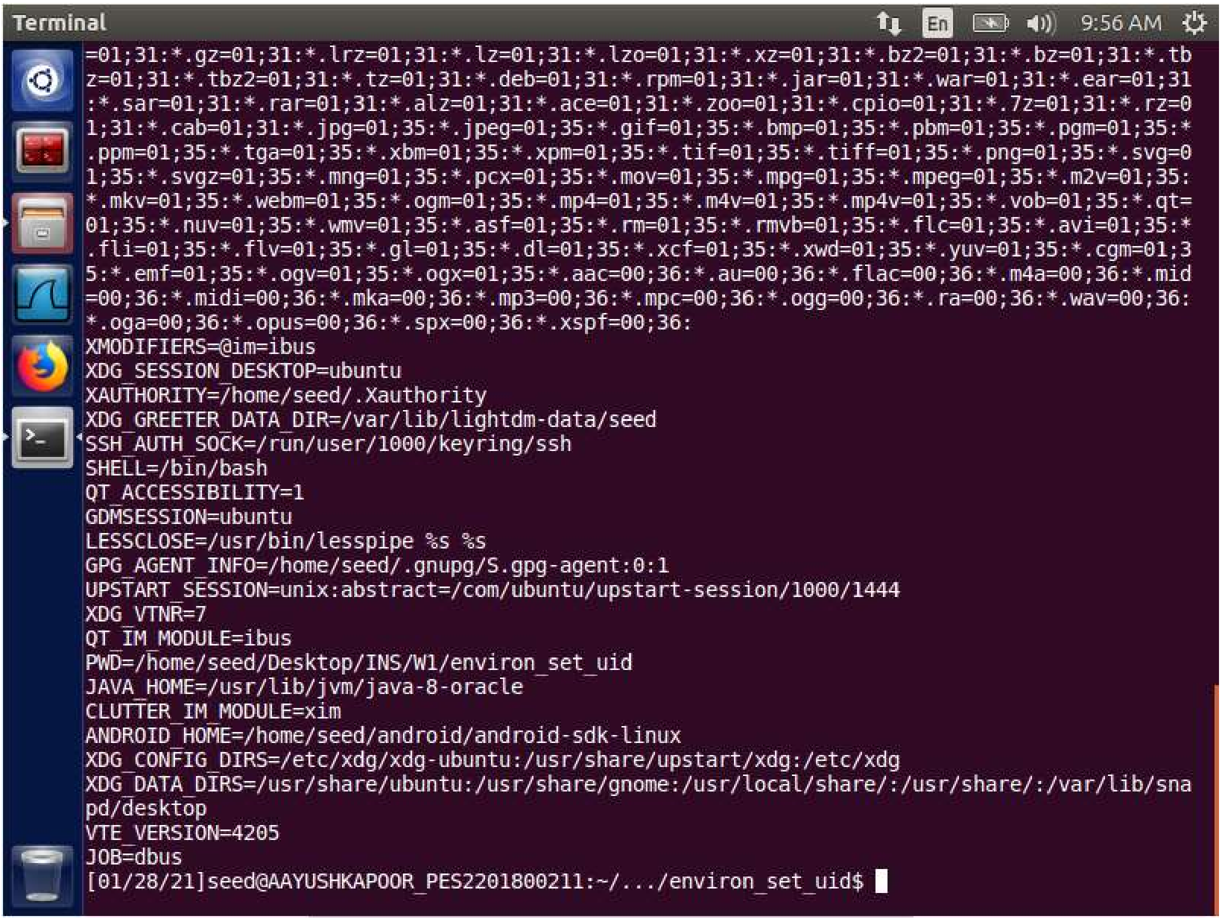
```
XMODIFIERS=@im=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
GDM_LANG=en_US
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
SHLVL=1
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-4J8eMJAJ7l
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/sna
pd/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
_=./execenv
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ 
```

Like in the previous task, where the child inherits the environment variable from parent in the same way the calling program can set some arbitrary value to environment value and hence complete control over it. Yes the new program inherits the environment variable.

TASK 4:



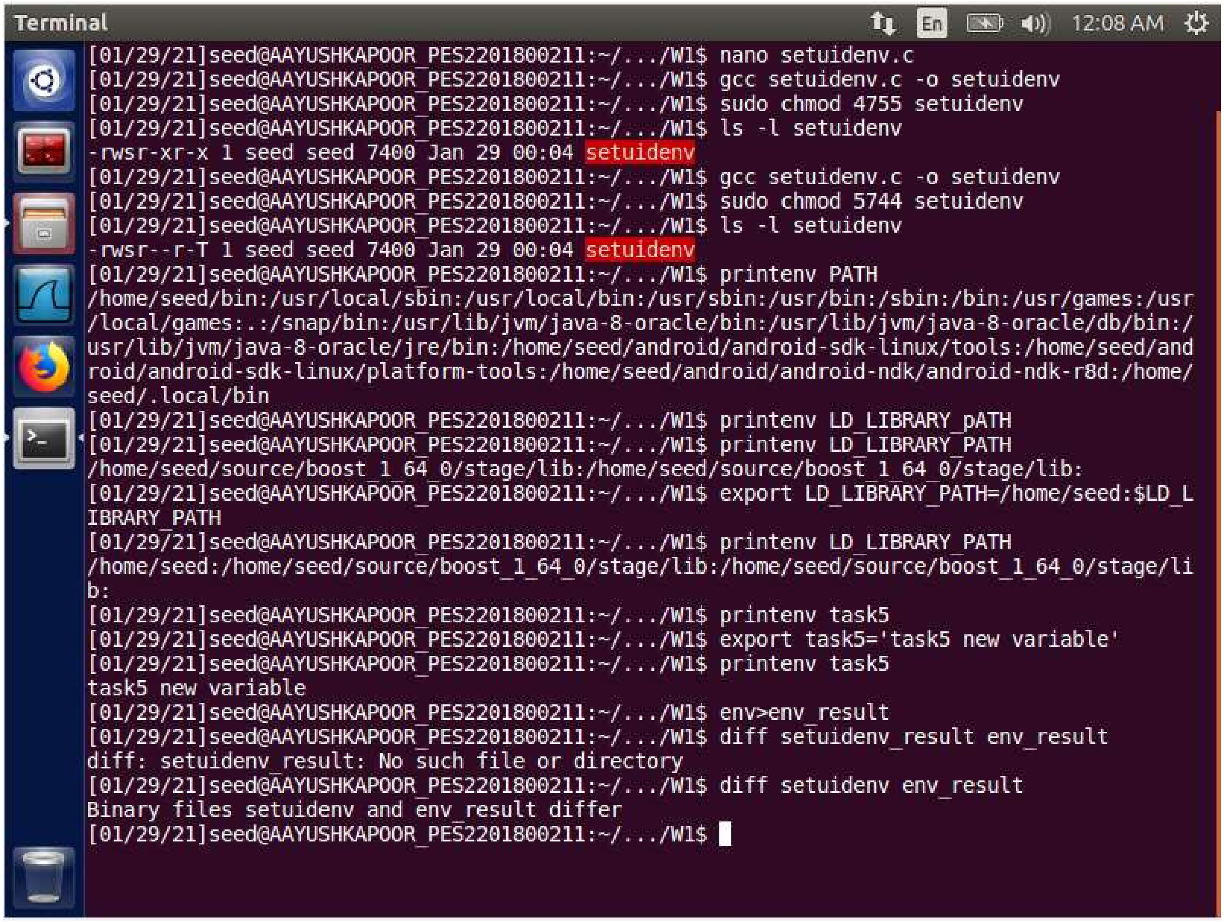
```
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../environ_set_uid$ gcc sysenv.c -o sysenv
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../environ_set_uid$ ./sysenv
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/sta
ge/lib:
SHLVL=1
LIBGL_ALWAYS_SOFTWARE=1
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
HOME=/home/seed
QT4_IM_MODULE=xim
OLDPWD=/home/seed/Desktop/INS/W1
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-4J8eMJAJ7l
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=58720266
_=./sysenv
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
```



```
=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tb
z=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=0
1;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=0
1;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;3
5:*.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/1000/1444
XDG_VTNR=7
QT_IM_MODULE=ibus
PWD=/home/seed/Desktop/INS/W1/environ_set_uid
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/sna
pd/desktop
VTE_VERSION=4205
JOB=dbus
[01/28/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../environ_set_uid$ 
```

From this task we can display that the calling process environment variable is passed to the called process i.e /bin/sh process.

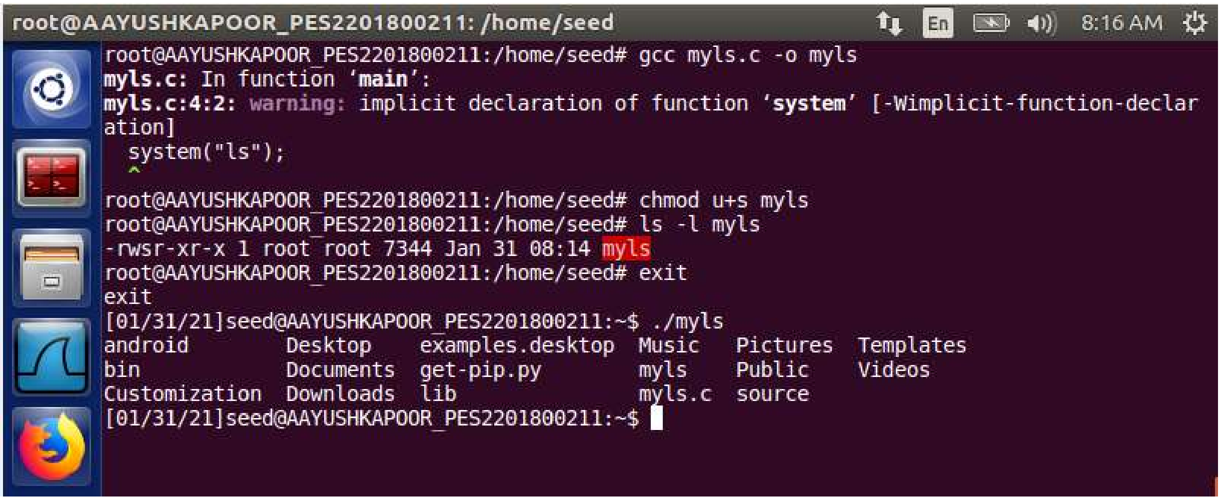
TASK 5:



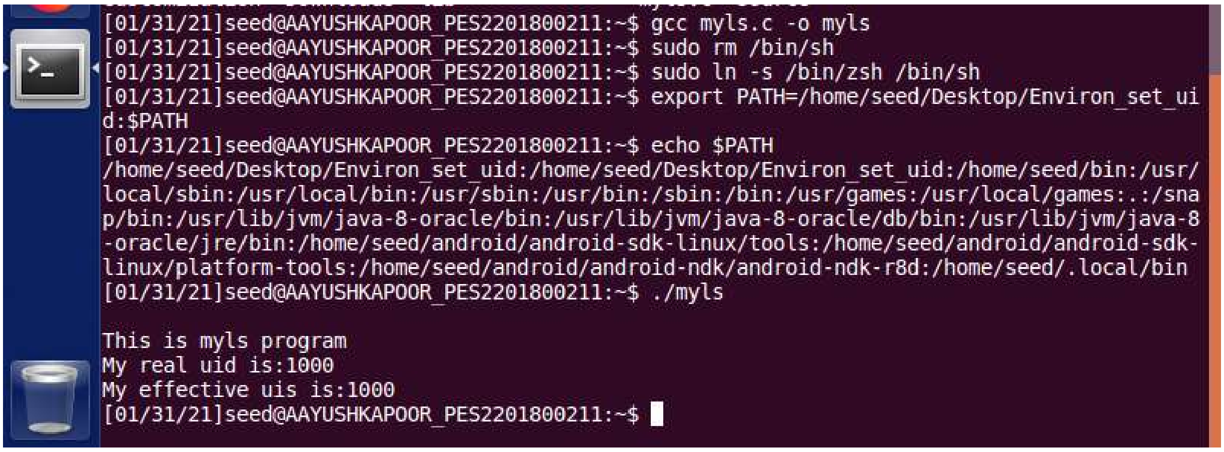
```
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ nano setuidenv.c
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc setuidenv.c -o setuidenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo chmod 4755 setuidenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l setuidenv
-rwsr-xr-x 1 seed seed 7400 Jan 29 00:04 setuidenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc setuidenv.c -o setuidenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo chmod 5744 setuidenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l setuidenv
-rwsr--r-T 1 seed seed 7400 Jan 29 00:04 setuidenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv 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/and
roid/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/
seed/.local/bin
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv LD_LIBRARY_pATH
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv LD_LIBRARY_PATH
/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ export LD_LIBRARY_PATH=/home/seed:$LD_L
IBRARY_PATH
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv LD_LIBRARY_PATH
/home/seed:/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/li
b:
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv task5
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ export task5='task5 new variable'
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ printenv task5
task5 new variable
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ env>env_result
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ diff setuidenv_result env_result
diff: setuidenv_result: No such file or directory
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ diff setuidenv env_result
Binary files setuidenv and env_result differ
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ 
```

Yes, all the environment variable set on parent process is inherited by child process.

TASK 6:



```
root@AAYUSHKAPOOR_PES2201800211:/home/seed# gcc myls.c -o myls
myls.c: In function ‘main’:
myls.c:4:2: warning: implicit declaration of function ‘system’ [-Wimplicit-function-declar
ation]
  system("ls");
  ^
root@AAYUSHKAPOOR_PES2201800211:/home/seed# chmod u+s myls
root@AAYUSHKAPOOR_PES2201800211:/home/seed# ls -l myls
-rwsr-xr-x 1 root root 7344 Jan 31 08:14 myls
root@AAYUSHKAPOOR_PES2201800211:/home/seed# exit
exit
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ ./myls
android        Desktop    examples.desktop  Music   Pictures  Templates
bin            Documents  get-pip.py        myls    Public    Videos
Customization  Downloads  lib               myls.c  source
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$
```

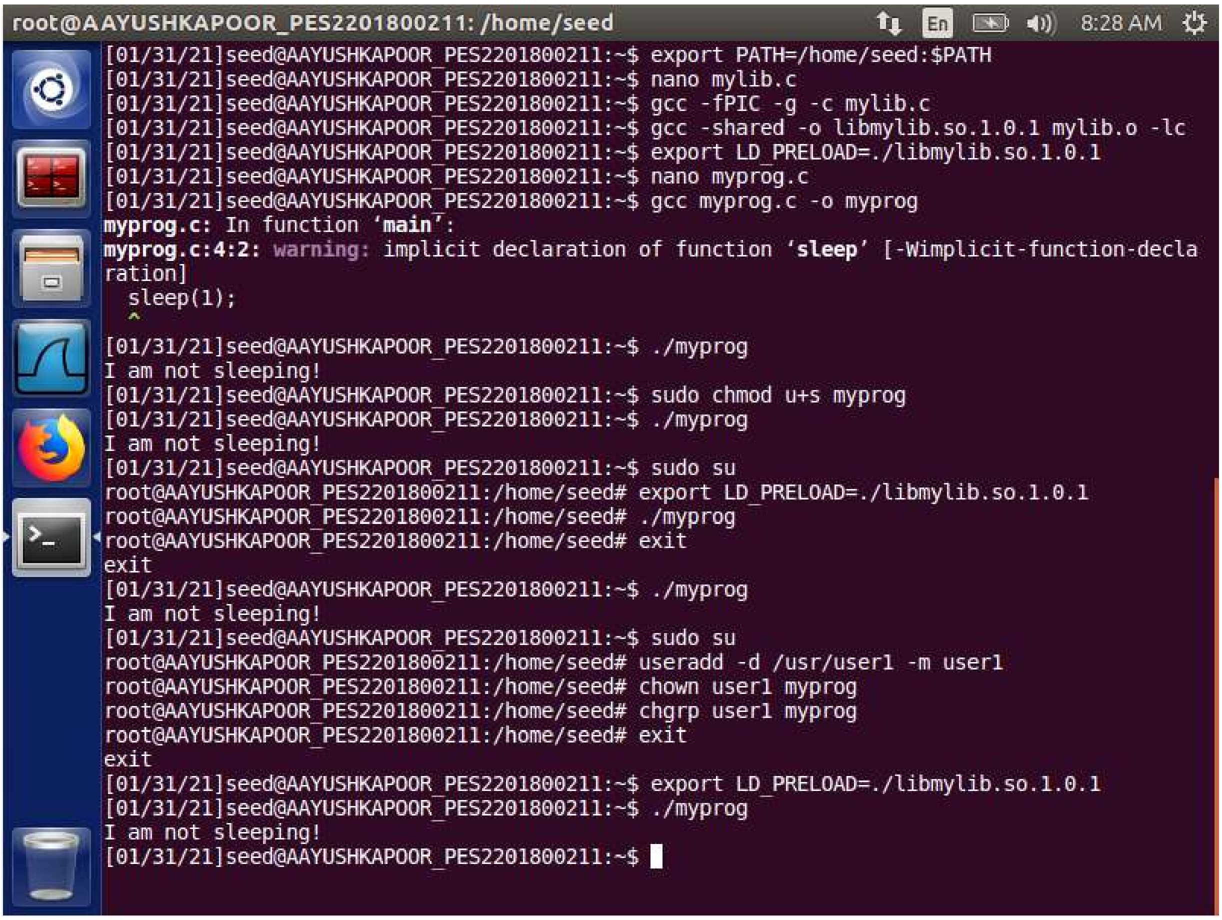


```
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ gcc myls.c -o myls
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ sudo rm /bin/sh
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ sudo ln -s /bin/zsh /bin/sh
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ export PATH=/home/seed/Desktop/Environ_set_ui
d:$PATH
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ echo $PATH
/home/seed/Desktop/Environ_set_uid:/home/seed/Desktop/Environ_set_uid:/home/seed/bin:/usr/
local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/sna
p/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8
-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-
linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ ./myls

This is myls program
My real uid is:1000
My effective uis is:1000
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$
```

Here we see the vulnerability issues of zsh whereas bash has protection against this flaw, bash does not share the set-uid exploit vulnerability with zsh. Yes the code is running with root privileges.

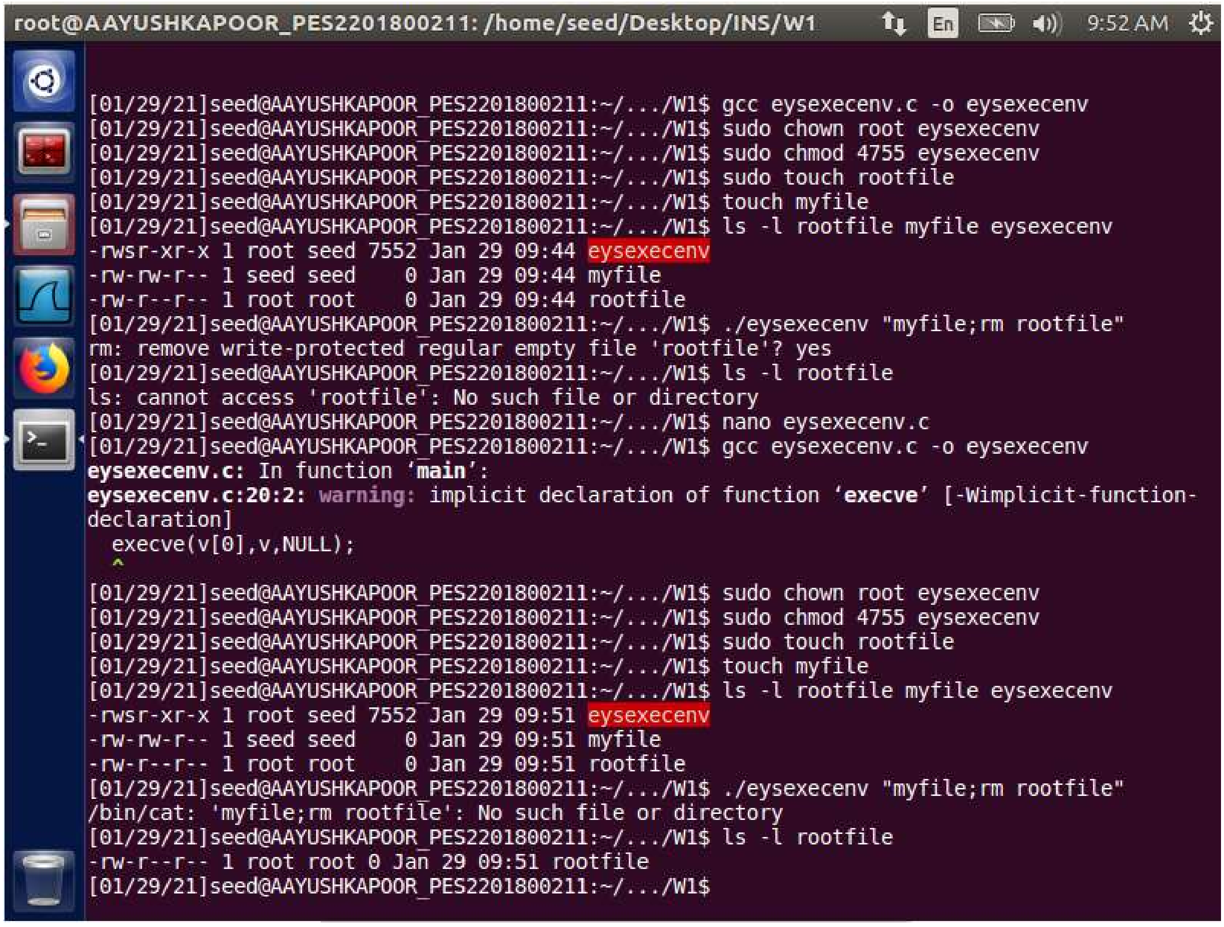
TASK 7:



```
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ export PATH=/home/seed:$PATH
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ nano mylib.c
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ gcc -fPIC -g -c mylib.c
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ nano myprog.c
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ gcc myprog.c -o myprog
myprog.c: In function ‘main’:
myprog.c:4:2: warning: implicit declaration of function ‘sleep’ [-Wimplicit-function-decla
ration]
  sleep(1);
  ^
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ ./myprog
I am not sleeping!
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ sudo chmod u+s myprog
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ ./myprog
I am not sleeping!
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ sudo su
root@AAYUSHKAPOOR_PES2201800211:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@AAYUSHKAPOOR_PES2201800211:/home/seed# ./myprog
root@AAYUSHKAPOOR_PES2201800211:/home/seed# exit
exit
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ ./myprog
I am not sleeping!
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ sudo su
root@AAYUSHKAPOOR_PES2201800211:/home/seed# useradd -d /usr/user1 -m user1
root@AAYUSHKAPOOR_PES2201800211:/home/seed# chown user1 myprog
root@AAYUSHKAPOOR_PES2201800211:/home/seed# chgrp user1 myprog
root@AAYUSHKAPOOR_PES2201800211:/home/seed# exit
exit
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$ ./myprog
I am not sleeping!
[01/31/21]seed@AAYUSHKAPOOR_PES2201800211:~$
```

The child does not inherit the LD_PRELOAD environment variables.
All the conditions are executed as displayed above, when in root privilege it does not give ‘*I am not sleeping!’* as output.

TASK 8:

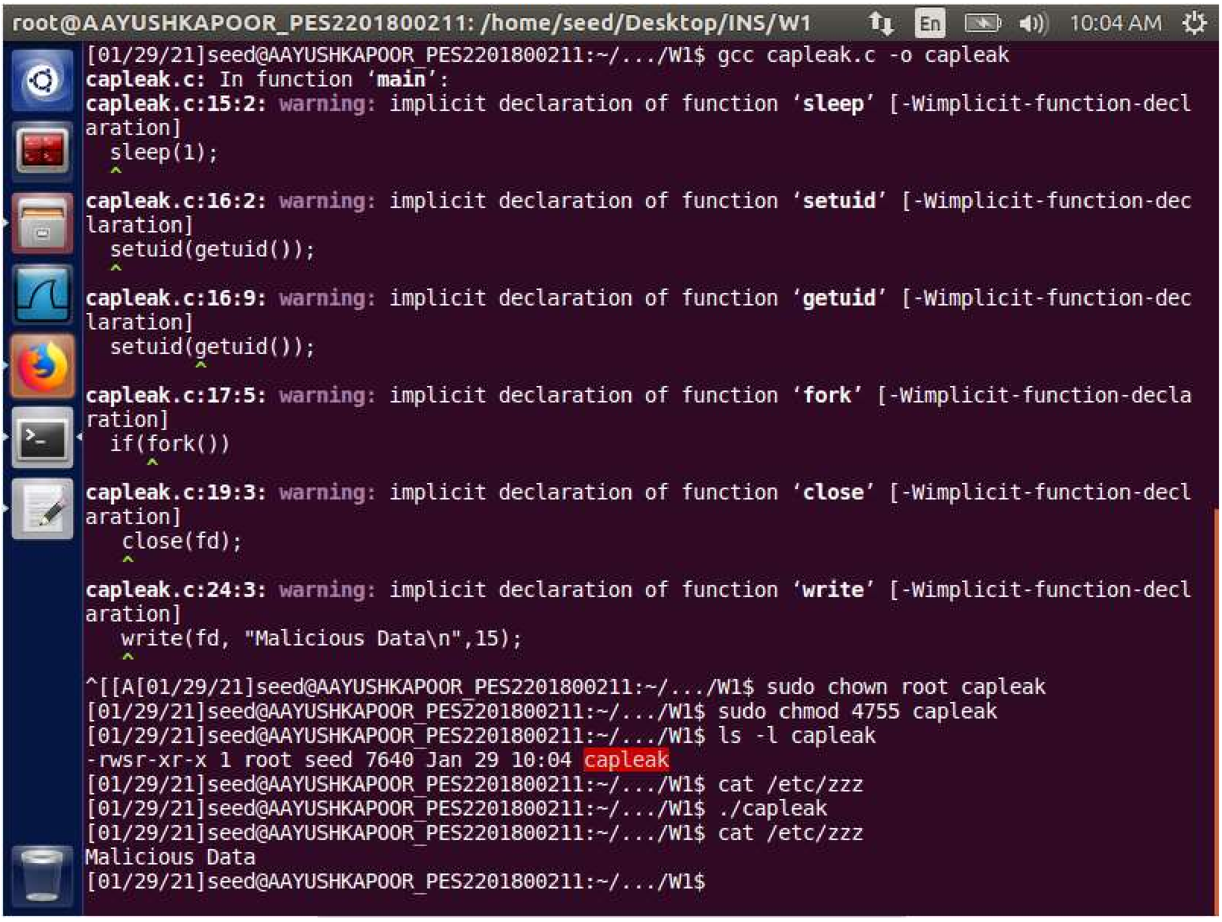


```
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc eysexecenv.c -o eysexecenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo chown root eysexecenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo chmod 4755 eysexecenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo touch rootfile
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ touch myfile
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l rootfile myfile eysexecenv
-rwsr-xr-x 1 root seed 7552 Jan 29 09:44 eysexecenv
-rw-rw-r-- 1 seed seed    0 Jan 29 09:44 myfile
-rw-r--r-- 1 root root    0 Jan 29 09:44 rootfile
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ./eysexecenv "myfile;rm rootfile"
rm: remove write-protected regular empty file 'rootfile'? yes
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l rootfile
ls: cannot access 'rootfile': No such file or directory
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ nano eysexecenv.c
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc eysexecenv.c -o eysexecenv
eysexecenv.c: In function ‘main’:
eysexecenv.c:20:2: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-declaration]
  execve(v[0],v,NULL);
  ^

[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo chown root eysexecenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo chmod 4755 eysexecenv
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo touch rootfile
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ touch myfile
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l rootfile myfile eysexecenv
-rwsr-xr-x 1 root seed 7552 Jan 29 09:51 eysexecenv
-rw-rw-r-- 1 seed seed    0 Jan 29 09:51 myfile
-rw-r--r-- 1 root root    0 Jan 29 09:51 rootfile
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ./eysexecenv "myfile;rm rootfile"
/bin/cat: 'myfile;rm rootfile': No such file or directory
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l rootfile
-rw-r--r-- 1 root root 0 Jan 29 09:51 rootfile
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$
```

No, the step 1 attack does not work, because system() is very dangerous as it can affect how the shell works whereas execve() program does not do this as it does not invoke shell like the former.

TASK 9:



```
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ gcc capleak.c -o capleak
capleak.c: In function ‘main’:
capleak.c:15:2: warning: implicit declaration of function ‘sleep’ [-Wimplicit-function-decl
aration]
  sleep(1);
  ^
capleak.c:16:2: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-dec
laration]
  setuid(getuid());
  ^
capleak.c:16:9: warning: implicit declaration of function ‘getuid’ [-Wimplicit-function-dec
laration]
  setuid(getuid());
         ^
capleak.c:17:5: warning: implicit declaration of function ‘fork’ [-Wimplicit-function-decla
ration]
  if(fork())
     ^
capleak.c:19:3: warning: implicit declaration of function ‘close’ [-Wimplicit-function-decl
aration]
   close(fd);
   ^
capleak.c:24:3: warning: implicit declaration of function ‘write’ [-Wimplicit-function-decl
aration]
   write(fd, "Malicious Data\n",15);
   ^
^[[A[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo chown root capleak
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ sudo chmod 4755 capleak
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ls -l capleak
-rwsr-xr-x 1 root seed 7640 Jan 29 10:04 capleak
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ cat /etc/zzz
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ ./capleak
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$ cat /etc/zzz
Malicious Data
[01/29/21]seed@AAYUSHKAPOOR_PES2201800211:~/.../W1$
```

Yes the data is modified as it has not lost its privilege capabilities even though its root privileged was downgraded to normal one.