

# Environment Variable and Set-UID Program Lab

## Task 1: Manipulating Environment Variables

### 1. Use **printenv** or **env** command to print out the environment variables

#### 1.1. **printenv** command to view ALL environment variables

```
[03/10/25]seed@VM:~/.../Labsetup$ printenv
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2166,unix/VM:/tmp/.ICE-unix/2166
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=2146
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Downloads/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
XAUTORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
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:*.lзма=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:*.tztst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.taz=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:*.sogv=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/651db957_4bc2_4e3c_bd66_621e8820939f
INVOCATION_ID=057279b25c534cce9c1caabe49534d2c
MANAGERPID=2021
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=:1.111
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:35520
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share:/usr/share:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
_=usr/bin/printenv
OLDPWD=/home/seed/Downloads
[03/10/25]seed@VM:~/.../Labsetup$ printenv PWD
/home/seed/Downloads/Labsetup
[03/10/25]seed@VM:~/.../Labsetup$ env
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2166,unix/VM:/tmp/.ICE-unix/2166
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=2146
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Downloads/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
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:*.tztz=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:*.s
vgz=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/651db957_4bc2_4e3c_bd66_621e8820939f
INVOCATION_ID=057279b25c534cce9c1caabe49534d2c
MANAGERPID=2021
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=:1.111
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:35520
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share:/var/lib/snapd/desktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
_/usr/bin/env
OLDPWD=/home/seed/Downloads

```

## 1.2. **env** command to check particular environment variable

```

[03/10/25] seed@VM:~/.../Labsetup$ env | grep PWD
PWD=/home/seed/Downloads/Labsetup
OLDPWD=/home/seed/Downloads

```

## 2. Use export and unset to set or unset environment variables

### 2.1. Use **export** to set an environment variable

Check if it was set correctly: print out a value of the environment variable named my\_var

```

[03/10/25] seed@VM:~/.../Labsetup$ export my_var="Hello, Lab2"
[03/10/25] seed@VM:~/.../Labsetup$ printenv my_var
Hello, Lab2

```

## 2.2. Use **unset** to unset an environment variable

Check if it was removed: the value of the environment variable named `my_var` that disappeared.

```
[03/10/25] seed@VM: ~/.../Labsetup$ unset my_var  
[03/10/25] seed@VM: ~/.../Labsetup$ printenv my_var  
[03/10/25] seed@VM: ~/.../Labsetup$ █
```

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

Step 1: compile and run myprintenv.c

```
[03/10/25]seed@VM:~/.../Labsetup$ /bin/ls
cap_leak.c  catall.c  myenv.c  myprintenv.c
[03/10/25]seed@VM:~/.../Labsetup$ gcc myprintenv.c
[03/10/25]seed@VM:~/.../Labsetup$ /bin/ls
a.out  cap_leak.c  catall.c  myenv.c  myprintenv.c
[03/12/25]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);
    }
}
```

```
seed@VM: ~/.../Labsetup
[03/12/25]seed@VM:~/.../Labsetup$ gcc myprintenv.c
[03/12/25]seed@VM:~/.../Labsetup$ a.out > out_child.txt
[03/12/25]seed@VM:~/.../Labsetup$ cat out_child.txt
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2055,unix/VM:/tmp/.ICE-unix/2055
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=2033
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Downloads/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
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: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:*.lzh=01;31:*.lzna=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:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tztst=01;31:*.bz2=0
1;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:*.wlm=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=0
1;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;3
5:*.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:*.flv=01;35:*.flv=0
1;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:*.n
4a=00;36:*.m4a=00;36:*.mld=00;36:*.nka=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=0
0;36:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/445c35cd_70f0_4799_b914_1042037cc10e
INVOCATION_ID=c1f74b6f3e6e46b588217a0f2bafd2e4
MANAGERPID=1904
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=:1.80
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37631
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/Downloads
_=./a.out
```

Step 2: Now comment out the `printenv()` statement in the child process case (Line ①), and uncomment the `printenv()` statement in the parent process case (Line `). Compile and run the code again

```
seed@VM: ~/.../Labsetup
[03/12/25]seed@VM:~/.../Labsetup$ vi myprintenv.c
[03/12/25]seed@VM:~/.../Labsetup$ gcc myprintenv.c
[03/12/25]seed@VM:~/.../Labsetup$ a.out > out_parent.txt
[03/12/25]seed@VM:~/.../Labsetup$ cat out_parent.txt
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2055,unix/VM:/tmp/.ICE-unix/2055
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=2033
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Downloads/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
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:*.lzn=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.diz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzt=01;31:*.bz2=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:*.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:*.wlm=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.njpg=01;35:*.mjpg=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:*.avl=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:*.m4d=00;36:*.m4p=00;36:*.m4v=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/445c35cd_70f0_4799_b914_1042037cc10e
INVOCATION_ID=c1f74b6f3e6e46b588217a0f2bafd2e4
MANAGERPID=1904
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=:1.80
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37631
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/Downloads
_=./a.out
```

Step 3: Compare the difference of these two files using the diff command

```
[03/12/25]seed@VM:~/.../Labsetup$ diff out_child.txt out_parent.txt
[03/12/25]seed@VM:~/.../Labsetup$
```

CONCLUSION:

the files out\_child.txt and out\_parent.txt are identical, will not output anything. This confirms that the child process inherits the environment variables from the parent process when using fork().

- Both the parent and child processes printed the same set of environment variables.
- This means that environment variables are copied to the child process when fork() is executed.

- Any changes to the environment variables after the fork will not affect the other process (if the child modifies an environment variable, it won't impact the parent, and vice versa).

### Task 3: Environment Variable and `execve()`

Step 1: compile and run `myenv.c`

Since `execve()` is called with a NULL third argument, the new program does not inherit any environment variables. As a result, the output is **empty**, meaning no environment variables are available in the new process.

```
[03/13/25]seed@VM:~/.../Labsetup$ gcc myenv.c
[03/13/25]seed@VM:~/.../Labsetup$ a.out > task3_null.txt
[03/13/25]seed@VM:~/.../Labsetup$ cat task3_null.txt
[03/13/25]seed@VM:~/.../Labsetup$ █
```

Step 2: Change the invocation of `execve()` in Line ①



```
seed@VM: ~/.../Labsetup

#include <unistd.h>

extern char **environ;

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

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

    // execve("/usr/bin/env", argv, NULL);
    execve("/usr/bin/env" , argv, environ);
    return 0 ;
}

[03/13/25]seed@VM:~/.../Labsetup$ vi myenv.c
[03/13/25]seed@VM:~/.../Labsetup$ gcc myenv.c
[03/13/25]seed@VM:~/.../Labsetup$ cat out.c
cat: out.c: No such file or directory
[03/13/25]seed@VM:~/.../Labsetup$ a.out > task3_envron.txt
[03/13/25]seed@VM:~/.../Labsetup$ cat task3_envron.txt
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2055,unix/VM:/tmp/.ICE-unix/2055
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=2033
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Downloads/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
LANG=en_US.UTF-8
LS_COLORS=rs=0;di=01;34;ln=01;36;nh=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;*.lza=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;*.tzt=01;31;*.bz2=0
1;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=0
1;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;3
5;*.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;*.ogp=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=0
1;35;*.gl=01;35;*.dl=01;35;*.xcf=01;35;*.xwd=01;35;*.yuv=01;35;*.cgm=01;35;*.enf=01;35;*.ogv=01;35;*.ogx=01;35;*.aac=00;36;*.au=00;36;*.flac=00;36;*.m
4a=00;36;*.m4p=00;36;*.m4b=00;36;*.m4r=00;36;*.m4v=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=0
0;36;
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/445c35cd_70f0_4799_b914_1042037cc10e
INVOCATION_ID=c1f74b6f3e6e46b588217a0f2baf2e4
MANAGERPID=1904
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=:1.80
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:37631
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/Downloads
_=./a.out
```



Describe:

We pass `environ`, which is a global variable holding the current environment variables.

The new program `/usr/bin/env` now prints all the environment variables that existed in the calling process.

This shows that the new program inherits the environment variables when they are explicitly passed.

Step 3: Conclusion about how the new program gets its environment variables

- If `NULL` is passed as the third argument to `execve()`, the new program starts with an empty environment.
- If the current process's `environ` is passed, the new program inherits the environment variables of the calling process.

⇒ This confirms that `execve()` does not automatically inherit environment variables; they must be explicitly passed as an argument.

## Task 4: Environment Variable and system()

```
seed@VM: ~/.../Labsetup

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

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

[03/13/25]seed@VM:~/.../Labsetup$ vi mysystem.c
[03/13/25]seed@VM:~/.../Labsetup$ gcc mysystem.c
[03/13/25]seed@VM:~/.../Labsetup$ a.out > task4_system.txt
[03/13/25]seed@VM:~/.../Labsetup$ cat task4_system.txt
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SSH_AGENT_PID=2033
XDG_SESSION_TYPE=x11
SHLVL=1
HOME=/home/seed
OLDPWD=/home/seed/Downloads
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gall:atk-bridge
MANAGERPID=1904
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
COLORTERM=truecolor
LOGNAME=seed
JOURNAL_STREAM=8:37631
_=/a.out
XDG_SESSION_CLASS=user
USERNAME=seed
TERM=xterm-256color
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
WINDOWPATH=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2055,unix/VM:/tmp/.ICE-unix/2055
INVOCATION_ID=c1f74b6f3e6e46b588217a0f2bafd2e4
XDG_MENU_PREFIX=gnome-
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/445c35cd_70f0_4799_b914_1042037cc10e
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
LANG=en_US.UTF-8
XDG_CURRENT_DESKTOP=ubuntu:GNOME
XMODIFIERS=@im=ibus
XDG_SESSION_DESKTOP=ubuntu
XAUTHORITY=/run/user/1000/gdm/Xauthority
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:*.zlp=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:*.tzt=01;31:*.bz2=0
1;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.t2=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:*.wlm=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.njpg=0
1;35:*.njpeg=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;3
5:*.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=0
1;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:*.m
4a=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=0
0;36:
GNOME_TERMINAL_SERVICE=:1.80
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
SHELL=/bin/bash
QT_ACCESSIBILITY=1
GDMSESSION=ubuntu
LESSCLOSE=/usr/bin/lesspipe %s %s
GJS_DEBUG_OUTPUT=stderr
QT_IM_MODULE=ibus
PWD=/home/seed/Downloads/Labsetup
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_DATA_DIRS=/usr/share/xdg/xdg-ubuntu:/usr/local/share:/usr/share:/var/lib/snapd/desktop
VTE_VERSION=6003
[03/13/25]seed@VM:~/.../Labsetup$
```

Since `system()` passes the calling process's environment variables to `/bin/sh`, `/usr/bin/env` will print all environment variables. `system()` does inherit the environment variables from the calling process because it indirectly uses `execve()` via `/bin/sh`.

## Task 5: Environment Variable and Set-UID Programs

Step 1: Write the following program that can print out all the environment variables in the current process.

```
seed@VM: ~/.../Labsetup

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

extern char **environ;
int main()
{
    int i = 0;
    while (environ[i] != NULL) {
        printf("%s\n", environ[i]);
        i++;
    }
}

[03/13/25]seed@VM:~/.../Labsetup$ vi foo.c
[03/13/25]seed@VM:~/.../Labsetup$ gcc -o foo foo.c
```

Step 2: Compile the above program, change its ownership to root, and make it a Set-UID program.

```

[03/13/25]seed@VM:~/.../Labsetup$ sudo chown root foo
[03/13/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 foo
[03/13/25]seed@VM:~/.../Labsetup$ ./foo
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/4890,unix/VM:/tmp/.ICE-unix/4890
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=4870
GTK_MODULES=gall:atk-bridge
PWD=/home/seed/Downloads/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
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:ml=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:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=0
1;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:*.wlm=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.njpg=0
1;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;3
5:*.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=0
1;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:*.m
4a=00;36:*.m4=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=0
0;36:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/046deddf_1a9d_4b50_86d3_9ef628a301a8
INVOCATION_ID=3da48f4762e14e6890e0cf7ad4743afa
MANAGERPID=4743
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=:1.73
DISPLAY=:1
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:71974
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
_=./foo

```

Step 3: Compile the above program, change its ownership to root, and make it a Set-UID program.

```
[03/13/25]seed@VM:~/.../Labsetup$ export PATH="/tmp:/usr/bin:/bin"
[03/13/25]seed@VM:~/.../Labsetup$ export LD_LIBRARY_PATH="/tmp"
[03/13/25]seed@VM:~/.../Labsetup$ export MY_VAR="HelloWorld"
[03/13/25]seed@VM:~/.../Labsetup$ ./foo
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/4890,unix/VM:/tmp/.ICE-unix/4890
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=4870
GTK_MODULES=gall:atk-bridge
PWD=/home/seed/Downloads/Labsetup
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
XAUTHORITY=/run/user/1000/gdm/Xauthority
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
LANG=en_US.UTF-8
MY_VAR=HelloWorld
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:*.lzh=01;31:*.lzn=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:*.lzo=01;31:*.x=01;31:*.zst=01;31:*.tzt=01;31:*.bz2=0
1;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=0
1;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;3
5:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.nov=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=0
1;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:*.m
4a=00;36:*.m4d=00;36:*.m4l=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=0
0;36:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/046deddf_1a9d_4b50_86d3_9ef628a301a8
INVOCATION_ID=3da48f4762e14e6890e0cf7ad4743afa
MANAGERPID=4743
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=:1.73
DISPLAY=:1
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=8:71974
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/tmp:/usr/bin:/bin
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed
_=./foo
```

MY\_VAR appears in the output → Custom environment variables (like MY\_VAR) are inherited.

PATH appears in the output → The PATH variable is inherited.

LD\_LIBRARY\_PATH is missing → It is not inherited for security reasons.

Conclusion:

- **Set-UID programs do not inherit all environment variables**—only non-sensitive ones.
- **Security-sensitive variables (LD\_LIBRARY\_PATH, LD\_PRELOAD) are removed** to prevent privilege escalation attacks.

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

- Compile the above program, change its owner to root, and make it a Set-UID program.

```
seed@VM: ~/.../Labsetup

#include <stdlib.h>
int main()
{
    system("ls");
    return 0;
}

[03/13/25]seed@VM:~/.../Labsetup$ vi task6_PATH.c
[03/13/25]seed@VM:~/.../Labsetup$ gcc -o task6_PATH task6_PATH.c

[03/13/25]seed@VM:~/.../Labsetup$ sudo chown root task6_PATH
[03/13/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 task6_PATH
[03/13/25]seed@VM:~/.../Labsetup$ ./task6_PATH
cap_leak.c  foo  myenv.c  mysystem.c  out_parent.txt  task3_null.txt  task5_set-UID.c  task6_PATH.c
catall.c    foo.c  myprintenv.c  out_child.txt  task3_environtxt  task4_system.txt  task6_PATH
[03/13/25]seed@VM:~/.../Labsetup$ bin/ls
bash: bin/ls: No such file or directory
[03/13/25]seed@VM:~/.../Labsetup$ /bin/ls
cap_leak.c  foo  myenv.c  mysystem.c  out_parent.txt  task3_null.txt  task5_set-UID.c  task6_PATH.c
catall.c    foo.c  myprintenv.c  out_child.txt  task3_environtxt  task4_system.txt  task6_PATH
```

- Get this Set-UID program to run your own malicious code, instead of /bin/ls. Your malicious code run with the root privilege.

```
[03/13/25]seed@VM:~/.../Labsetup$ echo '#!/bin/bash' > /home/seed/ls
[03/13/25]seed@VM:~/.../Labsetup$ echo 'echo "Malicious code executed!"' >> /home/seed/ls
[03/13/25]seed@VM:~/.../Labsetup$ chmod +x /home/seed/ls
[03/13/25]seed@VM:~/.../Labsetup$ export PATH=/home/seed:$PATH
[03/13/25]seed@VM:~/.../Labsetup$ ./task6_PATH
Malicious code executed!
[03/13/25]seed@VM:~/.../Labsetup$ sudo ln -sf /bin/zsh /bin/sh
[03/13/25]seed@VM:~/.../Labsetup$ ./task6_PATH
Malicious code executed!
```

- Describe:
  - This attack works if the vulnerable program calls system("ls") without using an absolute path.
  - By manipulating PATH, we can trick the program into executing our malicious script instead of /bin/ls.
  - Ubuntu prevents this attack using dash, but replacing /bin/sh with zsh bypasses the defense.
  - To prevent this vulnerability(Secure way), always use absolute paths in Set-UID programs:  
system("/bin/ls");
  - This puts /home/seed at the beginning of the PATH. When the vulnerable program calls system("ls"), it will execute /home/seed/ls instead of /bin/ls.

⇒ Always use absolute paths when calling external programs in privileged processes to prevent PATH hijacking.

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

Step 1: how these environment variables influence the behavior of dynamic loader/linker when running a normal program.

```
#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");
}

[03/13/25]seed@VM:~/.../Labsetup$ vi mylib.c
[03/13/25]seed@VM:~/.../Labsetup$ gcc -fPIC -g -c mylib.c
[03/13/25]seed@VM:~/.../Labsetup$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[03/13/25]seed@VM:~/.../Labsetup$ export LD_PRELOAD=./libmylib.so.1.0.1
[03/13/25]seed@VM:~/.../Labsetup$ vi myprog.c

#include <unistd.h>
int main()
{
    sleep(1);
    return 0;
}

[03/13/25]seed@VM:~/.../Labsetup$ gcc -o myprog myprog.c
```

Step 2: run myprog under the following conditions

- Case 1: Make myprog a regular program, and run it as a normal user

```
[03/13/25]seed@VM:~/.../Labsetup$ ./myprog
I am not sleeping!
```

LD\_PRELOAD successfully overrides sleep(), so the program prints our message instead of actually sleeping.

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

```
[03/13/25]seed@VM:~/.../Labsetup$ sudo chown root myprog
[03/13/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[03/13/25]seed@VM:~/.../Labsetup$ ./myprog
[03/13/25]seed@VM:~/.../Labsetup$ █
```

- LD\_PRELOAD is ignored for Set-UID programs.
  - The dynamic linker (ld.so) detects the Set-UID execution and discards unsafe environment variables like LD\_PRELOAD.
- Case 3: Make myprog a Set-UID **root program**, export the LD PRELOAD environment variable again in the **root account** and run it.



```
[03/13/25]seed@VM:~/.../Labsetup$ sudo -s
root@VM:/home/seed/Downloads/Labsetup# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Downloads/Labsetup# ./myprog
I am not sleeping!
root@VM:/home/seed/Downloads/Labsetup# █
```

- Switch to root shell
- Here, the **root user sets LD\_PRELOAD**, so it is respected.
- Since **root runs the program**, no privilege escalation occurs.
- The dynamic linker **trusts** environment variables from root.

- Case 4: Make myprog a Set-UID **user1 program** (i.e., the owner is user1, which is another user account), export the LD PRELOAD environment variable again in a **different user's account (not-root user)** and run it.

```
[03/13/25]seed@VM:~/.../Labsetup$ sudo chown user1 myprog
[03/13/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[03/13/25]seed@VM:~/.../Labsetup$ su user2
Password:
$ export LD_PRELOAD=./libmylob.so.1.0.1
$ ./myprog
$
```

- LD\_PRELOAD is ignored because myprog runs as user1 (Set-UID), but was executed by user2.

Step 3: different behaviors in the scenarios described above. What causes the difference. Environment variables play a role here.

Condition	LD_PRELOAD Works?	Reason
Normal user runs a normal program	Yes	No privilege change, environment variables inherited
Set-UID root program run by normal user	No	Dynamic linker ignores LD_PRELOAD for security
Set-UID root program run by root (LD_PRELOAD set by root)	Yes	Root has full control over execution
Set-UID user1 program run by user2 (LD_PRELOAD set by user2)	No	Dynamic linker discards LD_PRELOAD to prevent privilege escalation

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

Step 1: Compile the above program, make it a root-owned Set-UID program.

```
[03/16/25]seed@VM:~/.../Labsetup$ gcc -o catall catall.c
[03/16/25]seed@VM:~/.../Labsetup$ ./catall
Please type a file name.
[03/16/25]seed@VM:~/.../Labsetup$ sudo chown root catall
[03/16/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 catall
[03/16/25]seed@VM:~/.../Labsetup$ /bin/ls -l catall
-rwsr-xr-x 1 root seed 16928 Mar 16 12:11 catall
```

Question:

- If you were Bob, can you compromise the integrity of the system?
- For example, can you remove a file that is not writable to you?

Yes, Bob can remove or modify files, violating the system's integrity.

```
[03/16/25]seed@VM:~/.../Labsetup$ ./catall "catall.txt;rm catall.txt"
Please type a file name.
[03/17/25]seed@VM:~/.../Labsetup$ ./catall "catall.txt"
/bin/cat: catall.txt: No such file or directory
[03/17/25]seed@VM:~/.../Labsetup$
```

Step 2: Comment out the system(command) statement, and uncomment the execve() statement; the program will use execve() to invoke the command. Compile the program, and make it a root-owned Set-UID.

---

```
[03/17/25]seed@VM:~/.../Labsetup$ vi catall.c
```



seed@VM: ~/.../Labsetup

```
#include <string.h>

int main(int argc, char *argv[])
{
    char *v[3];
    char *command;

    if(argc < 2) {
        printf("Please type a file name.\n");
        return 1;
    }

    v[0] = "/bin/cat"; v[1] = argv[1]; v[2] = NULL;

    command = malloc(strlen(v[0]) + strlen(v[1]) + 2);
    sprintf(command, "%s %s", v[0], v[1]);

    // Use only one of the followings.
    // system(command);
    execve(v[0], v, NULL);

    return 0 ;
}
```

```

[03/17/25]seed@VM:~/../Labsetup$ gcc -o catall2 catall.c
[03/17/25]seed@VM:~/../Labsetup$ sudo chown root catall2
[03/17/25]seed@VM:~/../Labsetup$ sudo chmod 4755 catall2
[03/17/25]seed@VM:~/../Labsetup$ /bin/ls -l catall2
-rwsr-xr-x 1 root seed 16928 Mar 17 00:13 catall2
[03/17/25]seed@VM:~/../Labsetup$ ./catall2
Please type a file name.
[03/17/25]seed@VM:~/../Labsetup$ ./catall2 /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:::
list*:18474:0:99999:7:::
irc*:18474:0:99999:7:::
gnats*:18474:0:99999:7:::
nobody*:18474:0:99999:7:::
systemd-network*:18474:0:99999:7:::
systemd-resolve*:18474:0:99999:7:::
systemd-timesync*:18474:0:99999:7:::
messagebus*:18474:0:99999:7:::
syslog*:18474:0:99999:7:::
_apt*:18474:0:99999:7:::
tss*:18474:0:99999:7:::
uidd*:18474:0:99999:7:::
tcpdump*:18474:0:99999:7:::
avahi-autoipd*:18474:0:99999:7:::
usbmux*:18474:0:99999:7:::
rtkit*: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:::

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:$6$uy8095gm97WwBuUA$7A73jdze.1HHvT2o64GHRrDQxL04YR5GEY0RD7jSt.7kQPnonWxM05C6hg/JNxJbwfQ9d2064Ve00IFSoS5btu0:20138:0:99999:7:::
systemd-coredump:!:18590:0:99999:7:::
telnetd*:18590:0:99999:7:::
ftp*:18590:0:99999:7:::
sshd*:18590:0:99999:7:::
user1:$6$6YLzR8PIr92KMtPi$adKAUMd0NcWGxQ4N64Yxj.t/Wd.XYZVIOcnddFRN523E0.DQuIAJ22hsqatAsFzJTYlR0IoARv6hjEGwhIcn41:20160:0:99999:7:::
user2:$6$ENiqqU3/u9f586EU$W5xwYzXrXL5sEYtg4Ep18hJkKrx21t8LnZFJmQgnsk1bZeIpI4C/A7rabw1q5U3vAbIKJlNvUbZC40DCUR00.:20160:0:99999:7:::
[03/17/25]seed@VM:~/../Labsetup$ vi catall.txt

```

```

seed@VM: ~/.../Labsetup
Please type a file name.
~
~
~
~
~
~
[03/17/25]seed@VM:~/.../Labsetup$ ./catall2 catall.txt
Please type a file name.
[03/17/25]seed@VM:~/.../Labsetup$ ./catll2 "catall.txt;rm catall.txt"
bash: ./catll2: No such file or directory
[03/17/25]seed@VM:~/.../Labsetup$ ./catall2 "catall.txt;rm catall.txt"
/bin/cat: 'catall.txt;rm catall.txt': No such file or directory
[03/17/25]seed@VM:~/.../Labsetup$ ./catall2 catall.txt
Please type a file name.
[03/17/25]seed@VM:~/.../Labsetup$ █

```

- Do your attacks in Step 1 still work?  
The attack from Step 1 no longer works.
- Description:
  - + When the system function executes it doesn't execute the command directly it calls the shell instead and executes the command so if the program is a set uid program.
  - + The user will have temporary root privileges and can remove any file he wants with root privileges.
  - + Multiple commands can be passed together using quotation marks and the semicolon sign.
  - + System command calls the shell and the shell passes the string and handles quotation marks.
  - + Whereas execute function command replaces the program with the called program and passes the argument strings exactly as specified and doesn't interpret quotes so when we pass something.
  - + After the semicolon sign it is treated as a new command and root privileges would have been lost.
  - + So the rm command is executed using user privileges which is why it can't delete the file.

## Task 9: Capability Leaking

Compile the program, change its owner to root, and make it a Set-UID program. Run the program as a normal user.

```
[03/17/25]seed@VM:~/.../Labsetup$ gcc -o cap_leak cap_leak.c
```

```
root@VM: /etc

Task 9 Capability Leaks
~
~
~
~

[03/17/25]seed@VM:~/.../Labsetup$ sudo chown root cap_leak
[03/17/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 cap_leak
[03/17/25]seed@VM:~/.../Labsetup$ /bin/ls -l cap_leak
-rwsr-xr-x 1 root seed 17008 Mar 17 00:40 cap_leak
[03/17/25]seed@VM:~/.../Labsetup$ stat -c %a cap_leak
4755
[03/17/25]seed@VM:~/.../Labsetup$ sudo su
root@VM:/home/seed/Downloads/Labsetup# cd /etc/
root@VM:/etc# vi zzz
root@VM:/etc# cat zzz
Task 9 Capability Leaks
root@VM:/etc# /bin/ls -l zzz
-rw-r--r-- 1 root root 24 Mar 17 00:43 zzz
root@VM:/etc# exit
exit
[03/17/25]seed@VM:~/.../Labsetup$ ./cap_leak
fd is 3

$ cat /etc/zzz
Task 9 Capability Leaks
$ exit
[03/17/25]seed@VM:~/.../Labsetup$ █
```

- Can you exploit the capability leaking vulnerability in this program?  
Yes. I can exploit the capability leaking vulnerability in the cap\_leak program to write to /etc/zzz as a normal user.
  - + It starts with root privileges due to the Set-UID bit (chmod 4755 cap\_leak).
  - + It opens /etc/zzz with write access (O\_RDWR | O\_APPEND), obtaining a file descriptor (fd).
  - + It then drops root privileges using setuid(getuid());, but the file descriptor remains open.
  - + It spawns a new shell (execve("/bin/sh", ...)), and this shell inherits access to the open file descriptor.

- + Even though the shell is running as a normal user, it can still write to `/etc/zzz` via the leaked file descriptor.
- +