Babaiah Gandluru

R11899782

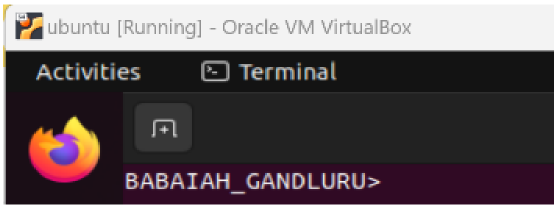
Introduction to Information and Computer Security

(CS-5340-001)

Environment Variable and Set-UID Program Lab

Assignment-1

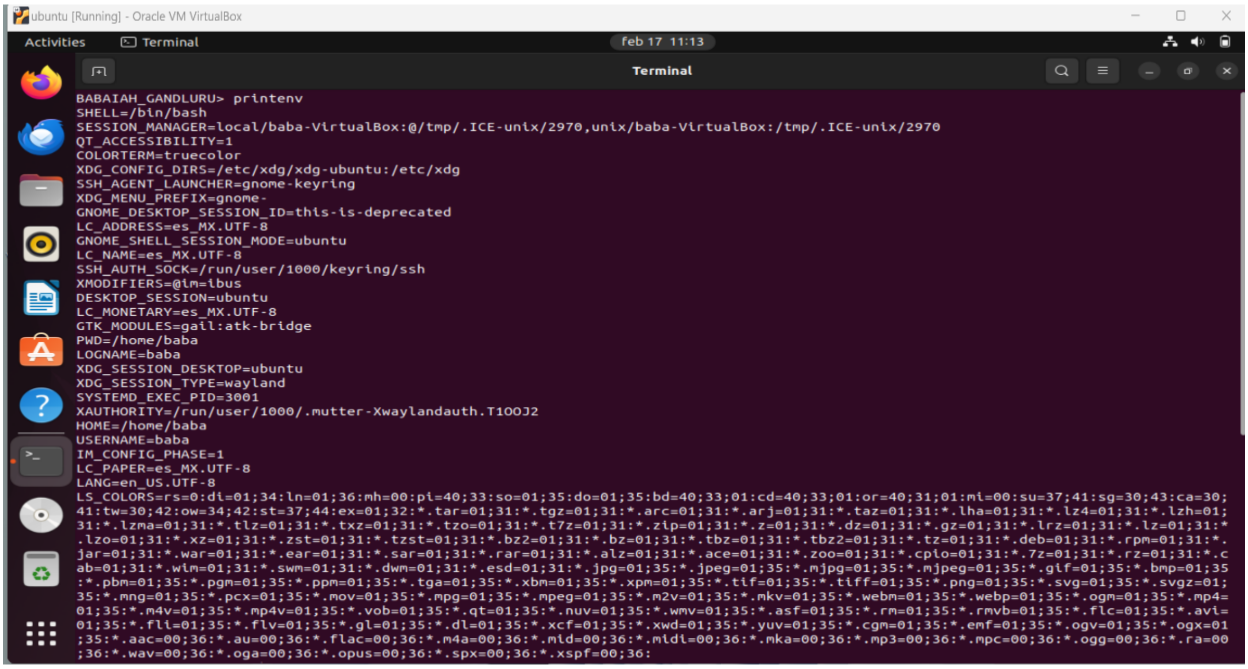
I executed all 9- tasks and explained them



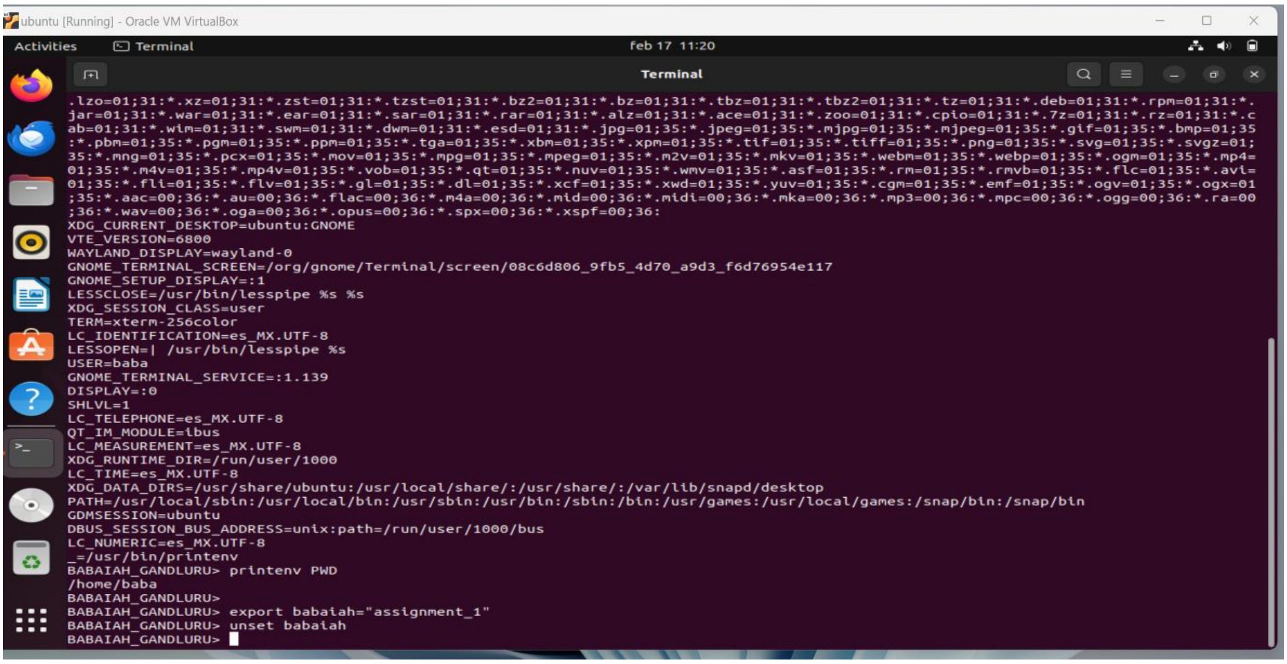
```
BABAIAH_GANDLURU>
```

Task-1

First I executed the command printenv to display the current environment variables in the terminal



```
BABAIAH_GANDLURU> printenv
SHELL=/bin/bash
SESSION_MANAGER=local/baba-VirtualBox:@/tmp/.ICE-unix/2970,unix/baba-VirtualBox:/tmp/.ICE-unix/2970
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
SSH_AGENT_LAUNCHER=gnome-keyring
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LC_ADDRESS=es_MX.UTF-8
GNOME_SHELL_SESSION_MODE=ubuntu
LC_NAME=es_MX.UTF-8
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
LC_MONETARY=es_MX.UTF-8
GTK_MODULES=gail:atk-bridge
PWD=/home/baba
LOGNAME=baba
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=3001
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.T1OOJ2
HOME=/home/baba
USERNAME=baba
IM_CONFIG_PHASE=1
LC_PAPER=es_MX.UTF-8
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:*.c
ab=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:*.webp=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:
```



```
.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:*.c
ab=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:*.webp=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=6800
WAYLAND_DISPLAY=wayland-0
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/08c6d806_9fb5_4d70_a9d3_f6d76954e117
GNOME_SETUP_DISPLAY=:1
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LC_IDENTIFICATION=es_MX.UTF-8
LESSOPEN=| /usr/bin/lesspipe %s
USER=baba
GNOME_TERMINAL_SERVICE=:1.139
DISPLAY=:0
SHLVL=1
LC_TELEPHONE=es_MX.UTF-8
QT_IM_MODULE=ibus
LC_MEASUREMENT=es_MX.UTF-8
XDG_RUNTIME_DIR=/run/user/1000
LC_TIME=es_MX.UTF-8
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:/snap/bin
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
LC_NUMERIC=es_MX.UTF-8
_=/usr/bin/printenv
BABAIAH_GANDLURU> printenv PWD
/home/baba
BABAIAH_GANDLURU>
BABAIAH_GANDLURU> export babaiah="assignment_1"
BABAIAH_GANDLURU> unset babaiah
BABAIAH_GANDLURU> █
```

Then I executed printenv PWD this command prints the value of the PWD variable in my virtual machine it is /home/baba

Then I executed commands like

export babaiah=”assignment_1”

unset babaiah

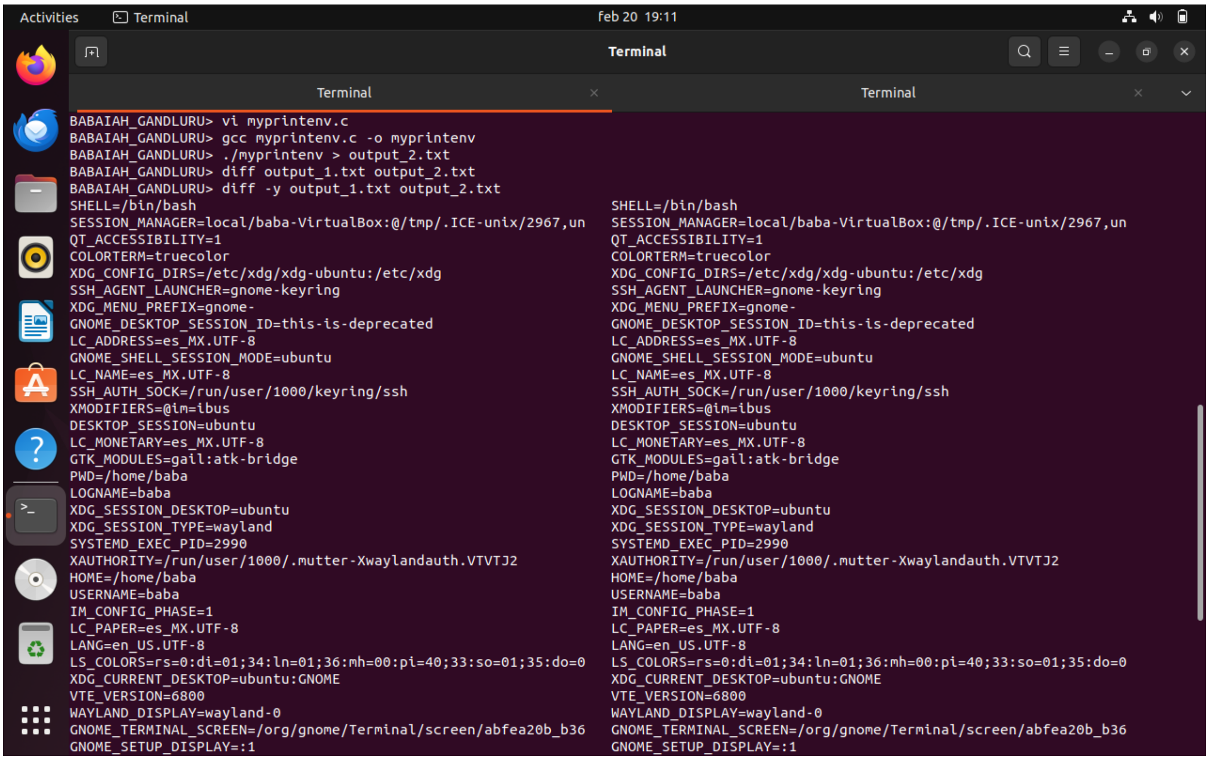
export is used to define a new environment variable (or) to update the value of an existing one.

unset is used to remove an environment variable from the current shell session.

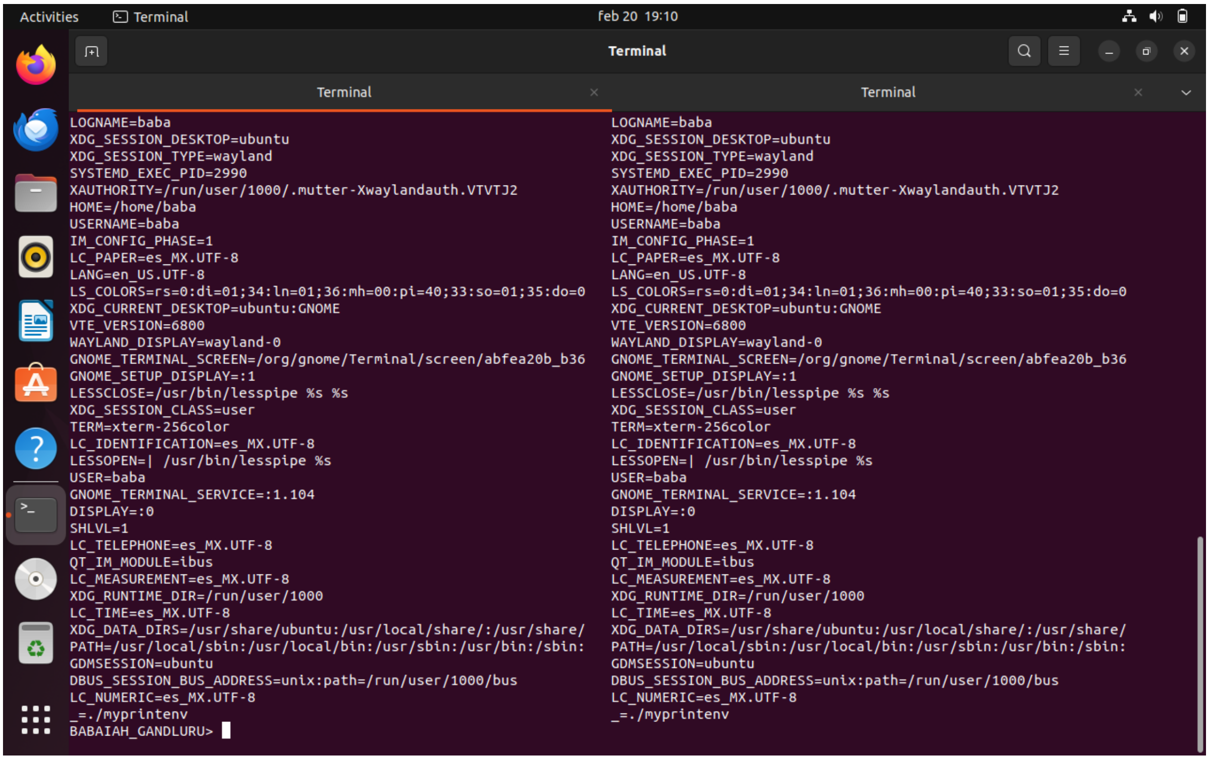
so i defined a new variable babaiah and assigned it value "assignment_1"

and removed it with unset command

Task-2



```
BABAIAH_GANDLURU> vi myprintenv.c
BABAIAH_GANDLURU> gcc myprintenv.c -o myprintenv
BABAIAH_GANDLURU> ./myprintenv > output_2.txt
BABAIAH_GANDLURU> diff output_1.txt output_2.txt
BABAIAH_GANDLURU> diff -y output_1.txt output_2.txt
SHELL=/bin/bash                                                 SHELL=/bin/bash
SESSION_MANAGER=local/baba-VirtualBox:@/tmp/.ICE-unix/2967,un   SESSION_MANAGER=local/baba-VirtualBox:@/tmp/.ICE-unix/2967,un
QT_ACCESSIBILITY=1                                              QT_ACCESSIBILITY=1
COLORTERM=truecolor                                             COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg                    XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
SSH_AGENT_LAUNCHER=gnome-keyring                                SSH_AGENT_LAUNCHER=gnome-keyring
XDG_MENU_PREFIX=gnome-                                          XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated                     GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LC_ADDRESS=es_MX.UTF-8                                          LC_ADDRESS=es_MX.UTF-8
GNOME_SHELL_SESSION_MODE=ubuntu                                 GNOME_SHELL_SESSION_MODE=ubuntu
LC_NAME=es_MX.UTF-8                                             LC_NAME=es_MX.UTF-8
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh                        SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus                                             XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu                                          DESKTOP_SESSION=ubuntu
LC_MONETARY=es_MX.UTF-8                                         LC_MONETARY=es_MX.UTF-8
GTK_MODULES=gail:atk-bridge                                     GTK_MODULES=gail:atk-bridge
PWD=/home/baba                                                  PWD=/home/baba
LOGNAME=baba                                                    LOGNAME=baba
XDG_SESSION_DESKTOP=ubuntu                                      XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland                                        XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=2990                                           SYSTEMD_EXEC_PID=2990
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.VTVTJ2           XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.VTVTJ2
HOME=/home/baba                                                 HOME=/home/baba
USERNAME=baba                                                   USERNAME=baba
IM_CONFIG_PHASE=1                                               IM_CONFIG_PHASE=1
LC_PAPER=es_MX.UTF-8                                            LC_PAPER=es_MX.UTF-8
LANG=en_US.UTF-8                                                LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=0   LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=0
XDG_CURRENT_DESKTOP=ubuntu:GNOME                                XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6800                                                VTE_VERSION=6800
WAYLAND_DISPLAY=wayland-0                                       WAYLAND_DISPLAY=wayland-0
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/abfea20b_b36   GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/abfea20b_b36
GNOME_SETUP_DISPLAY=:1                                          GNOME_SETUP_DISPLAY=:1
```



```
LOGNAME=baba                                                    LOGNAME=baba
XDG_SESSION_DESKTOP=ubuntu                                      XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland                                        XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=2990                                           SYSTEMD_EXEC_PID=2990
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.VTVTJ2           XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.VTVTJ2
HOME=/home/baba                                                 HOME=/home/baba
USERNAME=baba                                                   USERNAME=baba
IM_CONFIG_PHASE=1                                               IM_CONFIG_PHASE=1
LC_PAPER=es_MX.UTF-8                                            LC_PAPER=es_MX.UTF-8
LANG=en_US.UTF-8                                                LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=0   LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=0
XDG_CURRENT_DESKTOP=ubuntu:GNOME                                XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6800                                                VTE_VERSION=6800
WAYLAND_DISPLAY=wayland-0                                       WAYLAND_DISPLAY=wayland-0
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/abfea20b_b36   GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/abfea20b_b36
GNOME_SETUP_DISPLAY=:1                                          GNOME_SETUP_DISPLAY=:1
LESSCLOSE=/usr/bin/lesspipe %s %s                               LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user                                          XDG_SESSION_CLASS=user
TERM=xterm-256color                                             TERM=xterm-256color
LC_IDENTIFICATION=es_MX.UTF-8                                   LC_IDENTIFICATION=es_MX.UTF-8
LESSOPEN=| /usr/bin/lesspipe %s                                 LESSOPEN=| /usr/bin/lesspipe %s
USER=baba                                                       USER=baba
GNOME_TERMINAL_SERVICE=:1.104                                   GNOME_TERMINAL_SERVICE=:1.104
DISPLAY=:0                                                      DISPLAY=:0
SHLVL=1                                                         SHLVL=1
LC_TELEPHONE=es_MX.UTF-8                                        LC_TELEPHONE=es_MX.UTF-8
QT_IM_MODULE=ibus                                               QT_IM_MODULE=ibus
LC_MEASUREMENT=es_MX.UTF-8                                      LC_MEASUREMENT=es_MX.UTF-8
XDG_RUNTIME_DIR=/run/user/1000                                  XDG_RUNTIME_DIR=/run/user/1000
LC_TIME=es_MX.UTF-8                                             LC_TIME=es_MX.UTF-8
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/   XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:   PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:
GDMSESSION=ubuntu                                               GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus           DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
LC_NUMERIC=es_MX.UTF-8                                          LC_NUMERIC=es_MX.UTF-8
_=./myprintenv                                                  _=./myprintenv
BABAIAH_GANDLURU> 
```

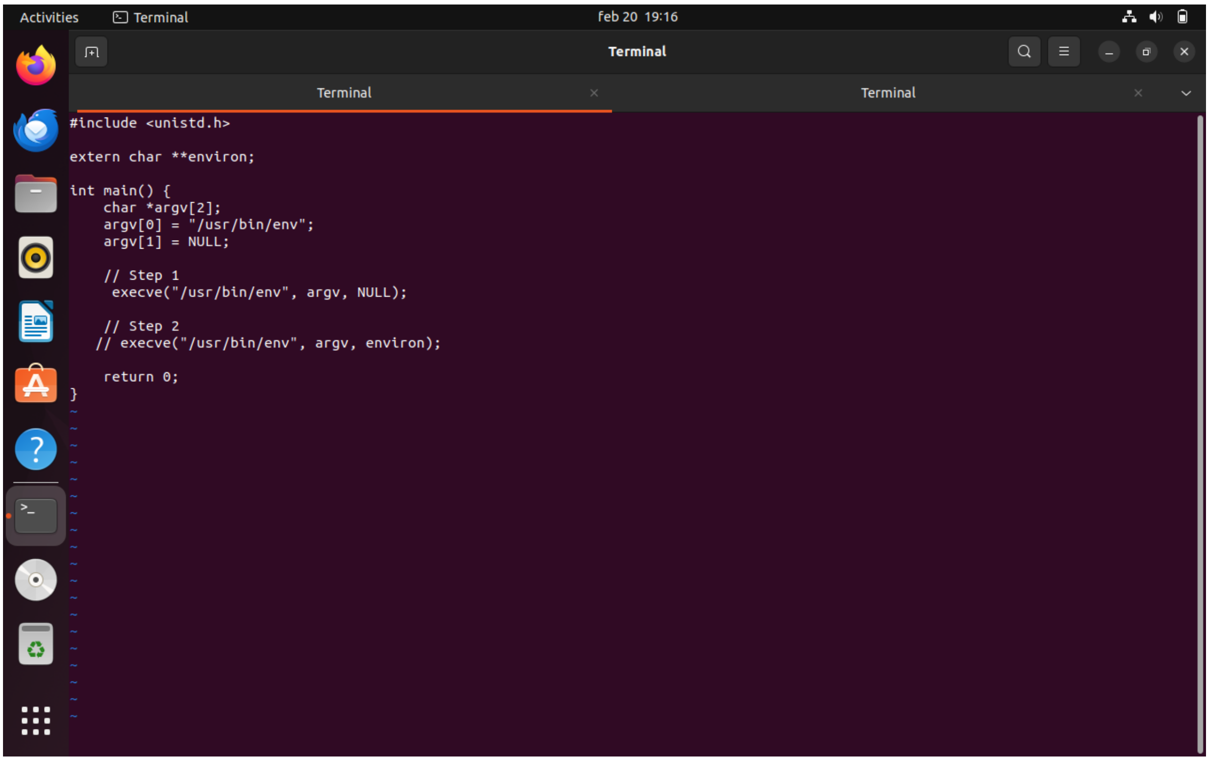
I executed both parent process and child process in output_1.txt file and output_2.txt file and then I executed diff command to see the differences in the outputs

I dont see any differences in the outputs both outputs are identical

So, In conclution

We can say that in systems like Unix, environment variables are inherited by child processes from their parent processes. This inheritance will allow child processes to access and utilize the same set of environment variables as their parent processes without explicitly passing them.

Task-3



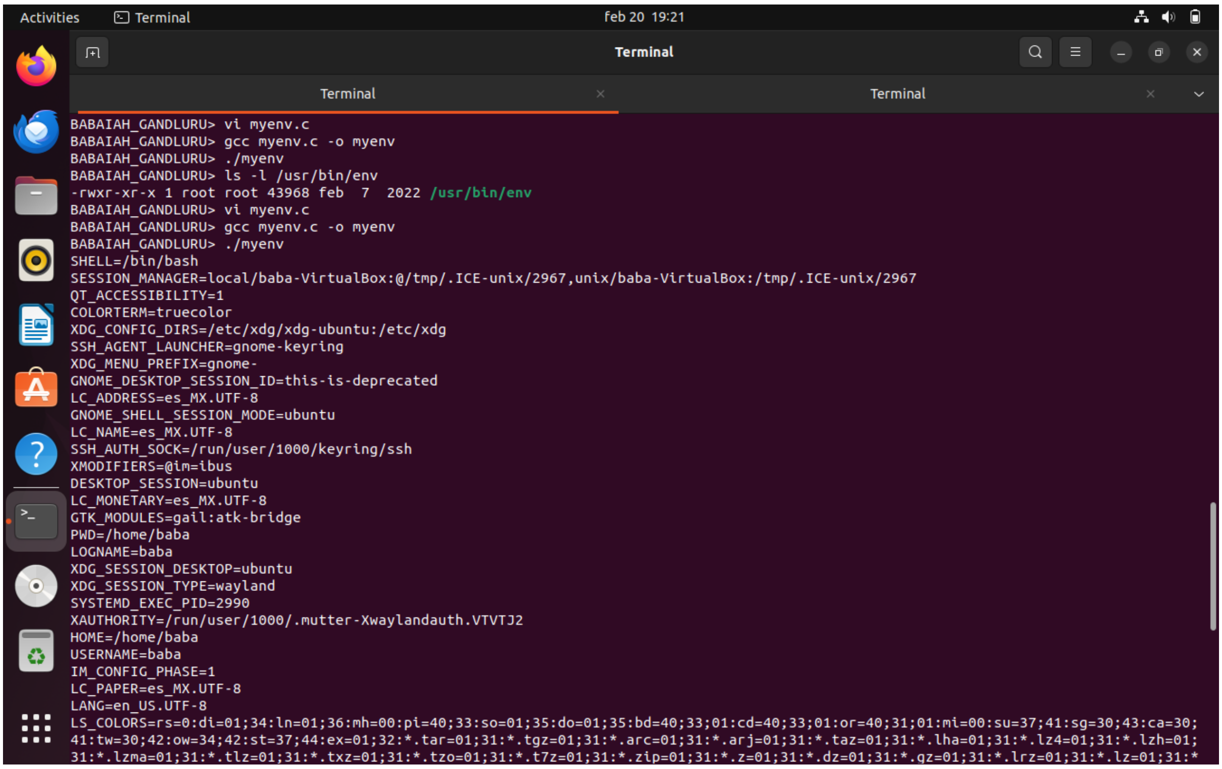
```
#include <unistd.h>

extern char **environ;

int main() {
    char *argv[2];
    argv[0] = "/usr/bin/env";
    argv[1] = NULL;

    // Step 1
     execve("/usr/bin/env", argv, NULL);

    // Step 2
   // execve("/usr/bin/env", argv, environ);

    return 0;
}
```

I executed both codes with “NULL” and “environ” arguments

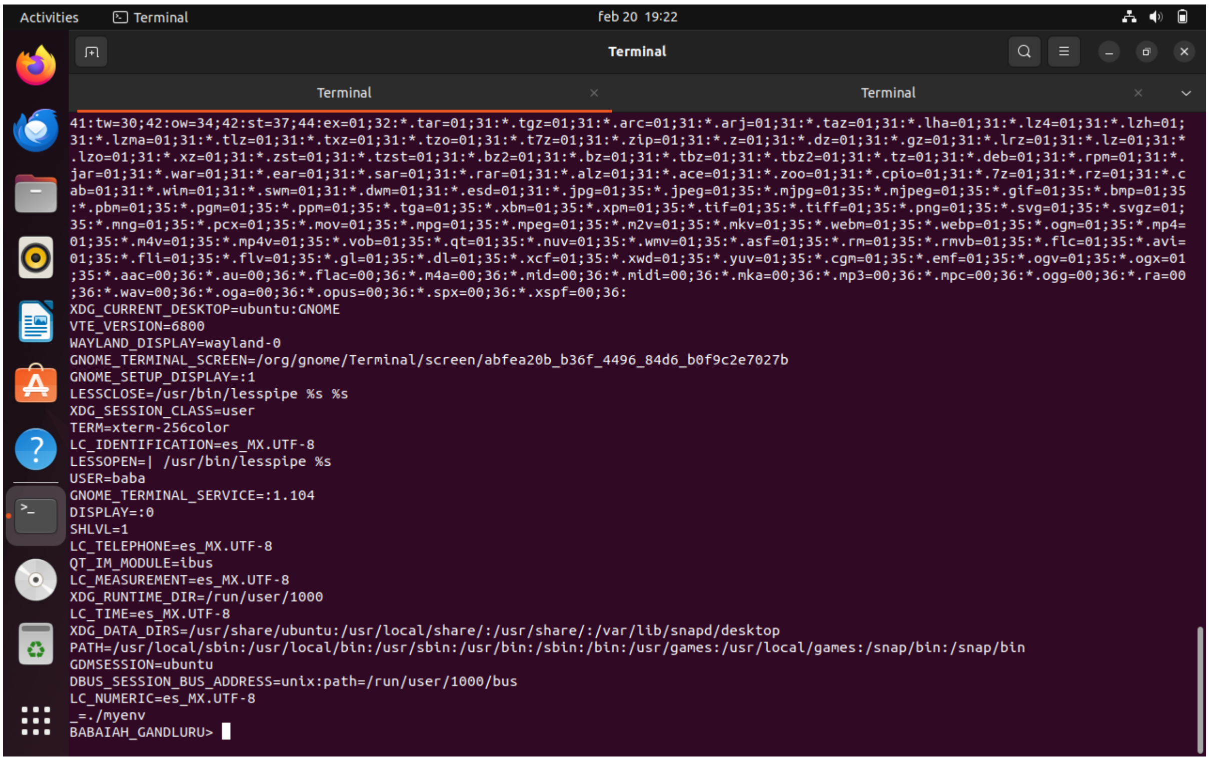
When NULL is passed as the envp argument the new program /usr/bin/env does not inherit the environment variables from the current process.

But when we pass environ as the argument to execve(), the current environment variables are passed to the new program /usr/bin/env. I got list of environment variables as shown in the screenshort

so, we can conclude that the new program inherited the environment variables from the current process.

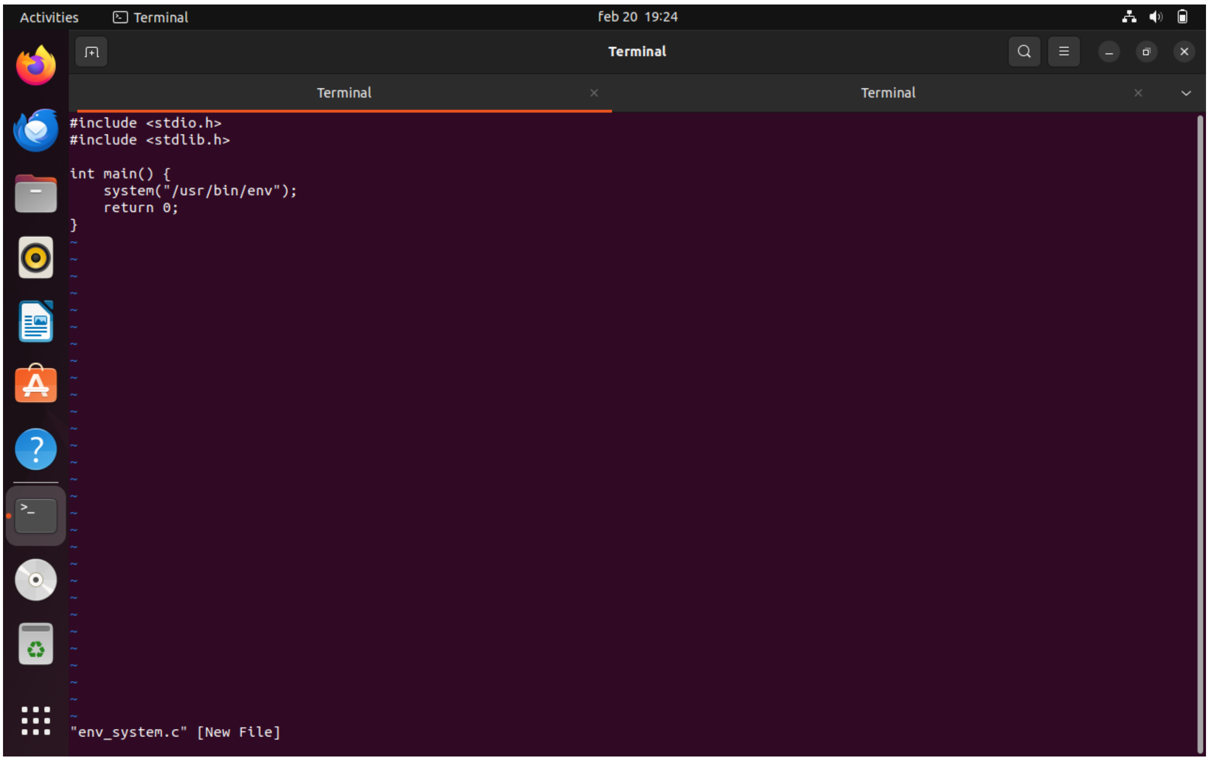


```
BABAIAH_GANDLURU> vi myenv.c
BABAIAH_GANDLURU> gcc myenv.c -o myenv
BABAIAH_GANDLURU> ./myenv
BABAIAH_GANDLURU> ls -l /usr/bin/env
-rwxr-xr-x 1 root root 43968 feb  7  2022 /usr/bin/env
BABAIAH_GANDLURU> vi myenv.c
BABAIAH_GANDLURU> gcc myenv.c -o myenv
BABAIAH_GANDLURU> ./myenv
SHELL=/bin/bash
SESSION_MANAGER=local/baba-VirtualBox:@/tmp/.ICE-unix/2967,unix/baba-VirtualBox:/tmp/.ICE-unix/2967
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
SSH_AGENT_LAUNCHER=gnome-keyring
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LC_ADDRESS=es_MX.UTF-8
GNOME_SHELL_SESSION_MODE=ubuntu
LC_NAME=es_MX.UTF-8
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
LC_MONETARY=es_MX.UTF-8
GTK_MODULES=gail:atk-bridge
PWD=/home/baba
LOGNAME=baba
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=2990
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.VTVTJ2
HOME=/home/baba
USERNAME=baba
IM_CONFIG_PHASE=1
LC_PAPER=es_MX.UTF-8
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:*
```

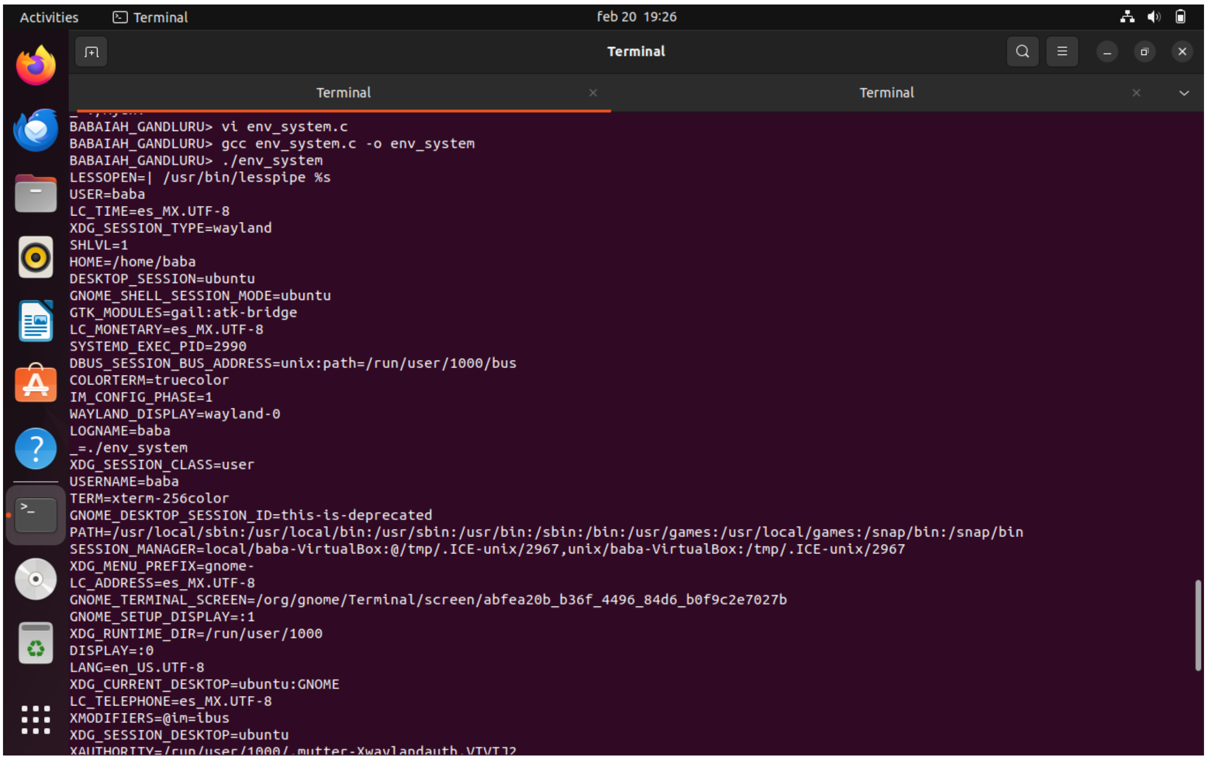


```
41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;
31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*
.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.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:*.c
ab=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:*.webp=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=6800
WAYLAND_DISPLAY=wayland-0
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/abfea20b_b36f_4496_84d6_b0f9c2e7027b
GNOME_SETUP_DISPLAY=:1
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LC_IDENTIFICATION=es_MX.UTF-8
LESSOPEN=| /usr/bin/lesspipe %s
USER=baba
GNOME_TERMINAL_SERVICE=:1.104
DISPLAY=:0
SHLVL=1
LC_TELEPHONE=es_MX.UTF-8
QT_IM_MODULE=ibus
LC_MEASUREMENT=es_MX.UTF-8
XDG_RUNTIME_DIR=/run/user/1000
LC_TIME=es_MX.UTF-8
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:/snap/bin
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
LC_NUMERIC=es_MX.UTF-8
_=./myenv
BABAIAH_GANDLURU> 
```

Task-4



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

int main() {
    system("/usr/bin/env");
    return 0;
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"env_system.c" [New File]
```

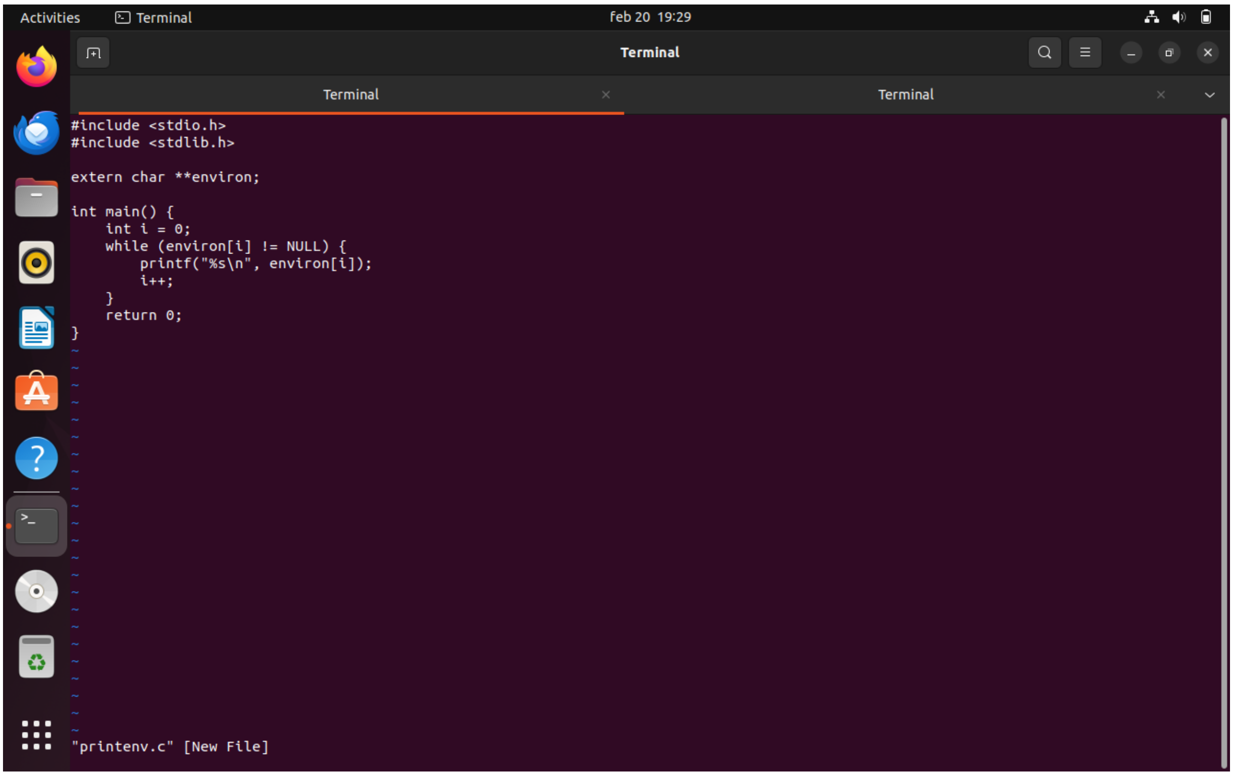


```
BABAIAH_GANDLURU> vi env_system.c
BABAIAH_GANDLURU> gcc env_system.c -o env_system
BABAIAH_GANDLURU> ./env_system
LESSOPEN=| /usr/bin/lesspipe %s
USER=baba
LC_TIME=es_MX.UTF-8
XDG_SESSION_TYPE=wayland
SHLVL=1
HOME=/home/baba
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gail:atk-bridge
LC_MONETARY=es_MX.UTF-8
SYSTEMD_EXEC_PID=2990
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
COLORTERM=truecolor
IM_CONFIG_PHASE=1
WAYLAND_DISPLAY=wayland-0
LOGNAME=baba
_=./env_system
XDG_SESSION_CLASS=user
USERNAME=baba
TERM=xterm-256color
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:/snap/bin
SESSION_MANAGER=local/baba-VirtualBox:@/tmp/.ICE-unix/2967,unix/baba-VirtualBox:/tmp/.ICE-unix/2967
XDG_MENU_PREFIX=gnome-
LC_ADDRESS=es_MX.UTF-8
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/abfea20b_b36f_4496_84d6_b0f9c2e7027b
GNOME_SETUP_DISPLAY=:1
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
LANG=en_US.UTF-8
XDG_CURRENT_DESKTOP=ubuntu:GNOME
LC_TELEPHONE=es_MX.UTF-8
XMODIFIERS=@im=ibus
XDG_SESSION_DESKTOP=ubuntu
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.VIVTJ2
```

I executed this code and the output of env command executed by /bin/sh includes the environment variables of the calling process so, we can conclude that the system() function in the code executes command by invoking /bin/sh

This is similar to using execve() to execute the command and inherit the environment variables

Task-5



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

extern char **environ;

int main() {
    int i = 0;
    while (environ[i] != NULL) {
        printf("%s\n", environ[i]);
        i++;
    }
    return 0;
}
"printenv.c" [New File]
```

I executed the code and following commands

sudo chown root foo

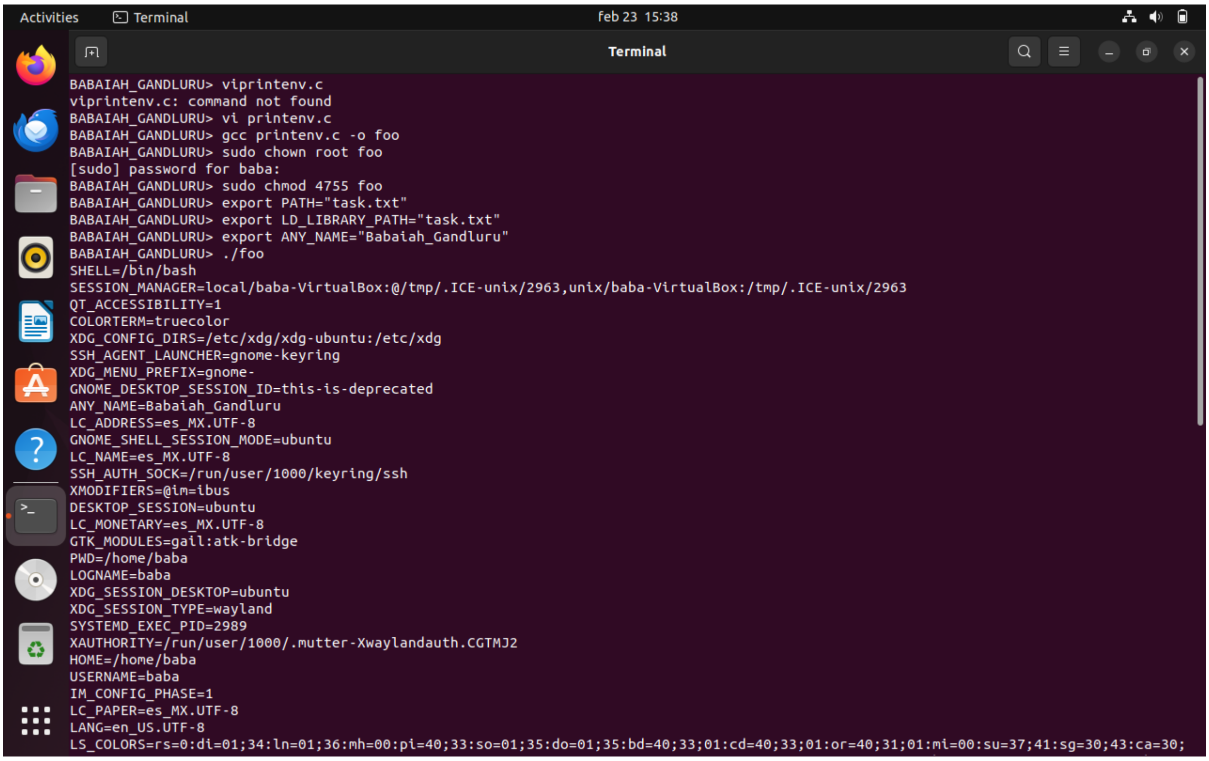
sudo chmod 4755 foo

export PATH="task.txt"

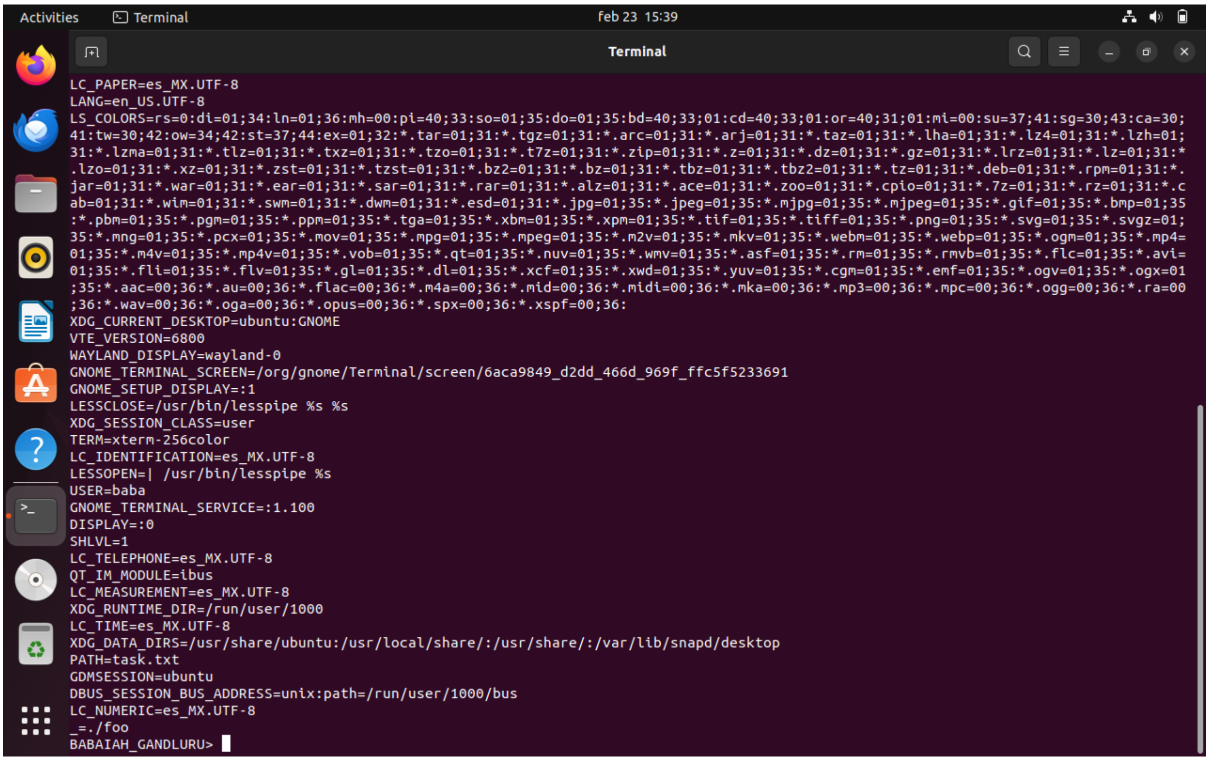
export LD_LIBRARY_PATH="task.txt"

export ANY_NAME="Babaiah_Gandluru"

./foo



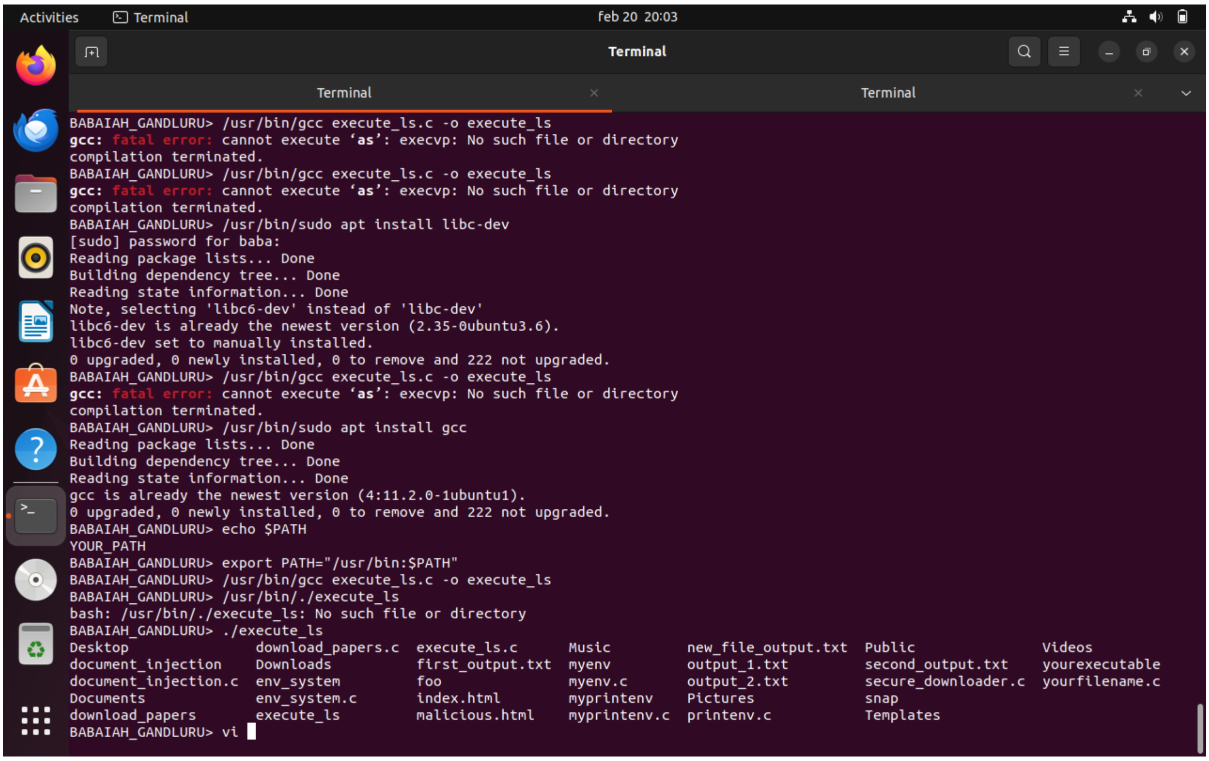
```
BABAIAH_GANDLURU> viprintenv.c
viprintenv.c: command not found
BABAIAH_GANDLURU> vi printenv.c
BABAIAH_GANDLURU> gcc printenv.c -o foo
BABAIAH_GANDLURU> sudo chown root foo
[sudo] password for baba:
BABAIAH_GANDLURU> sudo chmod 4755 foo
BABAIAH_GANDLURU> export PATH="task.txt"
BABAIAH_GANDLURU> export LD_LIBRARY_PATH="task.txt"
BABAIAH_GANDLURU> export ANY_NAME="Babaiah_Gandluru"
BABAIAH_GANDLURU> ./foo
SHELL=/bin/bash
SESSION_MANAGER=local/baba-VirtualBox:@/tmp/.ICE-unix/2963,unix/baba-VirtualBox:/tmp/.ICE-unix/2963
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
SSH_AGENT_LAUNCHER=gnome-keyring
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
ANY_NAME=Babaiah_Gandluru
LC_ADDRESS=es_MX.UTF-8
GNOME_SHELL_SESSION_MODE=ubuntu
LC_NAME=es_MX.UTF-8
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
LC_MONETARY=es_MX.UTF-8
GTK_MODULES=gail:atk-bridge
PWD=/home/baba
LOGNAME=baba
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=2989
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.CGTMJ2
HOME=/home/baba
USERNAME=baba
IM_CONFIG_PHASE=1
LC_PAPER=es_MX.UTF-8
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;
```



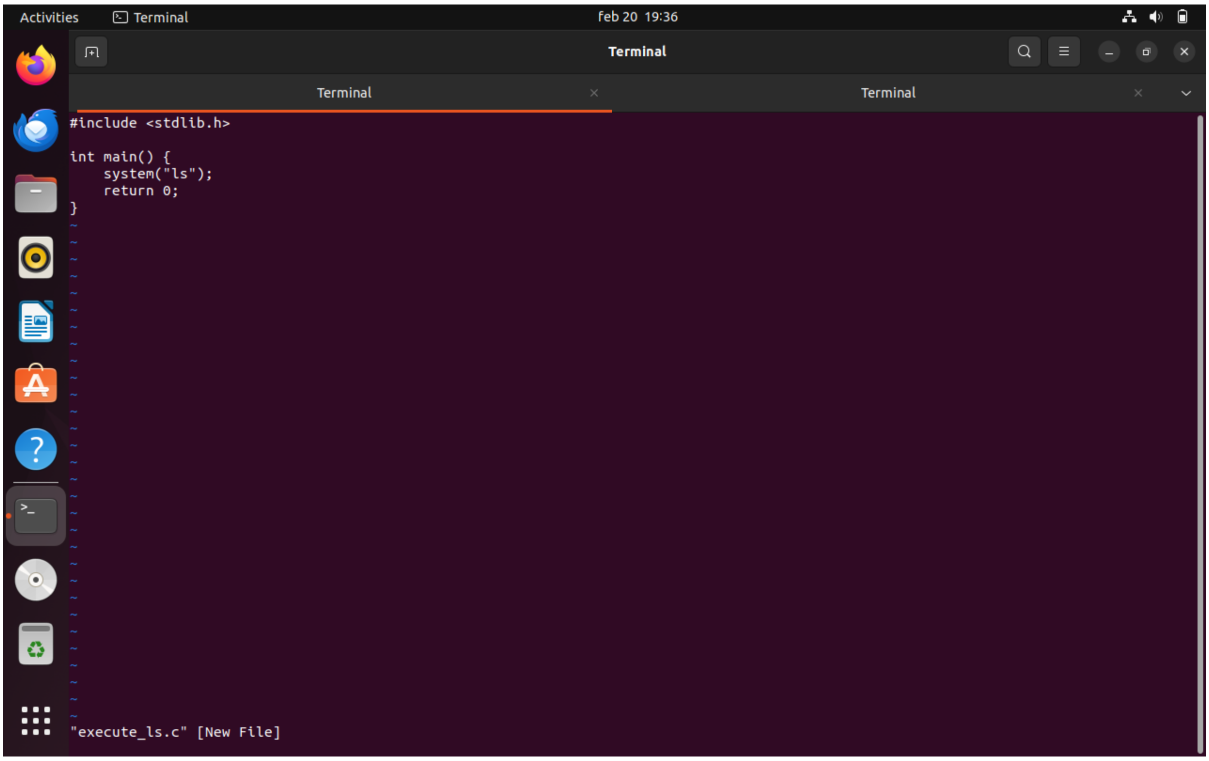
```
LC_PAPER=es_MX.UTF-8
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;
41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;
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:*.c
ab=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:*.webp=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=6800
WAYLAND_DISPLAY=wayland-0
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/6aca9849_d2dd_466d_969f_ffc5f5233691
GNOME_SETUP_DISPLAY=:1
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LC_IDENTIFICATION=es_MX.UTF-8
LESSOPEN=| /usr/bin/lesspipe %s
USER=baba
GNOME_TERMINAL_SERVICE=:1.100
DISPLAY=:0
SHLVL=1
LC_TELEPHONE=es_MX.UTF-8
QT_IM_MODULE=ibus
LC_MEASUREMENT=es_MX.UTF-8
XDG_RUNTIME_DIR=/run/user/1000
LC_TIME=es_MX.UTF-8
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
PATH=task.txt
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
LC_NUMERIC=es_MX.UTF-8
_=./foo
BABAIAH_GANDLURU> 
```

After running the Set-UID program foo, I observed that it gave me all the environment variables that were set in your shell process, including PATH, LD_LIBRARY_PATH, and ANY_NAME which is Babaiah_Gandluru. This conforms that environment variables set in the user's shell process are inherited by the Set-UID child process.

Task-6



```
BABAIAH_GANDLURU> /usr/bin/gcc execute_ls.c -o execute_ls
gcc: fatal error: cannot execute ‘as’: execvp: No such file or directory
compilation terminated.
BABAIAH_GANDLURU> /usr/bin/gcc execute_ls.c -o execute_ls
gcc: fatal error: cannot execute ‘as’: execvp: No such file or directory
compilation terminated.
BABAIAH_GANDLURU> /usr/bin/sudo apt install libc-dev
[sudo] password for baba:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'libc6-dev' instead of 'libc-dev'
libc6-dev is already the newest version (2.35-0ubuntu3.6).
libc6-dev set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 222 not upgraded.
BABAIAH_GANDLURU> /usr/bin/gcc execute_ls.c -o execute_ls
gcc: fatal error: cannot execute ‘as’: execvp: No such file or directory
compilation terminated.
BABAIAH_GANDLURU> /usr/bin/sudo apt install gcc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gcc is already the newest version (4:11.2.0-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 222 not upgraded.
BABAIAH_GANDLURU> echo $PATH
YOUR_PATH
BABAIAH_GANDLURU> export PATH="/usr/bin:$PATH"
BABAIAH_GANDLURU> /usr/bin/gcc execute_ls.c -o execute_ls
BABAIAH_GANDLURU> /usr/bin/./execute_ls
bash: /usr/bin/./execute_ls: No such file or directory
BABAIAH_GANDLURU> ./execute_ls
Desktop              download_papers.c  execute_ls.c      Music          new_file_output.txt  Public               Videos
document_injection   Downloads          first_output.txt  myenv          output_1.txt         second_output.txt    yourexecutable
document_injection.c env_system         foo               myenv.c        output_2.txt         secure_downloader.c  yourfilename.c
Documents            env_system.c       index.html        myprintenv     Pictures             snap
download_papers      execute_ls         malicious.html    myprintenv.c   printenv.c           Templates
BABAIAH_GANDLURU> vi
```



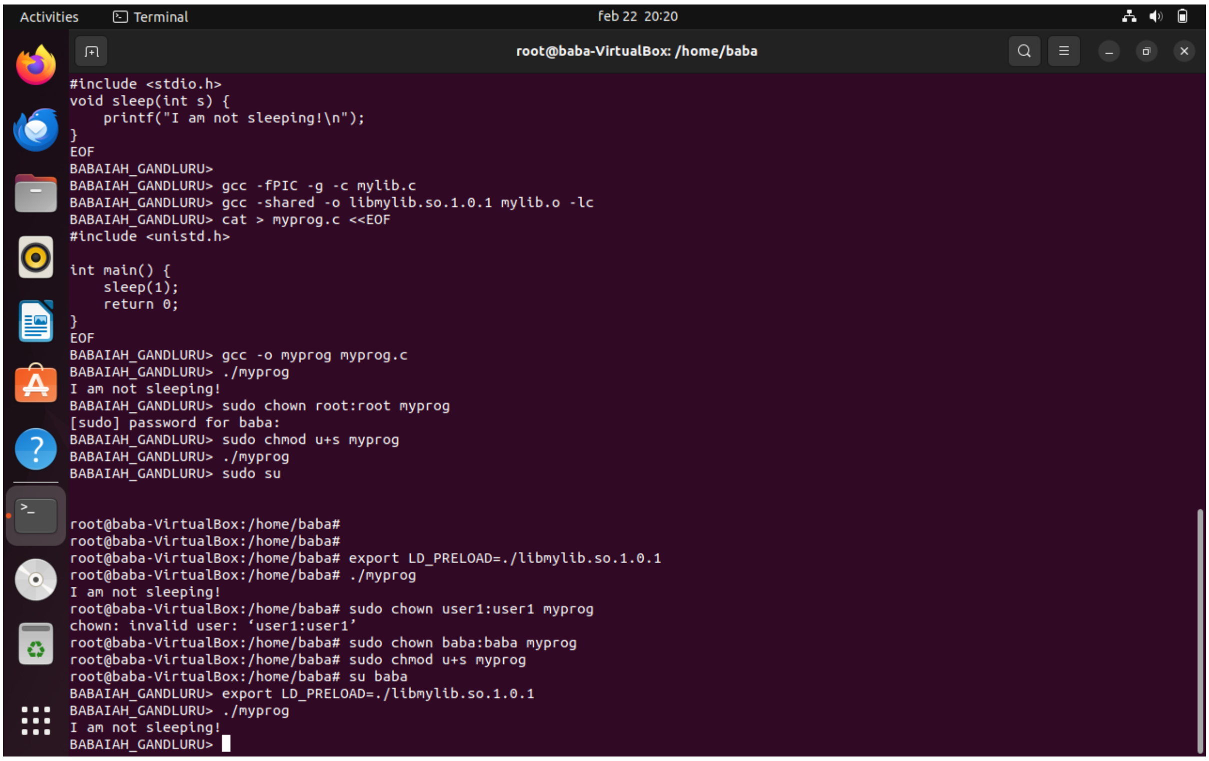
```
#include <stdlib.h>

int main() {
    system("ls");
    return 0;
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"execute_ls.c" [New File]
```

After running the Set-UID program execute_ls, I observed that it executes the "ls" command and lists all the contents of the current directory.

Since the program uses a relative path for the ls command (system("ls")), it relies on the shell's PATH environment variable to locate the ls executable.

I learnt that this can allow Malicious users to exploit by modifying the PATH environment variable to point to a different directory containing a malicious executable named ls. and When the Set-UID program is executed by the host user it would run the malicious code instead of /bin/ls.

Task-7



```
#include <stdio.h>
void sleep(int s) {
    printf("I am not sleeping!\n");
}
EOF
BABAIAH_GANDLURU>
BABAIAH_GANDLURU> gcc -fPIC -g -c mylib.c
BABAIAH_GANDLURU> gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
BABAIAH_GANDLURU> cat > myprog.c <<EOF
#include <unistd.h>

int main() {
    sleep(1);
    return 0;
}
EOF
BABAIAH_GANDLURU> gcc -o myprog myprog.c
BABAIAH_GANDLURU> ./myprog
I am not sleeping!
BABAIAH_GANDLURU> sudo chown root:root myprog
[sudo] password for baba:
BABAIAH_GANDLURU> sudo chmod u+s myprog
BABAIAH_GANDLURU> ./myprog
BABAIAH_GANDLURU> sudo su


root@baba-VirtualBox:/home/baba#
root@baba-VirtualBox:/home/baba#
root@baba-VirtualBox:/home/baba# export LD_PRELOAD=./libmylib.so.1.0.1
root@baba-VirtualBox:/home/baba# ./myprog
I am not sleeping!
root@baba-VirtualBox:/home/baba# sudo chown user1:user1 myprog
chown: invalid user: ‘user1:user1’
root@baba-VirtualBox:/home/baba# sudo chown baba:baba myprog
root@baba-VirtualBox:/home/baba# sudo chmod u+s myprog
root@baba-VirtualBox:/home/baba# su baba
BABAIAH_GANDLURU> export LD_PRELOAD=./libmylib.so.1.0.1
BABAIAH_GANDLURU> ./myprog
I am not sleeping!
BABAIAH_GANDLURU> 
```

I executed both myprog.c and mylib.c codes

I executed the myprog.c in 4 scenarios

1) when I executed myprog as regular program and as a normal user.

I got output as

I am not sleeping !

2) when I executed myprog as Set-UID root program and as a normal user.

I didnt get any output for this scenario

3) when I executed myprog as Set-UID root program and as the root account.

I got output as

I am not sleeping !

4) when I executed myprog as Set-UID "baba" program (i.e., the owner is user1, which is another user account).

I got output as

I am not sleeping !

The difference in the behavior is due to the LD_PRELOAD environment variable interactions with Set-UID programs. When LD_PRELOAD is set it loads the specified library before all other librarys.

But,in the case of Set-UID programs there are some restrictions imposed by the operating system for security reasons.

When I executed myprog as a regular program the LD_PRELOAD command worked as expected and the sleep() function from mylib.so is overridden and called.

I got "i am not sleeping !" message

But, when I executed myprog as a Set-UID root program:

In case if LD_PRELOAD is not set again within the program the LD_PRELOAD environment variable is not considered due to security restrictions. so the original sleep() function is executed in this case and

I didnt get "i am not sleeping !" message

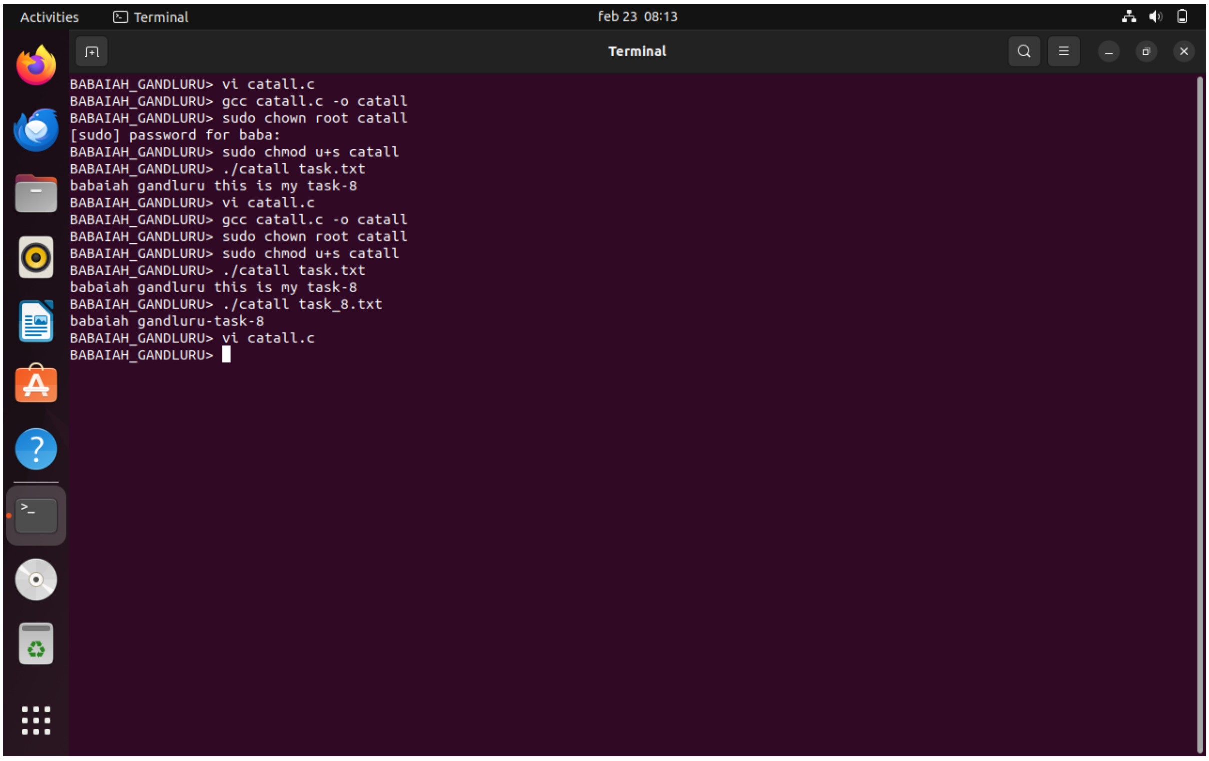
And In case If LD_PRELOAD is set again within the program it overrides the security restriction, and the overridden sleep() function from mylib.so is called. so

I got "i am not sleeping !" message

Similarly when I executed myprog as a Set-UID user1 program which is baba in my case where LD_PRELOAD set by a different user is not considered unless explicitly set again within the program.

So,I got "i am not sleeping !" message

Task-8



```
BABAIAH_GANDLURU> vi catall.c
BABAIAH_GANDLURU> gcc catall.c -o catall
BABAIAH_GANDLURU> sudo chown root catall
[sudo] password for baba:
BABAIAH_GANDLURU> sudo chmod u+s catall
BABAIAH_GANDLURU> ./catall task.txt
babaiah gandluru this is my task-8
BABAIAH_GANDLURU> vi catall.c
BABAIAH_GANDLURU> gcc catall.c -o catall
BABAIAH_GANDLURU> sudo chown root catall
BABAIAH_GANDLURU> sudo chmod u+s catall
BABAIAH_GANDLURU> ./catall task.txt
babaiah gandluru this is my task-8
BABAIAH_GANDLURU> ./catall task_8.txt
babaiah gandluru-task-8
BABAIAH_GANDLURU> vi catall.c
BABAIAH_GANDLURU> 
```

I am able to access the text file in the both scenarios of using the below commands

system(command);

execve(v[0], v, NULL);

I tried to acess the file task.txt and I am getting the text from task.txt file while using any one of the commands from

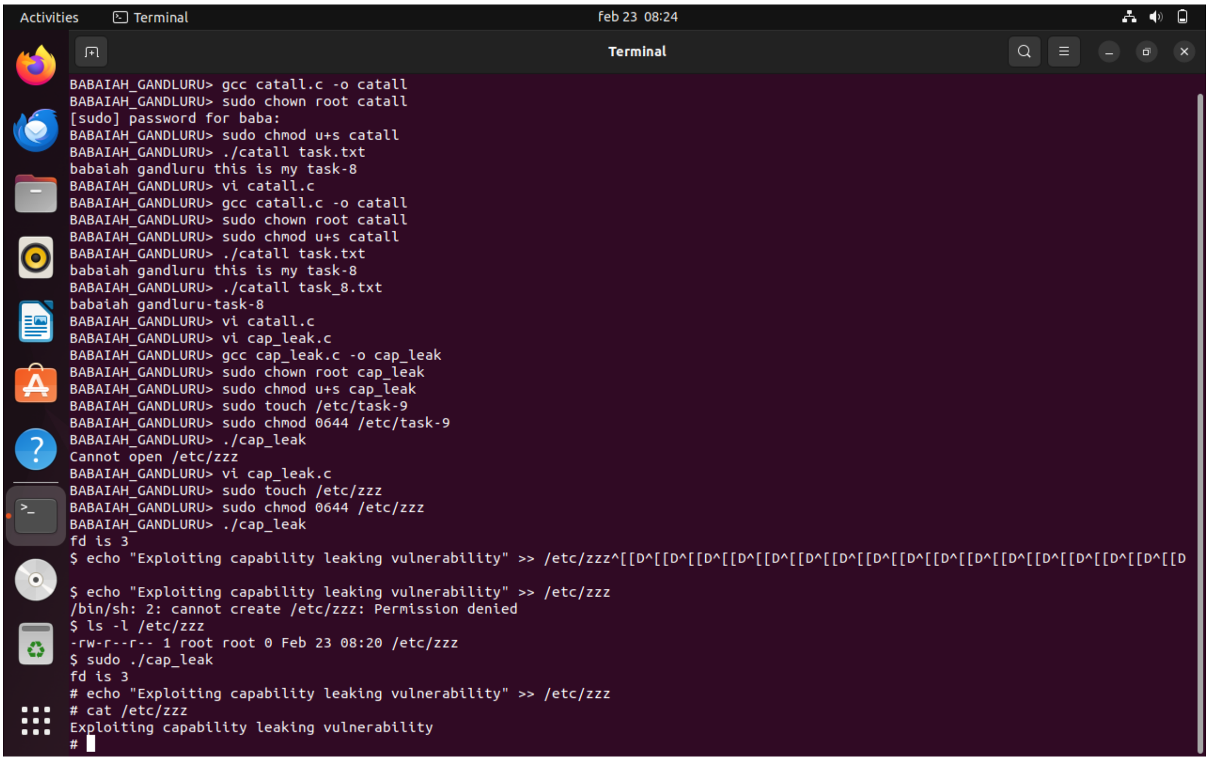
system(command);

I got acess to text file because system() invokes a shell and it allowed me to execute commands as if they were run directly from the command line with my own privileges.

execve(v[0], v, NULL);

I am still able to access the text inside the text file is that the program is directly executing /bin/cat using execve(). eventhough execve() doesn't invoke a shell. it still allows the execution of /bin/cat, which has permissions to read the contents of files. This program directly calls /bin/cat using execve() which bypasess any shell interpretation.

Task-9



```
BABAIAH_GANDLURU> gcc catall.c -o catall
BABAIAH_GANDLURU> sudo chown root catall
[sudo] password for baba:
BABAIAH_GANDLURU> sudo chmod u+s catall
BABAIAH_GANDLURU> ./catall task.txt
babaiah gandluru this is my task-8
BABAIAH_GANDLURU> vi catall.c
BABAIAH_GANDLURU> gcc catall.c -o catall
BABAIAH_GANDLURU> sudo chown root catall
BABAIAH_GANDLURU> sudo chmod u+s catall
BABAIAH_GANDLURU> ./catall task.txt
babaiah gandluru this is my task-8
BABAIAH_GANDLURU> ./catall task_8.txt
babaiah gandluru-task-8
BABAIAH_GANDLURU> vi catall.c
BABAIAH_GANDLURU> vi cap_leak.c
BABAIAH_GANDLURU> gcc cap_leak.c -o cap_leak
BABAIAH_GANDLURU> sudo chown root cap_leak
BABAIAH_GANDLURU> sudo chmod u+s cap_leak
BABAIAH_GANDLURU> sudo touch /etc/task-9
BABAIAH_GANDLURU> sudo chmod 0644 /etc/task-9
BABAIAH_GANDLURU> ./cap_leak
Cannot open /etc/zzz
BABAIAH_GANDLURU> vi cap_leak.c
BABAIAH_GANDLURU> sudo touch /etc/zzz
BABAIAH_GANDLURU> sudo chmod 0644 /etc/zzz
BABAIAH_GANDLURU> ./cap_leak
fd is 3
$ echo "Exploiting capability leaking vulnerability" >> /etc/zzz^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D^[[D

$ echo "Exploiting capability leaking vulnerability" >> /etc/zzz
/bin/sh: 2: cannot create /etc/zzz: Permission denied
$ ls -l /etc/zzz
-rw-r--r-- 1 root root 0 Feb 23 08:20 /etc/zzz
$ sudo ./cap_leak
fd is 3
# echo "Exploiting capability leaking vulnerability" >> /etc/zzz
# cat /etc/zzz
Exploiting capability leaking vulnerability
# 
```

I execude the code and sucessfully explited the vulnarbility using the code and I am able to acess the text file which i shouldnt have acess to. In this case file zzz.txt

This is because process retains some privileged capabilities even after dropping root privileges. I am able to exploit this to write to /etc/zzz as a normal user.