Author: Rajat Sethi

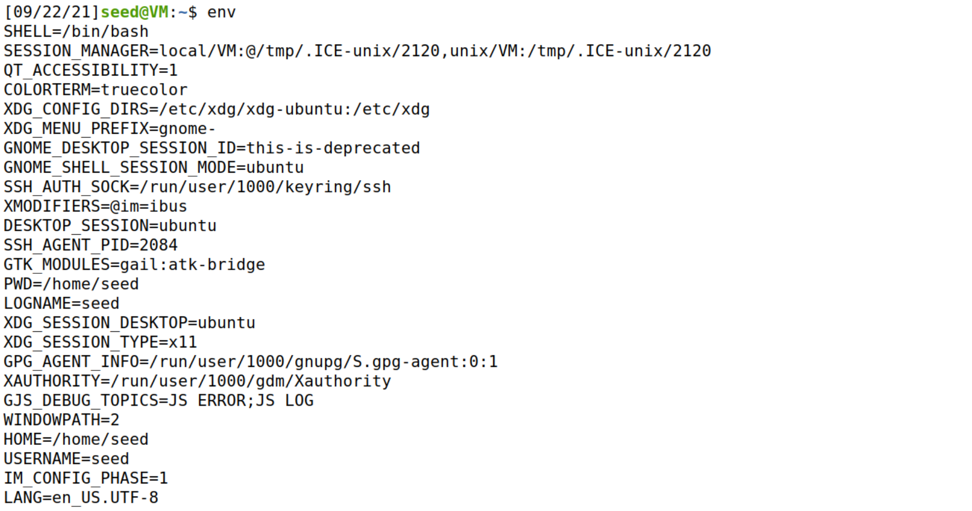
Class: CPSC-6200

Date: September 21, 2021

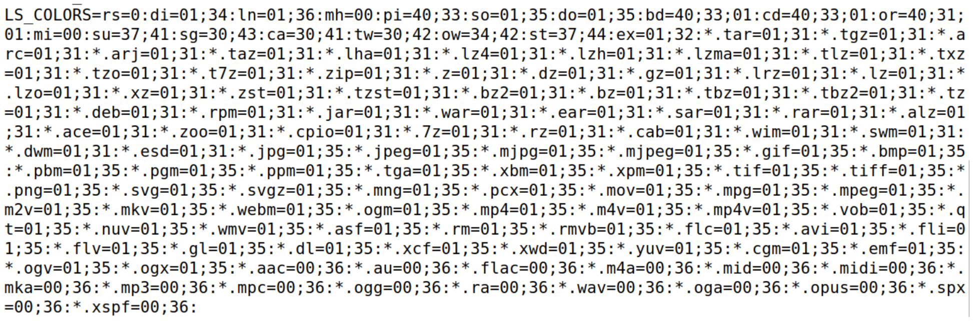
Assignment 1 Report – Environment Variables and Set-UID

Task 1.1:

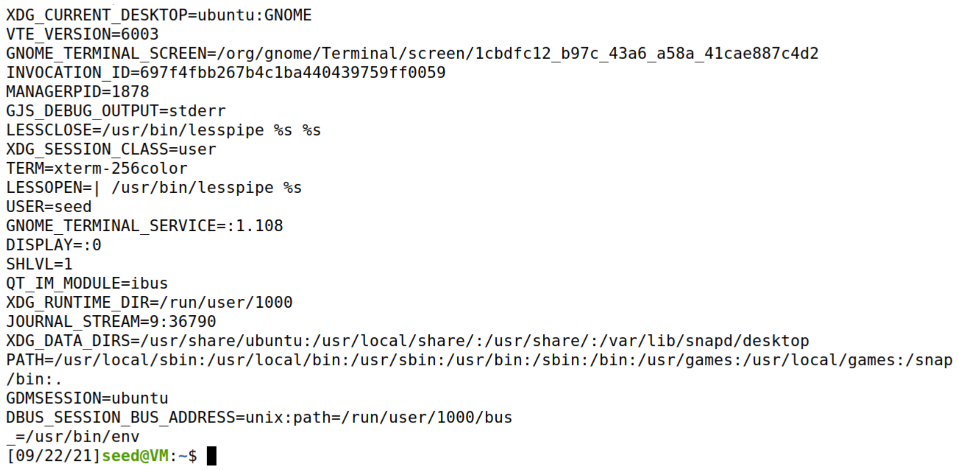
The following screenshots show the results of running “env” and “printenv PWD.”



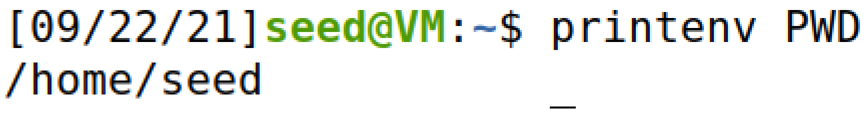
```
[09/22/21]seed@VM:~$ env
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2120,unix/VM:/tmp/.ICE-unix/2120
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2084
GTK_MODULES=gail:atk-bridge
PWD=/home/seed
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
```



```
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:*.a
rc=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:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*
.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz
=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01
;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:
*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35
:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*
.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.
m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.q
t=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=0
1;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:
*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.
mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx
=00;36:*.xspf=00;36:
```



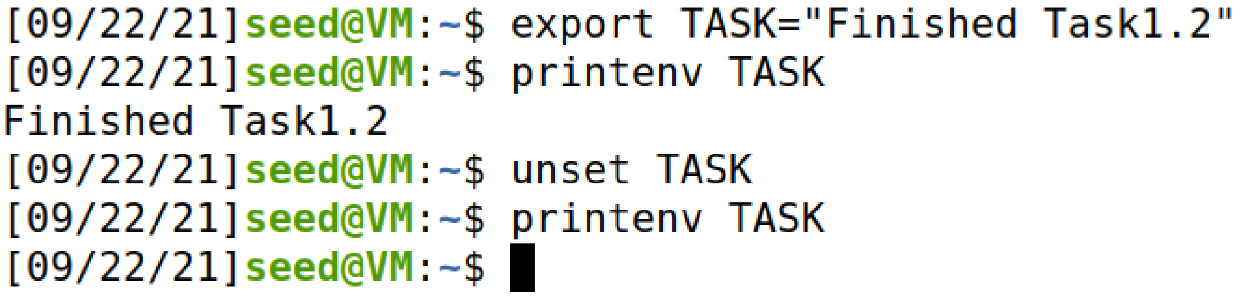
```
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/1cbdfc12_b97c_43a6_a58a_41cae887c4d2
INVOCATION_ID=697f4fbb267b4c1ba440439759ff0059
MANAGERPID=1878
GJS_DEBUG_OUTPUT=stderr
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
GNOME_TERMINAL_SERVICE=:1.108
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:36790
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap
/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
_=/usr/bin/env
[09/22/21]seed@VM:~$
```



```
[09/22/21]seed@VM:~$ printenv PWD
/home/seed
```

Task 1.2:

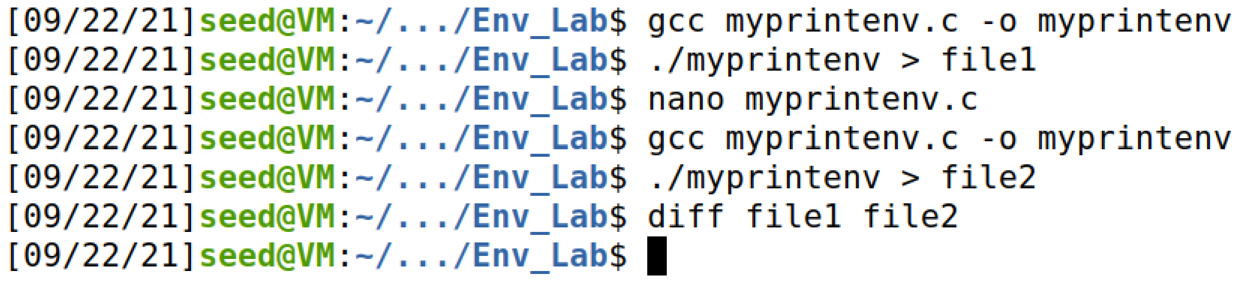
I used “export” to create an environment variable TASK, then removed it with “unset”



```
[09/22/21]seed@VM:~$ export TASK="Finished Task1.2"
[09/22/21]seed@VM:~$ printenv TASK
Finished Task1.2
[09/22/21]seed@VM:~$ unset TASK
[09/22/21]seed@VM:~$ printenv TASK
[09/22/21]seed@VM:~$
```

Task 2:

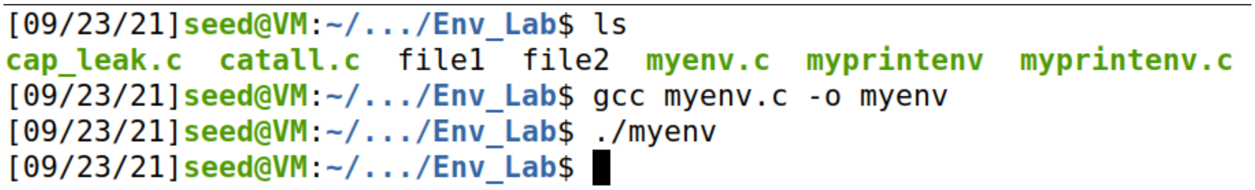
Conclusion - As shown in the screenshot, there is no difference between the child process’ environment variables and the parent process’



```
[09/22/21]seed@VM:~/.../Env_Lab$ gcc myprintenv.c -o myprintenv
[09/22/21]seed@VM:~/.../Env_Lab$ ./myprintenv > file1
[09/22/21]seed@VM:~/.../Env_Lab$ nano myprintenv.c
[09/22/21]seed@VM:~/.../Env_Lab$ gcc myprintenv.c -o myprintenv
[09/22/21]seed@VM:~/.../Env_Lab$ ./myprintenv > file2
[09/22/21]seed@VM:~/.../Env_Lab$ diff file1 file2
[09/22/21]seed@VM:~/.../Env_Lab$
```

Task 3.1:

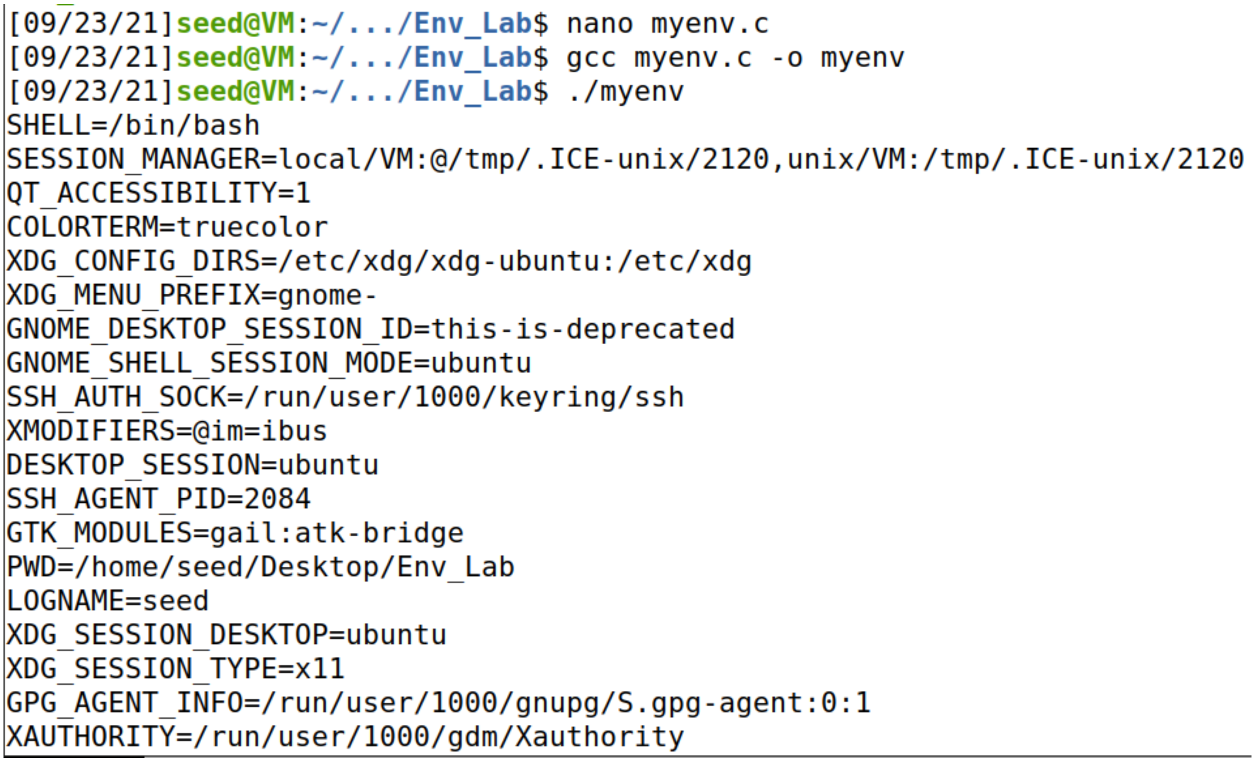
In its original form, ‘myenv.c’ cannot list any environment variables because execve() was not given an environment to look at.



```
[09/23/21]seed@VM:~/.../Env_Lab$ ls
cap_leak.c  catall.c  file1  file2  myenv.c  myprintenv  myprintenv.c
[09/23/21]seed@VM:~/.../Env_Lab$ gcc myenv.c -o myenv
[09/23/21]seed@VM:~/.../Env_Lab$ ./myenv
[09/23/21]seed@VM:~/.../Env_Lab$ 
```

Task 3.2:

When “environ” is passed in as a parameter to execve(), the program prints out all of the environment variables.

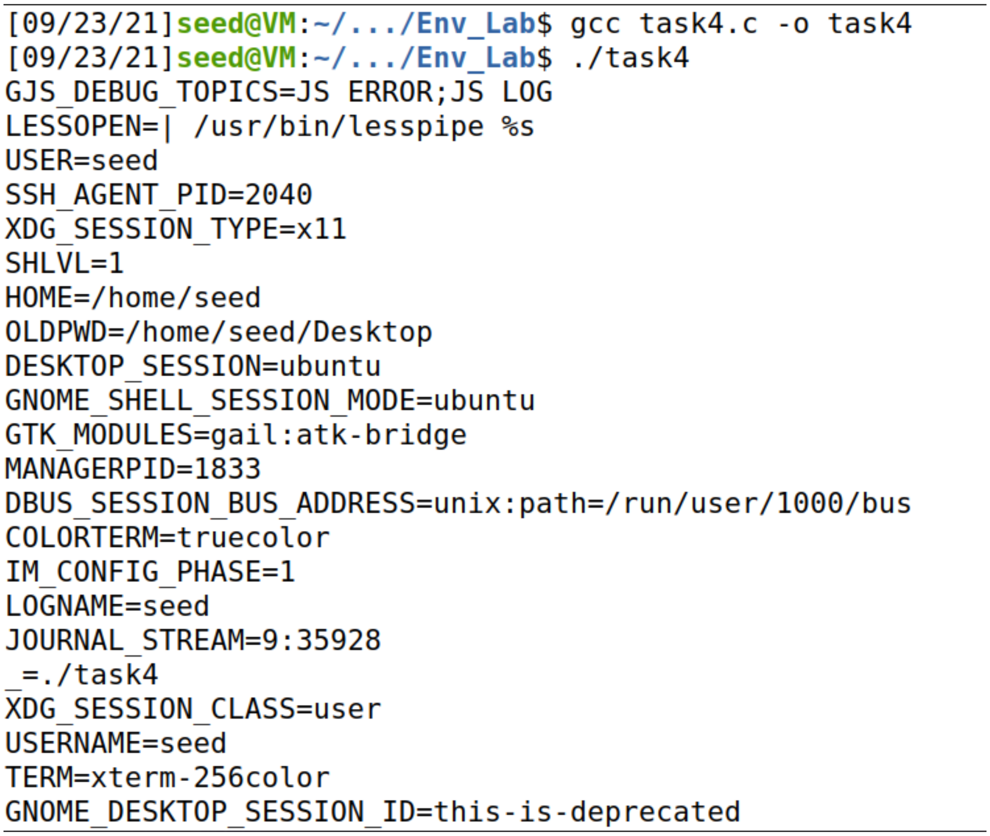


```
[09/23/21]seed@VM:~/.../Env_Lab$ nano myenv.c
[09/23/21]seed@VM:~/.../Env_Lab$ gcc myenv.c -o myenv
[09/23/21]seed@VM:~/.../Env_Lab$ ./myenv
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2120,unix/VM:/tmp/.ICE-unix/2120
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2084
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Env_Lab
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
```

Conclusion: “environ” is a special variable that exists in “GLIBC” library and can be declared using the extern keyword. It is a pointer to a list of strings (char**) that points to whatever the system environment is. When “environ” is declared and passed into the execve() function, it prints out the environment variables.

Task 4:

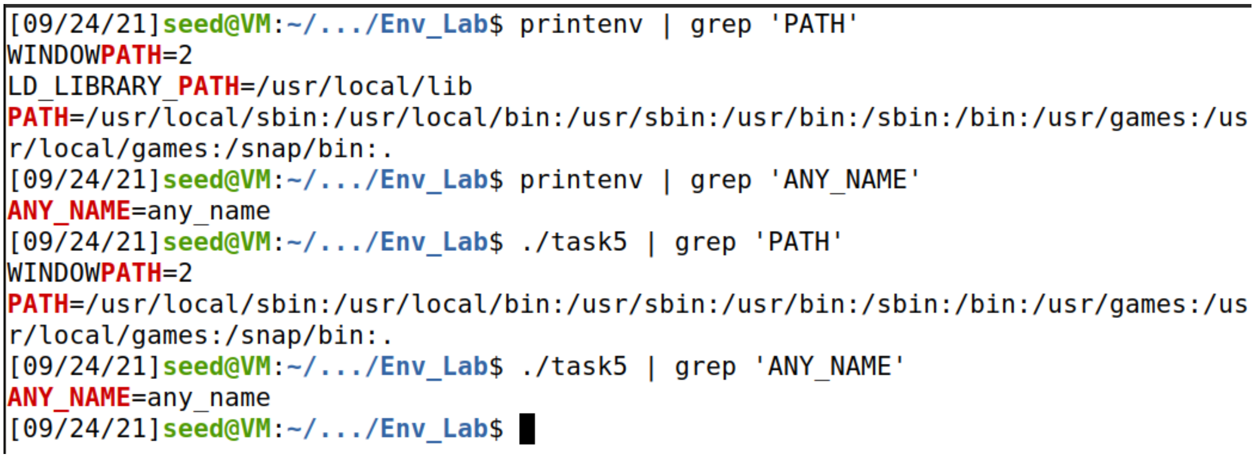
The output of running the code provided for Task 4 with the system(“usr/bin/env”) function.



```
[09/23/21]seed@VM:~/.../Env_Lab$ gcc task4.c -o task4
[09/23/21]seed@VM:~/.../Env_Lab$ ./task4
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SSH_AGENT_PID=2040
XDG_SESSION_TYPE=x11
SHLVL=1
HOME=/home/seed
OLDPWD=/home/seed/Desktop
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gail:atk-bridge
MANAGERPID=1833
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
COLORTERM=truecolor
IM_CONFIG_PHASE=1
LOGNAME=seed
JOURNAL_STREAM=9:35928
_=./task4
XDG_SESSION_CLASS=user
USERNAME=seed
TERM=xterm-256color
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
```

Task 5:

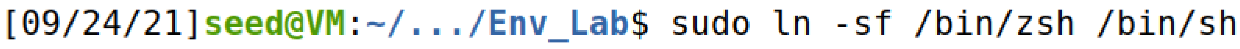
As shown in the following picture, PATH and ANY_NAME both existed in environ. However, even though LD_LIBRARY_PATH was exported like ANY_NAME, it was surprisingly not called in the program.



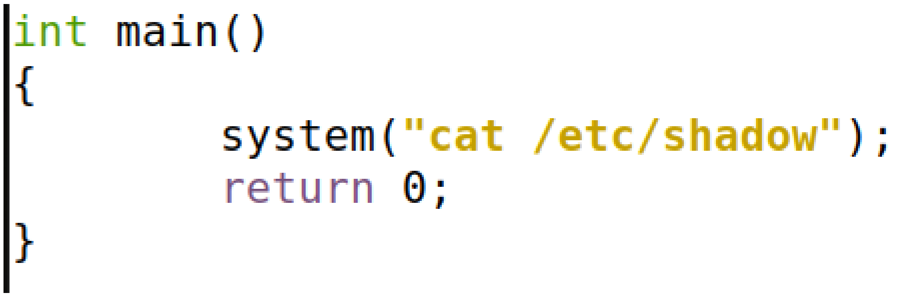
```
[09/24/21]seed@VM:~/.../Env_Lab$ printenv | grep 'PATH'
WINDOWPATH=2
LD_LIBRARY_PATH=/usr/local/lib
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games:/snap/bin:.
[09/24/21]seed@VM:~/.../Env_Lab$ printenv | grep 'ANY_NAME'
ANY_NAME=any_name
[09/24/21]seed@VM:~/.../Env_Lab$ ./task5 | grep 'PATH'
WINDOWPATH=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games:/snap/bin:.
[09/24/21]seed@VM:~/.../Env_Lab$ ./task5 | grep 'ANY_NAME'
ANY_NAME=any_name
[09/24/21]seed@VM:~/.../Env_Lab$ █
```

Task 6:

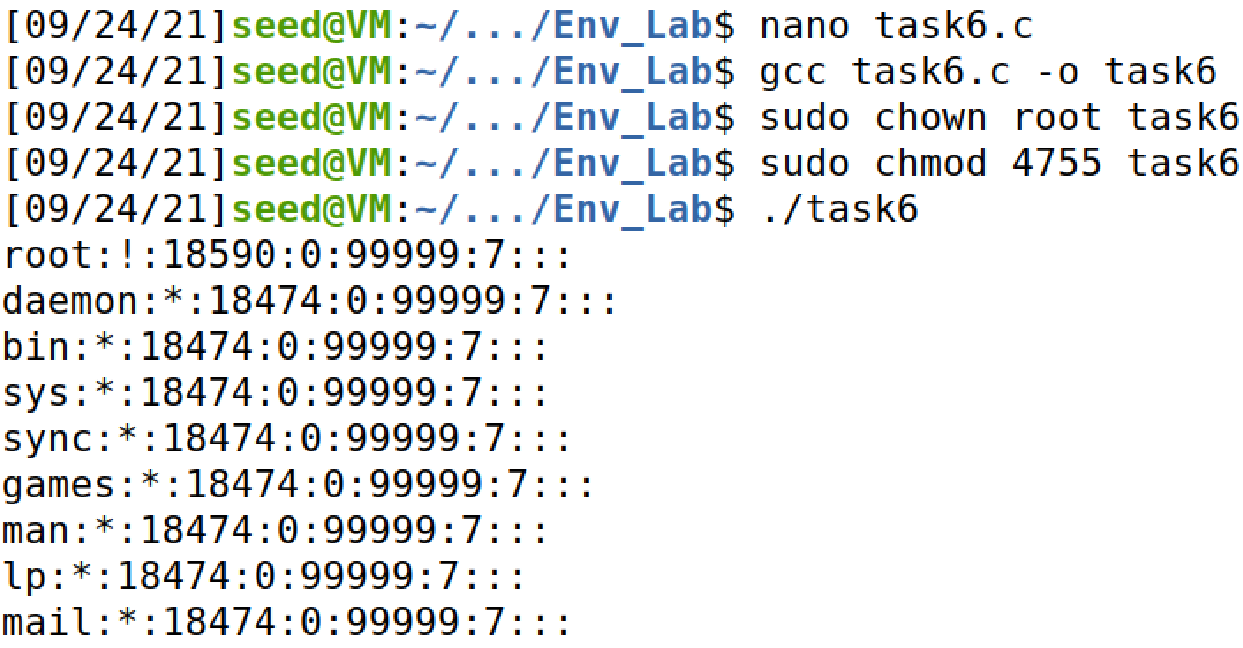
After changing the shell from /bin/sh to /bin/zsh, I was able to use the system() to print out the contents of /etc/shadow. Of course, this was only possible by changing the owner to root and turning on the Set-UID bit.



```
[09/24/21]seed@VM:~/.../Env_Lab$ sudo ln -sf /bin/zsh /bin/sh
```



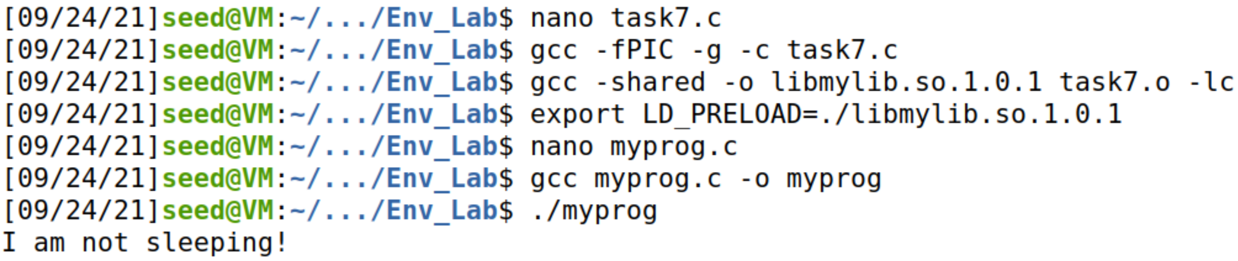
```
int main()
{
        system("cat /etc/shadow");
        return 0;
}
```



```
[09/24/21]seed@VM:~/.../Env_Lab$ nano task6.c
[09/24/21]seed@VM:~/.../Env_Lab$ gcc task6.c -o task6
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chown root task6
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chmod 4755 task6
[09/24/21]seed@VM:~/.../Env_Lab$ ./task6
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
```

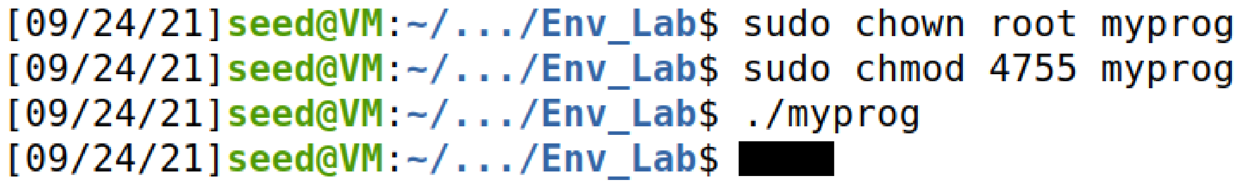
Task 7:

Running "myprog" as a normal user without changing owner or Set-UID. In this scenario, the code runs with the new sleep command, since LD_PRELOAD was changed and Set-UID is off.



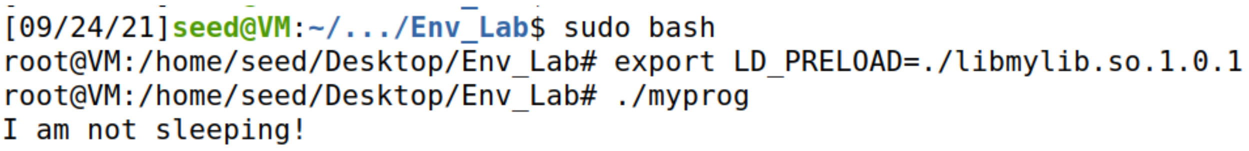
```
[09/24/21]seed@VM:~/.../Env_Lab$ nano task7.c
[09/24/21]seed@VM:~/.../Env_Lab$ gcc -fPIC -g -c task7.c
[09/24/21]seed@VM:~/.../Env_Lab$ gcc -shared -o libmylib.so.1.0.1 task7.o -lc
[09/24/21]seed@VM:~/.../Env_Lab$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/24/21]seed@VM:~/.../Env_Lab$ nano myprog.c
[09/24/21]seed@VM:~/.../Env_Lab$ gcc myprog.c -o myprog
[09/24/21]seed@VM:~/.../Env_Lab$ ./myprog
I am not sleeping!
```

Running “myprog” as the normal user, when it’s owned by root user, and Set-UID is on. In this scenario, nothing outputs (and the terminal goes to the next command). This is because the root user currently does not have the LD_PRELOAD environment variable set to libmylib.so.1.0.1, so the “sleep” command was not overwritten.



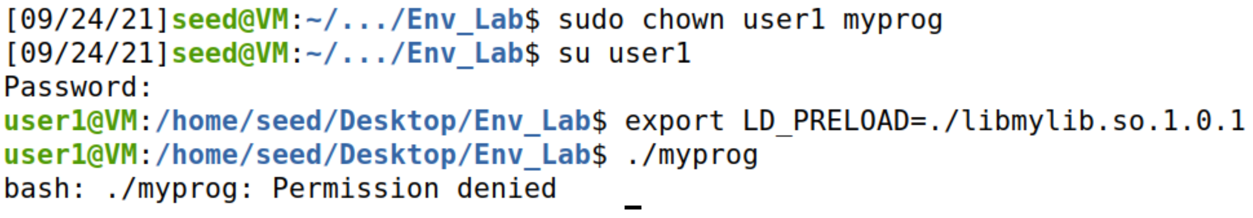
```
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chown root myprog
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chmod 4755 myprog
[09/24/21]seed@VM:~/.../Env_Lab$ ./myprog
[09/24/21]seed@VM:~/.../Env_Lab$ 
```

Running “myprog” as the root user, owned by the root user, and Set-UID is on. In this scenario, the code runs with the new sleep command as expected.



```
[09/24/21]seed@VM:~/.../Env_Lab$ sudo bash
root@VM:/home/seed/Desktop/Env_Lab# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Desktop/Env_Lab# ./myprog
I am not sleeping!
```

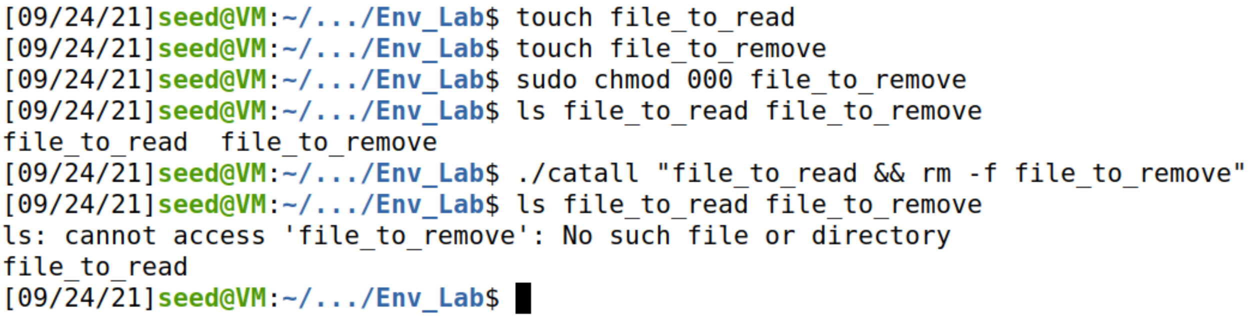
Running “myprog” as “user1,” owned by “user1,” and Set-UID is on. In this scenario, the regular user is denied because Set-UID is on.



```
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chown user1 myprog
[09/24/21]seed@VM:~/.../Env_Lab$ su user1
Password:
user1@VM:/home/seed/Desktop/Env_Lab$ export LD_PRELOAD=./libmylib.so.1.0.1
user1@VM:/home/seed/Desktop/Env_Lab$ ./myprog
bash: ./myprog: Permission denied
```

Task 8.1:

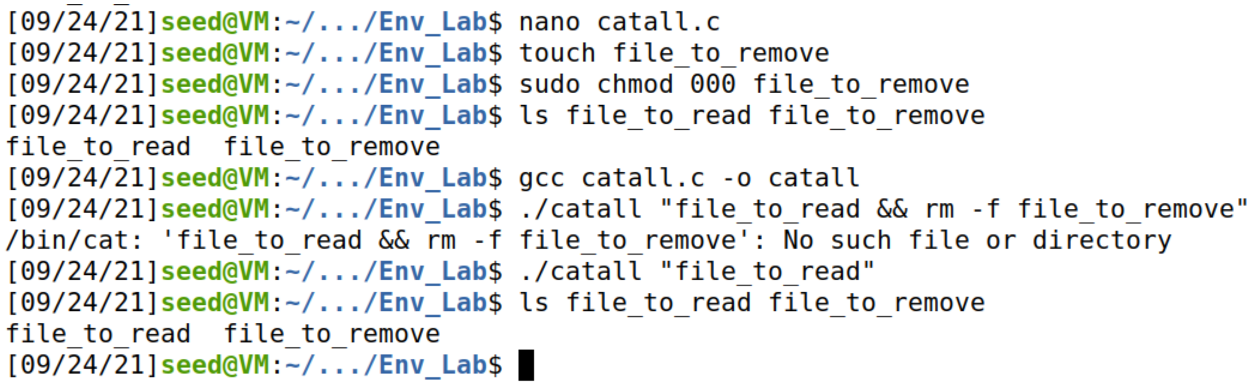
In the “catall” program, the system() function runs any command put into it. The input is not adequately filtered, and so anyone can use the “&&” operation to run any other command they want, as shown in the screenshot.



```
[09/24/21]seed@VM:~/.../Env_Lab$ touch file_to_read
[09/24/21]seed@VM:~/.../Env_Lab$ touch file_to_remove
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chmod 000 file_to_remove
[09/24/21]seed@VM:~/.../Env_Lab$ ls file_to_read file_to_remove
file_to_read  file_to_remove
[09/24/21]seed@VM:~/.../Env_Lab$ ./catall "file_to_read && rm -f file_to_remove"
[09/24/21]seed@VM:~/.../Env_Lab$ ls file_to_read file_to_remove
ls: cannot access 'file_to_remove': No such file or directory
file_to_read
[09/24/21]seed@VM:~/.../Env_Lab$ 
```

Task 8.2:

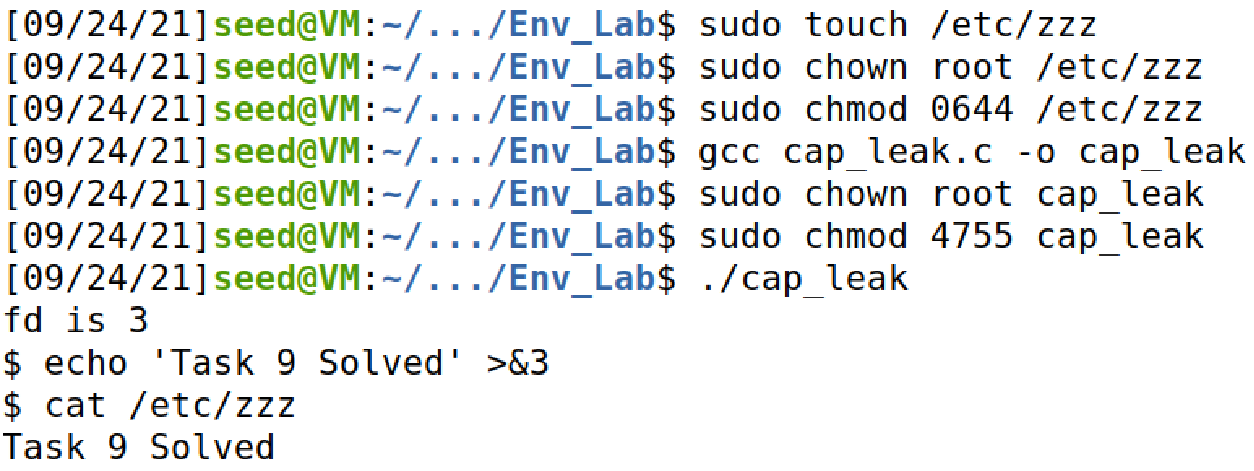
With system() replaced with execve(), the exploit no longer works and I can no longer run any command of my choosing, as shown in the screenshot.



```
[09/24/21]seed@VM:~/.../Env_Lab$ nano catall.c
[09/24/21]seed@VM:~/.../Env_Lab$ touch file_to_remove
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chmod 000 file_to_remove
[09/24/21]seed@VM:~/.../Env_Lab$ ls file_to_read file_to_remove
file_to_read  file_to_remove
[09/24/21]seed@VM:~/.../Env_Lab$ gcc catall.c -o catall
[09/24/21]seed@VM:~/.../Env_Lab$ ./catall "file_to_read && rm -f file_to_remove"
/bin/cat: 'file_to_read && rm -f file_to_remove': No such file or directory
[09/24/21]seed@VM:~/.../Env_Lab$ ./catall "file_to_read"
[09/24/21]seed@VM:~/.../Env_Lab$ ls file_to_read file_to_remove
file_to_read  file_to_remove
[09/24/21]seed@VM:~/.../Env_Lab$ 
```

Task 9:

Using the file pointer and capability leak given in the problem, I was able to echo a line into /etc/zzz and overwrite the file’s contents.



```
[09/24/21]seed@VM:~/.../Env_Lab$ sudo touch /etc/zzz
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chown root /etc/zzz
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chmod 0644 /etc/zzz
[09/24/21]seed@VM:~/.../Env_Lab$ gcc cap_leak.c -o cap_leak
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chown root cap_leak
[09/24/21]seed@VM:~/.../Env_Lab$ sudo chmod 4755 cap_leak
[09/24/21]seed@VM:~/.../Env_Lab$ ./cap_leak
fd is 3
$ echo 'Task 9 Solved' >&3
$ cat /etc/zzz
Task 9 Solved
```