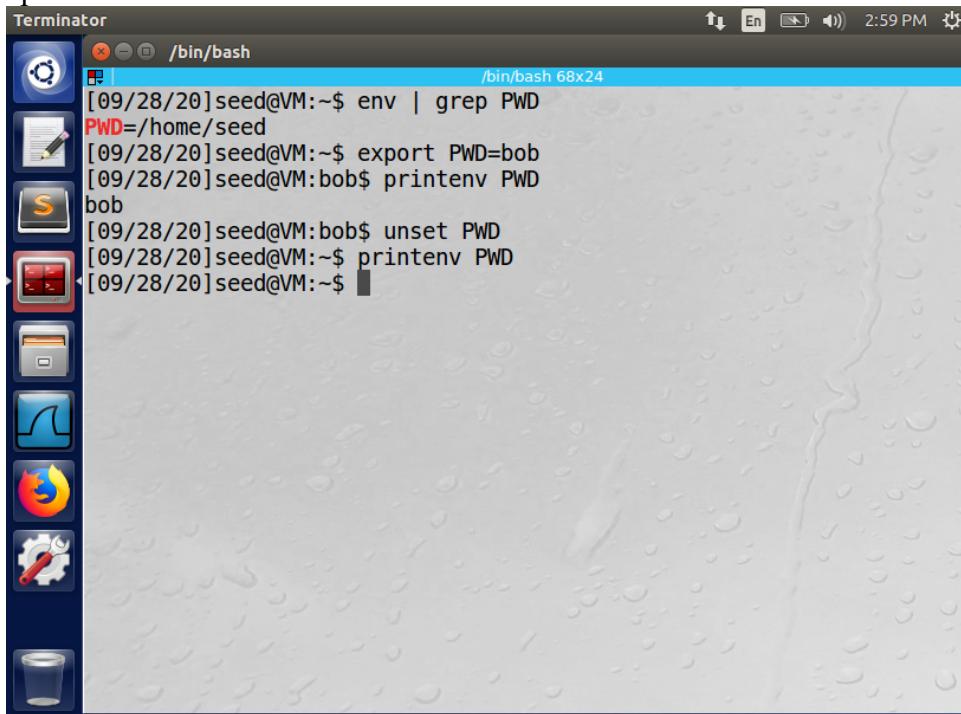


Man Tik Li
CS 377 - 001
September 28, 2020

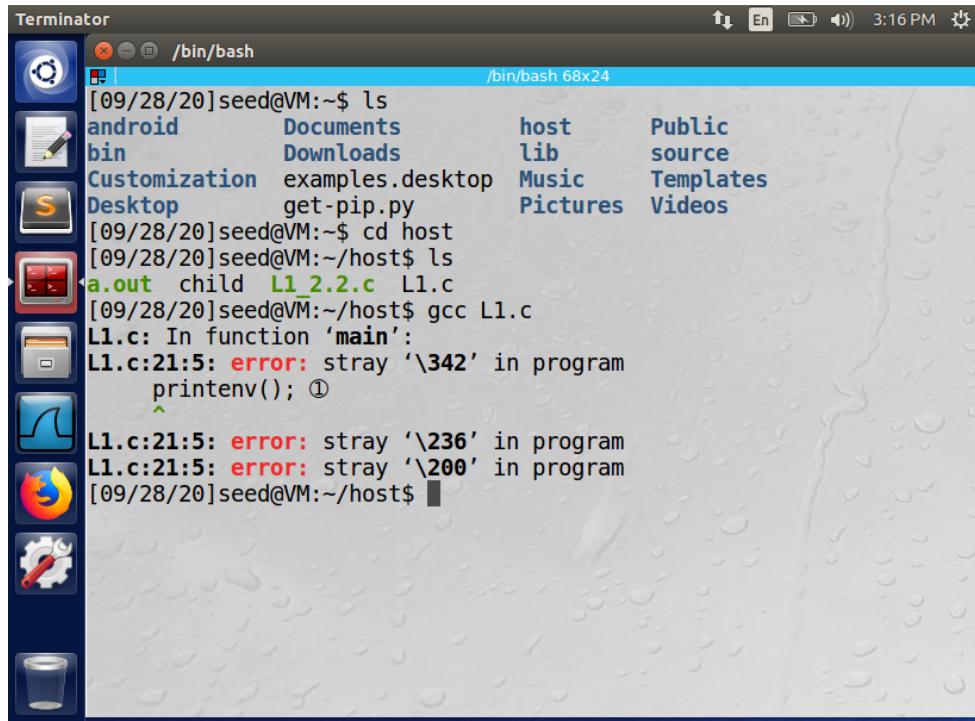
Lab 1

1. First use “env | grep PWD” to find the value of PWD. Then use “export” to change the value of PWD to bob and use “printenv PWD” to print out the value of PWD has changed to bob. After that, I used “unset” function to delete the variable and used “printenv PWD” to check that no value in PWD.



```
[09/28/20]seed@VM:~$ env | grep PWD
PWD=/home/seed
[09/28/20]seed@VM:~$ export PWD=bob
[09/28/20]seed@VM:bob$ printenv PWD
bob
[09/28/20]seed@VM:bob$ unset PWD
[09/28/20]seed@VM:~$ printenv PWD
[09/28/20]seed@VM:~$
```

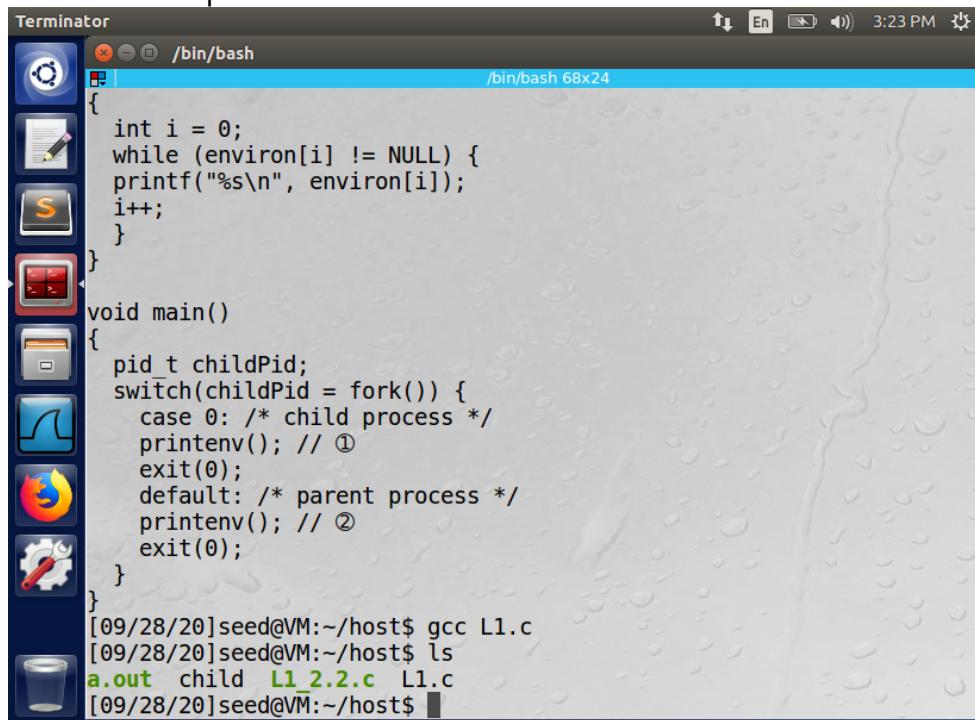
2. Step1 1: When completing the program, I got an error on printenv() because of the Line ① sign that after the printenv statement.



A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window titled "Terminator". The terminal window has a blue header bar with the title "Terminator" and the path "/bin/bash". The status bar at the top right shows the date and time as "3:16 PM". The terminal window displays a command-line session:

```
[09/28/20]seed@VM:~$ ls
android      Documents      host      Public
bin          Downloads      lib       source
Customization examples.desktop Music    Templates
Desktop      get-pip.py    Pictures   Videos
[09/28/20]seed@VM:~$ cd host
[09/28/20]seed@VM:~/host$ ls
a.out  child  L1_2.2.c  L1.c
[09/28/20]seed@VM:~/host$ gcc L1.c
L1.c: In function 'main':
L1.c:21:5: error: stray '\342' in program
     printenv(); ①
^
L1.c:21:5: error: stray '\236' in program
L1.c:21:5: error: stray '\200' in program
[09/28/20]seed@VM:~/host$
```

Step 2: After commenting out the Line ① and Line ②, the program successfully compiles and run. The code prints the values of the specified environment variables that part of environment.



A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window titled "Terminator". The terminal window has a blue header bar with the title "Terminator" and the path "/bin/bash". The status bar at the top right shows the date and time as "3:23 PM". The terminal window displays a command-line session:

```
{
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(); // ①
exit(0);
default: /* parent process */
printenv(); // ②
exit(0);
}
[09/28/20]seed@VM:~/host$ gcc L1.c
[09/28/20]seed@VM:~/host$ ls
a.out  child  L1_2.2.c  L1.c
[09/28/20]seed@VM:~/host$
```

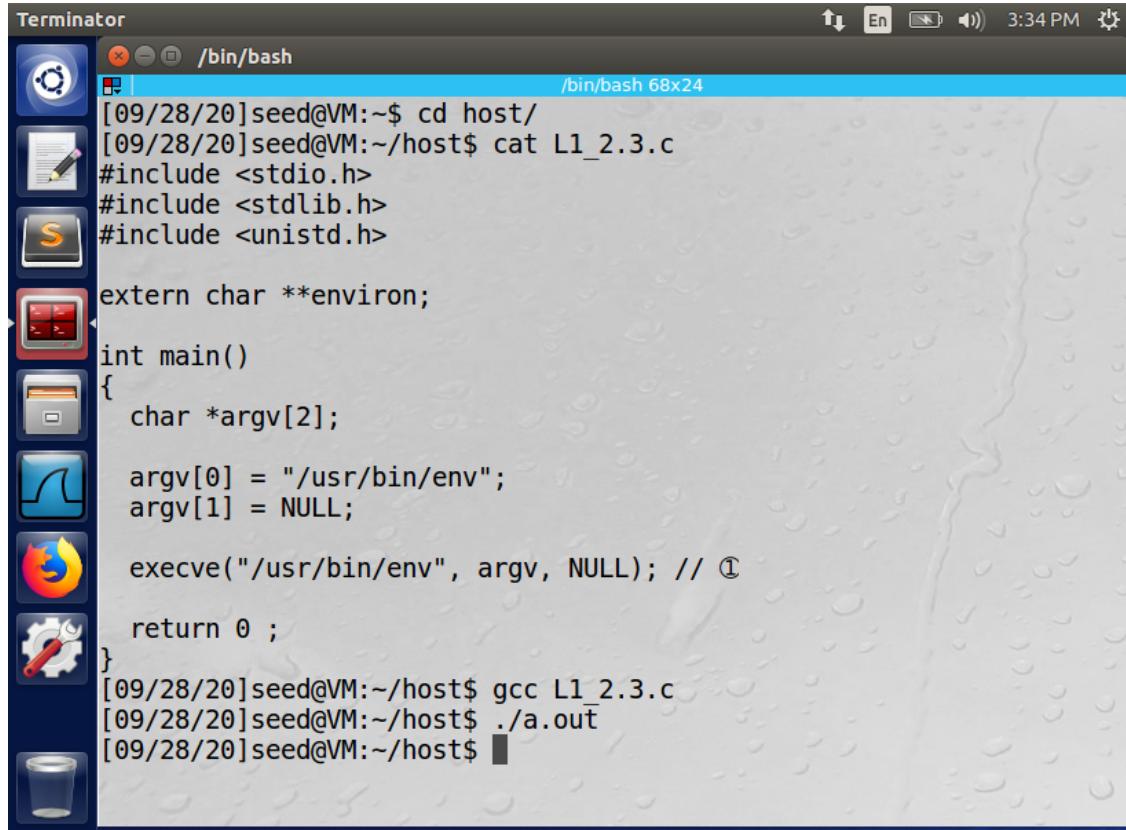
Output: I captured the first and the last part of the output.

The image shows two side-by-side terminal windows from the Terminator application. Both terminals are running a bash shell and display a list of environment variables. The top terminal window has its title bar set to "/bin/bash" and shows the date and time as "[09/28/20]seed@VM:~/host\$./a.out". The bottom terminal window also has its title bar set to "/bin/bash" and shows the date and time as "[09/28/20]seed@VM:~/host\$". Both windows show nearly identical environment variable outputs, with minor differences in the order of some variables like XDG_SESSION_ID and XDG_CURRENT_DESKTOP.

```
[09/28/20]seed@VM:~/host$ ./a.out
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:bf4f2390-2d15-460f-a258-1ed3df7c494d
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=3630
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
WINDOWID=35651588
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1146
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed

[09/28/20]seed@VM:~/host$ Search your computer
UPSTART_INSTANCE=
XDG_SESSION_DESKTOP=ubuntu
UPSTART_EVENTS=xsession started
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-71y3V6jGvQ
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 %
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
COLORTERM=gnome-terminal
OLDPWD=/home/seed
./a.out
[09/28/20]seed@VM:~/host$
```

3. After compile and run the code, the program didn't print out any value from environment variables.



```
Terminator /bin/bash /bin/bash 68x24
[09/28/20]seed@VM:~$ cd host/
[09/28/20]seed@VM:~/host$ cat L1_2.3.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

extern char **environ;

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

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

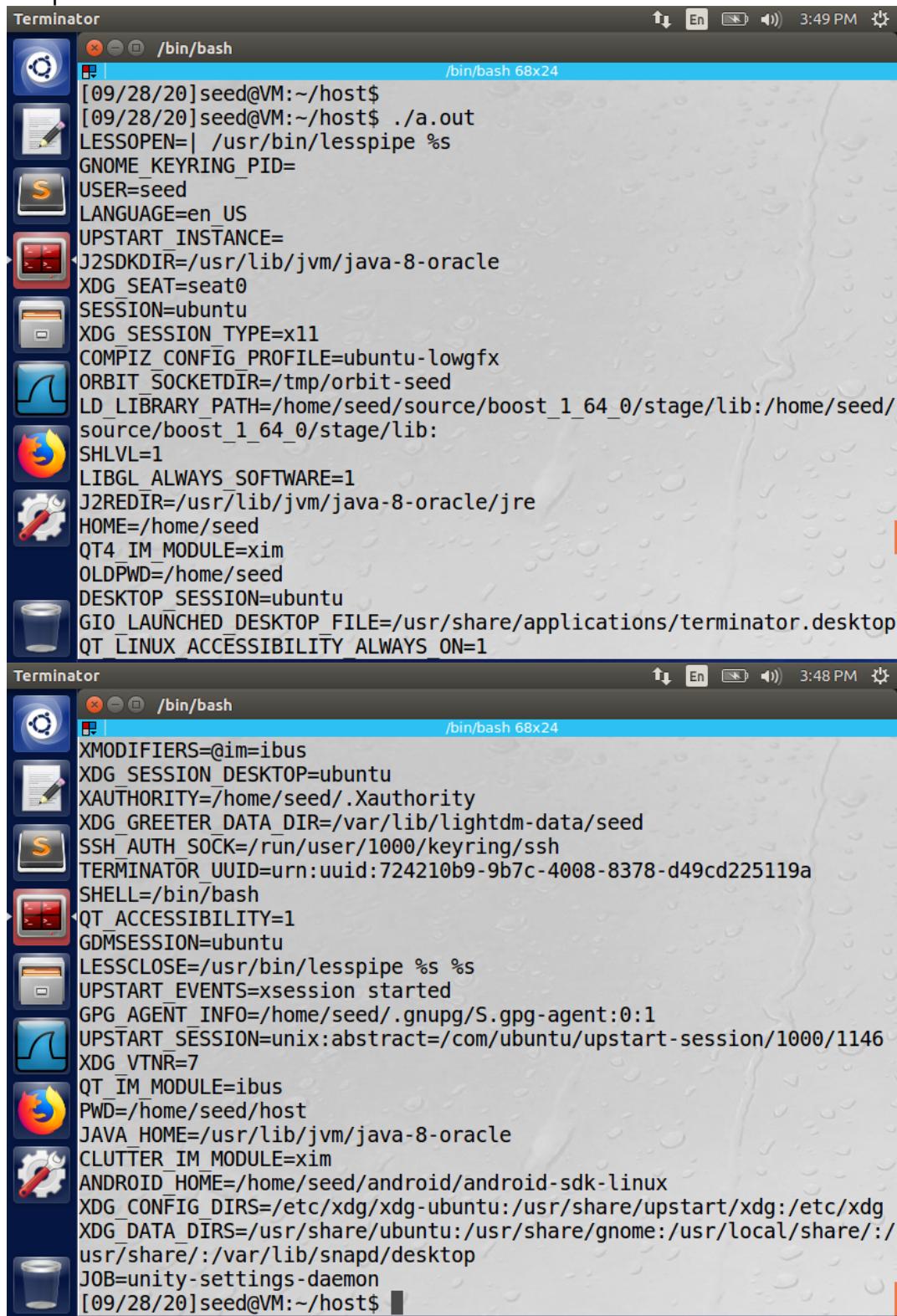
    execve("/usr/bin/env", argv, NULL); // ①

    return 0 ;
}
[09/28/20]seed@VM:~/host$ gcc L1_2.3.c
[09/28/20]seed@VM:~/host$ ./a.out
[09/28/20]seed@VM:~/host$
```

After change the third arguments in execve from NULL to environ, the program prints all the environment variables.

Conclusion: The execve() has three parameters: filename, array contains the arguments, and the envp array contains the environment variables. If set the third arguments in execve() to NULL, the process does not pass any environment variable. If change it to environ, it passing all the environment variables.

4. Output:



The image shows two side-by-side terminal windows from the Terminator application. Both windows are running a bash shell and displaying a list of environment variables.

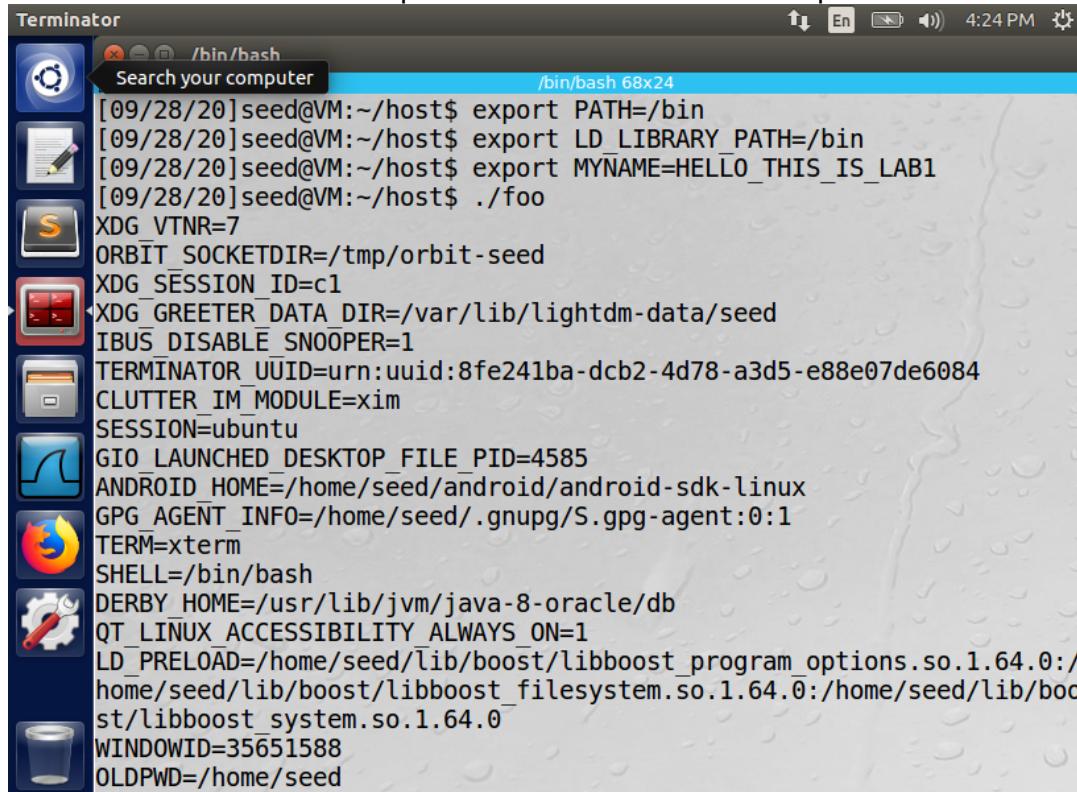
Terminal 1 (Top):

```
[09/28/20]seed@VM:~/host$  
[09/28/20]seed@VM:~/host$ ./a.out  
LESSOPEN=| /usr/bin/lesspipe %s  
GNOME_KEYRING_PID=  
USER=seed  
LANGUAGE=en_US  
UPSTART_INSTANCE=  
J2SDKDIR=/usr/lib/jvm/java-8-oracle  
XDG_SEAT=seat0  
SESSION=ubuntu  
XDG_SESSION_TYPE=x11  
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx  
ORBIT_SOCKETDIR=/tmp/orbit-seed  
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/  
source/boost_1_64_0/stage/lib:  
SHLVL=1  
LIBGL_ALWAYS_SOFTWARE=1  
J2REDIR=/usr/lib/jvm/java-8-oracle/jre  
HOME=/home/seed  
QT4_IM_MODULE=xim  
OLDPWD=/home/seed  
DESKTOP_SESSION=ubuntu  
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop  
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
```

Terminal 2 (Bottom):

```
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  
TERMINATOR_UUID=urn:uuid:724210b9-9b7c-4008-8378-d49cd225119a  
SHELL=/bin/bash  
QT_ACCESSIBILITY=1  
GDMSESSION=ubuntu  
LESSCLOSE=/usr/bin/lesspipe %s %s  
UPSTART_EVENTS=xsession started  
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1  
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1146  
XDG_VTNR=7  
QT_IM_MODULE=ibus  
PWD=/home/seed/host  
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  
JOB=unity-settings-daemon  
[09/28/20]seed@VM:~/host$
```

5. The program will change the value for PATH, LD_LIBRARY_PATH, and the user defined variable to what I defined in screenshot. The reason we can change the value and create new variable because of the ownership permission of the file has change to root. When the file is under root, any non-root user cannot access the file. In this case, all the new process will be fork with root permission.



The screenshot shows a Terminator terminal window with the title bar "Terminator" and the path "/bin/bash". The window contains a terminal session with the following output:

```
[09/28/20]seed@VM:~/host$ export PATH=/bin
[09/28/20]seed@VM:~/host$ export LD_LIBRARY_PATH=/bin
[09/28/20]seed@VM:~/host$ export MYNAME=HELLO_THIS_IS_LAB1
[09/28/20]seed@VM:~/host$ ./foo
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:8fe241ba-dcb2-4d78-a3d5-e88e07de6084
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=4585
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
WINDOWID=35651588
OLDPWD=/home/seed
```

Terminator

/bin/bash

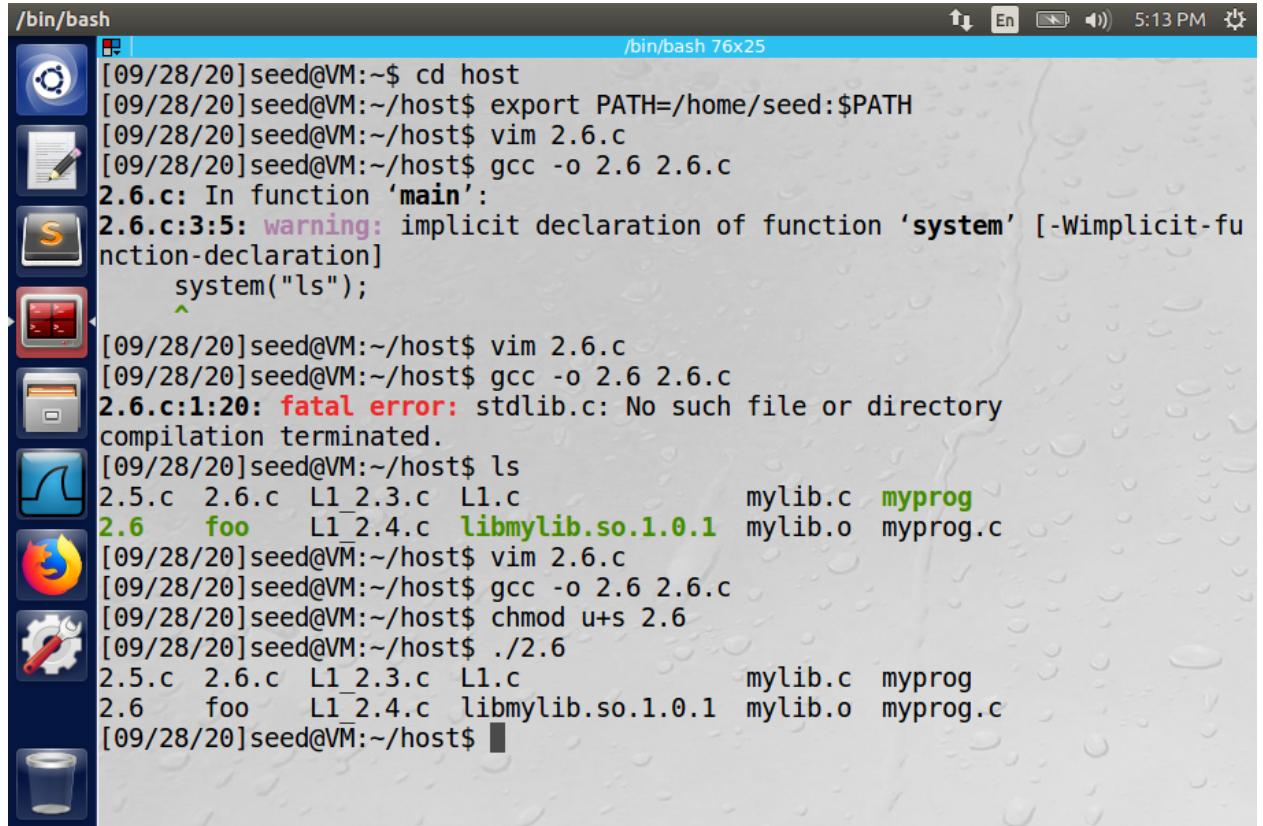
```
0;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:  
QT_ACCESSIBILITY=1  
LD_LIBRARY_PATH=/bin  
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0  
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0  
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh  
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path  
·GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop  
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg  
DESKTOP_SESSION=ubuntu  
PATH=/bin  
QT_IM_MODULE=ibus  
QT_QPA_PLATFORMTHEME=appmenu-qt5  
XDG_SESSION_TYPE=x11  
PWD=/home/seed/host  
JOB=unity-settings-daemon  
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
```

Terminator

/bin/bash

```
0;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:  
QT_ACCESSIBILITY=1  
LD_LIBRARY_PATH=/bin  
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  
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop  
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg  
DESKTOP_SESSION=ubuntu  
PATH=/bin  
QT_IM_MODULE=ibus  
QT_QPA_PLATFORMTHEME=appmenu-qt5  
XDG_SESSION_TYPE=x11  
PWD=/home/seed/host  
JOB=unity-settings-daemon  
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  
MYNAME=HELLO_THIS_IS_LAB1  
SESSIONTYPE=gnome-session
```

6. Yes, you can let set-uid program that is owned by root to run the code. However, it is unsafe.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is '/bin/bash' and the size is 76x25. The terminal content is as follows:

```
[09/28/20]seed@VM:~$ cd host
[09/28/20]seed@VM:~/host$ export PATH=/home/seed:$PATH
[09/28/20]seed@VM:~/host$ vim 2.6.c
[09/28/20]seed@VM:~/host$ gcc -o 2.6 2.6.c
2.6.c: In function 'main':
2.6.c:3:5: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
    system("ls");
^
[09/28/20]seed@VM:~/host$ vim 2.6.c
[09/28/20]seed@VM:~/host$ gcc -o 2.6 2.6.c
2.6.c:1:20: fatal error: stdlib.c: No such file or directory
compilation terminated.
[09/28/20]seed@VM:~/host$ ls
2.5.c 2.6.c L1_2.3.c L1.c           mylib.c  myprog
2.6   foo   L1_2.4.c libmylib.so.1.0.1 mylib.o  myprog.c
[09/28/20]seed@VM:~/host$ vim 2.6.c
[09/28/20]seed@VM:~/host$ gcc -o 2.6 2.6.c
[09/28/20]seed@VM:~/host$ chmod u+s 2.6
[09/28/20]seed@VM:~/host$ ./2.6
2.5.c 2.6.c L1_2.3.c L1.c           mylib.c  myprog
2.6   foo   L1_2.4.c libmylib.so.1.0.1 mylib.o  myprog.c
[09/28/20]seed@VM:~/host$
```

7.

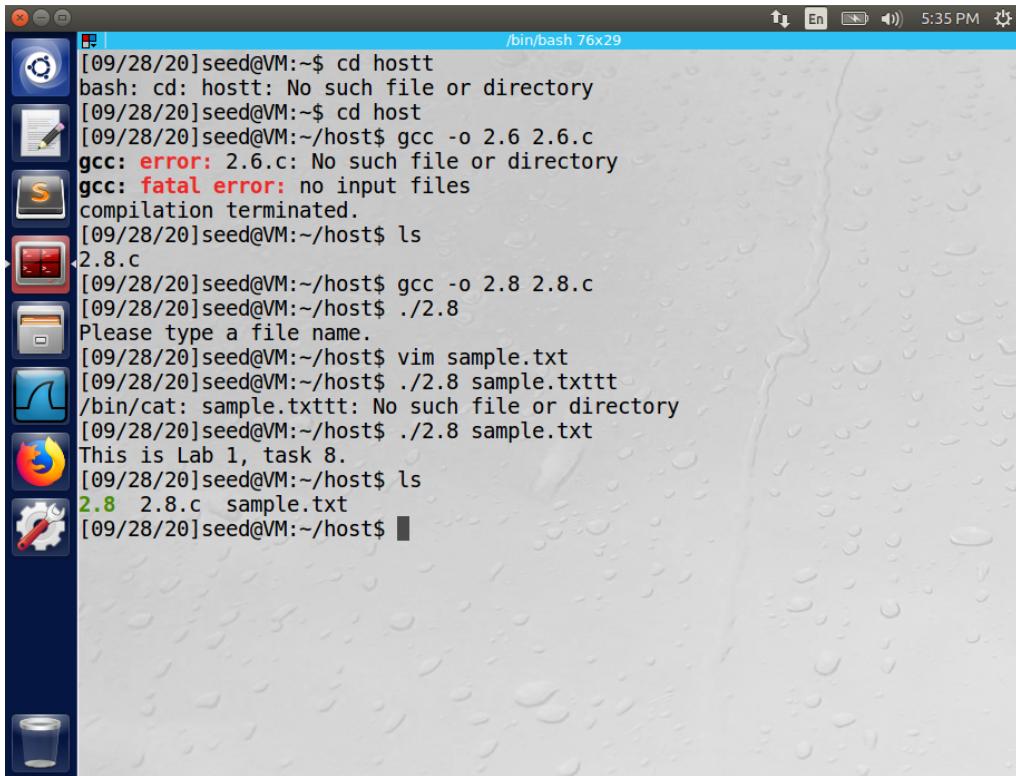
```
[09/28/20]seed@VM:~$ man sleep
[09/28/20]seed@VM:~$ vim myprog.c
[09/28/20]seed@VM:~$ gcc -o myprog myprog.c
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo chmod u+s myprog
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo su
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# gedit .bashrc

(gedit:5716): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
^C
root@VM:/home/seed# ./myprog
root@VM:/home/seed# exit
exit
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo su
root@VM:/home/seed# useradd -d /usr/user1 -m user1
root@VM:/home/seed# chown user1 myprog
root@VM:/home/seed# chgrp user1 myprog
root@VM:/home/seed# exit
exit
[09/28/20]seed@VM:~$
```

```
[09/28/20]seed@VM:~$ sudo chmod u+s myprog
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo su
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# gedit .bashrc

(gedit:5716): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
^C
root@VM:/home/seed# ./myprog
root@VM:/home/seed# exit
exit
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ sudo su
root@VM:/home/seed# useradd -d /usr/user1 -m user1
root@VM:/home/seed# chown user1 myprog
root@VM:/home/seed# chgrp user1 myprog
root@VM:/home/seed# exit
exit
[09/28/20]seed@VM:~$ 
[09/28/20]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/28/20]seed@VM:~$ ./myprog
bash: ./myprog: No such file or directory
[09/28/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/28/20]seed@VM:~$ 
```

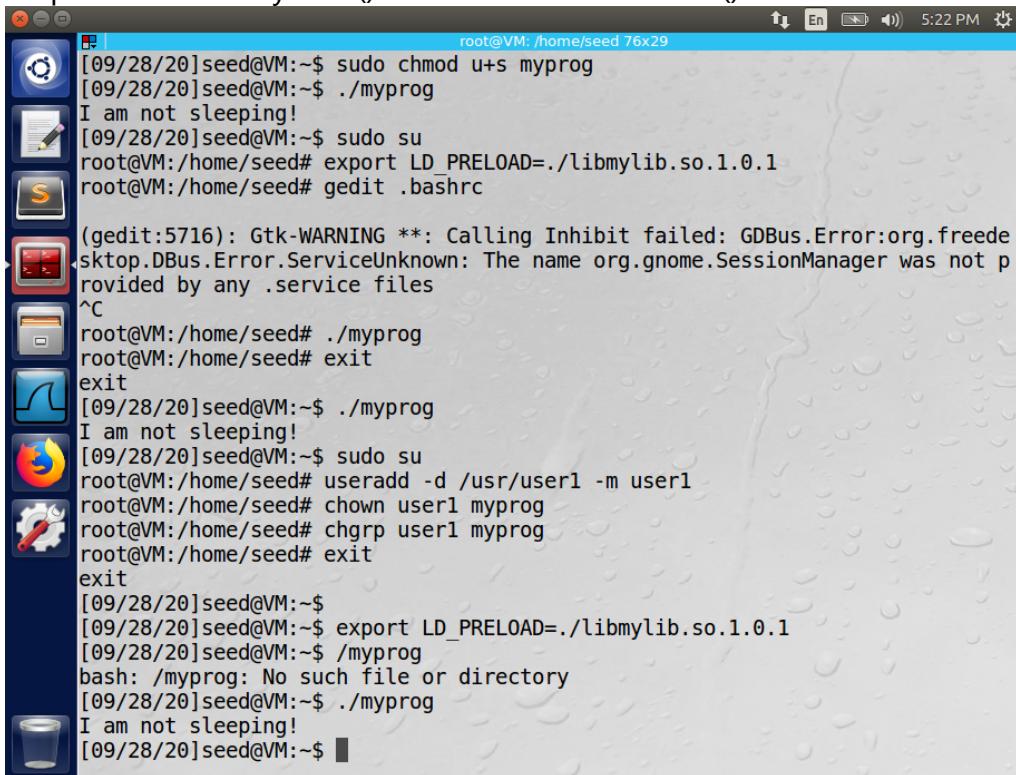
8. Step1:



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is '/bin/bash 76x29'. The session log is as follows:

```
[09/28/20]seed@VM:~$ cd hostt  
bash: cd: hostt: No such file or directory  
[09/28/20]seed@VM:~$ cd host  
[09/28/20]seed@VM:~/host$ gcc -o 2.6 2.6.c  
gcc: error: 2.6.c: No such file or directory  
gcc: fatal error: no input files  
compilation terminated.  
[09/28/20]seed@VM:~/host$ ls  
2.8.c  
[09/28/20]seed@VM:~/host$ gcc -o 2.8 2.8.c  
[09/28/20]seed@VM:~/host$ ./2.8  
Please type a file name.  
[09/28/20]seed@VM:~/host$ vim sample.txt  
[09/28/20]seed@VM:~/host$ ./2.8 sample.txttt  
/bin/cat: sample.txttt: No such file or directory  
[09/28/20]seed@VM:~/host$ ./2.8 sample.txt  
This is Lab 1, task 8.  
[09/28/20]seed@VM:~/host$ ls  
2.8 2.8.c sample.txt  
[09/28/20]seed@VM:~/host$
```

Step 2: Comment system() and uncomment execve()



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is 'root@VM: /home/seed 76x29'. The session log is as follows:

```
[09/28/20]seed@VM:~$ sudo chmod u+s myprog  
[09/28/20]seed@VM:~$ ./myprog  
I am not sleeping!  
[09/28/20]seed@VM:~$ sudo su  
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1  
root@VM:/home/seed# gedit .bashrc  
(gedit:5716): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files  
^C  
root@VM:/home/seed# ./myprog  
root@VM:/home/seed# exit  
[09/28/20]seed@VM:~$ ./myprog  
I am not sleeping!  
[09/28/20]seed@VM:~$ sudo su  
root@VM:/home/seed# useradd -d /usr/user1 -m user1  
root@VM:/home/seed# chown user1 myprog  
root@VM:/home/seed# chgrp user1 myprog  
root@VM:/home/seed# exit  
[09/28/20]seed@VM:~$  
[09/28/20]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1  
[09/28/20]seed@VM:~$ ./myprog  
bash: ./myprog: No such file or directory  
[09/28/20]seed@VM:~$ ./myprog  
I am not sleeping!  
[09/28/20]seed@VM:~$
```

Yes, attacks in Step 1 still work, I can read the file content.

```
root@VM: /home/seed/host
root@VM: /home/seed/host 76x29
nction-declaration]
sleep(1);
^
2.9.c:19:1: warning: implicit declaration of function 'setuid' [-Wimplicit-f
unction-declaration]
setuid(getuid()); /* getuid() returns the real uid */
^
2.9.c:19:8: warning: implicit declaration of function 'getuid' [-Wimplicit-f
Terminator   [claration]
setuid(getuid()); /* getuid() returns the real uid */
^
2.9.c:20:5: warning: implicit declaration of function 'fork' [-Wimplicit-fun
ction-declaration]
if (fork()) { /* In the parent process */
^
2.9.c:21:1: warning: implicit declaration of function 'close' [-Wimplicit-fu
nction-declaration]
close (fd);
^
2.9.c:27:1: warning: implicit declaration of function 'write' [-Wimplicit-fu
nction-declaration]
write (fd, "Malicious Data\n", 15);
^
[09/28/20]seed@VM:~/host$ gcc 2.9.c
[09/28/20]seed@VM:~/host$ sudo chown root a.out
[09/28/20]seed@VM:~/host$ sudo chmod 4755 a.out
[09/28/20]seed@VM:~/host$ ./a.out
Cannot open /etc/zzz
[09/28/20]seed@VM:~/host$
```

9.