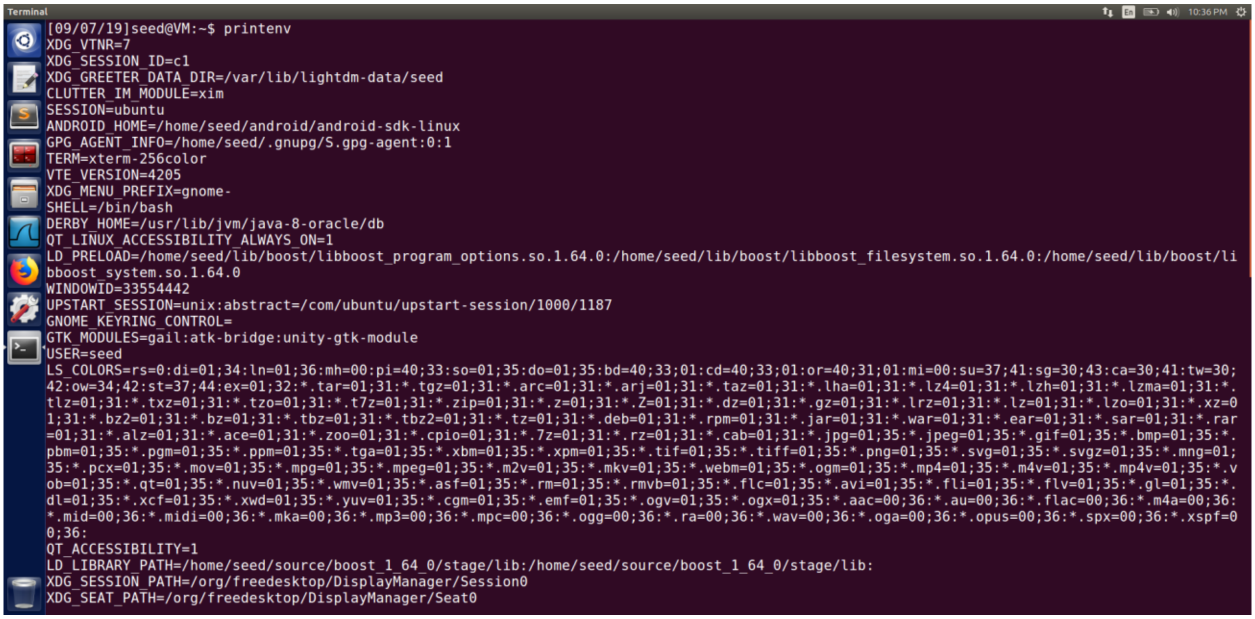
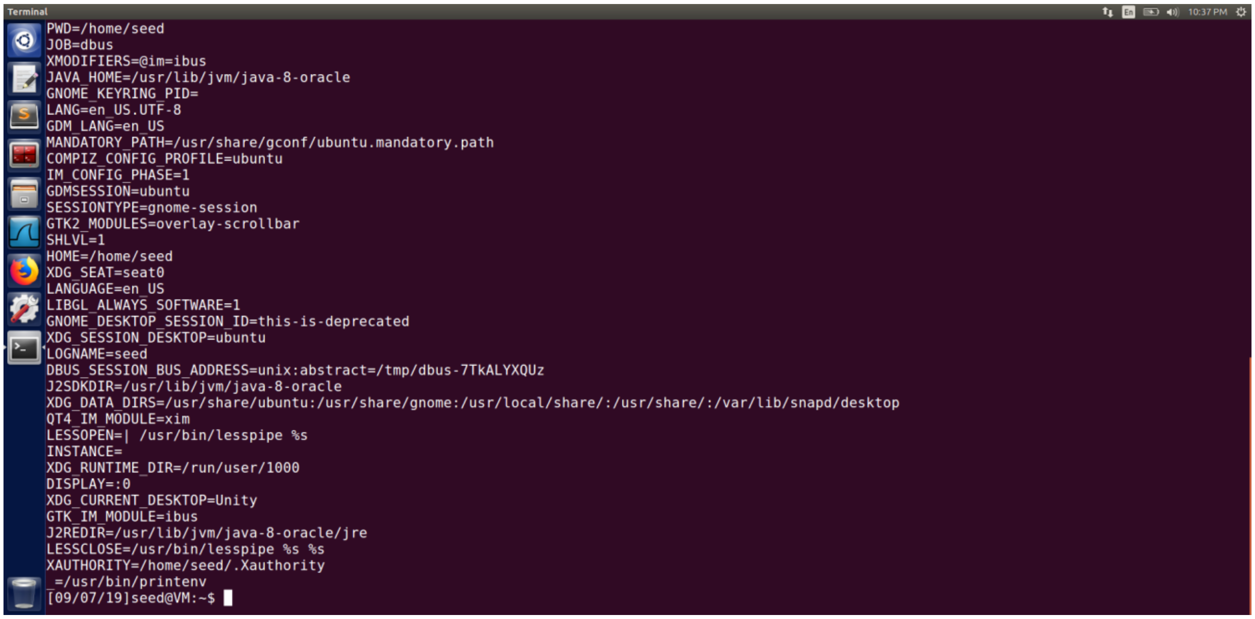
Lab 1 – Set-UID

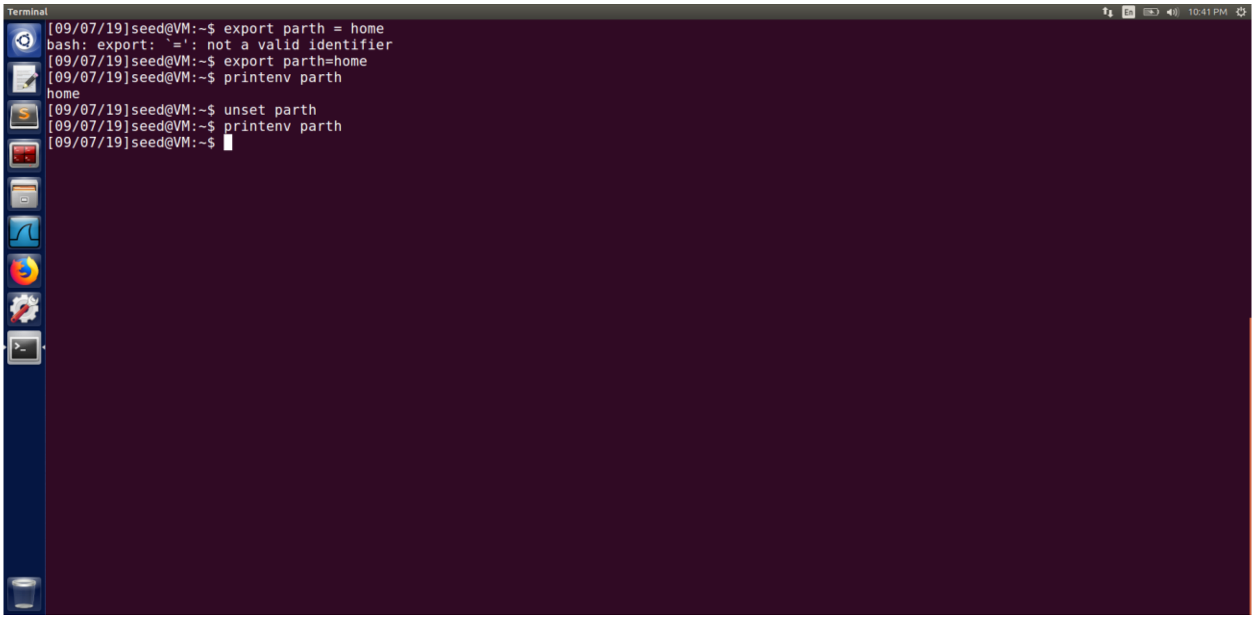
Task 1



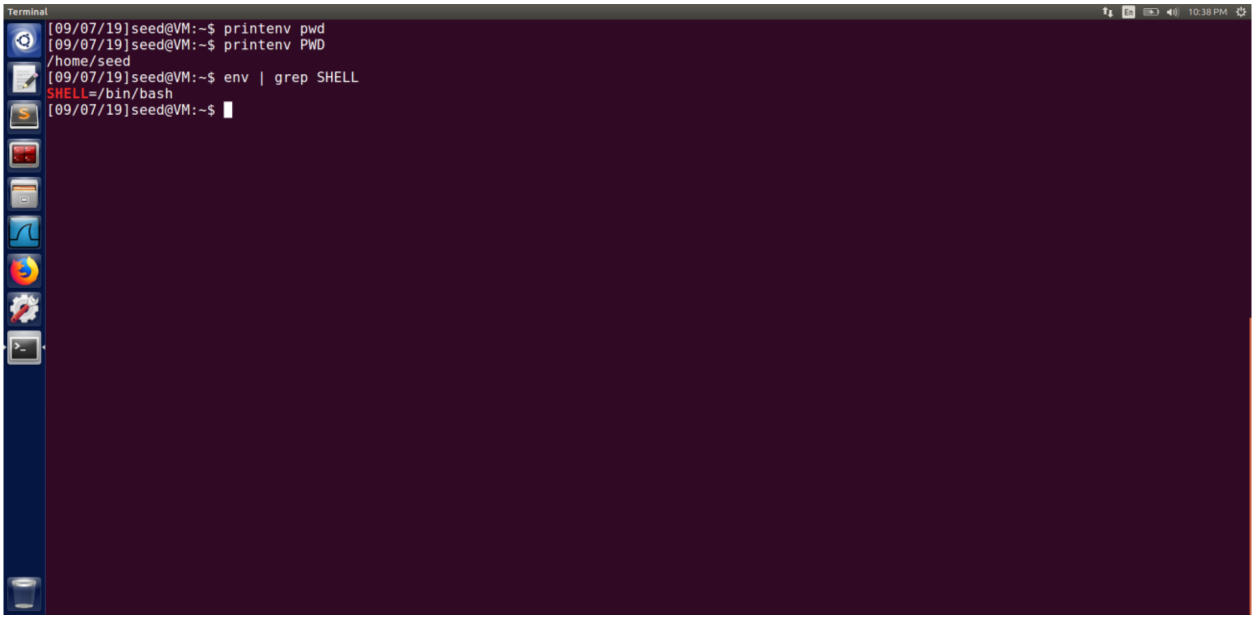
```
[09/07/19]seed@VM:~$ printenv
XDG_VTNR=7
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm-256color
VTE_VERSION=4205
XDG_MENU_PREFIX=gnome-
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/li
bboost_system.so.1.64.0
WINDOWID=33554442
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1187
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=0
1;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:*.v
ob=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=0
0;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
```



```
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-7TkALYXQUz
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
[09/07/19]seed@VM:~$ 
```



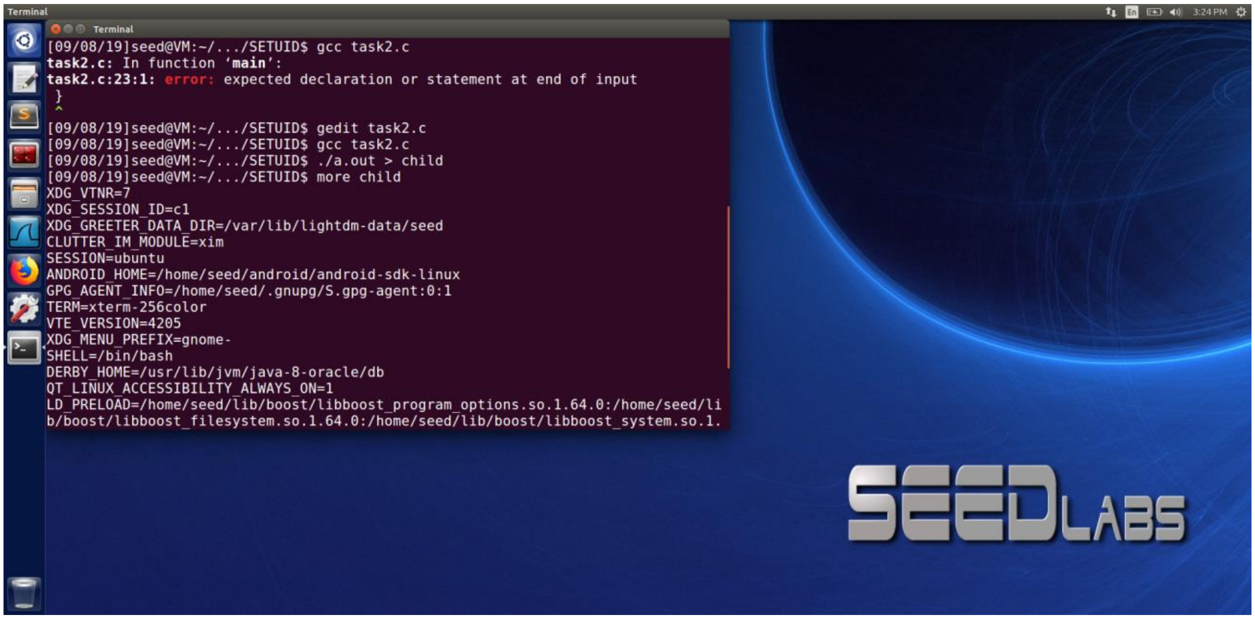
```
[09/07/19]seed@VM:~$ export parth = home
bash: export: `=': not a valid identifier
[09/07/19]seed@VM:~$ export parth=home
[09/07/19]seed@VM:~$ printenv parth
home
[09/07/19]seed@VM:~$ unset parth
[09/07/19]seed@VM:~$ printenv parth
[09/07/19]seed@VM:~$ 
```



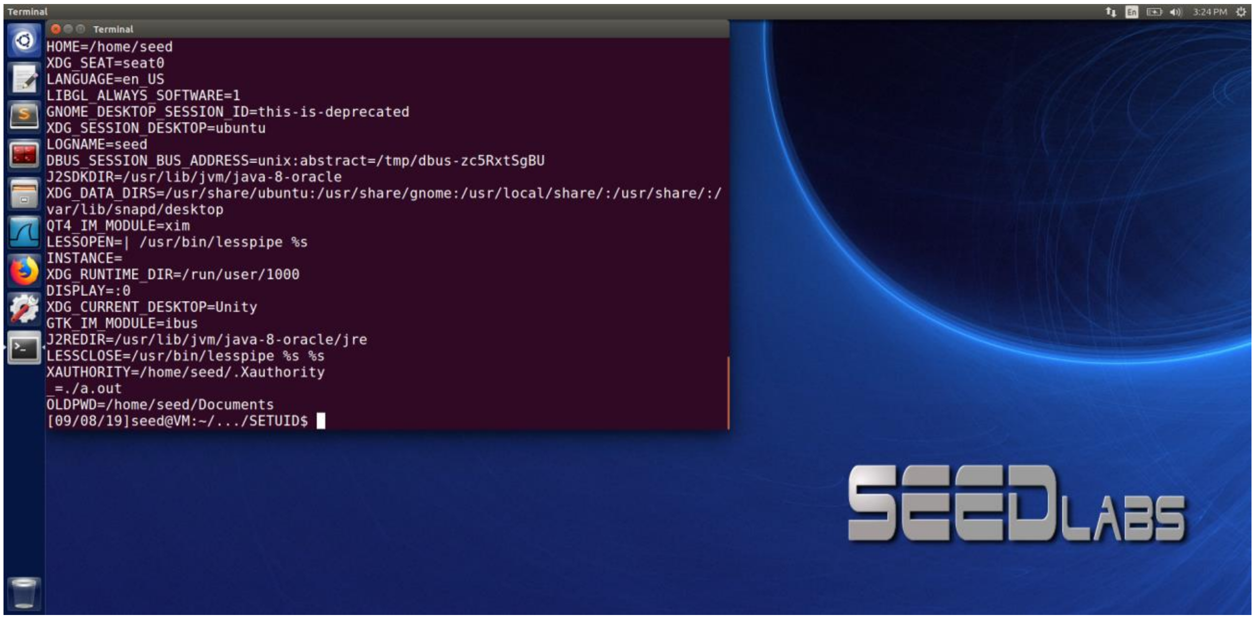
```
[09/07/19]seed@VM:~$ printenv pwd
[09/07/19]seed@VM:~$ printenv PWD
/home/seed
[09/07/19]seed@VM:~$ env | grep SHELL
SHELL=/bin/bash
[09/07/19]seed@VM:~$ 
```

Printenv command is used to print all the environment variables in the system whereas grep command is used to search for a particular environment variables. And that unset command is used to unset any environment variable.

Task 2

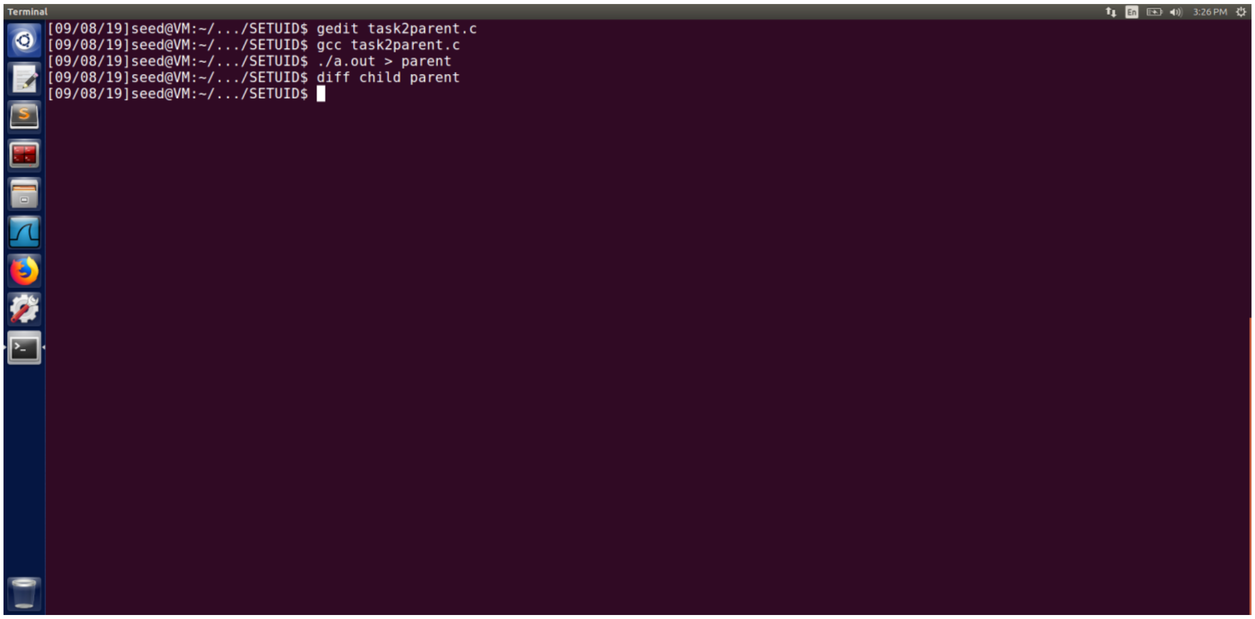


```
[09/08/19]seed@VM:~/.../SETUID$ gcc task2.c
task2.c: In function ‘main’:
task2.c:23:1: error: expected declaration or statement at end of input
 }
 ^
[09/08/19]seed@VM:~/.../SETUID$ gedit task2.c
[09/08/19]seed@VM:~/.../SETUID$ gcc task2.c
[09/08/19]seed@VM:~/.../SETUID$ ./a.out > child
[09/08/19]seed@VM:~/.../SETUID$ more child
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/li
b/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.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-zc5RxtSgBU
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
_=./a.out
OLDPWD=/home/seed/Documents
[09/08/19]seed@VM:~/.../SETUID$
```

We compiled and ran the child process first and saw that it prints all the environment variables of both child process and as well as the parent

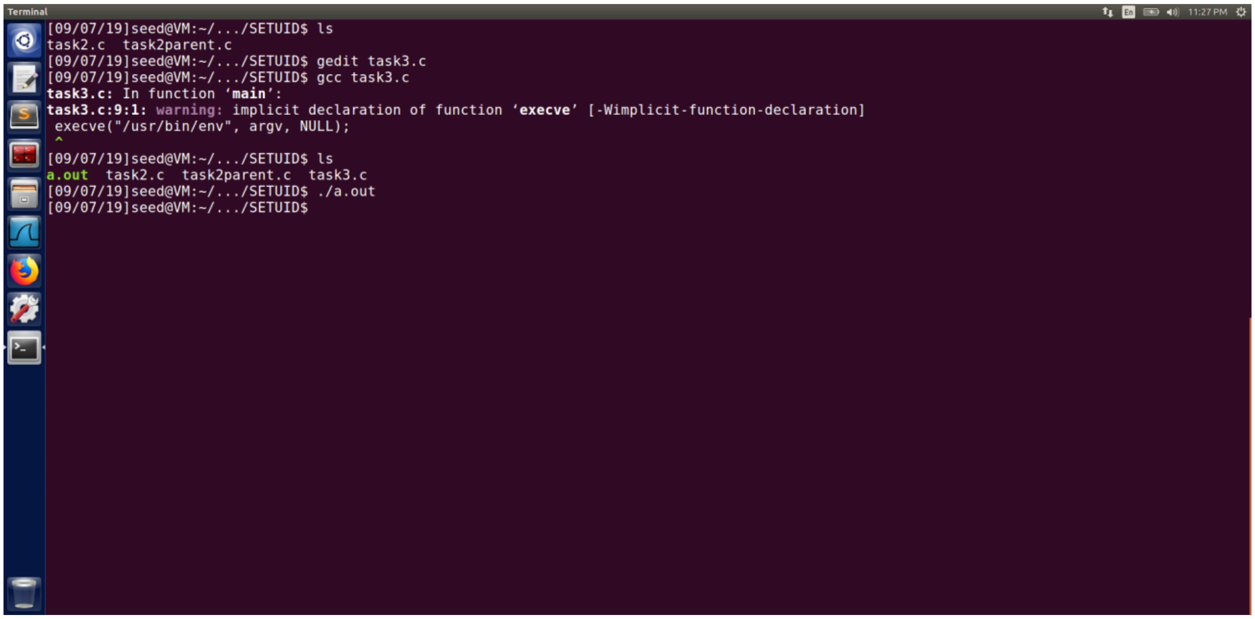


```
[09/08/19]seed@VM:~/.../SETUID$ gedit task2parent.c
[09/08/19]seed@VM:~/.../SETUID$ gcc task2parent.c
[09/08/19]seed@VM:~/.../SETUID$ ./a.out > parent
[09/08/19]seed@VM:~/.../SETUID$ diff child parent
[09/08/19]seed@VM:~/.../SETUID$
```

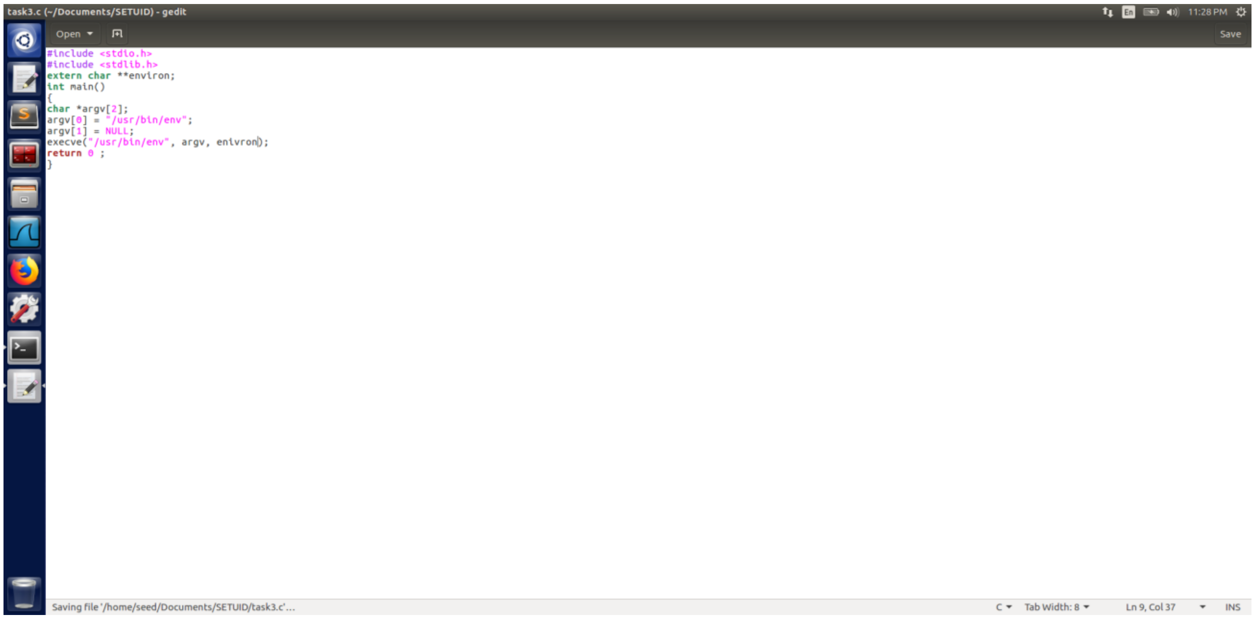
process.

When we use the diff command to child’s and parent’s environment variables we see that there is no difference because the child has inherited all of the parents environment.

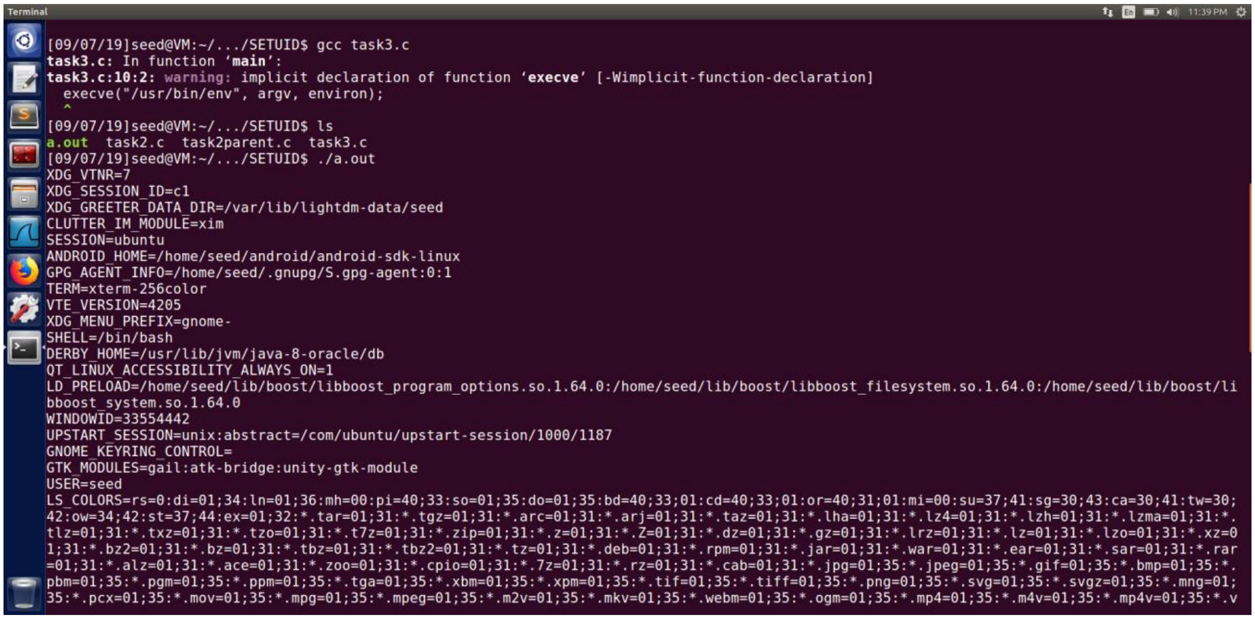
Task 3



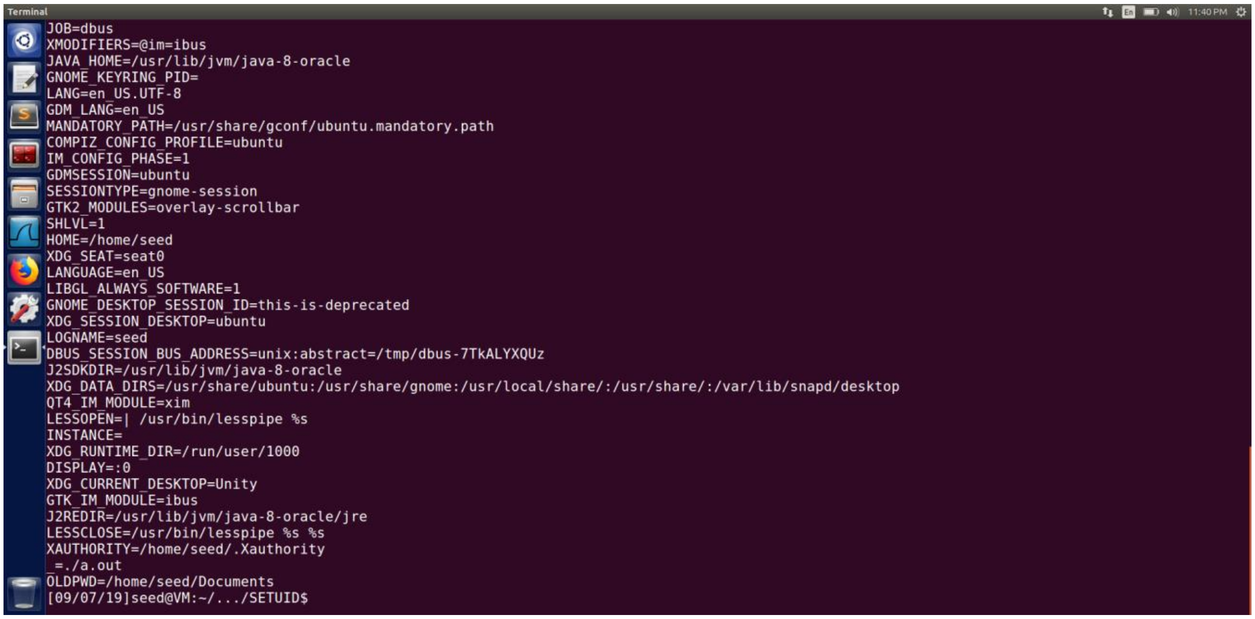
```
[09/07/19]seed@VM:~/.../SETUID$ ls
task2.c  task2parent.c
[09/07/19]seed@VM:~/.../SETUID$ gedit task3.c
[09/07/19]seed@VM:~/.../SETUID$ gcc task3.c
task3.c: In function ‘main’:
task3.c:9:1: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-declaration]
 execve("/usr/bin/env", argv, NULL);
 ^
[09/07/19]seed@VM:~/.../SETUID$ ls
a.out  task2.c  task2parent.c  task3.c
[09/07/19]seed@VM:~/.../SETUID$ ./a.out
[09/07/19]seed@VM:~/.../SETUID$
```


task3.c (~/Documents/SETUID) - gedit
11:28 PM
Open
Save
Saving file '/home/seed/Documents/SETUID/task3.c'...
C
Tab Width: 8
Ln 9, Col 37
INS

```c
#include <stdio.h>
#include <stdlib.h>
extern char **environ;
int main()
{
char *argv[2];
argv[0] = "/usr/bin/env";
argv[1] = NULL;
execve("/usr/bin/env", argv, enivron);
return 0 ;
}
```



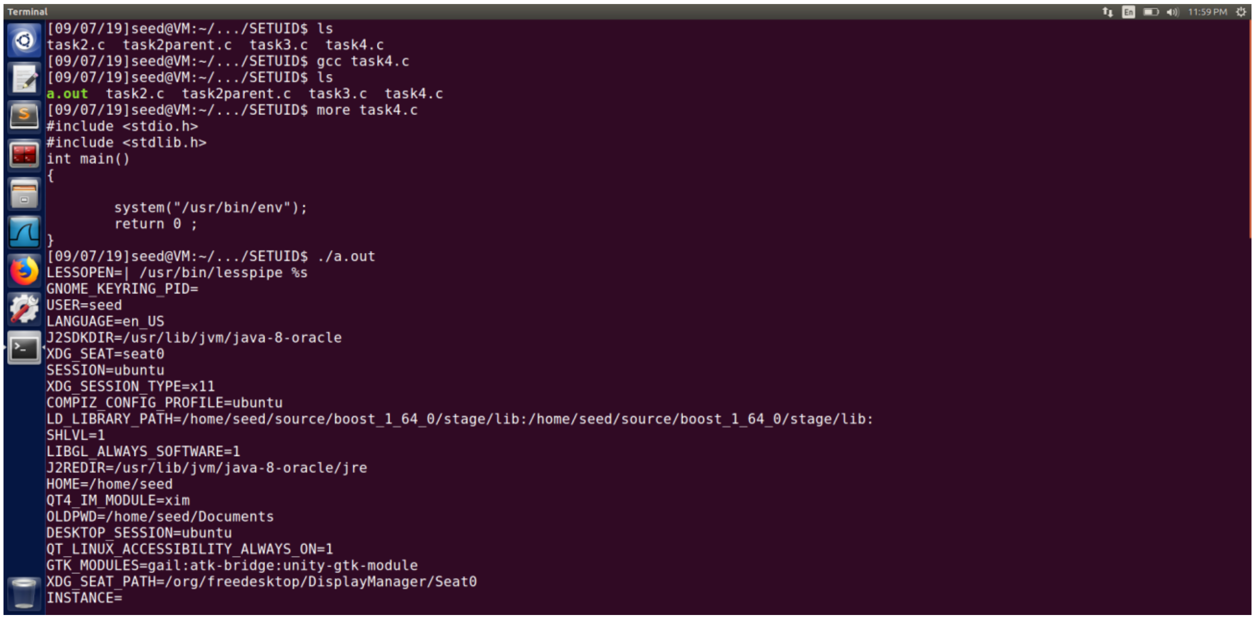
```
[09/07/19]seed@VM:~/.../SETUID$ gcc task3.c
task3.c: In function ‘main’:
task3.c:10:2: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-declaration]
  execve("/usr/bin/env", argv, environ);
  ^
[09/07/19]seed@VM:~/.../SETUID$ ls
a.out  task2.c  task2parent.c  task3.c
[09/07/19]seed@VM:~/.../SETUID$ ./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/li
bboost_system.so.1.64.0
WINDOWID=33554442
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1187
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=0
1;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:*.v
```



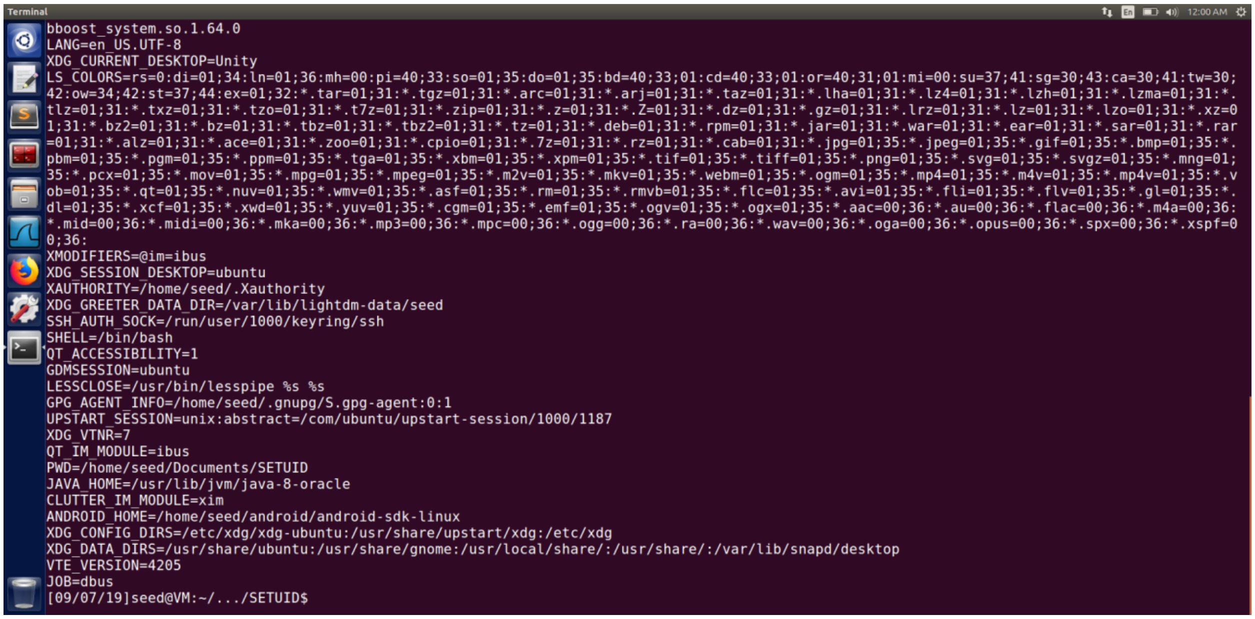
```
JOB=dbus
XMODIFIERS=@im=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
GDM_LANG=en_US
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
COMPIZ_CONFIG_PROFILE=ubuntu
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
SHLVL=1
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-7TkALYXQUz
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
_=./a.out
OLDPWD=/home/seed/Documents
[09/07/19]seed@VM:~/.../SETUID$
```

When the 3rd argument of the execve() command was NULL we saw that it prints nothing since only shell is returned however, when we replace that with environ we can see that all the environment variables are printed.

Task 4



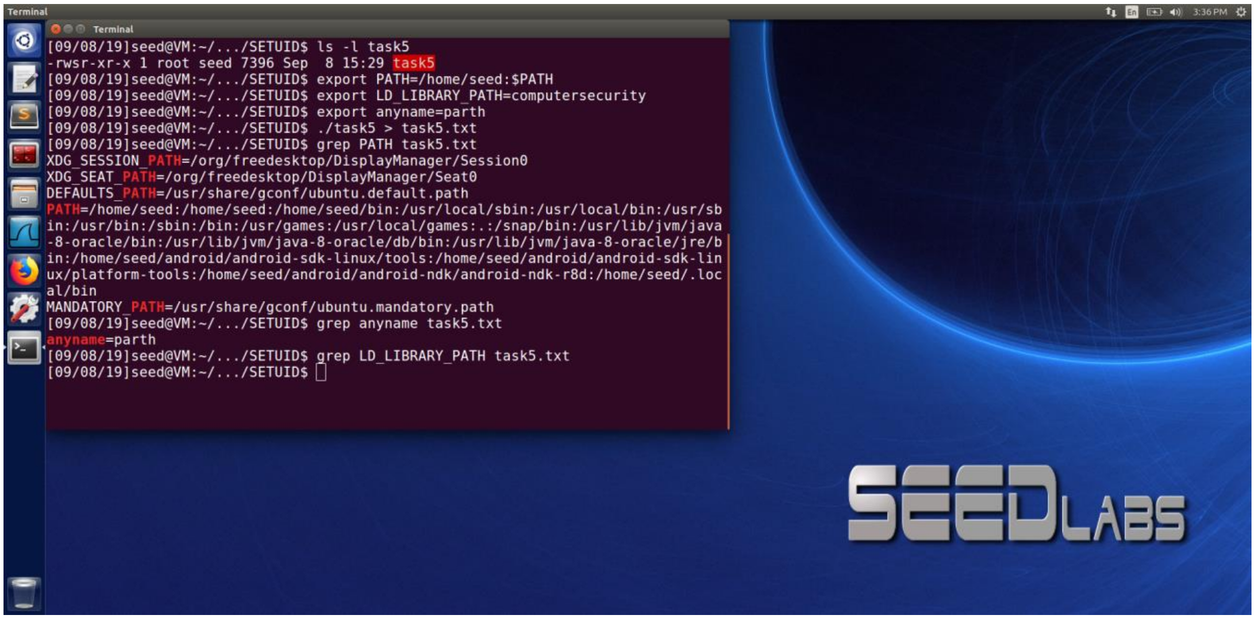
```
[09/07/19]seed@VM:~/.../SETUID$ ls
task2.c  task2parent.c  task3.c  task4.c
[09/07/19]seed@VM:~/.../SETUID$ gcc task4.c
[09/07/19]seed@VM:~/.../SETUID$ ls
a.out  task2.c  task2parent.c  task3.c  task4.c
[09/07/19]seed@VM:~/.../SETUID$ more task4.c
#include <stdio.h>
#include <stdlib.h>
int main()
{

        system("/usr/bin/env");
        return 0 ;
}
[09/07/19]seed@VM:~/.../SETUID$ ./a.out
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/seed/Documents
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=
```



```
bboost_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=0
1;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:*.v
ob=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=0
0;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/1000/1187
XDG_VTNR=7
QT_IM_MODULE=ibus
PWD=/home/seed/Documents/SETUID
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
[09/07/19]seed@VM:~/.../SETUID$
```

We can see from the above screenshot that when the program is executed it is not executed directly. First, it calls the shell which then executes the command. The environment variables are passed to the shell and then it is executed by the execve function.

Task 5

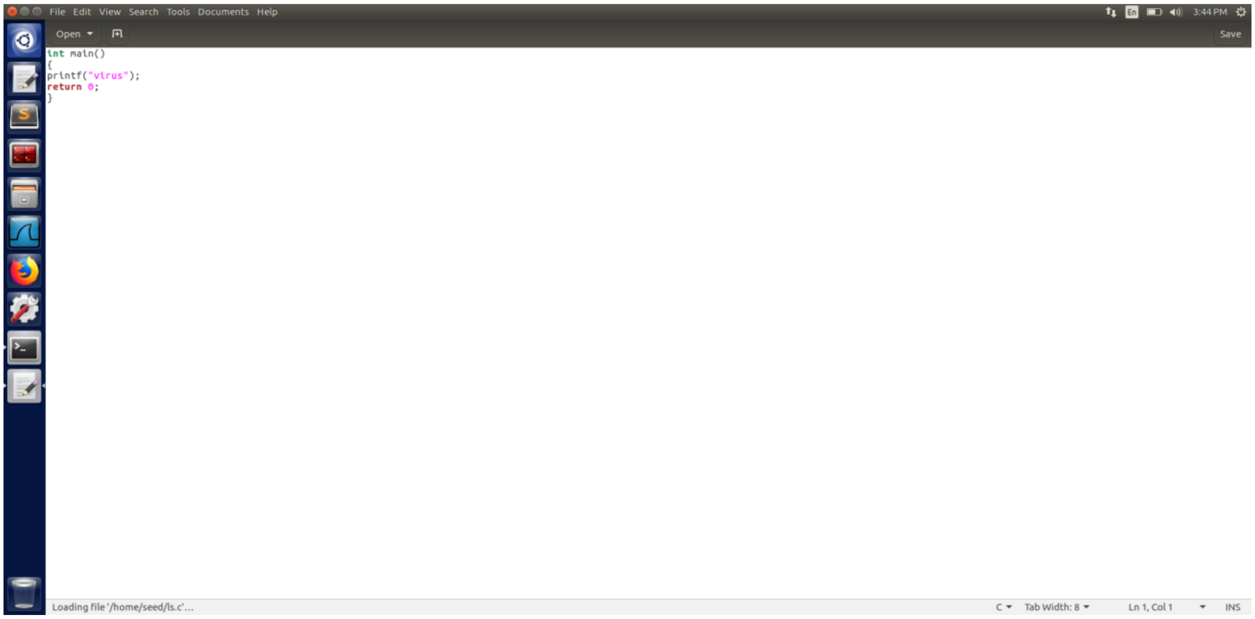


```
[09/08/19]seed@VM:~/.../SETUID$ ls -l task5
-rwsr-xr-x 1 root seed 7396 Sep  8 15:29 task5
[09/08/19]seed@VM:~/.../SETUID$ export PATH=/home/seed:$PATH
[09/08/19]seed@VM:~/.../SETUID$ export LD_LIBRARY_PATH=computersecurity
[09/08/19]seed@VM:~/.../SETUID$ export anyname=parth
[09/08/19]seed@VM:~/.../SETUID$ ./task5 > task5.txt
[09/08/19]seed@VM:~/.../SETUID$ grep PATH task5.txt
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
PATH=/home/seed:/home/seed:/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sb
in:/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/b
in:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-lin
ux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.loc
al/bin
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
[09/08/19]seed@VM:~/.../SETUID$ grep anyname task5.txt
anyname=parth
[09/08/19]seed@VM:~/.../SETUID$ grep LD_LIBRARY_PATH task5.txt
[09/08/19]seed@VM:~/.../SETUID$
```

After compiling and running the program and changing its ownership to root and then making it a setuid program and then setting the 3 environment variable. And then after running the program we can see that all of the export command except LD_LIBRARY _PATH are inherited.

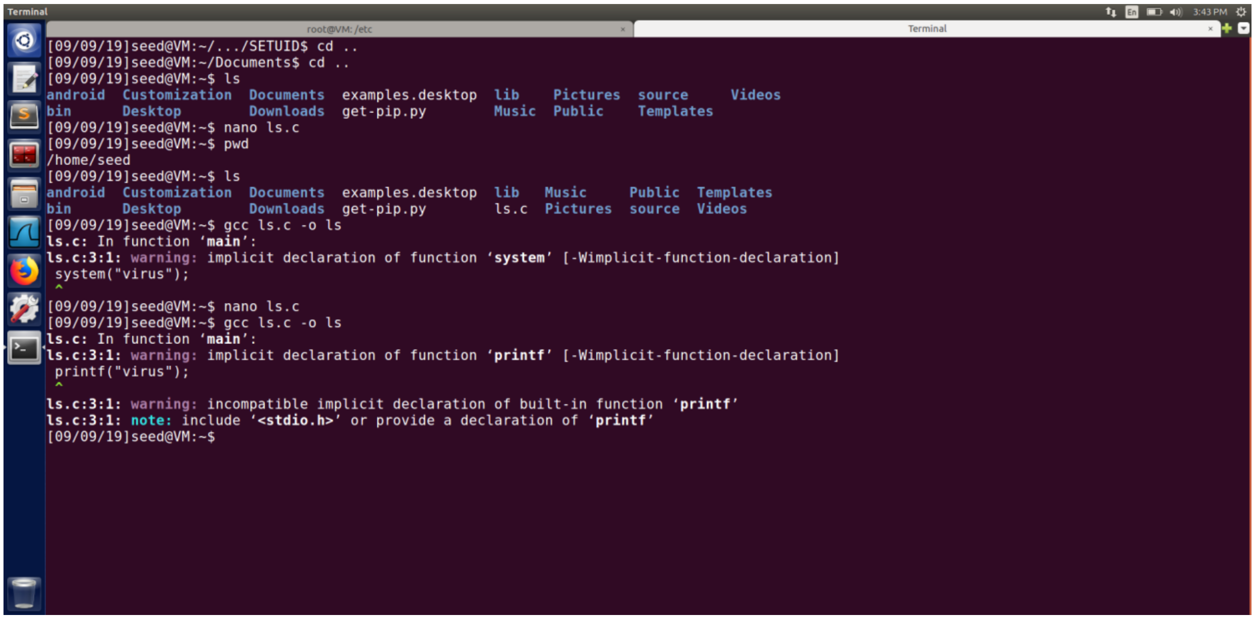
It is because there is some protection for this environment variable as it is used for shared libraries and therefore, preventing any malicious file from being placed into shared library.

Task 6

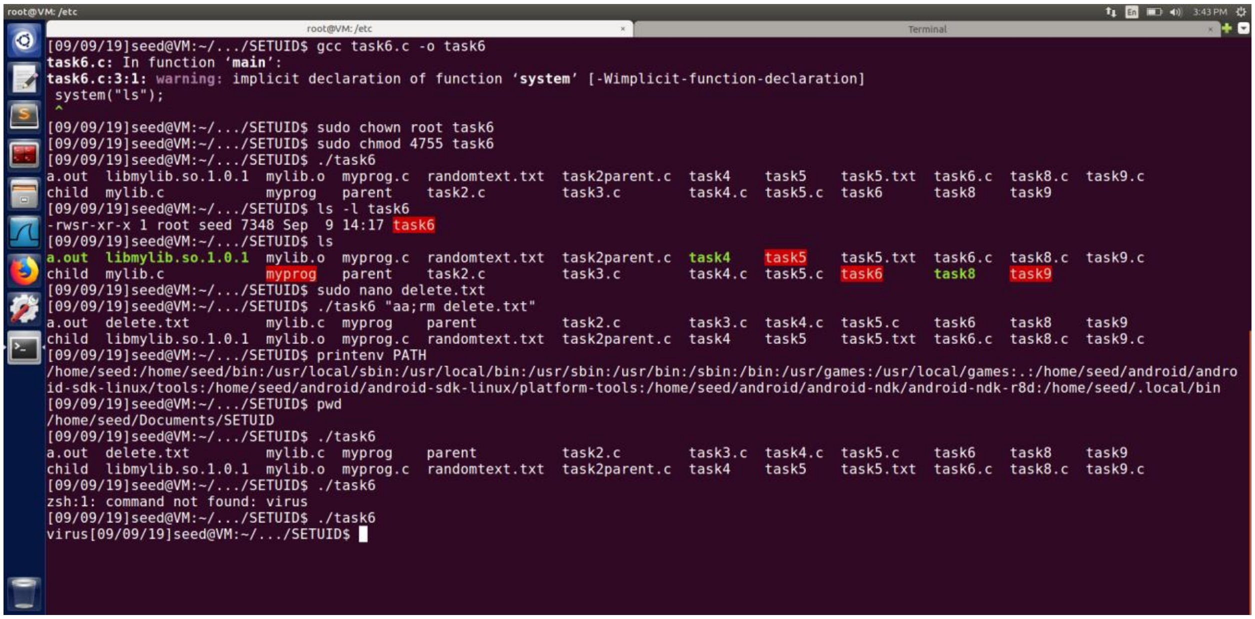


```
int main()
{
printf("virus");
return 0;
}
```

Loading file '/home/seed/ls.c'...



```
[09/09/19]seed@VM:~/.../SETUID$ cd ..
[09/09/19]seed@VM:~/Documents$ cd ..
[09/09/19]seed@VM:~$ ls
android  Customization  Documents  examples.desktop  lib    Pictures  source     Videos
bin      Desktop        Downloads  get-pip.py        Music  Public    Templates
[09/09/19]seed@VM:~$ nano ls.c
[09/09/19]seed@VM:~$ pwd
/home/seed
[09/09/19]seed@VM:~$ ls
android  Customization  Documents  examples.desktop  lib   Music     Public  Templates
bin      Desktop        Downloads  get-pip.py        ls.c  Pictures  source  Videos
[09/09/19]seed@VM:~$ gcc ls.c -o ls
ls.c: In function ‘main’:
ls.c:3:1: warning: implicit declaration of function ‘system’ [-Wimplicit-function-declaration]
 system("virus");
 ^

[09/09/19]seed@VM:~$ nano ls.c
[09/09/19]seed@VM:~$ gcc ls.c -o ls
ls.c: In function ‘main’:
ls.c:3:1: warning: implicit declaration of function ‘printf’ [-Wimplicit-function-declaration]
 printf("virus");
 ^

ls.c:3:1: warning: incompatible implicit declaration of built-in function ‘printf’
ls.c:3:1: note: include ‘<stdio.h>’ or provide a declaration of ‘printf’
[09/09/19]seed@VM:~$
```

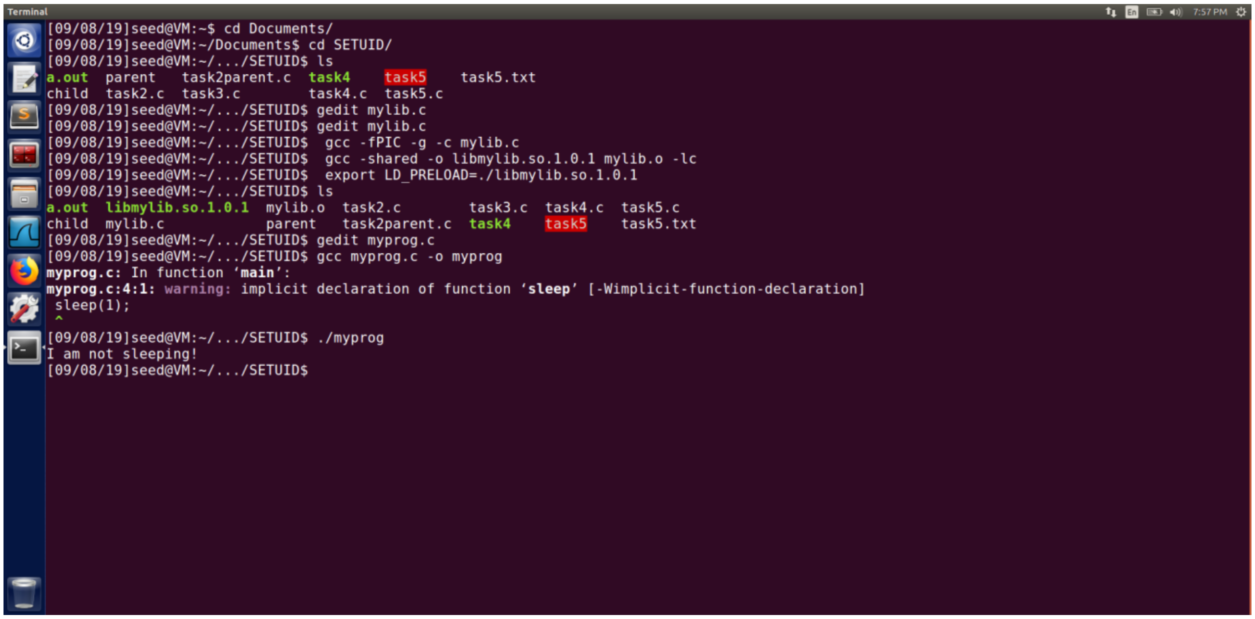


```
[09/09/19]seed@VM:~/.../SETUID$ gcc task6.c -o task6
task6.c: In function ‘main’:
task6.c:3:1: warning: implicit declaration of function ‘system’ [-Wimplicit-function-declaration]
 system("ls");
 ^
[09/09/19]seed@VM:~/.../SETUID$ sudo chown root task6
[09/09/19]seed@VM:~/.../SETUID$ sudo chmod 4755 task6
[09/09/19]seed@VM:~/.../SETUID$ ./task6
a.out  libmylib.so.1.0.1  mylib.o  myprog.c  randomtext.txt  task2parent.c  task4    task5    task5.txt  task6.c  task8.c  task9.c
child  mylib.c            myprog   parent    task2.c         task3.c        task4.c  task5.c  task6      task8    task9
[09/09/19]seed@VM:~/.../SETUID$ ls -l task6
-rwsr-xr-x 1 root seed 7348 Sep  9 14:17 task6
[09/09/19]seed@VM:~/.../SETUID$ ls
a.out  libmylib.so.1.0.1  mylib.o  myprog.c  randomtext.txt  task2parent.c  task4    task5    task5.txt  task6.c  task8.c  task9.c
child  mylib.c            myprog   parent    task2.c         task3.c        task4.c  task5.c  task6      task8    task9
[09/09/19]seed@VM:~/.../SETUID$ sudo nano delete.txt
[09/09/19]seed@VM:~/.../SETUID$ ./task6 "aa;rm delete.txt"
a.out  delete.txt         mylib.c  myprog    parent          task2.c        task3.c  task4.c  task5.c    task6    task8    task9
child  libmylib.so.1.0.1  mylib.o  myprog.c  randomtext.txt  task2parent.c  task4    task5    task5.txt  task6.c  task8.c  task9.c
[09/09/19]seed@VM:~/.../SETUID$ printenv PATH
/home/seed:/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/home/seed/android/andro
id-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
[09/09/19]seed@VM:~/.../SETUID$ pwd
/home/seed/Documents/SETUID
[09/09/19]seed@VM:~/.../SETUID$ ./task6
a.out  delete.txt         mylib.c  myprog    parent          task2.c        task3.c  task4.c  task5.c    task6    task8    task9
child  libmylib.so.1.0.1  mylib.o  myprog.c  randomtext.txt  task2parent.c  task4    task5    task5.txt  task6.c  task8.c  task9.c
[09/09/19]seed@VM:~/.../SETUID$ ./task6
zsh:1: command not found: virus
[09/09/19]seed@VM:~/.../SETUID$ ./task6
virus[09/09/19]seed@VM:~/.../SETUID$ 
```

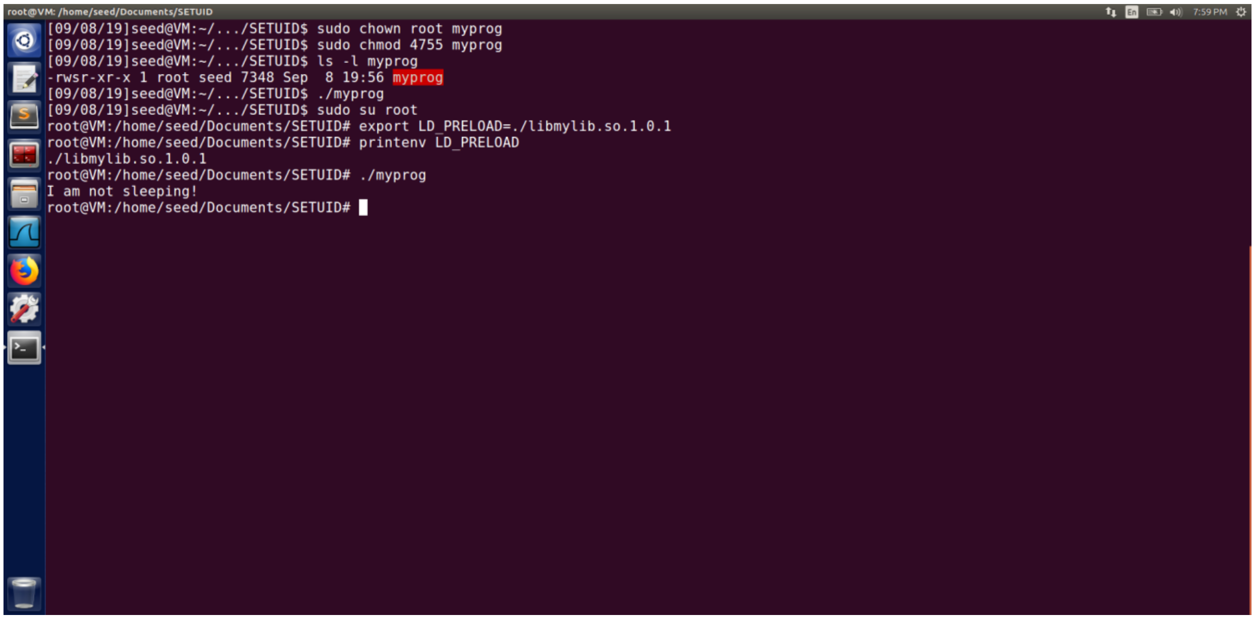
We first created the program with name task6.c and then compiled and changed its ownership to root and made it a setuid program after which we change the PATH environment variable. And then we create a new program ls and compile it.

We can see from the above screenshot that when the ls command is being searched it runs that program instead of the shell ls command which means that SET-UID program may run malicious file if the PATH variable is changed.

Task 7

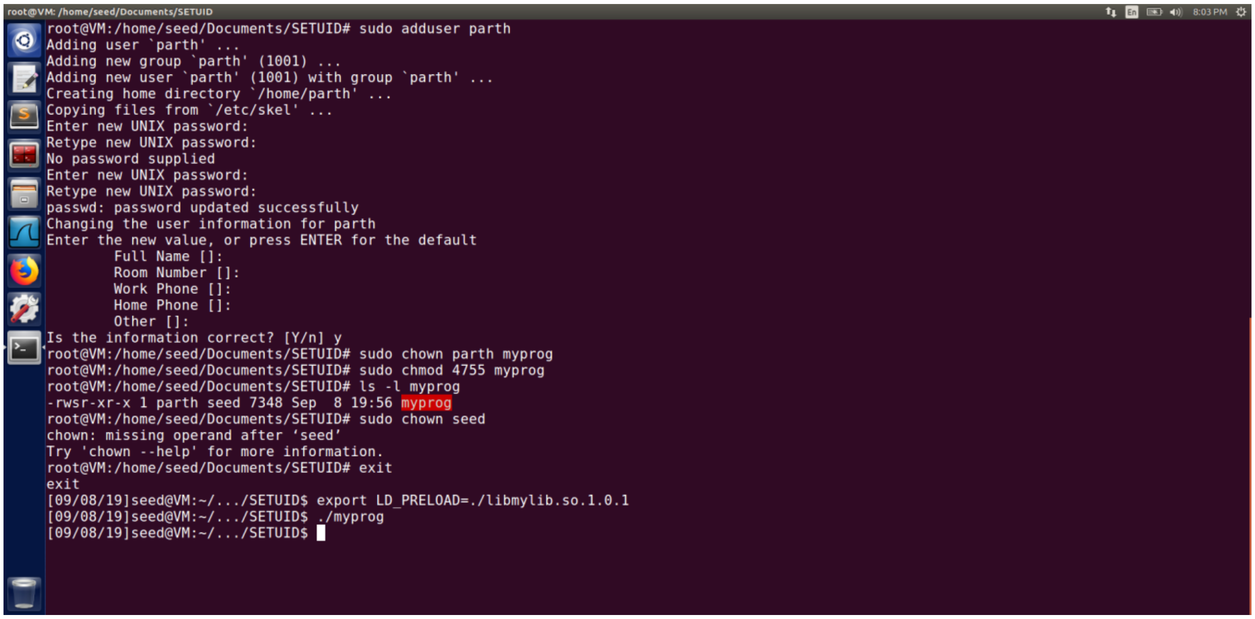


```
[09/08/19]seed@VM:~$ cd Documents/
[09/08/19]seed@VM:~/Documents$ cd SETUID/
[09/08/19]seed@VM:~/.../SETUID$ ls
a.out  parent   task2parent.c  task4    task5    task5.txt
child  task2.c  task3.c        task4.c  task5.c
[09/08/19]seed@VM:~/.../SETUID$ gedit mylib.c
[09/08/19]seed@VM:~/.../SETUID$ gedit mylib.c
[09/08/19]seed@VM:~/.../SETUID$  gcc -fPIC -g -c mylib.c
[09/08/19]seed@VM:~/.../SETUID$  gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[09/08/19]seed@VM:~/.../SETUID$  export LD_PRELOAD=./libmylib.so.1.0.1
[09/08/19]seed@VM:~/.../SETUID$ ls
a.out  libmylib.so.1.0.1  mylib.o  task2.c        task3.c  task4.c  task5.c
child  mylib.c            parent   task2parent.c  task4    task5    task5.txt
[09/08/19]seed@VM:~/.../SETUID$ gedit myprog.c
[09/08/19]seed@VM:~/.../SETUID$ gcc myprog.c -o myprog
myprog.c: In function ‘main’:
myprog.c:4:1: warning: implicit declaration of function ‘sleep’ [-Wimplicit-function-declaration]
 sleep(1);
 ^
[09/08/19]seed@VM:~/.../SETUID$ ./myprog
I am not sleeping!
[09/08/19]seed@VM:~/.../SETUID$
```



```
[09/08/19]seed@VM:~/.../SETUID$ sudo chown root myprog
[09/08/19]seed@VM:~/.../SETUID$ sudo chmod 4755 myprog
[09/08/19]seed@VM:~/.../SETUID$ ls -l myprog
-rwsr-xr-x 1 root seed 7348 Sep  8 19:56 myprog
[09/08/19]seed@VM:~/.../SETUID$ ./myprog
[09/08/19]seed@VM:~/.../SETUID$ sudo su root
root@VM:/home/seed/Documents/SETUID# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Documents/SETUID# printenv LD_PRELOAD
./libmylib.so.1.0.1
root@VM:/home/seed/Documents/SETUID# ./myprog
I am not sleeping!
root@VM:/home/seed/Documents/SETUID# 
```

We can see from the above screenshot that after creating, compiling and then executing myprog program from the root account. Also, setting the LD_PRELOAD pointing to dll we can see that the program calls the mylib dll



```
root@VM:/home/seed/Documents/SETUID# sudo adduser parth
Adding user `parth' ...
Adding new group `parth' (1001) ...
Adding new user `parth' (1001) with group `parth' ...
Creating home directory `/home/parth' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
No password supplied
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for parth
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@VM:/home/seed/Documents/SETUID# sudo chown parth myprog
root@VM:/home/seed/Documents/SETUID# sudo chmod 4755 myprog
root@VM:/home/seed/Documents/SETUID# ls -l myprog
-rwsr-xr-x 1 parth seed 7348 Sep  8 19:56 myprog
root@VM:/home/seed/Documents/SETUID# sudo chown seed
chown: missing operand after ‘seed’
Try 'chown --help' for more information.
root@VM:/home/seed/Documents/SETUID# exit
exit
[09/08/19]seed@VM:~/.../SETUID$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/08/19]seed@VM:~/.../SETUID$ ./myprog
[09/08/19]seed@VM:~/.../SETUID$ 
```

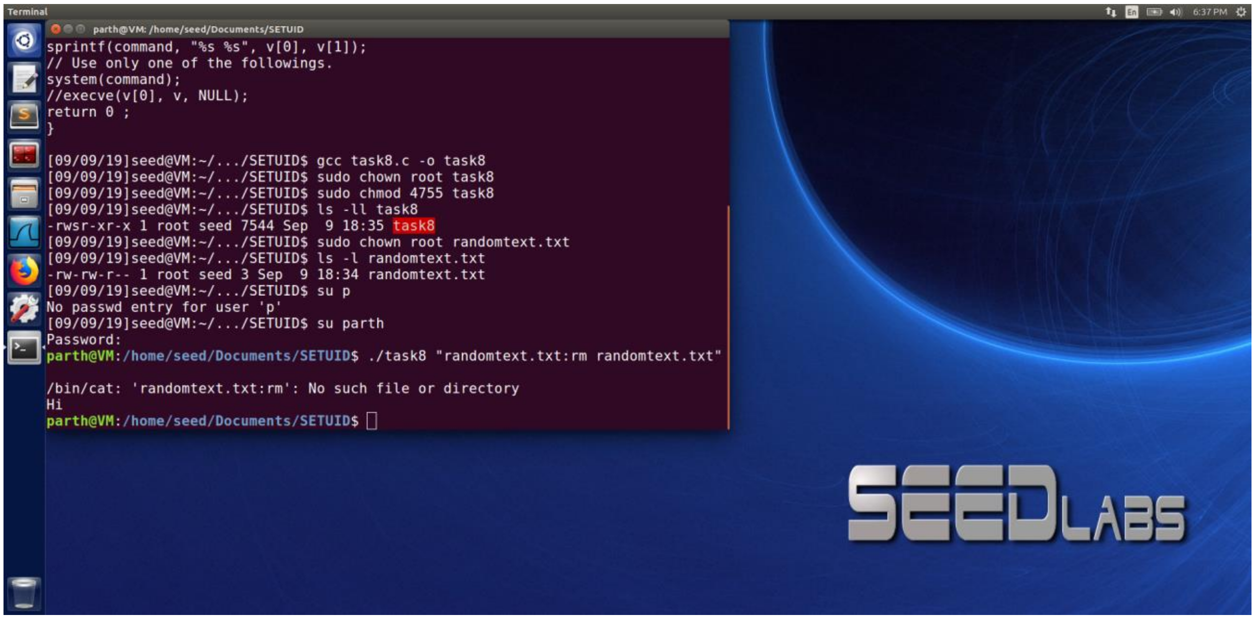
Now, when we make the myprog a setuid program that is owned by a new user named ‘parth’ and then running the program from another account ‘seed’ we can see that myprog doesn’t invoke the DLL.

LD_PRELOAD is ignored if SETUID program tries to access it acting as a protection.

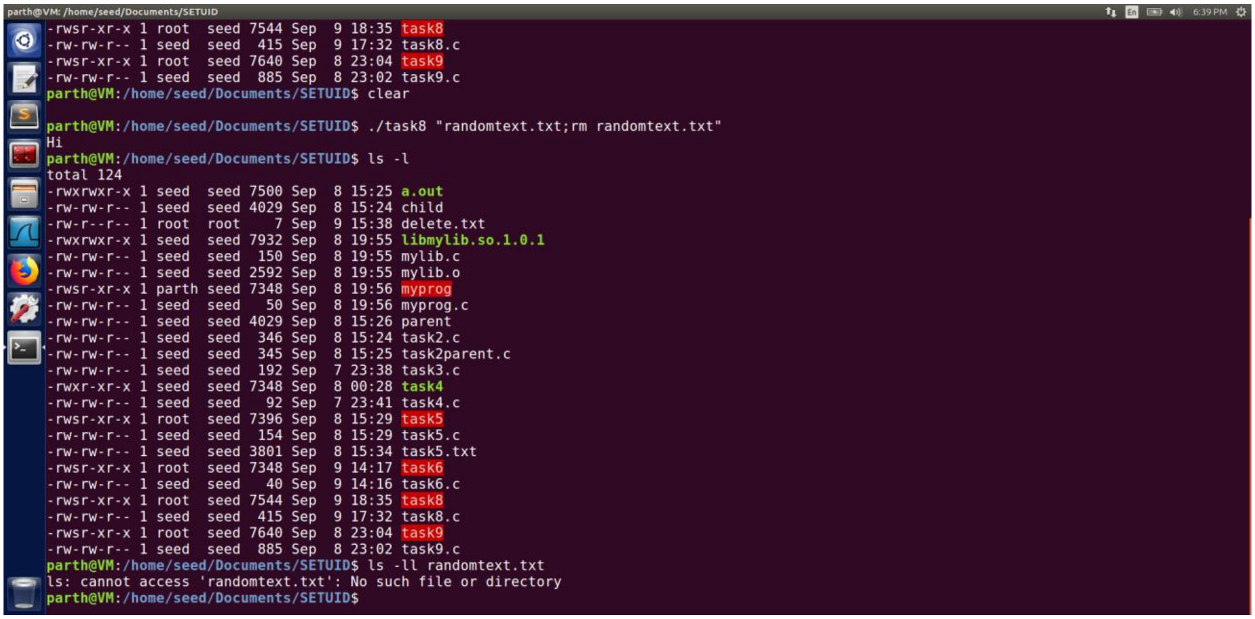
In the 1st screenshot it was executed without a setuid program and therefore LD_PRELOAD is not ignored whereas, in the 2nd case myprog being a setuid and run by a normal user the LD_PRELOAD is ignored and the file created by us isn't accessed. And that while executing the same with the root account both being accessible by root it can run the DLL that we created.

Task 8

i.



```
sprintf(command, "%s %s", v[0], v[1]);
// Use only one of the followings.
system(command);
//execve(v[0], v, NULL);
return 0 ;
}

[09/09/19]seed@VM:~/.../SETUID$ gcc task8.c -o task8
[09/09/19]seed@VM:~/.../SETUID$ sudo chown root task8
[09/09/19]seed@VM:~/.../SETUID$ sudo chmod 4755 task8
[09/09/19]seed@VM:~/.../SETUID$ ls -ll task8
-rwsr-xr-x 1 root seed 7544 Sep  9 18:35 task8
[09/09/19]seed@VM:~/.../SETUID$ sudo chown root randomtext.txt
[09/09/19]seed@VM:~/.../SETUID$ ls -l randomtext.txt
-rw-rw-r-- 1 root seed 3 Sep  9 18:34 randomtext.txt
[09/09/19]seed@VM:~/.../SETUID$ su p
No passwd entry for user 'p'
[09/09/19]seed@VM:~/.../SETUID$ su parth
Password:
parth@VM:/home/seed/Documents/SETUID$ ./task8 "randomtext.txt:rm randomtext.txt"

/bin/cat: 'randomtext.txt:rm': No such file or directory
Hi
parth@VM:/home/seed/Documents/SETUID$ 
```

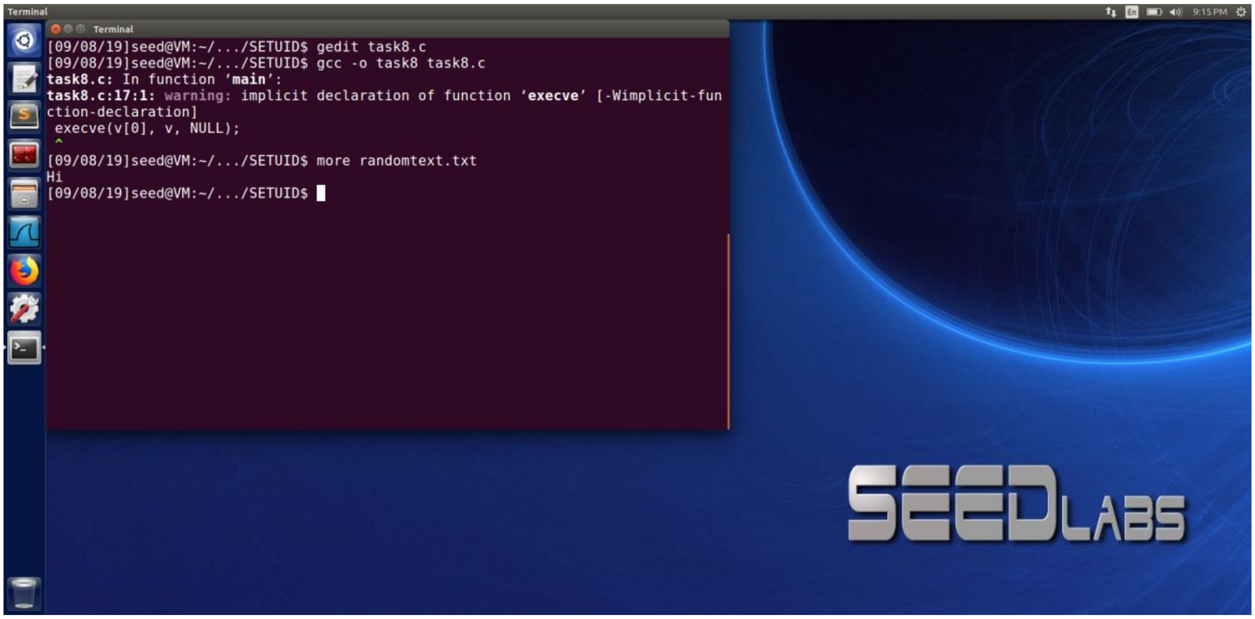


```
-rwsr-xr-x 1 root  seed 7544 Sep  9 18:35 task8
-rw-rw-r-- 1 seed  seed  415 Sep  9 17:32 task8.c
-rwsr-xr-x 1 root  seed 7640 Sep  8 23:04 task9
-rw-rw-r-- 1 seed  seed  885 Sep  8 23:02 task9.c
parth@VM:/home/seed/Documents/SETUID$ clear

parth@VM:/home/seed/Documents/SETUID$ ./task8 "randomtext.txt;rm randomtext.txt"
Hi
parth@VM:/home/seed/Documents/SETUID$ ls -l
total 124
-rwxrwxr-x 1 seed  seed 7500 Sep  8 15:25 a.out
-rw-rw-r-- 1 seed  seed 4029 Sep  8 15:24 child
-rw-r--r-- 1 root  root    7 Sep  9 15:38 delete.txt
-rwxrwxr-x 1 seed  seed 7932 Sep  8 19:55 libmylib.so.1.0.1
-rw-rw-r-- 1 seed  seed  150 Sep  8 19:55 mylib.c
-rw-rw-r-- 1 seed  seed 2592 Sep  8 19:55 mylib.o
-rwsr-xr-x 1 parth seed 7348 Sep  8 19:56 myprog
-rw-rw-r-- 1 seed  seed   50 Sep  8 19:56 myprog.c
-rw-rw-r-- 1 seed  seed 4029 Sep  8 15:26 parent
-rw-rw-r-- 1 seed  seed  346 Sep  8 15:24 task2.c
-rw-rw-r-- 1 seed  seed  345 Sep  8 15:25 task2parent.c
-rw-rw-r-- 1 seed  seed  192 Sep  7 23:38 task3.c
-rwxr-xr-x 1 seed  seed 7348 Sep  8 00:28 task4
-rw-rw-r-- 1 seed  seed   92 Sep  7 23:41 task4.c
-rwsr-xr-x 1 root  seed 7396 Sep  8 15:29 task5
-rw-rw-r-- 1 seed  seed  154 Sep  8 15:29 task5.c
-rw-rw-r-- 1 seed  seed 3801 Sep  8 15:34 task5.txt
-rwsr-xr-x 1 root  seed 7348 Sep  9 14:17 task6
-rw-rw-r-- 1 seed  seed   40 Sep  9 14:16 task6.c
-rwsr-xr-x 1 root  seed 7544 Sep  9 18:35 task8
-rw-rw-r-- 1 seed  seed  415 Sep  9 17:32 task8.c
-rwsr-xr-x 1 root  seed 7640 Sep  8 23:04 task9
-rw-rw-r-- 1 seed  seed  885 Sep  8 23:02 task9.c
parth@VM:/home/seed/Documents/SETUID$ ls -ll randomtext.txt
ls: cannot access 'randomtext.txt': No such file or directory
parth@VM:/home/seed/Documents/SETUID$
```

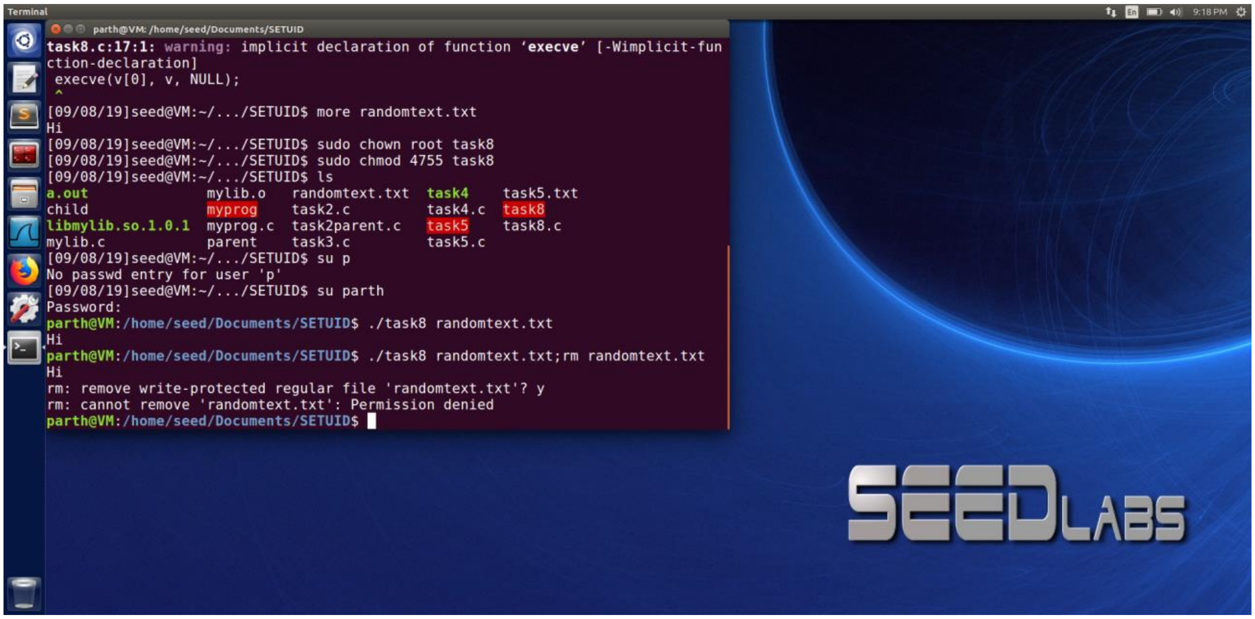
We first create a program compile it, change its owner to root and make it a set uid program after which we create another file named ' randomtext.txt' and change its owner to root. Now we login to another user named 'parth' and try to remove the file. It states 'No Such file or Directory' which means that the file has been deleted.

When system() command is executed it doesn't execute the command directly instead it calls the shell which then executes further therefore when the program has setuid the user gets the root privileges which is why it is then able to remove the files with root privileges.

ii.



```
[09/08/19]seed@VM:~/.../SETUID$ gedit task8.c
[09/08/19]seed@VM:~/.../SETUID$ gcc -o task8 task8.c
task8.c: In function ‘main’:
task8.c:17:1: warning: implicit declaration of function ‘execve’ [-Wimplicit-fun
ction-declaration]
 execve(v[0], v, NULL);
 ^
[09/08/19]seed@VM:~/.../SETUID$ more randomtext.txt
Hi
[09/08/19]seed@VM:~/.../SETUID$ 
```

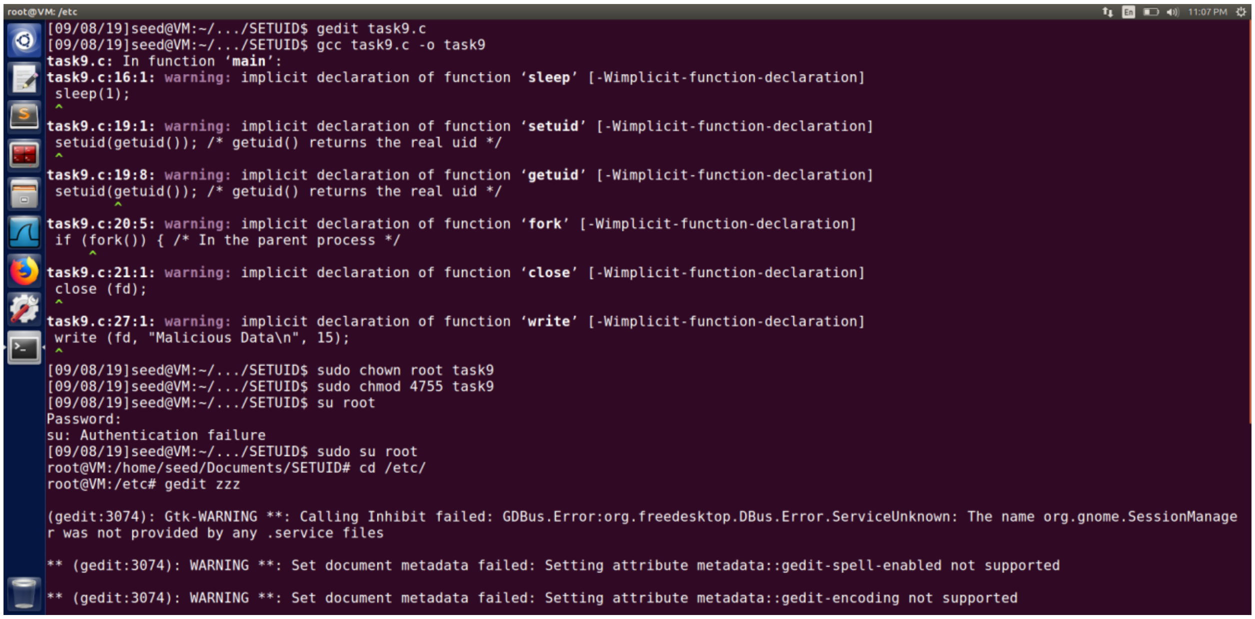


```
task8.c:17:1: warning: implicit declaration of function ‘execve’ [-Wimplicit-fun
ction-declaration]
 execve(v[0], v, NULL);
 ^
[09/08/19]seed@VM:~/.../SETUID$ more randomtext.txt
Hi
[09/08/19]seed@VM:~/.../SETUID$ sudo chown root task8
[09/08/19]seed@VM:~/.../SETUID$ sudo chmod 4755 task8
[09/08/19]seed@VM:~/.../SETUID$ ls
a.out              mylib.o   randomtext.txt  task4    task5.txt
child              myprog    task2.c         task4.c  task8
libmylib.so.1.0.1  myprog.c  task2parent.c   task5    task8.c
mylib.c            parent    task3.c         task5.c
[09/08/19]seed@VM:~/.../SETUID$ su p
No passwd entry for user 'p'
[09/08/19]seed@VM:~/.../SETUID$ su parth
Password:
parth@VM:/home/seed/Documents/SETUID$ ./task8 randomtext.txt
Hi
parth@VM:/home/seed/Documents/SETUID$ ./task8 randomtext.txt;rm randomtext.txt
Hi
rm: remove write-protected regular file 'randomtext.txt'? y
rm: cannot remove 'randomtext.txt': Permission denied
parth@VM:/home/seed/Documents/SETUID$
```

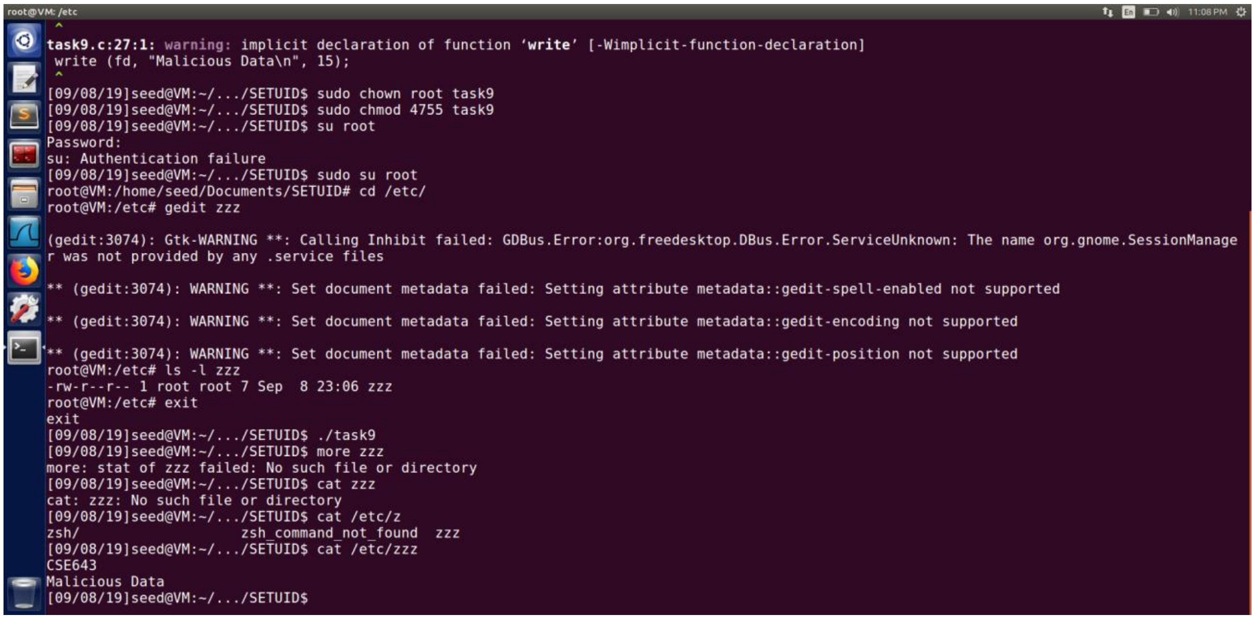
We first uncommented the execve function and commented the system command and then compiled the program changed its ownership to root and made it a setuid program andthen ran the code from a another user named ‘parth’ we can see that we are not able to remove the file.

This is because as soon we put something after ‘;’ it is assumed to be a new command and the root privileges are gone and therefore the command is executed with the privileges that the user name parth has which is why it cannot delete the file.

Task 9



```
[09/08/19]seed@VM:~/.../SETUID$ gedit task9.c
[09/08/19]seed@VM:~/.../SETUID$ gcc task9.c -o task9
task9.c: In function ‘main’:
task9.c:16:1: warning: implicit declaration of function ‘sleep’ [-Wimplicit-function-declaration]
 sleep(1);
 ^
task9.c:19:1: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
 setuid(getuid()); /* getuid() returns the real uid */
 ^
task9.c:19:8: warning: implicit declaration of function ‘getuid’ [-Wimplicit-function-declaration]
 setuid(getuid()); /* getuid() returns the real uid */
        ^
task9.c:20:5: warning: implicit declaration of function ‘fork’ [-Wimplicit-function-declaration]
 if (fork()) { /* In the parent process */
     ^
task9.c:21:1: warning: implicit declaration of function ‘close’ [-Wimplicit-function-declaration]
 close (fd);
 ^
task9.c:27:1: warning: implicit declaration of function ‘write’ [-Wimplicit-function-declaration]
 write (fd, "Malicious Data\n", 15);
 ^
[09/08/19]seed@VM:~/.../SETUID$ sudo chown root task9
[09/08/19]seed@VM:~/.../SETUID$ sudo chmod 4755 task9
[09/08/19]seed@VM:~/.../SETUID$ su root
Password:
su: Authentication failure
[09/08/19]seed@VM:~/.../SETUID$ sudo su root
root@VM:/home/seed/Documents/SETUID# cd /etc/
root@VM:/etc# gedit zzz

(gedit:3074): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManage
r was not provided by any .service files

** (gedit:3074): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported

** (gedit:3074): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
```



```
 ^
task9.c:27:1: warning: implicit declaration of function ‘write’ [-Wimplicit-function-declaration]
 write (fd, "Malicious Data\n", 15);
 ^
[09/08/19]seed@VM:~/.../SETUID$ sudo chown root task9
[09/08/19]seed@VM:~/.../SETUID$ sudo chmod 4755 task9
[09/08/19]seed@VM:~/.../SETUID$ su root
Password:
su: Authentication failure
[09/08/19]seed@VM:~/.../SETUID$ sudo su root
root@VM:/home/seed/Documents/SETUID# cd /etc/
root@VM:/etc# gedit zzz

(gedit:3074): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManage
r was not provided by any .service files

** (gedit:3074): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported

** (gedit:3074): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

** (gedit:3074): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
root@VM:/etc# ls -l zzz
-rw-r--r-- 1 root root 7 Sep  8 23:06 zzz
root@VM:/etc# exit
exit
[09/08/19]seed@VM:~/.../SETUID$ ./task9
[09/08/19]seed@VM:~/.../SETUID$ more zzz
more: stat of zzz failed: No such file or directory
[09/08/19]seed@VM:~/.../SETUID$ cat zzz
cat: zzz: No such file or directory
[09/08/19]seed@VM:~/.../SETUID$ cat /etc/z
zsh/                   zsh_command_not_found  zzz
[09/08/19]seed@VM:~/.../SETUID$ cat /etc/zzz
CSE643
Malicious Data
[09/08/19]seed@VM:~/.../SETUID$
```

As seen from the above screenshot that we created a new file named task9.c which we compiled, changed its ownership to root and made it a set uid bit. After which we change the user to ‘root’ and in the /etc/ directory we create a new file named zzz with the content ‘ CSE643’. And now we again go back to the account ‘seed’ from where we execute the command .

This is because the parents privileges were not downgraded because of which the child process was also able to access the file. This is known as capability leaking. To avoid this kind of attacks the ‘fd’ has to be closed before the new fork call.