Environment Variable and Set-UID Program Lab 1

Jeffrey DeOcampo

February 25, 2025

Using cloud approach:

```
*** System restart required ***
Last login: Mon Feb 24 04:28:23 2025 from 35.235.244.32
jjdeocampo20@instance-20250224-035723:~$ ls
Labsetup.zip  src-cloud  src-cloud.zip
jjdeocampo20@instance-20250224-035723:~$ sudo su seed
seed@instance-20250224-035723:~$ ls
Desktop  Labsetup  Labsetup.zip  test
seed@instance-20250224-035723:~$ cd Labsetup/
seed@instance-20250224-035723:~/Labsetup$ ls -l
total 44
-rwxrwxr-x 1 seed seed 16888 Feb 24 04:41 a.out
-rw-rw-r-- 1 seed seed   761 Dec 27  2020 cap_leak.c
-rw-rw-r-- 1 seed seed   471 Feb 19  2021 catall.c
-rw-rw-r-- 1 seed seed  1933 Feb 24 04:40 file1
-rw-rw-r-- 1 seed seed  1933 Feb 24 04:42 file2
-rw-rw-r-- 1 seed seed   180 Dec 27  2020 myenv.c
-rw-rw-r-- 1 seed seed   418 Feb 24 04:41 myprintenv.c
```

(proof of name before switching users from jjdeocampo20 to seed)

Task 1: Manipulating Environment Variables

In this task, we utilize methods to view environment variables

```
seed@instance-20250224-035723:~/Labsetup$ printenv PWD
/home/seed/Labsetup
seed@instance-20250224-035723:~/Labsetup$ env | grep PWD
PWD=/home/seed/Labsetup
OLDPWD=/home/seed
```

(printenv prints all environment variables, however here we specify to print the path, and also using piping to get only lines containing the string “PWD”)

1.1 env and printenv

- printenv is used to print all environment variables or any variable that is specified after it
- env displays **both** environment variables and can be used to run commands with a modified environment

1.2 export and unset

- export can be used to define environment variables and make it available to child processes
- unset command is used to delete an environment variable

```
seed@instance-20250224-035723:~/Labsetup$ export TEST="Hello"
seed@instance-20250224-035723:~/Labsetup$ printenv TEST
Hello
seed@instance-20250224-035723:~/Labsetup$ unset TEST
seed@instance-20250224-035723:~/Labsetup$ printenv TEST
seed@instance-20250224-035723:~/Labsetup$
```

(here we define the environment variable TEST and print the variable showing its value. Then unset it and printed the variable showing it has been removed)

Task 2: Passing Environment Variables from Parent Process to Child Process

1.1 ./a.out > file1

- Running gcc myprintenv.c creates a.out, which we saved the output into file1
- This prints all the environment variables of the child process
- This involves the original code where printenv() is in the child process

```c
#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);
  }
}
```

(original code)

```
seed@instance-20250224-035723:~/Labsetup$ gcc myprintenv.c
seed@instance-20250224-035723:~/Labsetup$ ./a.out > file1
```

(saving output to file1)

Output saved to file1:

```
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=jjdeocampo20
PWD=/home/seed/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.UTF-8
MY_VAR=Hello, Linux!
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=3
7;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:*.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;3
1:*.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:*.w
im=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:*.b
mp=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:*.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=00;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1001
MAIL=/var/mail/seed
TEST=JEFFREY
OLDPWD=/home/seed
_=./a.out
```

(added env variable TEST)

1.2 ./a.out > file2

- We run it again after commenting out the printenv() in the child process. Recompiling it and saving the output to file2
- This prints all environment variables of the parent process

```c
#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);
  }
}
```

```
seed@instance-20250224-035723:~/Labsetup$ gcc myprintenv.c
seed@instance-20250224-035723:~/Labsetup$ ./a.out > file2
```

(saving output to file2 after modifying myprintenv.c)

Output saved to file2:

```
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=jjdeocampo20
PWD=/home/seed/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.UTF-8
MY_VAR=Hello, Linux!
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=3
7;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:*.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;3
1:*.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:*.w
im=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:*.b
mp=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:*.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=00;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1001
MAIL=/var/mail/seed
TEST=JEFFREY
OLDPWD=/home/seed
_=./a.out
~
```

(TEST is printed in file2 because the current environment variables were captured by the program)

1.3 diff command

- diff compares the outputs of two files and finds any differences

```
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ diff file1 file2
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$
```

(here we see no difference between file1 and file2)

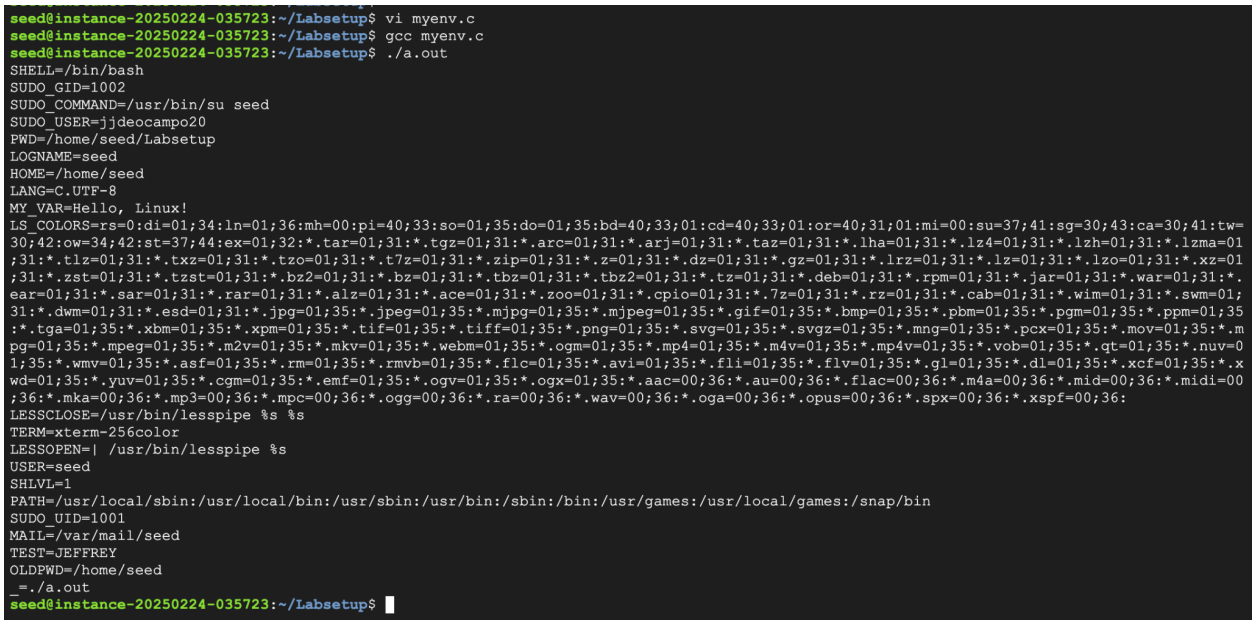
Task 3: Environment Variables and execve()

1.1 Execve()

- In this task, we see how execve() can load commands and execute them inside a process

```
seed@instance-20250224-035723:~/Labsetup$ vi myenv.c
seed@instance-20250224-035723:~/Labsetup$ gcc myenv.c
seed@instance-20250224-035723:~/Labsetup$ ./a.out
seed@instance-20250224-035723:~/Labsetup$
```

(By compiling " execve("/usr/bin/env", argv, NULL); " we see that there is no output, no environment variables are printed)



(ran myenv.c with the line execve("/usr/bin/env", argv, environ);)

- When using "environ" over "NULL," the environment variables are printed.
- This time the third argument is `environ`, which holds the current environment variables of the running process.
- This means the new process (`/usr/bin/env`) will inherit and print all existing environment variables.

Task 4: Environment Variables and system()

1.1 This task demonstrates how the system() function passes the calling process's environment variables to a new shell that executes the "/usr/bin/env" command, printing the environment variables of the calling process.

```
seed@instance-20250224-035723:~/Labsetup$ gcc task4.c -o task4.out
seed@instance-20250224-035723:~/Labsetup$ ls
a.out  a.out.backup  cap_leak.c  catall.c  file1  file2  myenv.c  myprintenv.c  task4.c  task4.out
seed@instance-20250224-035723:~/Labsetup$ ./task4.out
SUDO_GID=1002
LESSOPEN=| /usr/bin/lesspipe %s
MAIL=/var/mail/seed
USER=seed
SHLVL=1
HOME=/home/seed
OLDPWD=/home/seed
MY_VAR=Hello, Linux!
SUDO_UID=1001
LOGNAME=seed
_=./task4.out
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
LANG=C.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:*.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:*.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:*.m
pg=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=0
1;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:*.x
wd=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:
SUDO_COMMAND=/usr/bin/su seed
TEST=JEFFREY
SHELL=/bin/bash
SUDO_USER=jjdeocampo20
LESSCLOSE=/usr/bin/lesspipe %s %s
PWD=/home/seed/Labsetup
```

(using the system program, it prints the environment variables as seen by the shell executing the command)

Task 5: Environment Variable and Set-UID Programs

1.1 We will see if this Set-UID program will inherit env variables from the user's process

- task5.c holds the set-UID program and here we printed out the environment variables of the current process

```
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ vi task5.c
seed@instance-20250224-035723:~/Labsetup$ gcc task5.c -o task5.out
seed@instance-20250224-035723:~/Labsetup$ ./task5.out
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=jjdeocampo20
PWD=/home/seed/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.UTF-8
MY_VAR=Hello, Linux!
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:*.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:*.m
pg=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=0
1;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:*.x
wd=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:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1001
MAIL=/var/mail/seed
TEST=JEFFREY
OLDPWD=/home/seed
_=./task5.out
seed@instance-20250224-035723:~/Labsetup$
```

```
seed@instance-20250224-035723:~/Labsetup$ ls -l task5.out
-rwxrwxr-x 1 seed seed 16768 Feb 25 11:33 task5.out
seed@instance-20250224-035723:~/Labsetup$
```

(using this line of code, we can see the permissions and owner ID of task5.out before switching to root)

1.2 Changing ownership of program to root, making it a set-UID program

```
seed@instance-20250224-035723:~/Labsetup$ ls -l task5.out
-rwxrwxr-x 1 seed seed 16768 Feb 25 11:33 task5.out
seed@instance-20250224-035723:~/Labsetup$ sudo chown root task5.out
seed@instance-20250224-035723:~/Labsetup$ ls -l task5.out
-rwxrwxr-x 1 root seed 16768 Feb 25 11:33 task5.out
seed@instance-20250224-035723:~/Labsetup$ sudo chmod 4755 task5.out
seed@instance-20250224-035723:~/Labsetup$ ls -l task5.out
-rwsr-xr-x 1 root seed 16768 Feb 25 11:33 task5.out
seed@instance-20250224-035723:~/Labsetup$
```

(we see now the permissions have changed for group users and the owner is now root)

1.3 Export environment variables set in shell to be inherited into set-UID process

```
seed@instance-20250224-035723:~/Labsetup$ export LD_LIBRARY_PATH=/tmp
seed@instance-20250224-035723:~/Labsetup$ env | grep LD_LIBRARY_PATH
LD_LIBRARY_PATH=/tmp
seed@instance-20250224-035723:~/Labsetup$ env | grep PATH
LD_LIBRARY_PATH=/tmp
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
seed@instance-20250224-035723:~/Labsetup$ env | grep TEST
seed@instance-20250224-035723:~/Labsetup$ export TEST=JEFFREY
seed@instance-20250224-035723:~/Labsetup$ env | grep TEST
TEST=JEFFREY
```

(PATH is not needed here since it was already set)

```
seed@instance-20250224-035723:~/Labsetup$ ./task5.out
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=jjdeocampo20
PWD=/home/seed/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.UTF-8
MY_VAR=Hello, Linux!
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:*.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:*.m
pg=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=0
1;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:*.x
wd=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:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1001
MAIL=/var/mail/seed
TEST=JEFFREY
OLDPWD=/home/seed
_=./task5.out
seed@instance-20250224-035723:~/Labsetup$
```

- As a seed user, we see here that when we can change the ownership of the program to root and the permission to execute, so as a seed user we are able to execute the root program
- That root program inherited the environment vars of the seed user except for LD_LIBRARY_PATH
- LD_LIBRARY_PATH has special permissions so it did not show up and it doesn't get inherited into the child process

Task 6: The PATH Environment Variable and Set-UID Programs

1.1 In bash, we are changing the PATH env var by adding a directory, in turn controlling the behavior of the program.

```
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ export PATH=/home/seed:$PATH
seed@instance-20250224-035723:~/Labsetup$ printenv
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=jjdeocampo20
PWD=/home/seed/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.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=3
7;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:*.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;3
1:*.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:*.w
im=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:*.b
mp=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:*.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=00;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/home/seed:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/b
in
SUDO_UID=1001
MAIL=/var/mail/seed
OLDPWD=/home/seed
_=/usr/bin/printenv
seed@instance-20250224-035723:~/Labsetup$
```

(using "export PATH=/home/seed:$PATH" we can see that we added /home/seed: in the beginning of the variable)

1.2 Creating task6.c and compiling it

```
seed@instance-20250224-035723:~/Labsetup$ vi task6.c
seed@instance-20250224-035723:~/Labsetup$ gcc task6.c -o task6.out
task6.c: In function 'main':
task6.c:3:5: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
    3 |     system("ls");
      |     ^~~~~~
```

- The code in task6.c executes the /bin/ls command

```
seed@instance-20250224-035723:~/Labsetup$ sudo chown root task6.out
seed@instance-20250224-035723:~/Labsetup$ sudo chmod 4755 task6.out
seed@instance-20250224-035723:~/Labsetup$ ls -l task6.out
-rwsr-xr-x 1 root seed 16696 Feb 26 01:43 task6.out
```

(here we change the owner to root and make it a set-uid program. We can see the permissions using “ls - l”)

1.3 Running own malicious code

- By putting /home/seed in the beginning of the path, the program searches from the beginning for the command “ls”, which is overriding the system “/bin/ls” command with our own malicious “ls” command

```
seed@instance-20250224-035723:~/Labsetup$ cd
seed@instance-20250224-035723:~$ pwd
/home/seed
seed@instance-20250224-035723:~$ vi maliciousCode.sh
seed@instance-20250224-035723:~$ chmod u+x maliciousCode.sh
seed@instance-20250224-035723:~$ ./maliciousCode.sh
Running malicious code
seed@instance-20250224-035723:~$ mv maliciousCode.sh ls
seed@instance-20250224-035723:~$ ./ls
Running malicious code
```

(created a file called “ls” in /home/seed)

```
seed@instance-20250224-035723:~$ chmod +x ls
seed@instance-20250224-035723:~$ ls -l
total 20
drwxrwxr-x 2 seed seed 4096 Feb 24 04:09 Desktop
drwxrwxr-x 2 seed seed 4096 Feb 26 02:15 Labsetup
-rw-rw-r-- 1 seed seed 2819 Feb 24 04:16 Labsetup.zip
-rwxrwxrwx 1 seed seed   30 Feb 26 02:12 ls
drwxrwxr-x 3 seed seed 4096 Feb 24 04:26 test
```

- Before running the malicious code, we added execute permissions to “ls”

```
seed@instance-20250224-035723:~/Labsetup$ ./task6.out
Running malicious code
seed@instance-20250224-035723:~/Labsetup$
```

- task6.out runs our malicious code instead of /bin/ls

Task 6: The LD_PRELOAD Environment Variable and Set-UID Programs

1.1 Building a dynamic link library

```
seed@instance-20250224-035723:~/Labsetup$ vi mylib.c
seed@instance-20250224-035723:~/Labsetup$ gcc -fPIC -g -c mylib.c
seed@instance-20250224-035723:~/Labsetup$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
seed@instance-20250224-035723:~/Labsetup$ export LD_PRELOAD=./libmylib.so.1.0.1
seed@instance-20250224-035723:~/Labsetup$ vi myprog.c
```

- We created a program mylib.c and links the program to the dynamic loader/linker

1.2 Running myprog under conditions

1. Running myprog as a regular program:

```
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ ls -l myprog.out
-rwxrwxr-x 1 seed seed 16696 Feb 26 02:48 myprog.out
seed@instance-20250224-035723:~/Labsetup$ ./myprog.out
I am not sleeping!
seed@instance-20250224-035723:~/Labsetup$
```

(User ID is seed and it prints out the code in mylib.c)

- This shows that the sleep function in myprog() was replaced by the sleep() function in mylib.c()

2. Make myprog a Set-UID root program, and run it as a normal user.

```
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ sudo chown root myprog.out
seed@instance-20250224-035723:~/Labsetup$ sudo chmod 4755 myprog.out
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ ./myprog.out
seed@instance-20250224-035723:~/Labsetup$ ./myprog.out
```

(when we run ./myprog we can see it slept for one second)

- This shows that the sleep function in myprog was ran over the one in mylib.c

3. Make myprog a set-uid root program and switch to root user and export the LD_PRELOAD env

```
root@instance-20250224-035723:/home/seed/Labsetup#
root@instance-20250224-035723:/home/seed/Labsetup#
root@instance-20250224-035723:/home/seed/Labsetup# export LD_PRELOAD=./libmylib.so.1.0.1
root@instance-20250224-035723:/home/seed/Labsetup# ./myprog.out
I am not sleeping!
root@instance-20250224-035723:/home/seed/Labsetup#
```

- This shows that the sleep function in mylib.c overruns the normal sleep command

4. Make myprog a set-uid user1 program. export the LD_PRELOAD environment variable again in a different user's account (not-root user) and run it

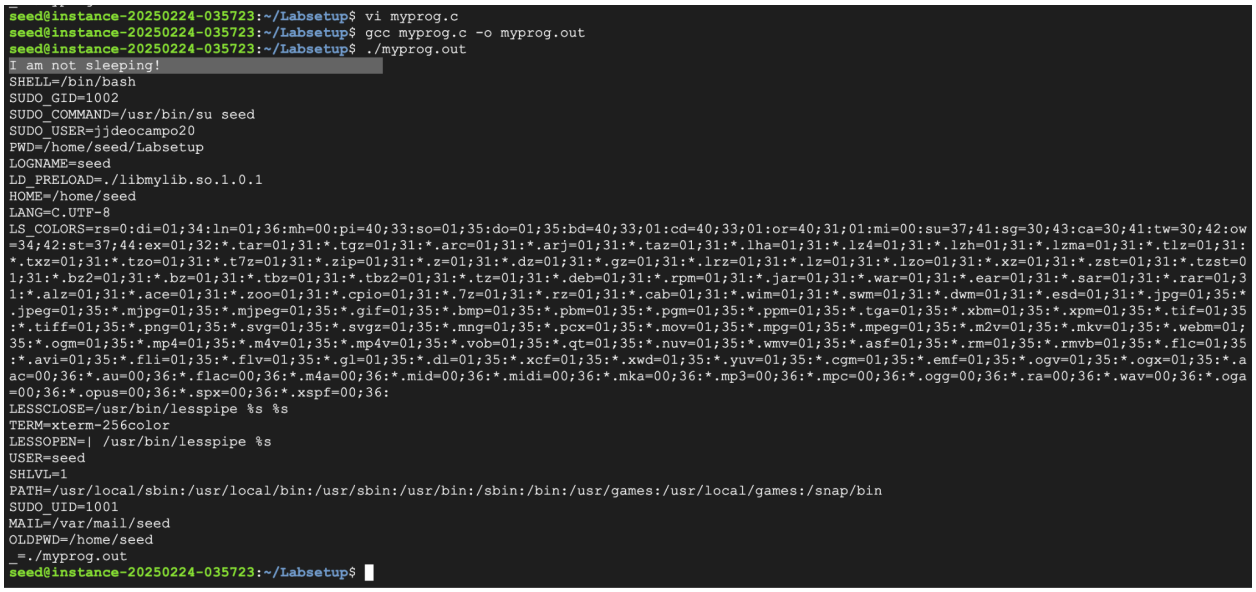
```
jjdeocampo20@instance-20250224-035723:/home/seed/Labsetup$
jjdeocampo20@instance-20250224-035723:/home/seed/Labsetup$ export LD_PRELOAD=./libmylib.so.1.0.1
jjdeocampo20@instance-20250224-035723:/home/seed/Labsetup$ ./myprog.out
I am not sleeping!
jjdeocampo20@instance-20250224-035723:/home/seed/Labsetup$
```

- This shows the function uses the shared libraries and overrides normal sleep command

1.3 An experiment to discover why

- We put myenv.c execve command in myprog.c in order to see the environment variables that it contains

1. For condition 1 (seed user and myprog.c is regular program)



- Here we see that since myprog.c is a non-root program and we are a normal user, the LD_PRELOAD was used
- Both RUID and EUID is seed

2. For condition 2 (myprog is set-uid program, user is seed)

```
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ sudo chown root myprog.out
seed@instance-20250224-035723:~/Labsetup$ sudo chmod 4755 myprog.out
seed@instance-20250224-035723:~/Labsetup$ env | grep LD_PRELOAD
LD_PRELOAD=./libmylib.so.1.0.1
seed@instance-20250224-035723:~/Labsetup$ ./myprog.out
SHELL=/bin/bash
SUDO_GID=1002
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=jjdeocampo20
PWD=/home/seed/Labsetup
LOGNAME=seed
HOME=/home/seed
LANG=C.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:*.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:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=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;3
1:*.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:*.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:*.a
ac=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:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1001
MAIL=/var/mail/seed
OLDPWD=/home/seed
_=./myprog.out
seed@instance-20250224-035723:~/Labsetup$ env | grep LD_PRELOAD
LD_PRELOAD=./libmylib.so.1.0.1
```

(changing the program to root and running it as seed)

- Here, we see that LD_PRELOAD is a env var in seed (RUID), however, when we run the program with root permission and ownership (EUID), the program slept and LD_PRELOAD is not an env var
- This shows that LD_PRELOAD was not inherited by the child process (EUID)

3. Condition 3 (switch to root user and run a set-uid program)

```
seed@instance-20250224-035723:~/Labsetup$ sudo su
root@instance-20250224-035723:/home/seed/Labsetup# env | grep LD_PRELOAD
root@instance-20250224-035723:/home/seed/Labsetup# export LD_PRELOAD=./libmylib.so.1.0.1
root@instance-20250224-035723:/home/seed/Labsetup# ./myprog.out
I am not sleeping!
SHELL=/bin/bash
SUDO_GID=1003
SUDO_COMMAND=/usr/bin/su
SUDO_USER=seed
PWD=/home/seed/Labsetup
LOGNAME=root
LD_PRELOAD=./libmylib.so.1.0.1
HOME=/root
LANG=C.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:o
=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:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=
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;
1:*.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;3
:*.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:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;3
:*.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:*.
ac=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:*.og
=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=root
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1002
MAIL=/var/mail/root
_=./myprog.out
root@instance-20250224-035723:/home/seed/Labsetup#
```

(change user to root and run set-uid root program)

- Here we see that when we export LD_PRELOAD as the root user, it is used and is an env variable
- RUID and EUID are both root

4. Condition 4 (switch to other user and myprog as a set-uid program)

```
jjdeocampo20@instance-20250224-035723:/home/seed/Labsetup$ ./myprog.out
I am not sleeping!
SHELL=/bin/bash
SSH_AUTH_SOCK=/tmp/ssh-pZAtG2MvTQ/agent.52792
PWD=/home/seed/Labsetup
LOGNAME=jjdeocampo20
XDG_SESSION_TYPE=tty
MOTD_SHOWN=pam
LD_PRELOAD=./libmylib.so.1.0.1
HOME=/home/jjdeocampo20
LANG=C.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:*.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:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=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;3
1:*.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:*.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:*.a
ac=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:
SSH_CONNECTION=35.235.244.34 40519 10.128.0.3 22
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=jjdeocampo20
SHLVL=1
XDG_SESSION_ID=65
XDG_RUNTIME_DIR=/run/user/1001
SSH_CLIENT=35.235.244.34 40519 22
XDG_DATA_DIRS=/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
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1001/bus
SSH_TTY=/dev/pts/1
OLDPWD=/home/seed
_=./myprog.out
jjdeocampo20@instance-20250224-035723:/home/seed/Labsetup$
```

(switch to jjdeocampo20 and made myprog a set-uid jjdeocampo20 program)

- Here we see that LD_PRELOAD is used because we exported it and it is non-root account

Task 8: Invoking External Programs Using system() versus execve()

1.1 Compromising integrity of the system in catall.c

System(): dangerous in Set-UID programs because it invokes a shell (/bin/sh -c) to execute the command, allowing command injection attacks.

- Creating root owned file as seed so we have no permissions

```
seed@instance-20250224-035723:~/Labsetup$ sudo touch /etc/test
seed@instance-20250224-035723:~/Labsetup$ ls -l /etc/test
-rw-r--r-- 1 root root 0 Feb 26 04:44 /etc/test
seed@instance-20250224-035723:~/Labsetup$ rm /etc/test
rm: remove write-protected regular empty file '/etc/test'? yes
rm: cannot remove '/etc/test': Permission denied
seed@instance-20250224-035723:~/Labsetup$
```

(could not remove file)

```
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ ./catall.out "/etc/test;/bin/sh"
# pwd
/home/seed/Labsetup
# ls -l /etc/test
-rw-r--r-- 1 root root 0 Feb 26 04:44 /etc/test
# rm /etc/test
# ls -l /etc/test
ls: cannot access '/etc/test': No such file or directory
#
```

- We can inject a shell command with a semicolon when we run catall.out
- This gives us the root shell where we can remove the root file /etc/test

1.2 Using exceve() instead of system()

```
seed@instance-20250224-035723:~/Labsetup$ vi catall.c
seed@instance-20250224-035723:~/Labsetup$ gcc catall.c -o catall.out
seed@instance-20250224-035723:~/Labsetup$ ls -l catall.out
-rwxrwxr-x 1 seed seed 16928 Feb 26 05:43 catall.out
seed@instance-20250224-035723:~/Labsetup$ sudo chown root catall.out
seed@instance-20250224-035723:~/Labsetup$ sudo chmod 4755 catall.out
seed@instance-20250224-035723:~/Labsetup$ sudo touch /etc/test
seed@instance-20250224-035723:~/Labsetup$
seed@instance-20250224-035723:~/Labsetup$ ./catall.out "/etc/test;/bin/sh"
/bin/cat: '/etc/test;/bin/sh': No such file or directory
seed@instance-20250224-035723:~/Labsetup$
```

- The same attack doesn't work against execve() because it doesn't invoke a shell

Task 9: Capability Leaking

1.1 In the file cap_leak.c ….

```
seed@instance-20250224-035723:~/Labsetup$ ./cap_leak.out
fd is 3
$ ds
$ whoami
seed
```

- We are trying to write to /etc/zzz/ but this is owned by root.

- When we revoke privileges, the RUID is seed and the EUID is root, and EUID calls set-uid to set to RUID which is seed (downgrading), it then executes /bin/sh without closing the file descriptor.
- Here we see that there is a capability leak in the file, so when we run it,

```
$ echo ccccc >& 3
$ exit
seed@instance-20250224-035723:~/Labsetup$ cat /etc/zzz
ccccc
seed@instance-20250224-035723:~/Labsetup$
```

- We can see that this allows us to modify files with root ownership as seed