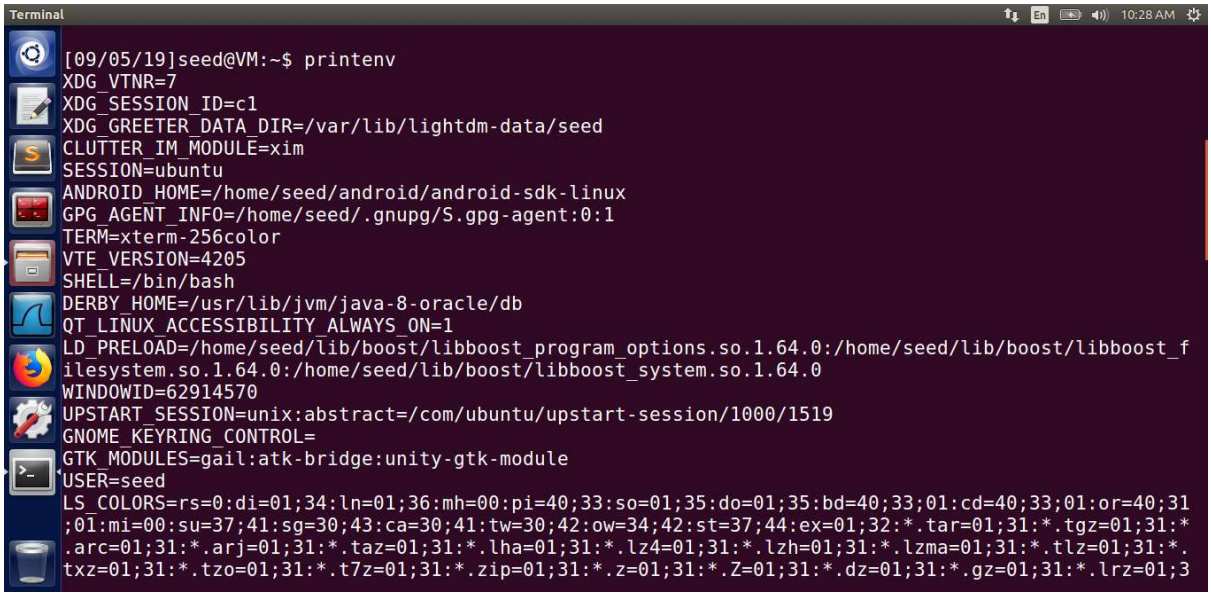
Assignment 1

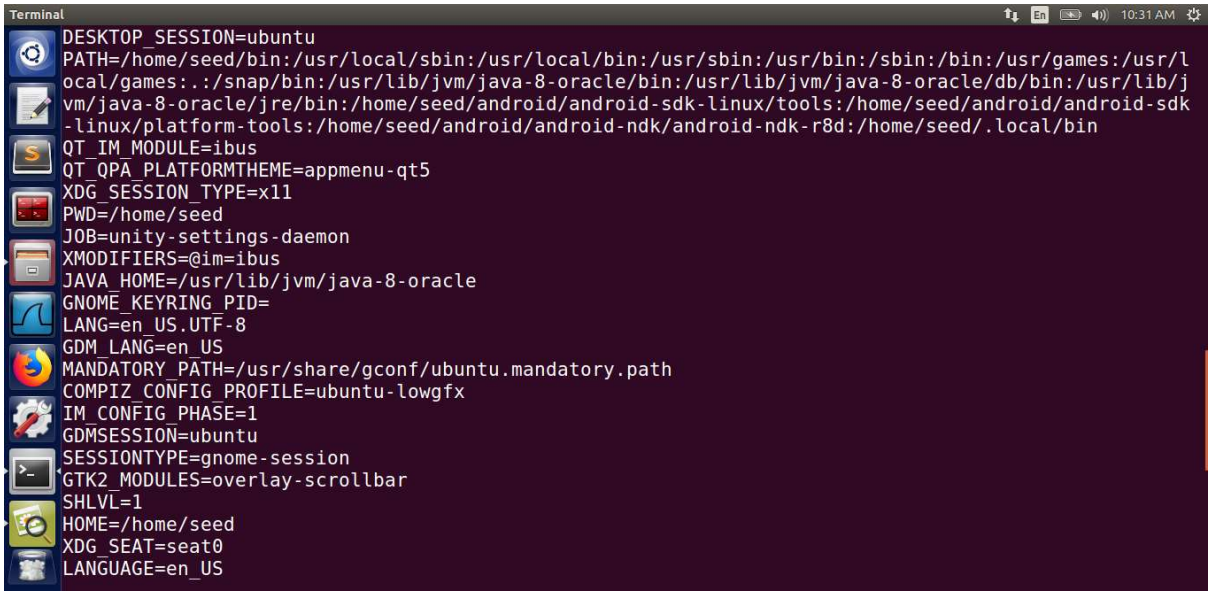
NAME: RISHI KUMAR SONI

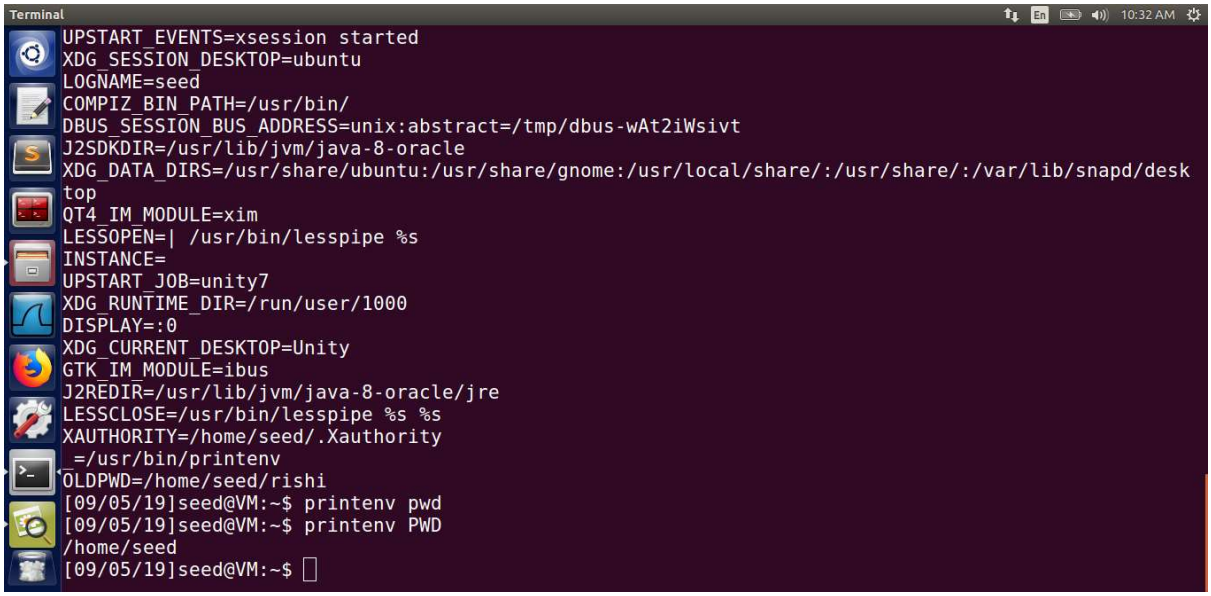
UTA-ID: 1001774020

Task 1

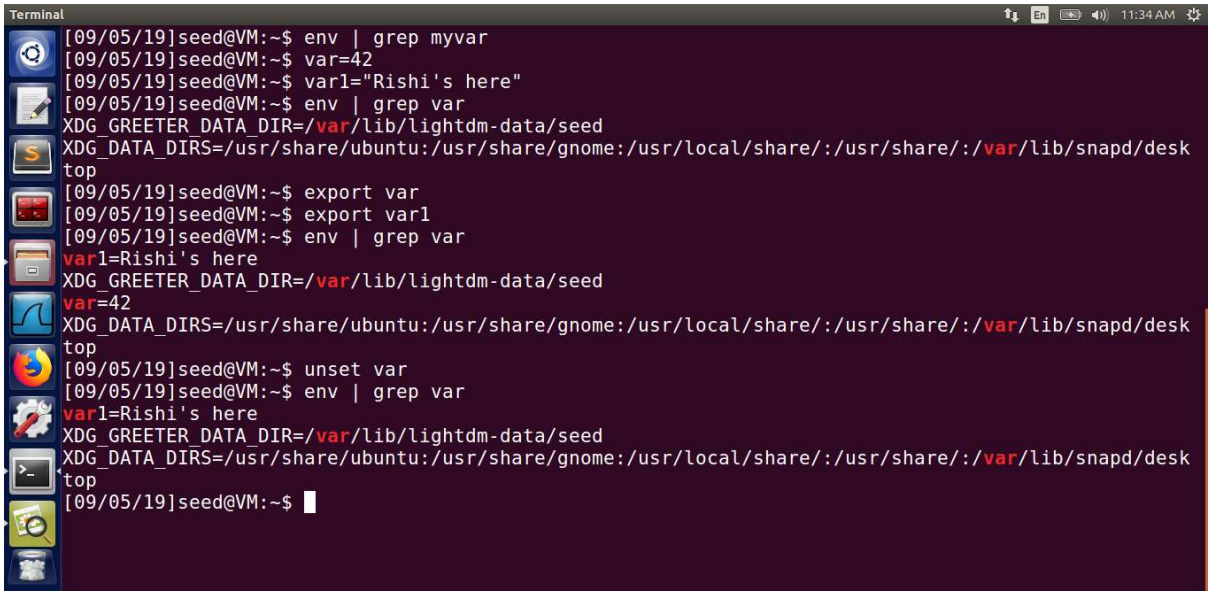
Environment Variable



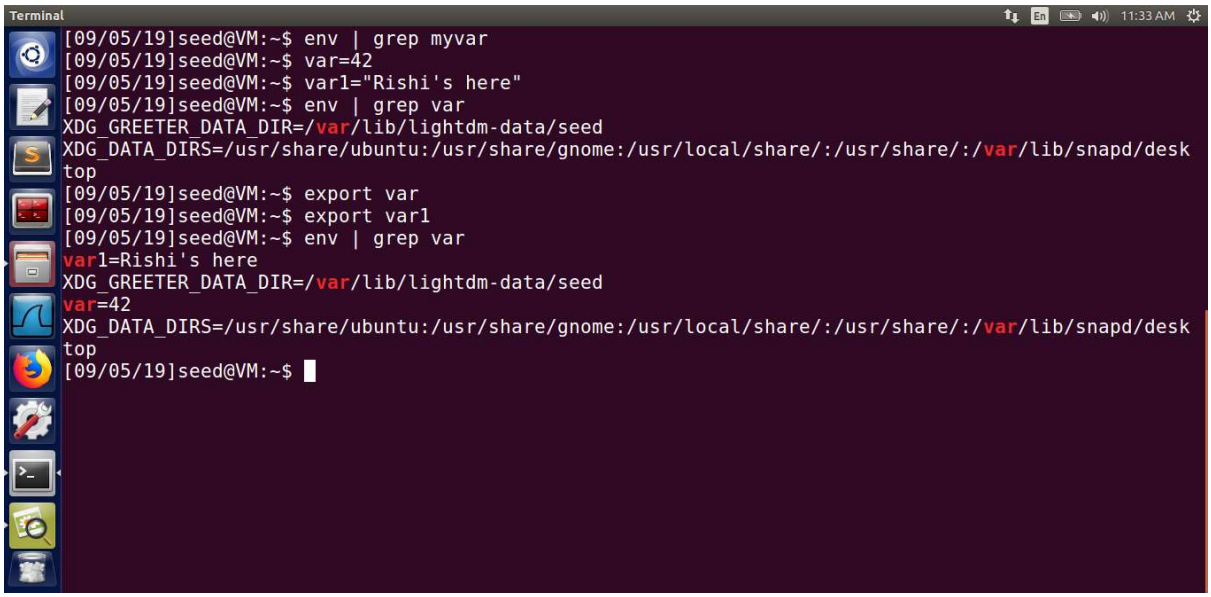




SET AND UNSET



VARIABLE EXPORT

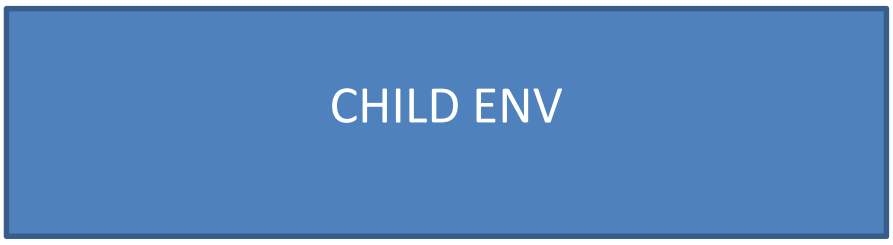


Task 2

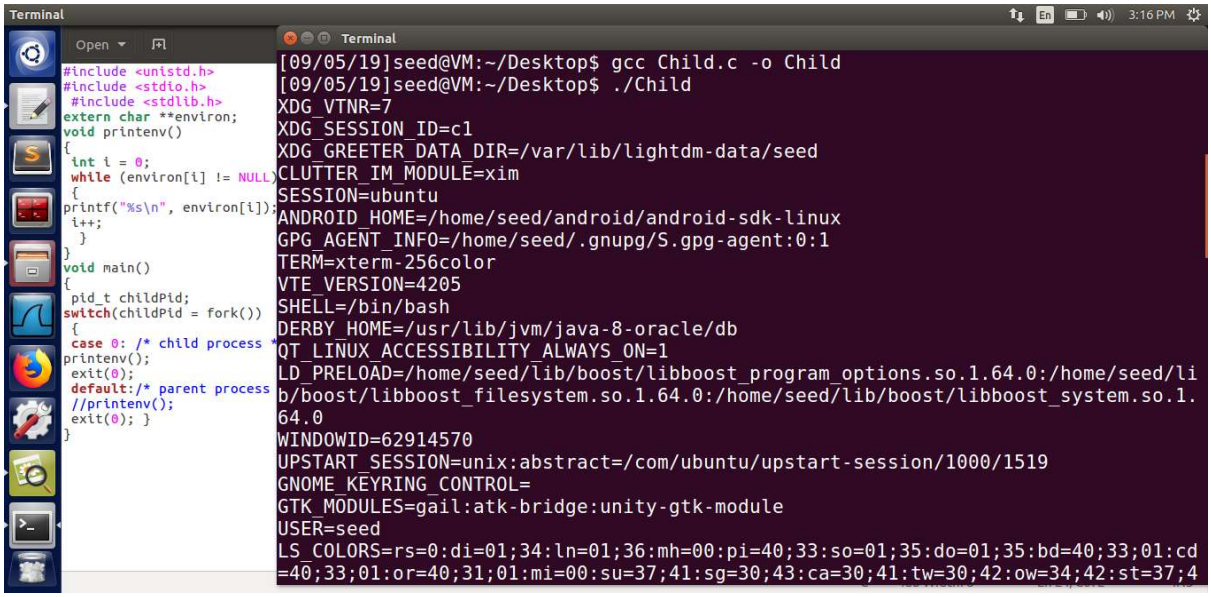
CODE SNIPPET

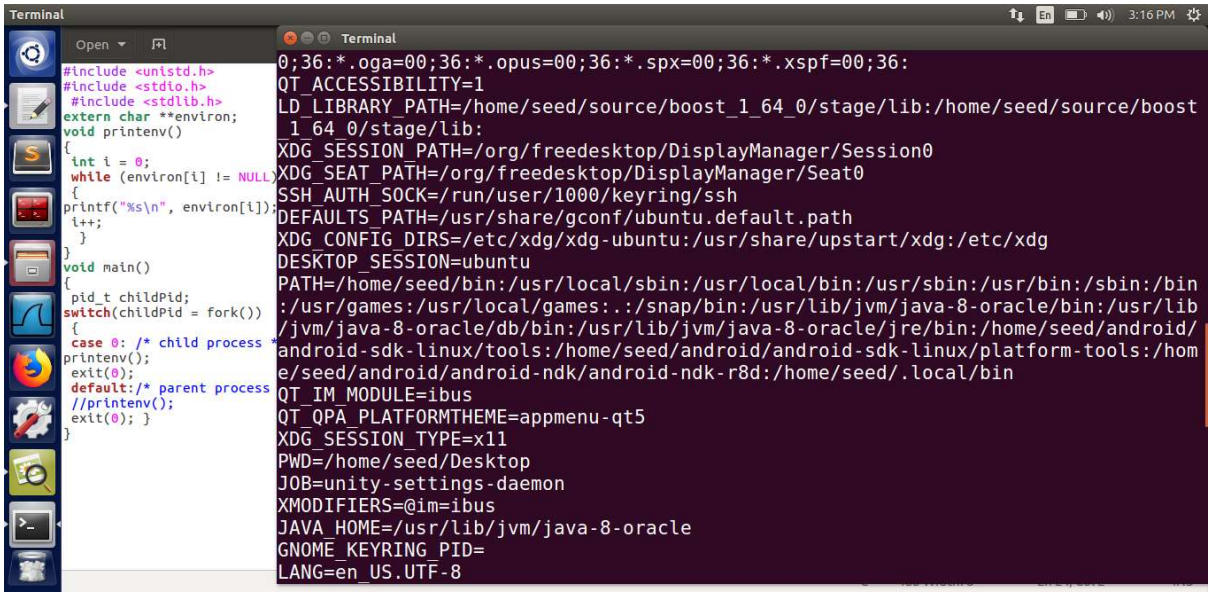
-Inheriting Environment Variable from parent

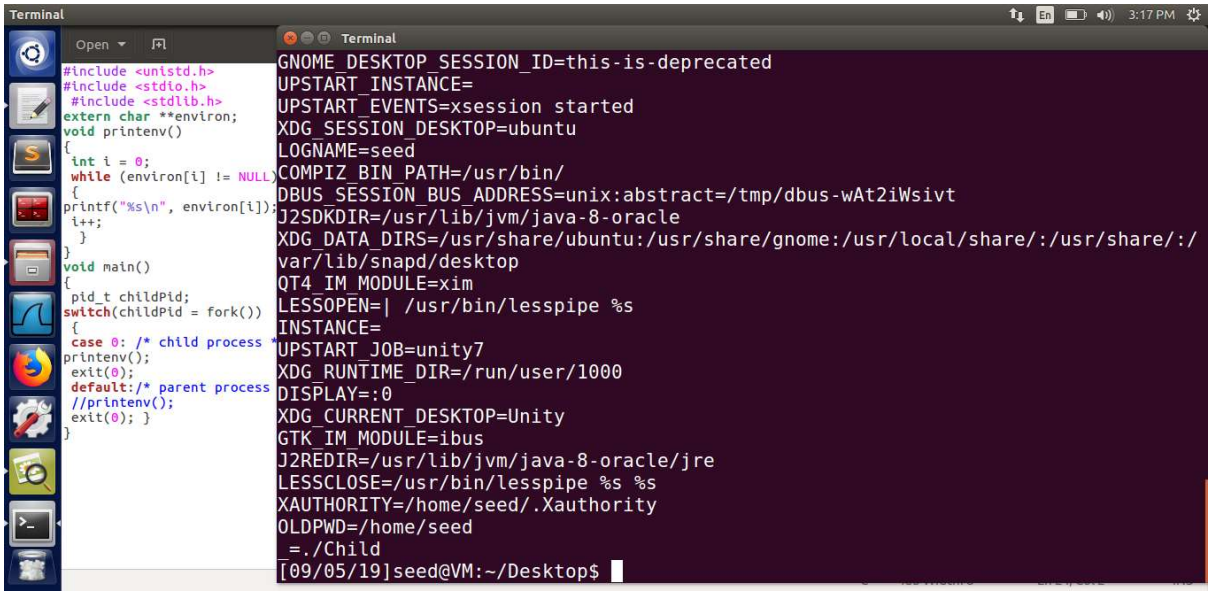
```
#include<unistd.h>
#include<stdio.h>
#include<stdlib.h>

extern char **environ;

void printenv()
{
int i = 0;
while(environ[i] != NULL) {
printf("%s\n", environ[i]);
i++;
}
}

void main()
{
pid_t childPid;

switch(childPid = fork()) {
case 0:
printenv();
exit(0);
default:

exit(0);
}
```



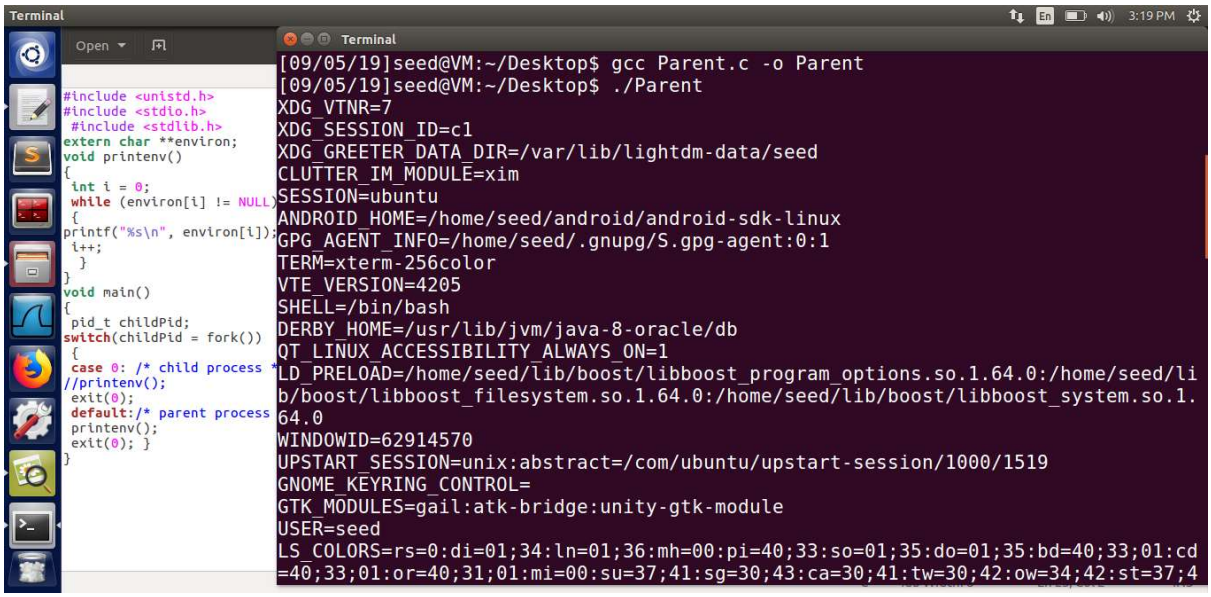
-

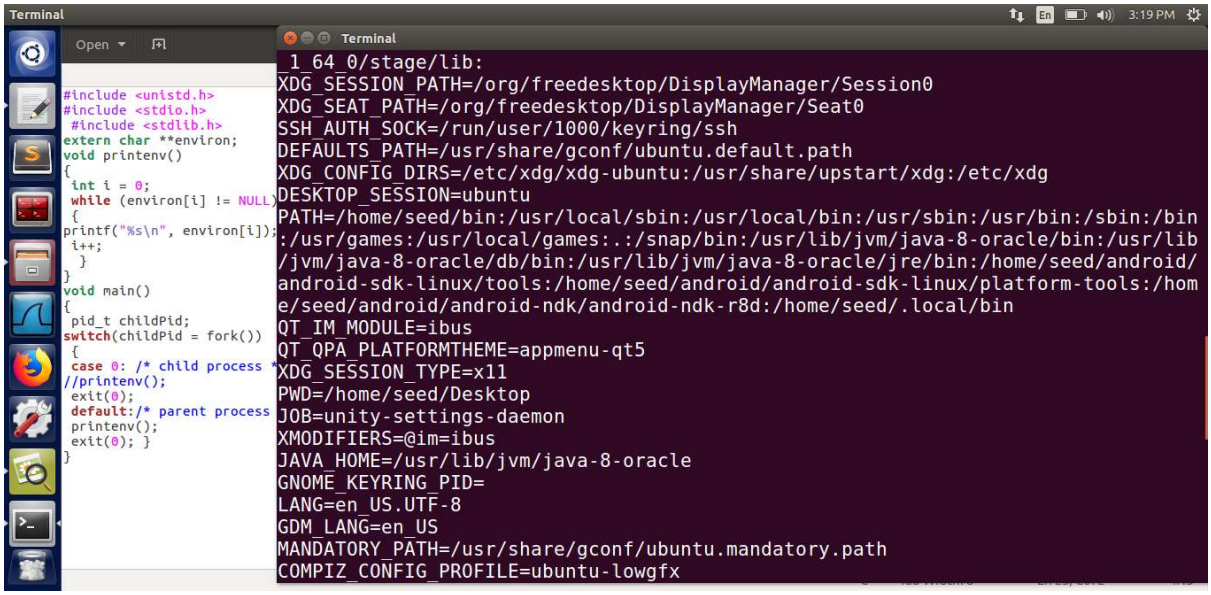

Terminal
3:16 PM
Open
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
extern char **environ;
void printenv()
{
int i = 0;
while (environ[i] != NULL)
{
printf("%s\n", environ[i]);
i++;
}
}
void main()
{
pid_t childPid;
switch(childPid = fork())
{
case 0: /* child process *
printenv();
exit(0);
default:/* parent process
//printenv();
exit(0); }
}
Terminal
[09/05/19]seed@VM:~/Desktop$ gcc Child.c -o Child
[09/05/19]seed@VM:~/Desktop$ ./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
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.
64.0
WINDOWID=62914570
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1519
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;4

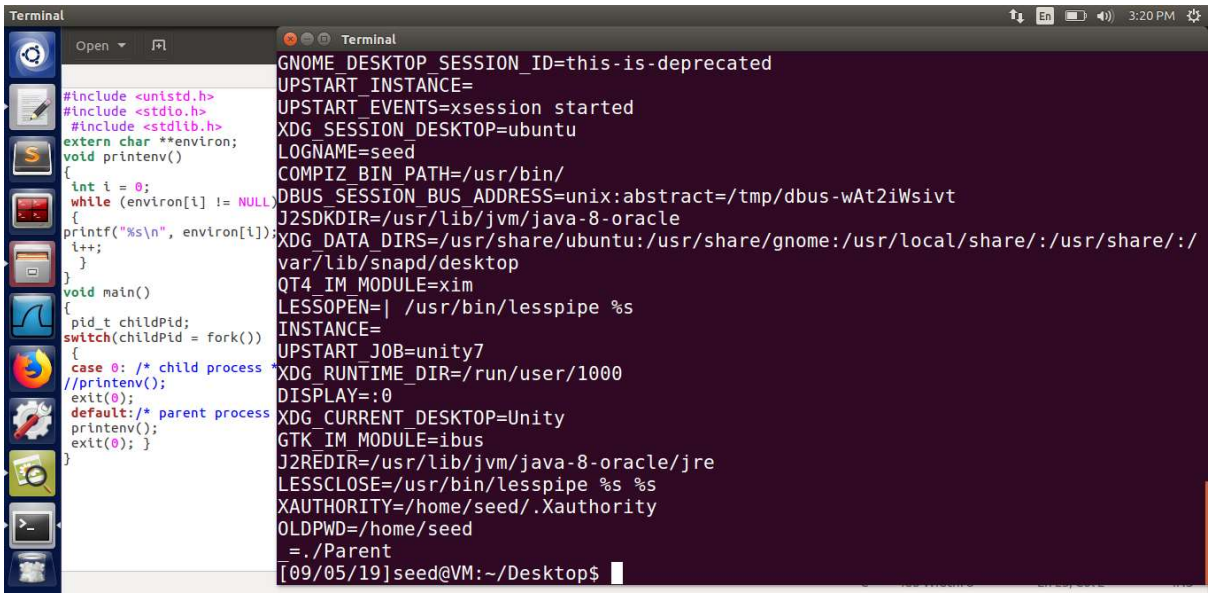

Terminal
3:16 PM
Open
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
extern char **environ;
void printenv()
{
int i = 0;
while (environ[i] != NULL)
{
printf("%s\n", environ[i]);
i++;
}
}
void main()
{
pid_t childPid;
switch(childPid = fork())
{
case 0: /* child process *
printenv();
exit(0);
default:/* parent process
//printenv();
exit(0); }
}
Terminal
0;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost
_1_64_0/stage/lib:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
DESKTOP_SESSION=ubuntu
PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib
/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/
android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/hom
e/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
QT_IM_MODULE=ibus
QT_QPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed/Desktop
JOB=unity-settings-daemon
XMODIFIERS=@im=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
GNOME_KEYRING_PID=
LANG=en_US.UTF-8


Terminal
3:17 PM
Open
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
extern char **environ;
void printenv()
{
int i = 0;
while (environ[i] != NULL)
{
printf("%s\n", environ[i]);
i++;
}
}
void main()
{
pid_t childPid;
switch(childPid = fork())
{
case 0: /* child process *
printenv();
exit(0);
default:/* parent process
//printenv();
exit(0); }
}
Terminal
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-wAt2iWsivt
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
OLDPWD=/home/seed
_=./Child
[09/05/19]seed@VM:~/Desktop$

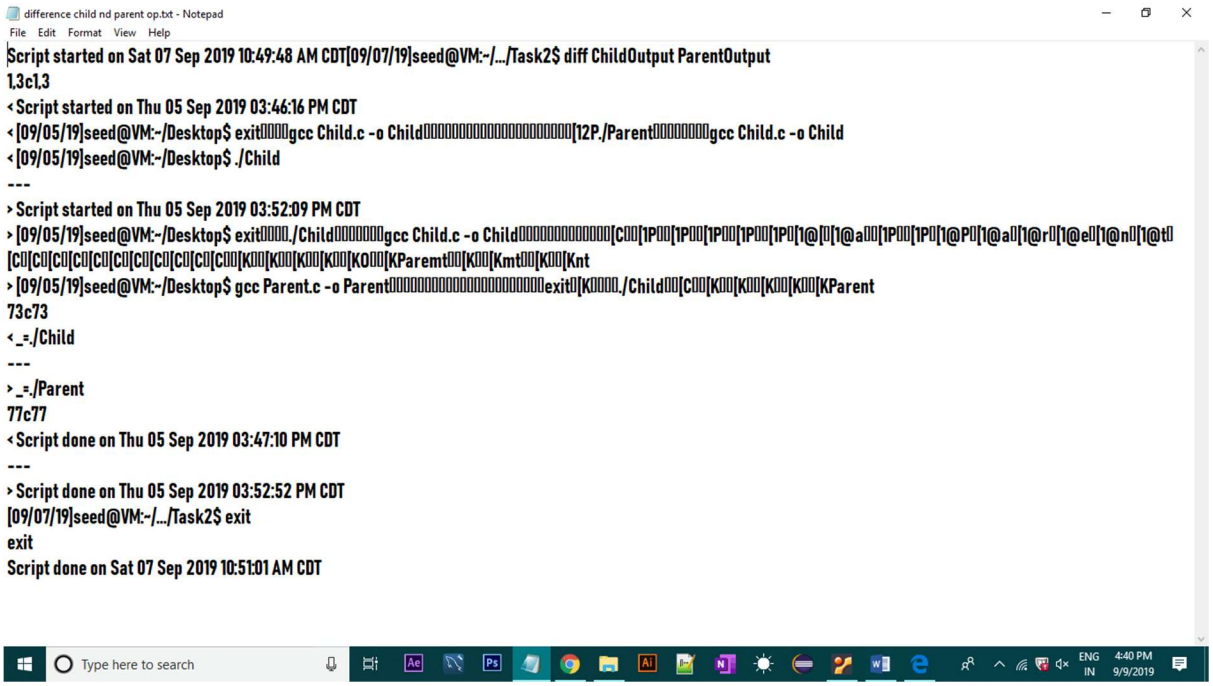
PARENT ENV


Terminal
3:19 PM
Open
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
extern char **environ;
void printenv()
{
int i = 0;
while (environ[i] != NULL)
{
printf("%s\n", environ[i]);
i++;
}
}
void main()
{
pid_t childPid;
switch(childPid = fork())
{
case 0: /* child process *
//printenv();
exit(0);
default:/* parent process
printenv();
exit(0); }
}
Terminal
[09/05/19]seed@VM:~/Desktop$ gcc Parent.c -o Parent
[09/05/19]seed@VM:~/Desktop$ ./Parent
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
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.
64.0
WINDOWID=62914570
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1519
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;4





DIFFERENCE BETWEEN PARENT AND CHILD ENV

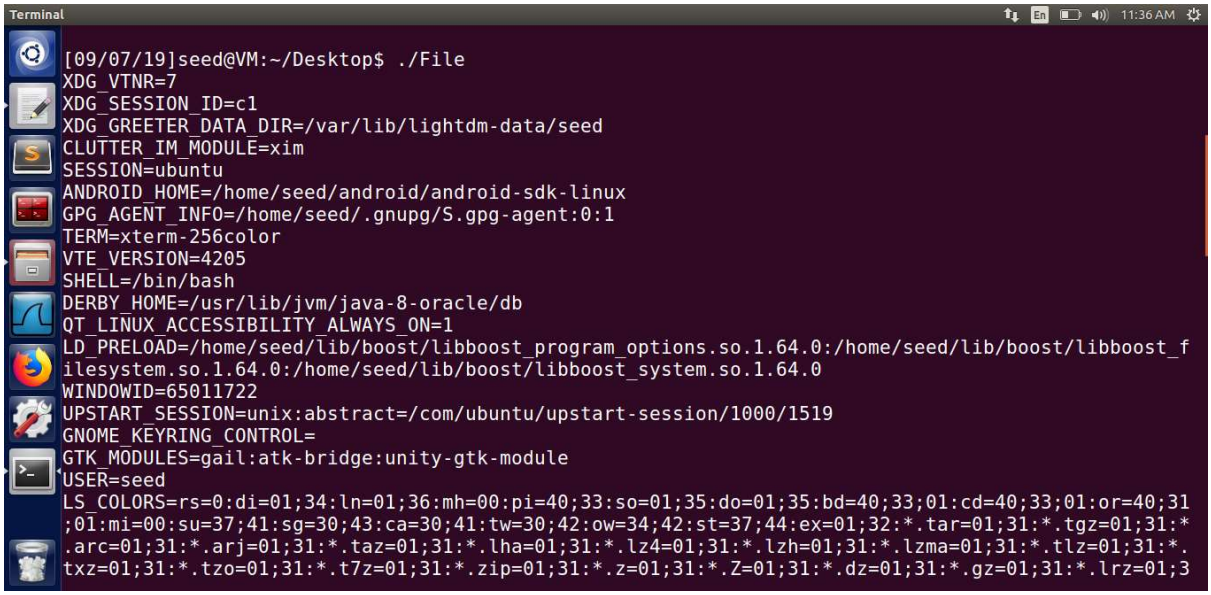


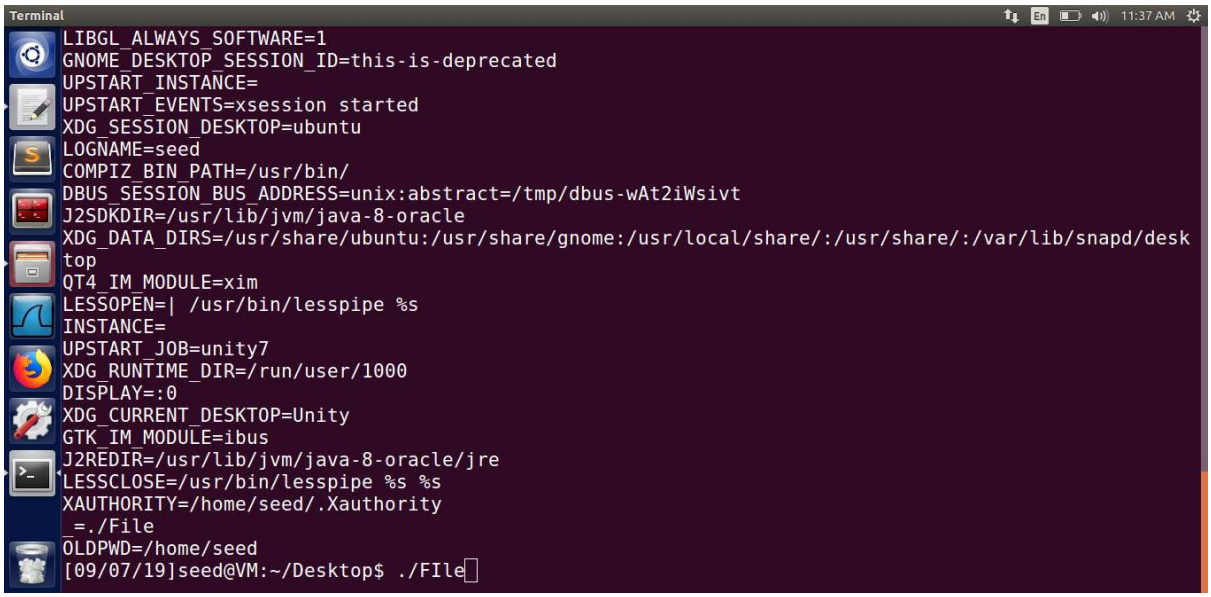
Observation

Child and Parent uses the different address spaces.

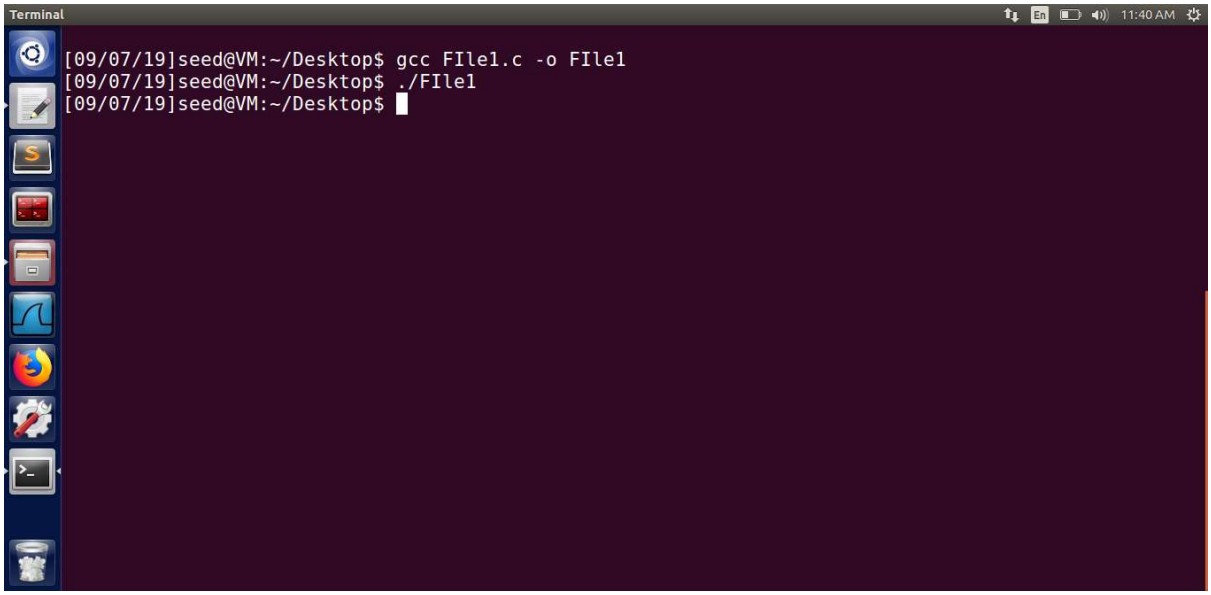
Task3

ENVIRONMENT VARIABLE

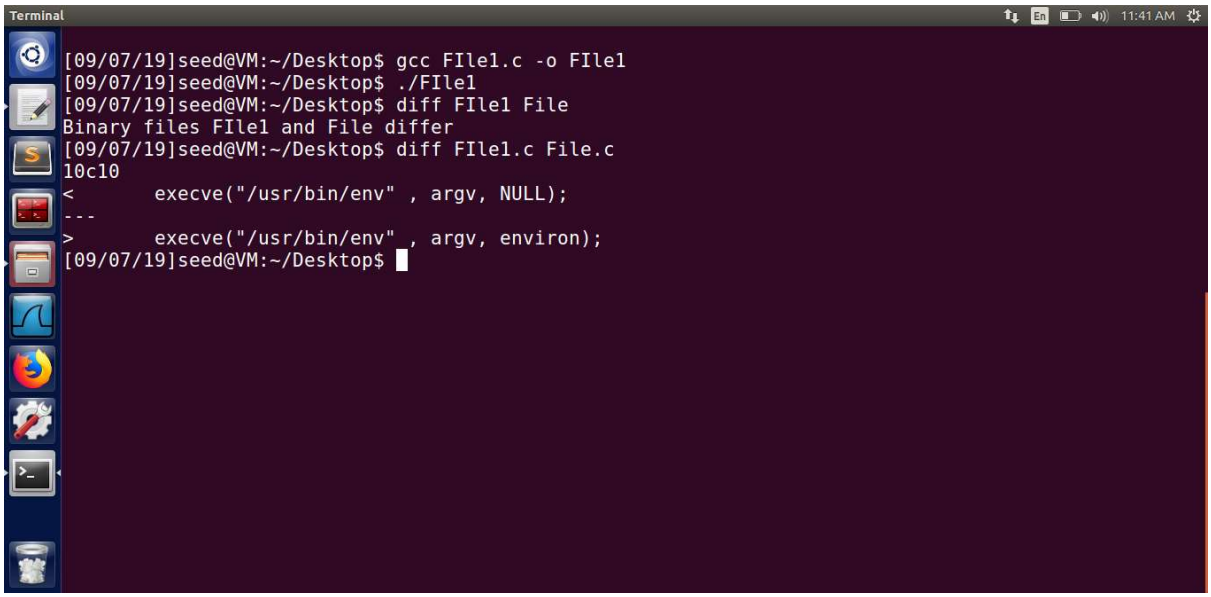




NULL ARGUMENT



DIFFERENCE BETWEEN NULL AND ENVIRONMENT VARIABLBE



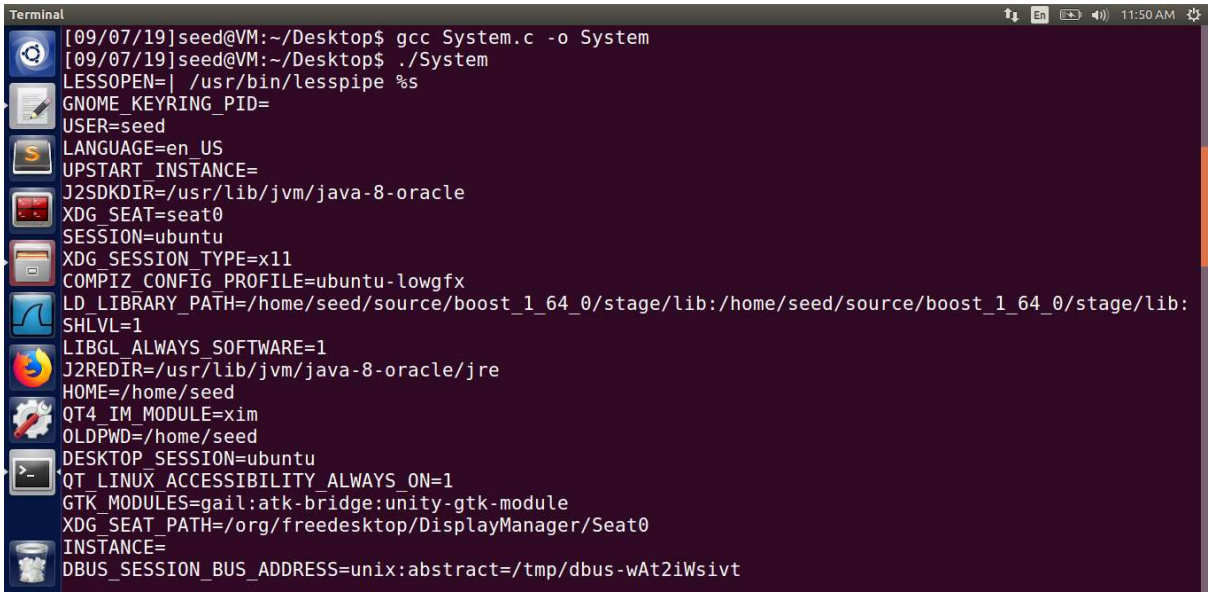
CODE SNIPPET

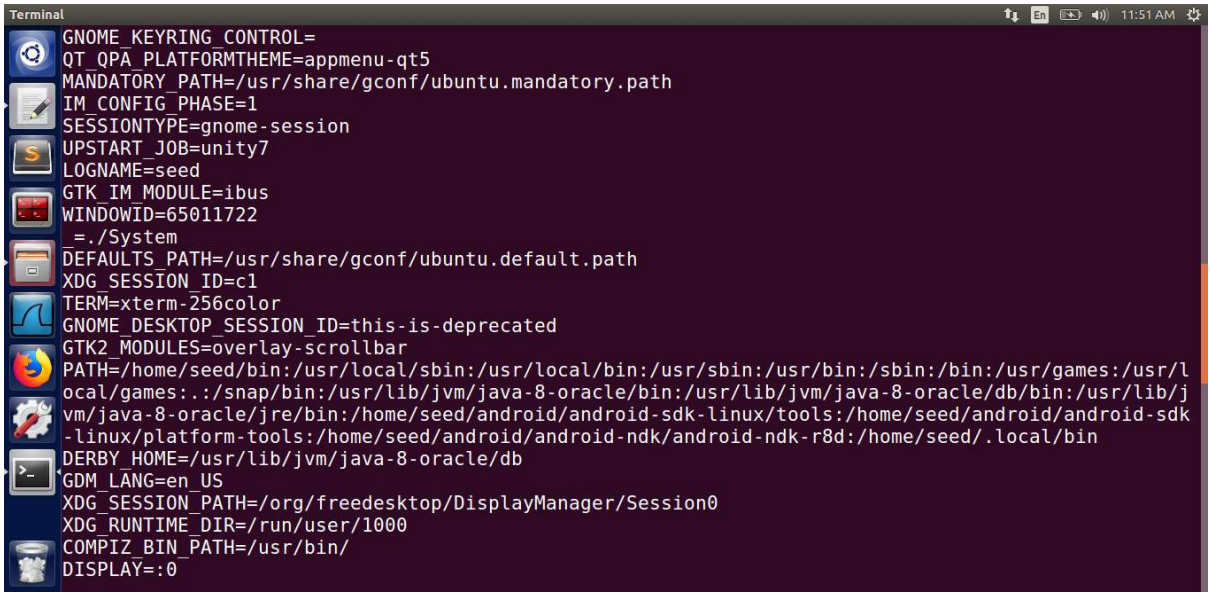
```c
#include<stdio.h>
#include<stdlib.h>

extern char **environ;

int main()
{
char *argv[2];
```

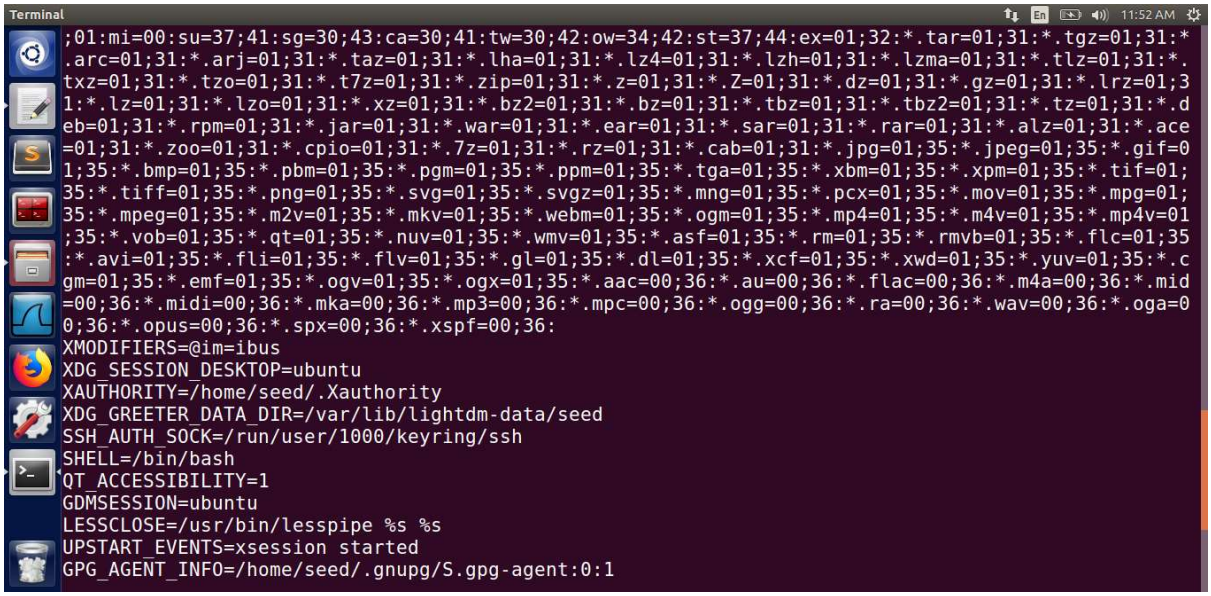
```
argv[0] = "/usr/bin/env";
argv[1] = NULL;

execve("/usr/bin/env", argv, NULL);

return 0;
}
```

Task 4

Environment Variable and System







CODE SNIPPET

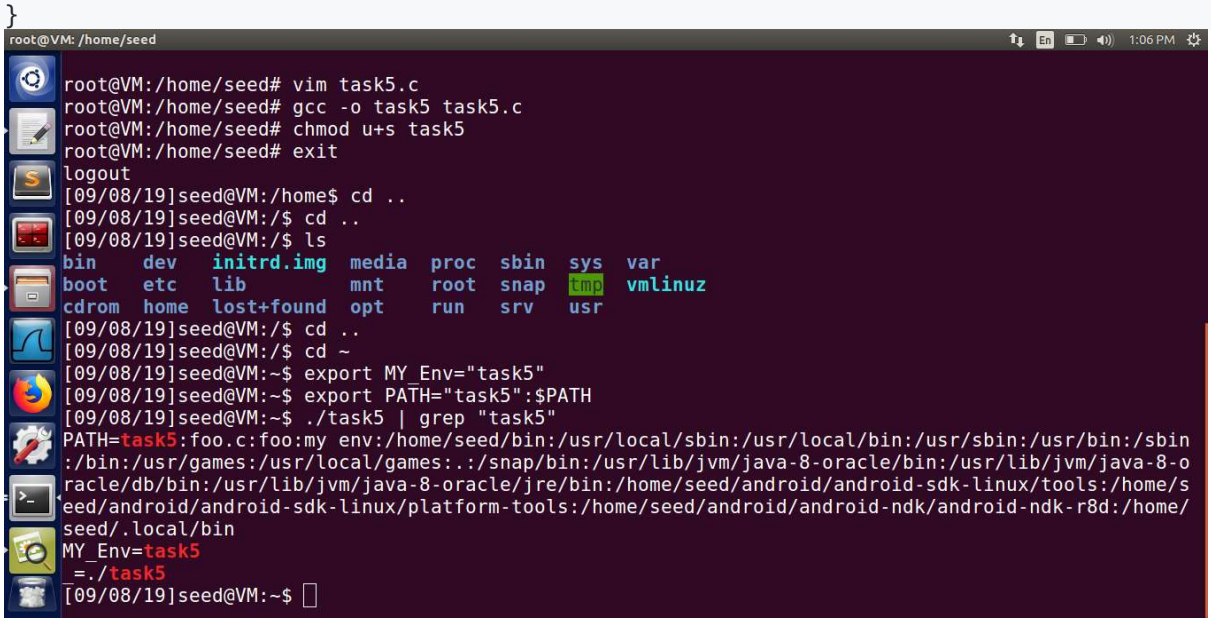
```c
#include<stdio.h>
#include<stdlib.h>

int main()
{
system("/usr/bin/env");

return 0;
}
```

Task 5

-Environment and Set UID

CODE SNIPPET

```c
#include<stdio.h>
#include<stdlib.h>

extern char **environ;

void main()
{
int i = 0;
while(environ[i] != NULL) {
printf("%s\n", environ[i]);
i++;
}
}
```

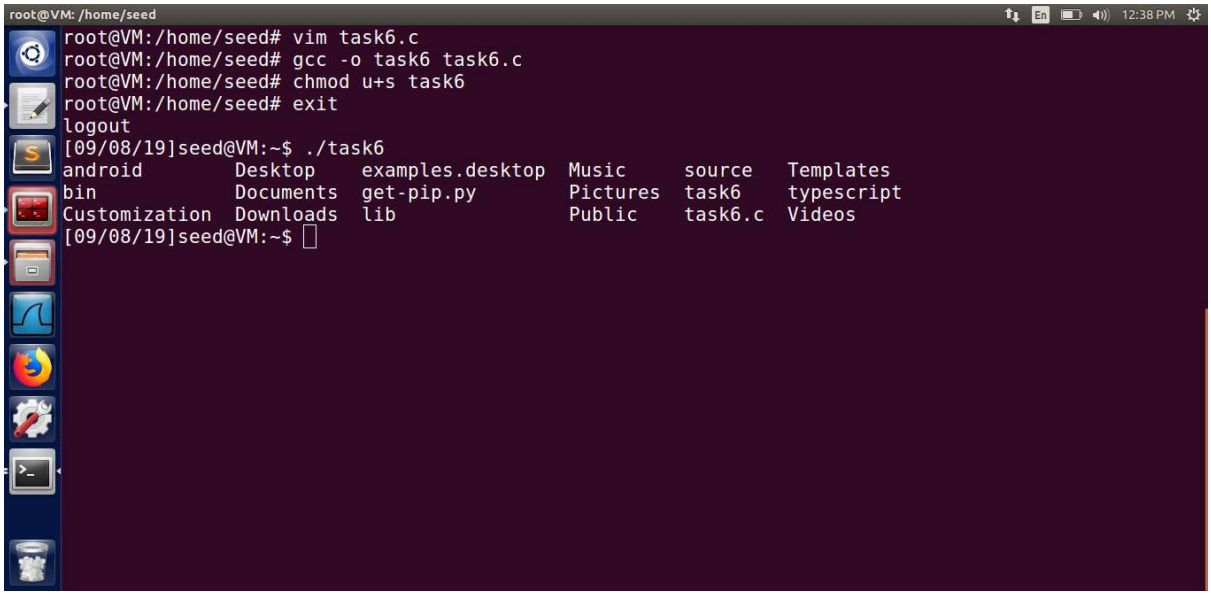


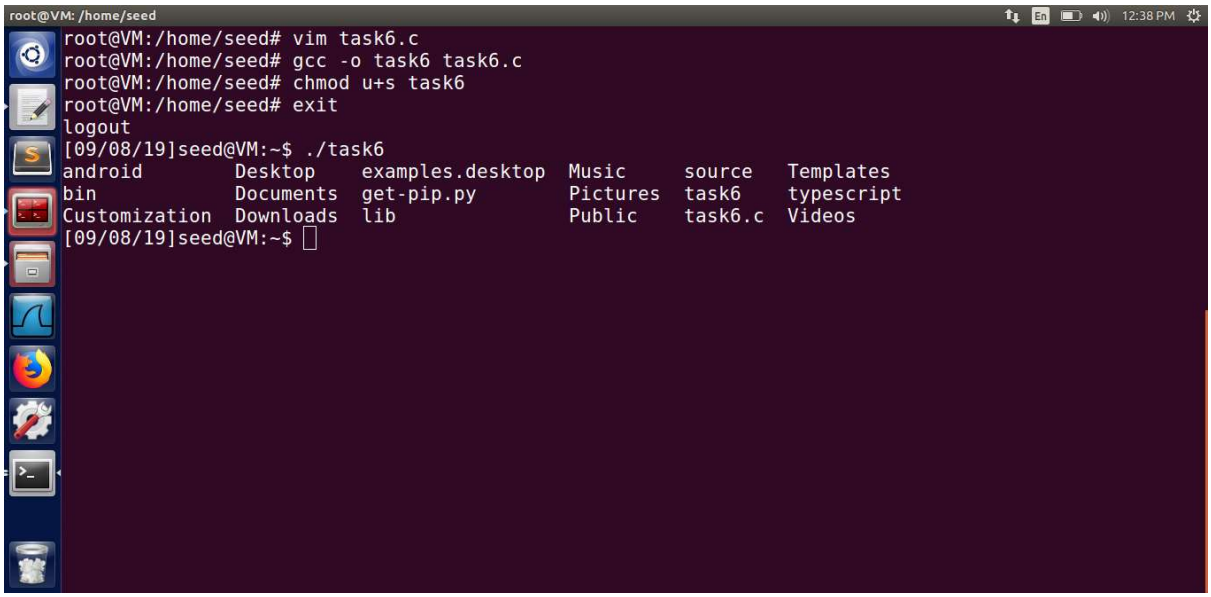
Task6

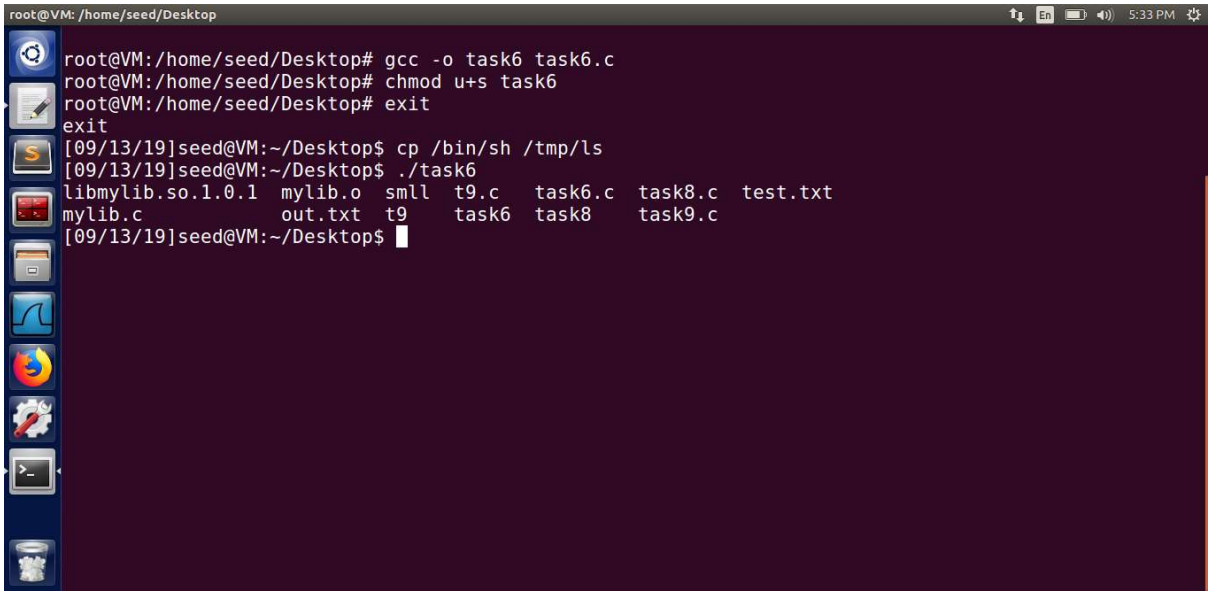
-The Path Environment Variable and Set-UID

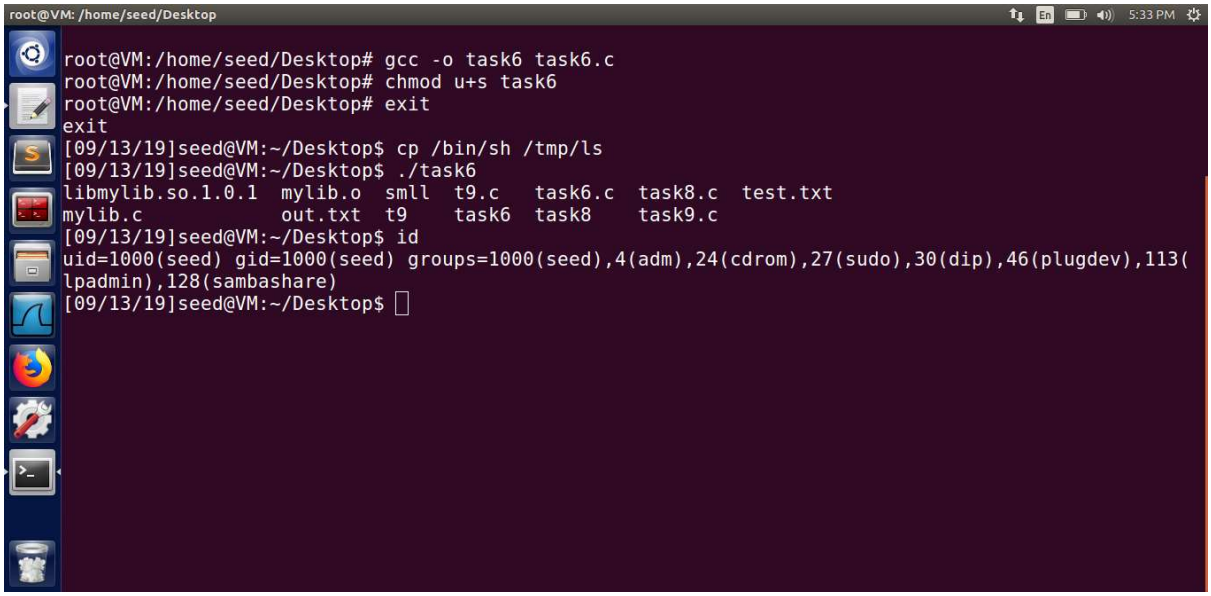
CODE SNIPPET

```c
int main()
{
system("ls");
return 0;
}
```


root@VM: /home/seed
12:38 PM
root@VM:/home/seed# vim task6.c
root@VM:/home/seed# gcc -o task6 task6.c
root@VM:/home/seed# chmod u+s task6
root@VM:/home/seed# exit
logout
[09/08/19]seed@VM:~$ ./task6
android Desktop examples.desktop Music source Templates
bin Documents get-pip.py Pictures task6 typescript
Customization Downloads lib Public task6.c Videos
[09/08/19]seed@VM:~$


root@VM: /home/seed
12:38 PM
root@VM:/home/seed# vim task6.c
root@VM:/home/seed# gcc -o task6 task6.c
root@VM:/home/seed# chmod u+s task6
root@VM:/home/seed# exit
logout
[09/08/19]seed@VM:~$ ./task6
android Desktop examples.desktop Music source Templates
bin Documents get-pip.py Pictures task6 typescript
Customization Downloads lib Public task6.c Videos
[09/08/19]seed@VM:~$





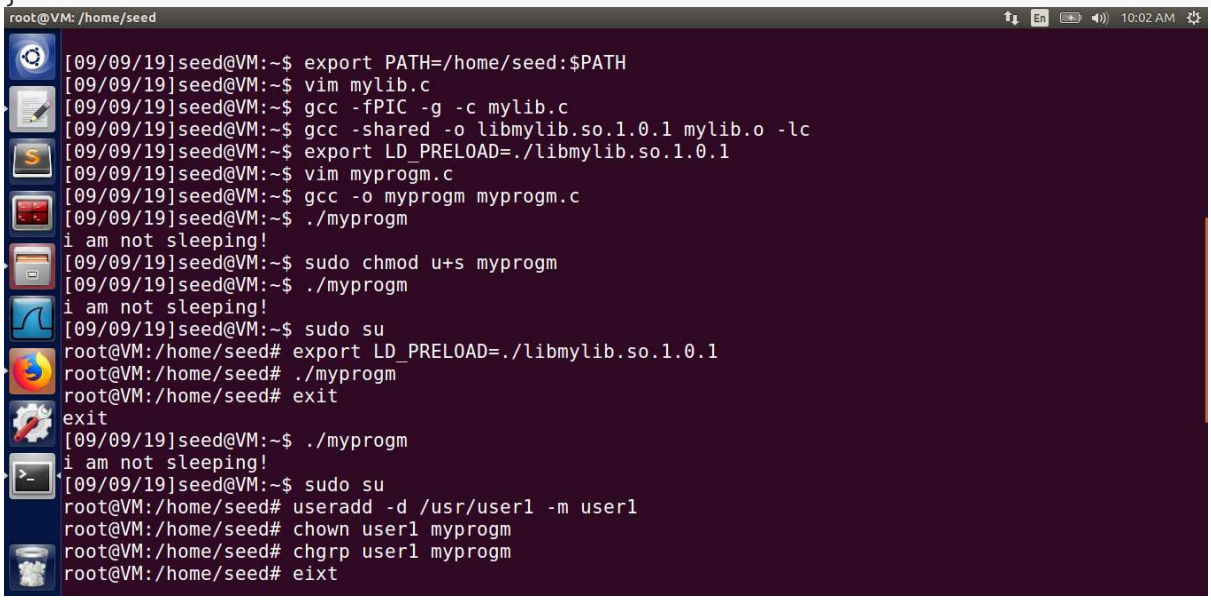
Observation

It can have root privilege, copy `/bin/sh` to `/tmp/ls`.Then compile and run `system` program and we will get root privilege.

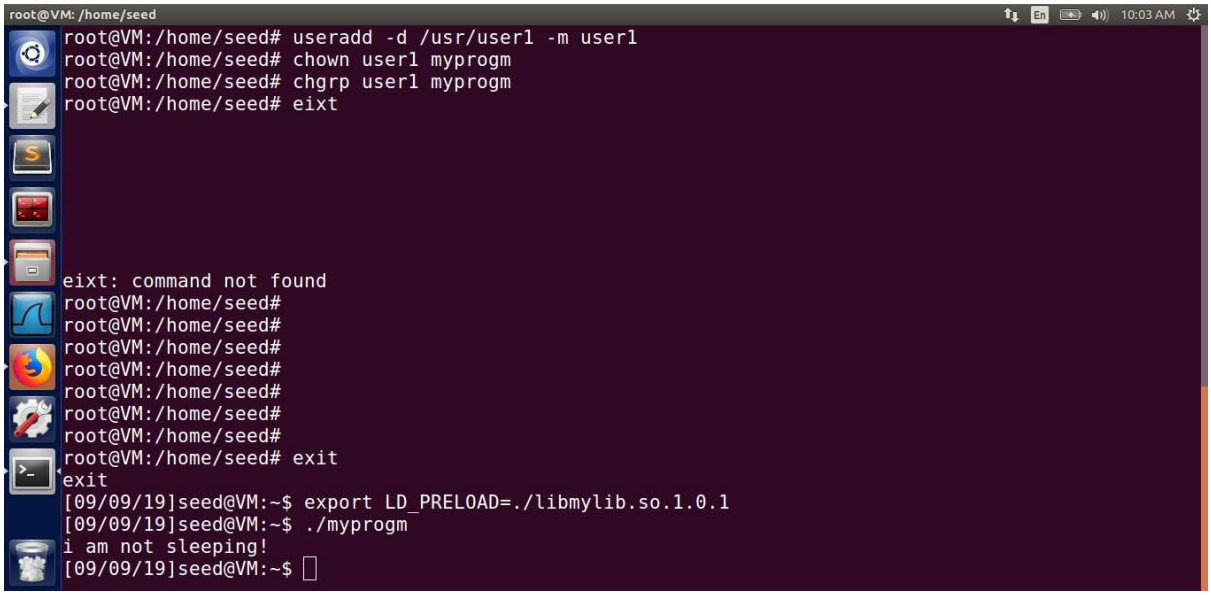
Task7

CODE SNIPPET

```c
#include<stdio.h>
void sleep(int s)
{
printf("I am not sleeping!\n");
}
```




```c
//myprog.c
int main()
{
sleep(1);
return 0;
}
```



Observation

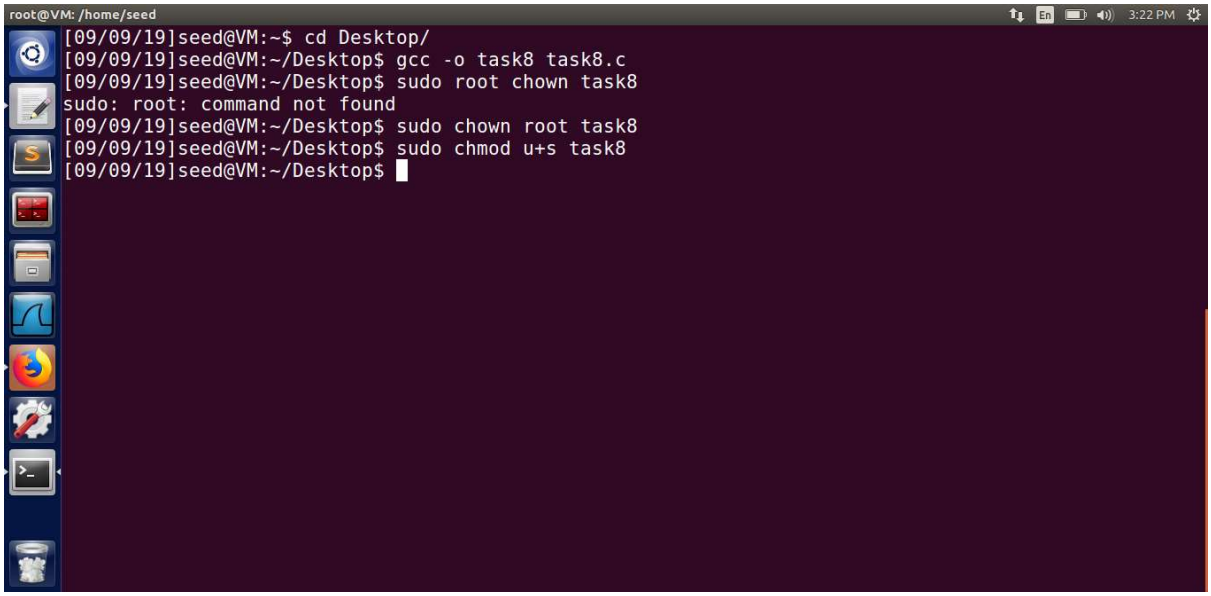
From the four conditions, we know that only a user run the program created by himself, `LD_PRELOAD` environment valiable can be used and `sleep ()` function can be override.

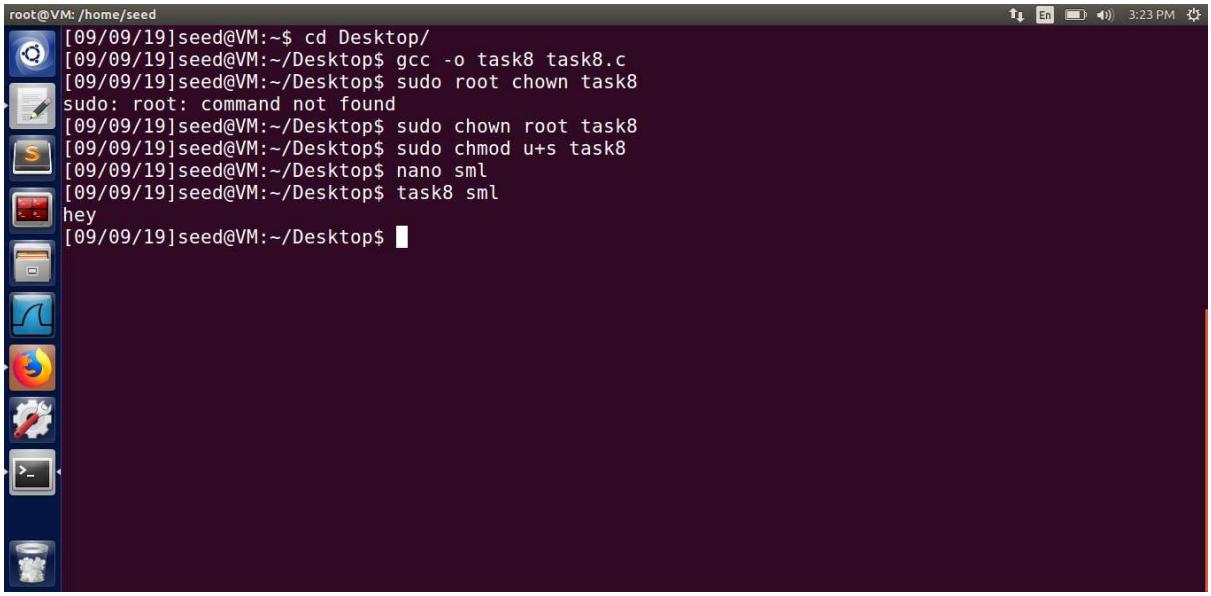
Task 8

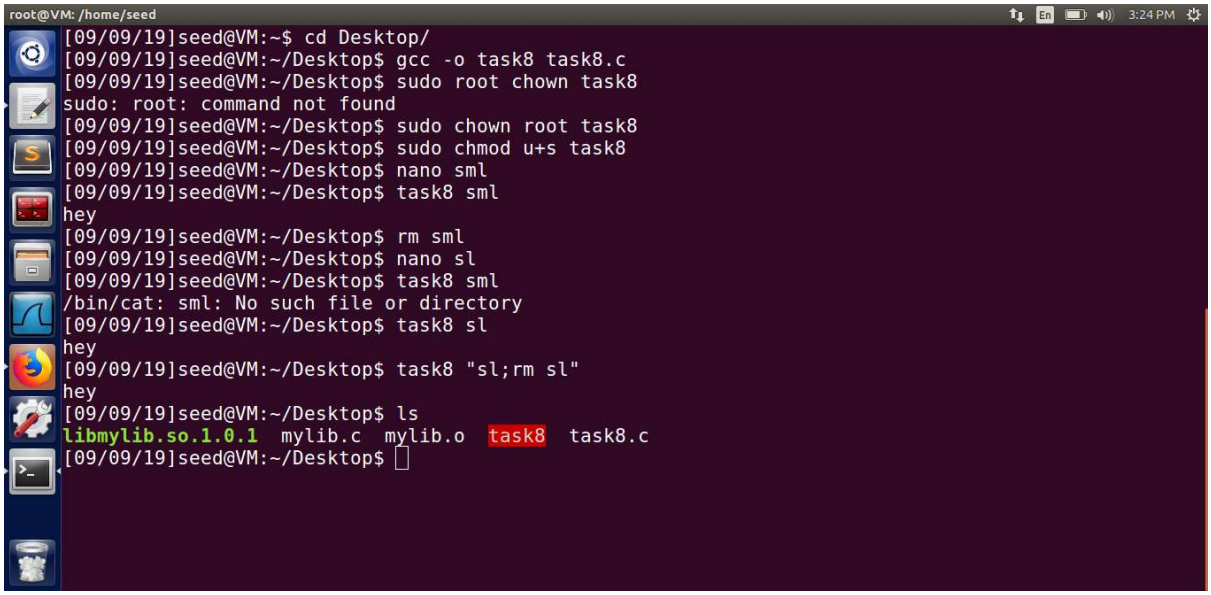
CODE SNIPPET

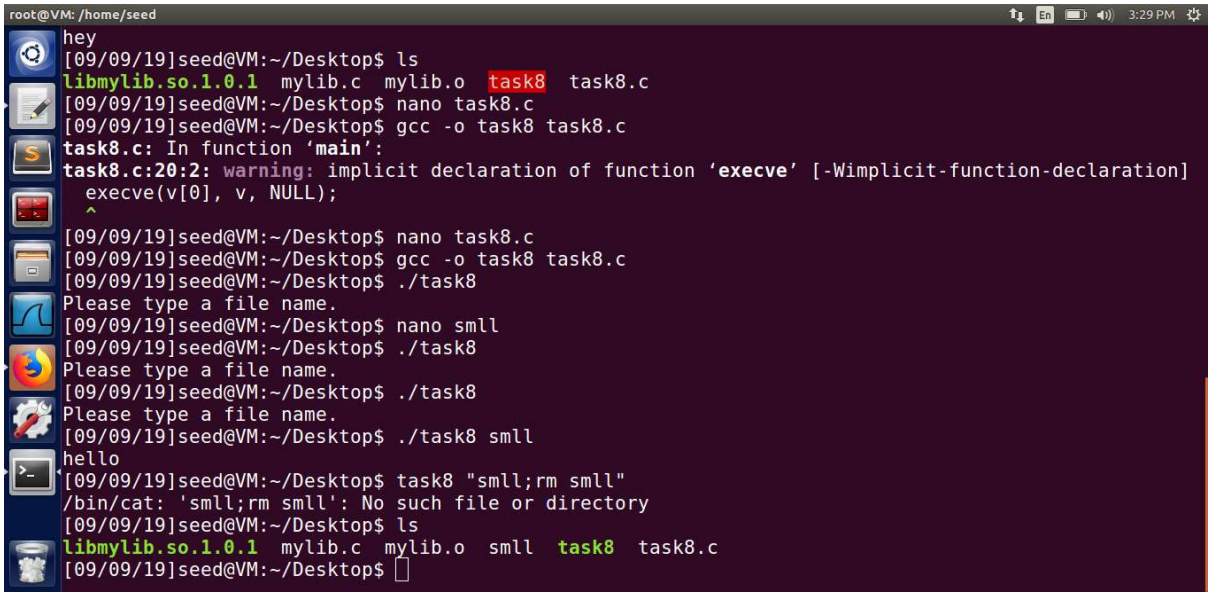
```
#include <string.h>
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char *argv[])
{
char *v[3];
char *command;

if(argc < 2) {
printf("Please type a file name.\n");
return 1;
}
```

```c
v[0] = "/bin/cat"; v[1] = argv[1]; v[2] = NULL;

command = malloc(strlen(v[0]) + strlen(v[1]) + 2);
sprintf(command, "%s %s", v[0], v[1]);

// Use only one of the followings.
system(command);
// execve(v[0], v, NULL);

return 0;
}
```







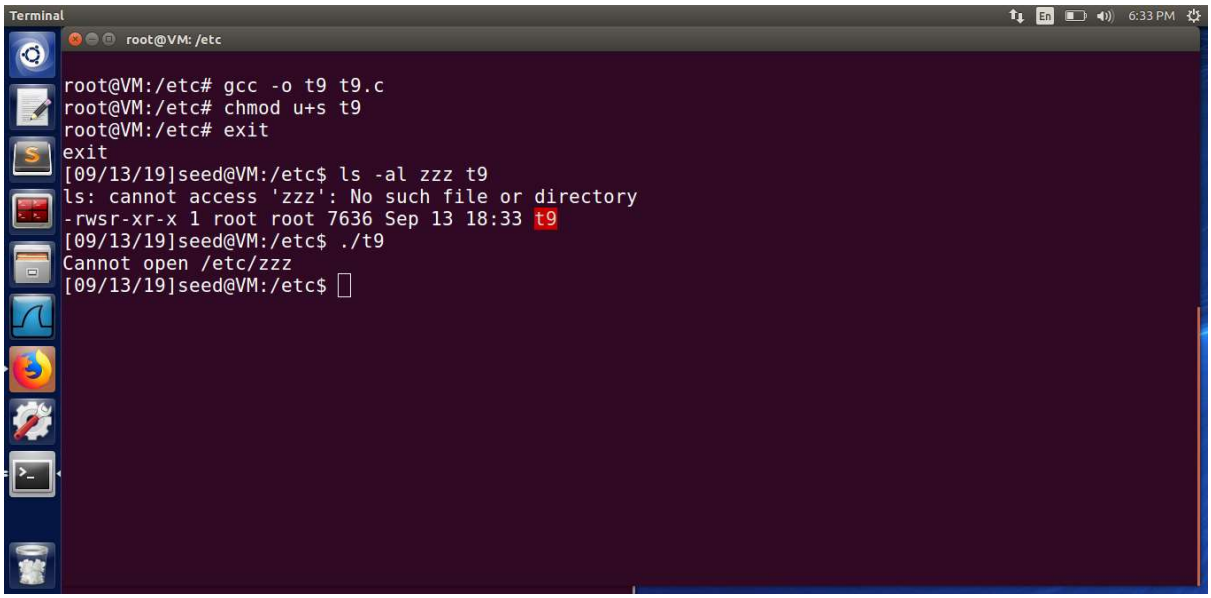


Observation

The task8 file is not safe, Bob can read, write or move files which only root user can run.

Task 9

CODE SNIPPET



As we can see, the file hasn't been modified, the reason is file zzz can't be opened after the set uid.