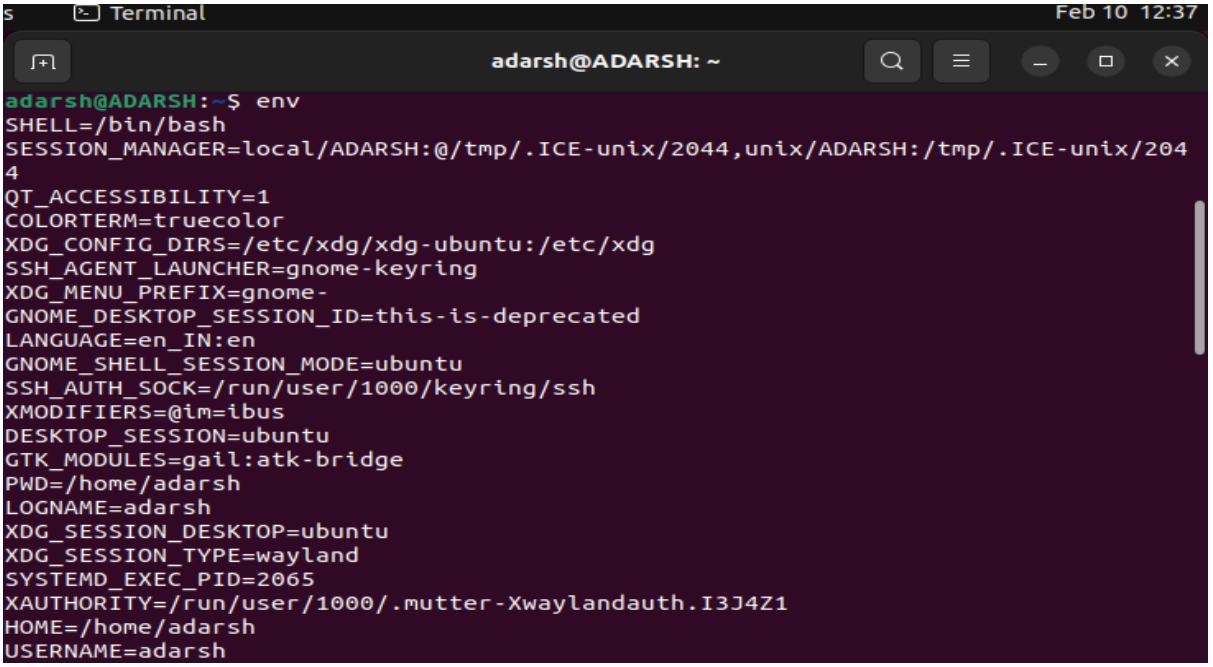
Assignment 04

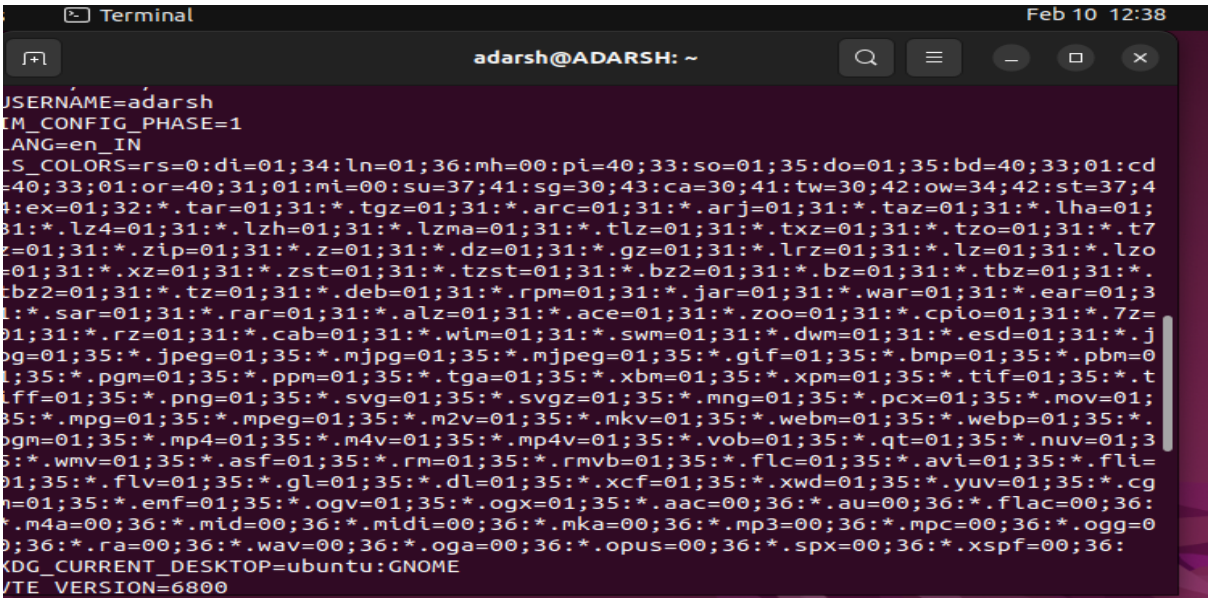
Information Security

ADARSH
2022pis0026
11 February 2023

1. Manipulating Environment Variables

Showing Environment Variables





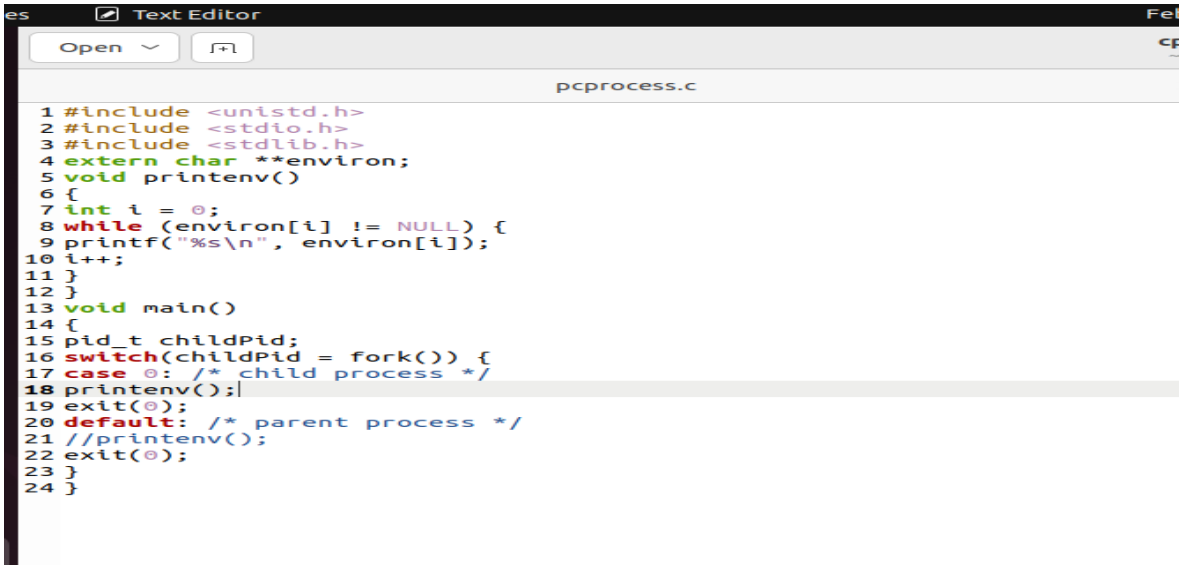
2. Passing Environment Variables (Parent Process to Child Process)

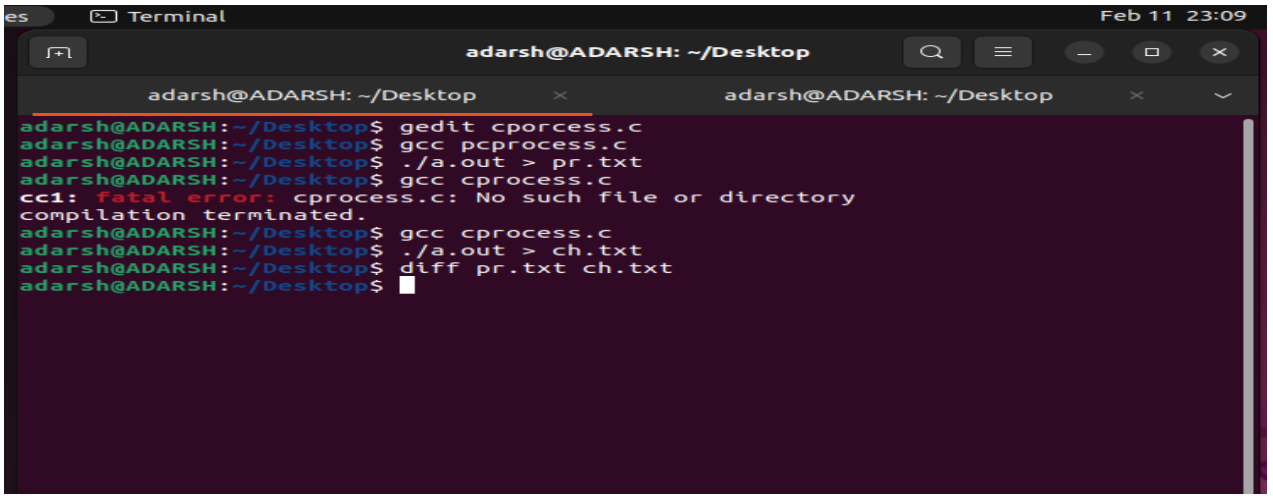
1. Running *printenv()* for the child *process* and *parent process* gives the same Environment variables as output. That means Environment variables are passed from *parent* to *child* when *fork()* is used.

Open

pcprocess.c

```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);
}
}
```





Observation:- Using the diff command we can verify this.

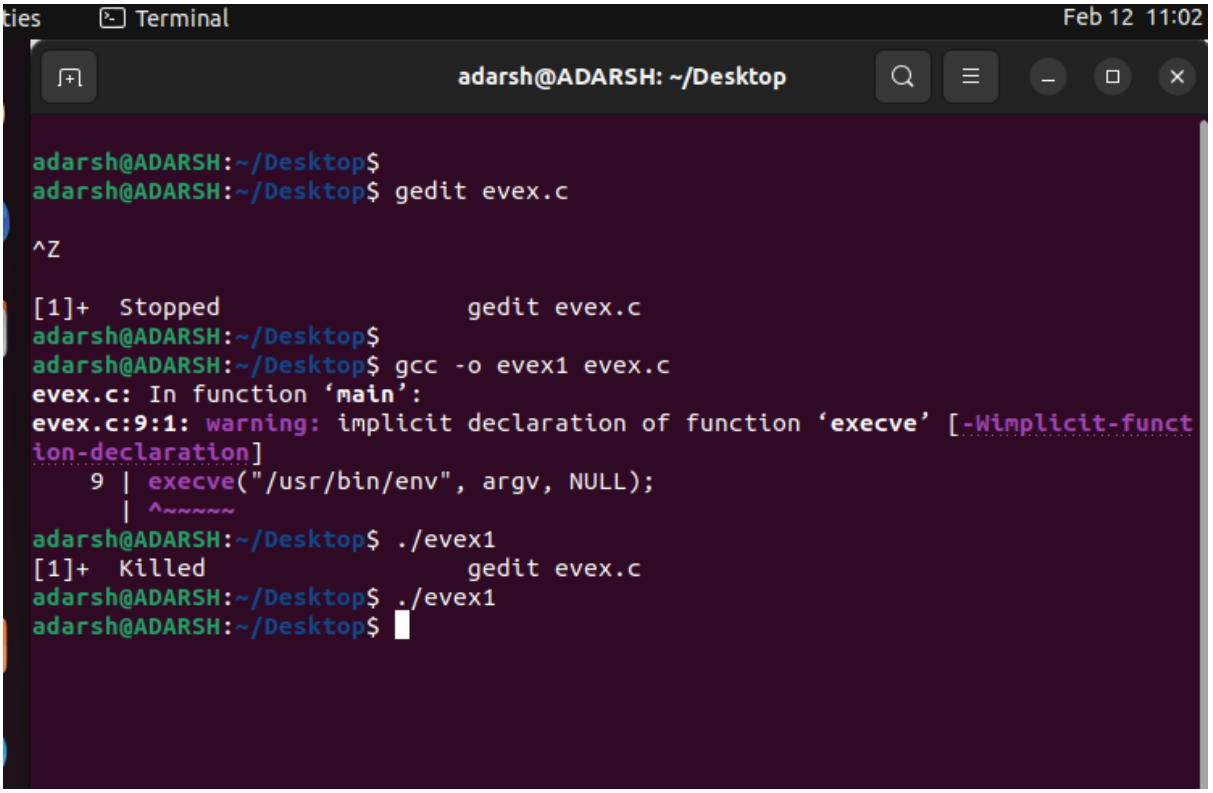
3. Environment Variables and *execve()*

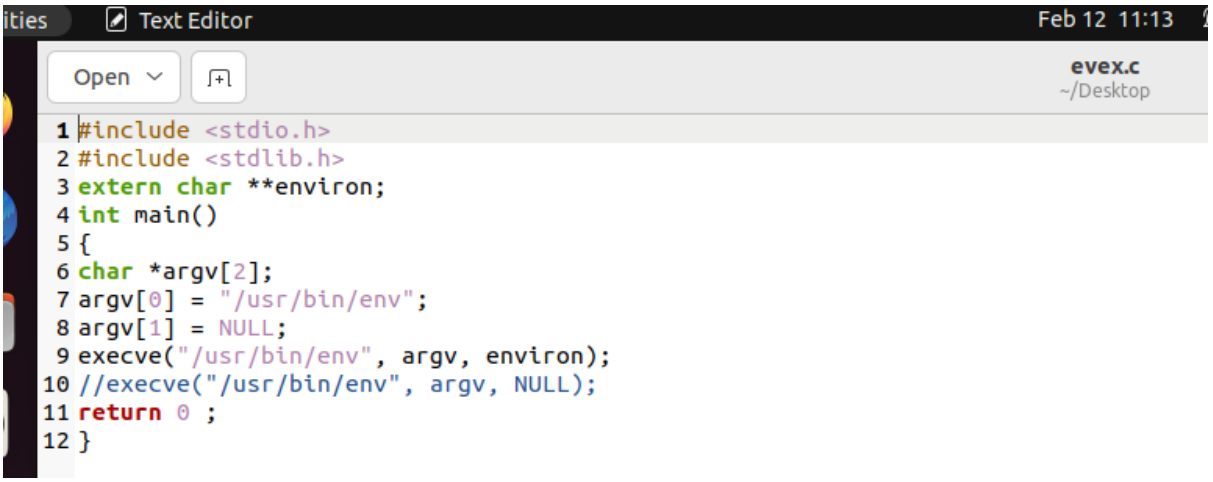
1. *execve(const char *pathname, char *const argv[], char *const envp[])* - replaces the parent process by a new child process with newly initialized stack, heap etc. And Environment Variables are transferred from parent to child through *envp*.

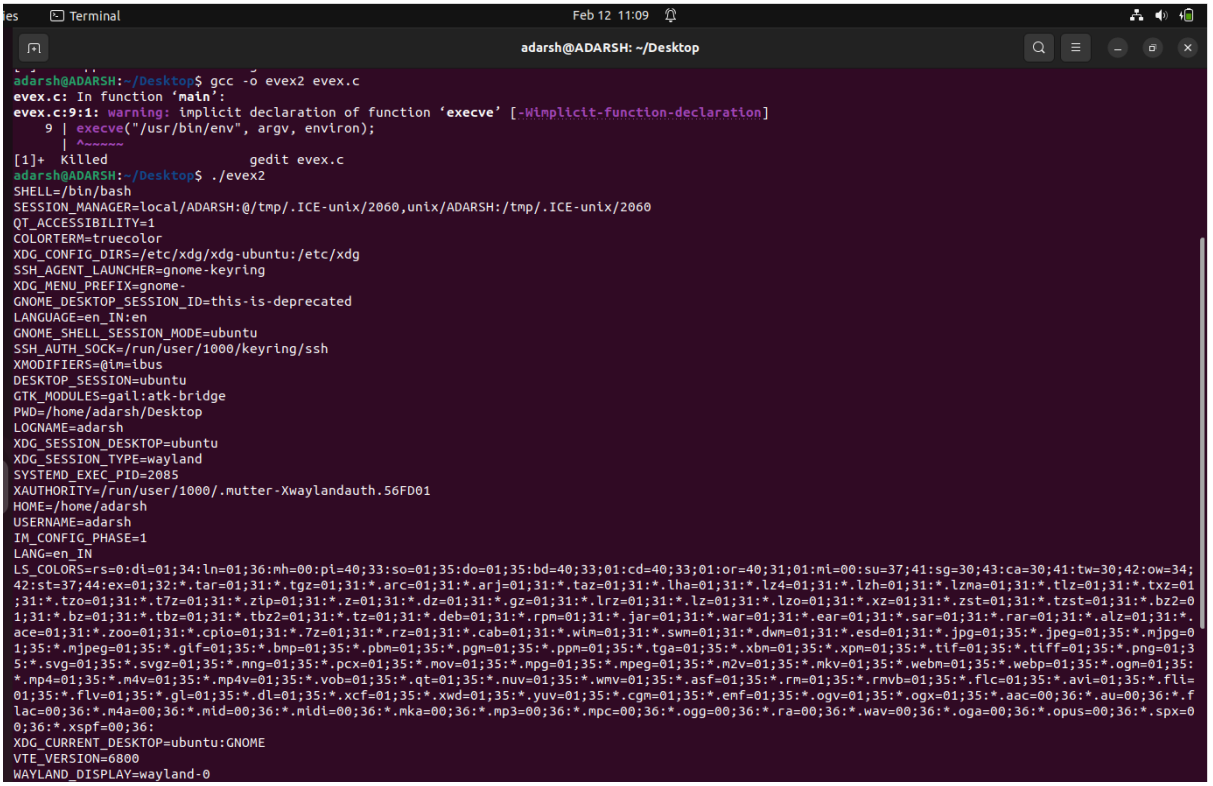
2. *pathname* is set to "*/usr/bin/env*". This will execute the program *env* which prints Environment Variables.

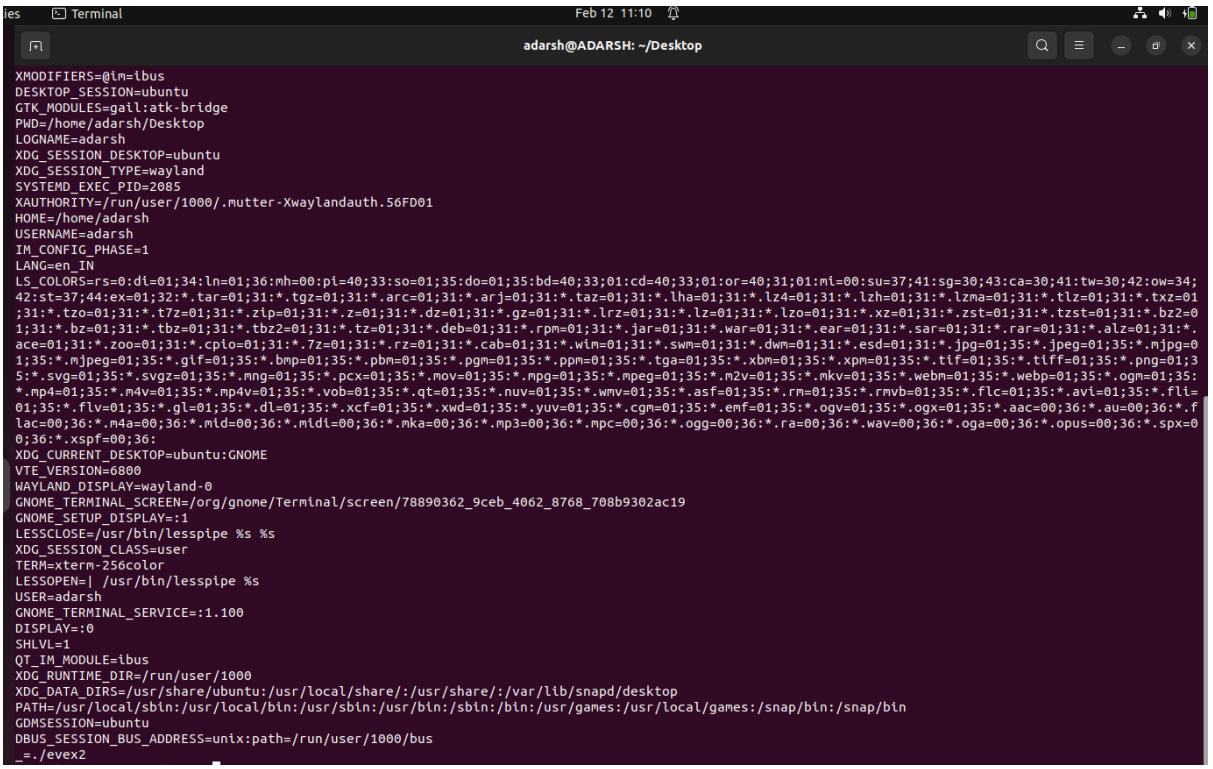
3. In the first program no Environment Variables were passed(*env* = *NULL*). So, the program didn't print any Environment Variables.

4. In the second program Environment Variables were passed using environ variables. So, all Environment variables were printed.


ties
Terminal
Feb 12 11:02
adarsh@ADARSH: ~/Desktop
adarsh@ADARSH:~/Desktop$
adarsh@ADARSH:~/Desktop$ gedit evex.c
^Z
[1]+ Stopped gedit evex.c
adarsh@ADARSH:~/Desktop$
adarsh@ADARSH:~/Desktop$ gcc -o evex1 evex.c
evex.c: In function 'main':
evex.c:9:1: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
9 | execve("/usr/bin/env", argv, NULL);
| ^~~~~~
adarsh@ADARSH:~/Desktop$ ./evex1
[1]+ Killed gedit evex.c
adarsh@ADARSH:~/Desktop$ ./evex1
adarsh@ADARSH:~/Desktop$

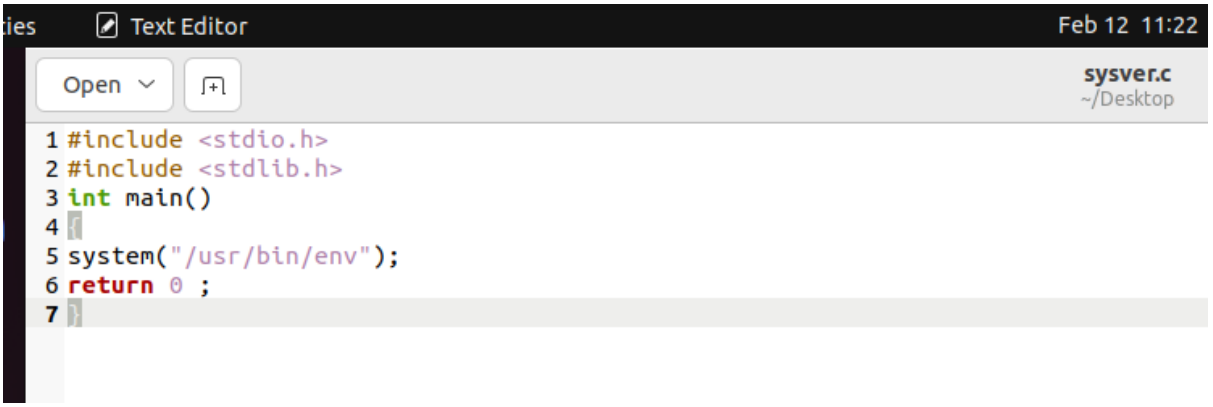

ities
Text Editor
Feb 12 11:13
Open
evex.c
~/Desktop
1 #include <stdio.h>
2 #include <stdlib.h>
3 extern char **environ;
4 int main()
5 {
6 char *argv[2];
7 argv[0] = "/usr/bin/env";
8 argv[1] = NULL;
9 execve("/usr/bin/env", argv, environ);
10 //execve("/usr/bin/env", argv, NULL);
11 return 0 ;
12 }

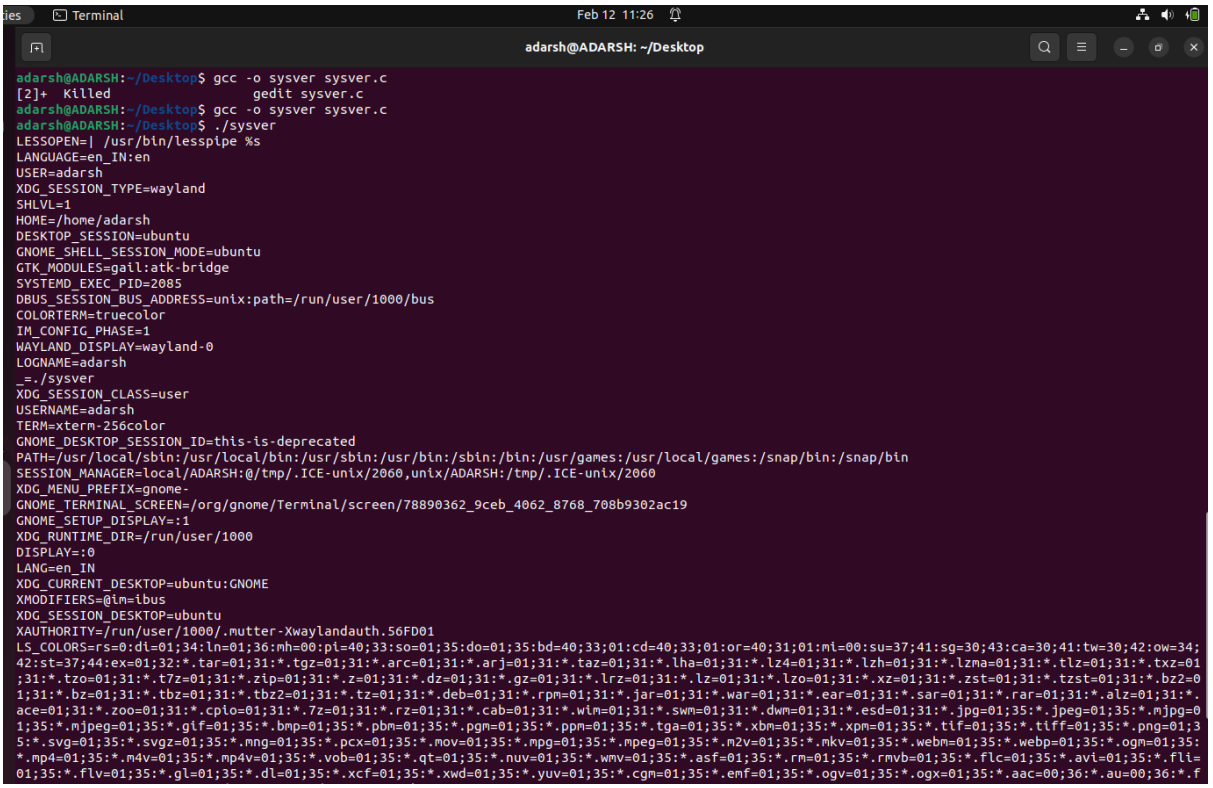


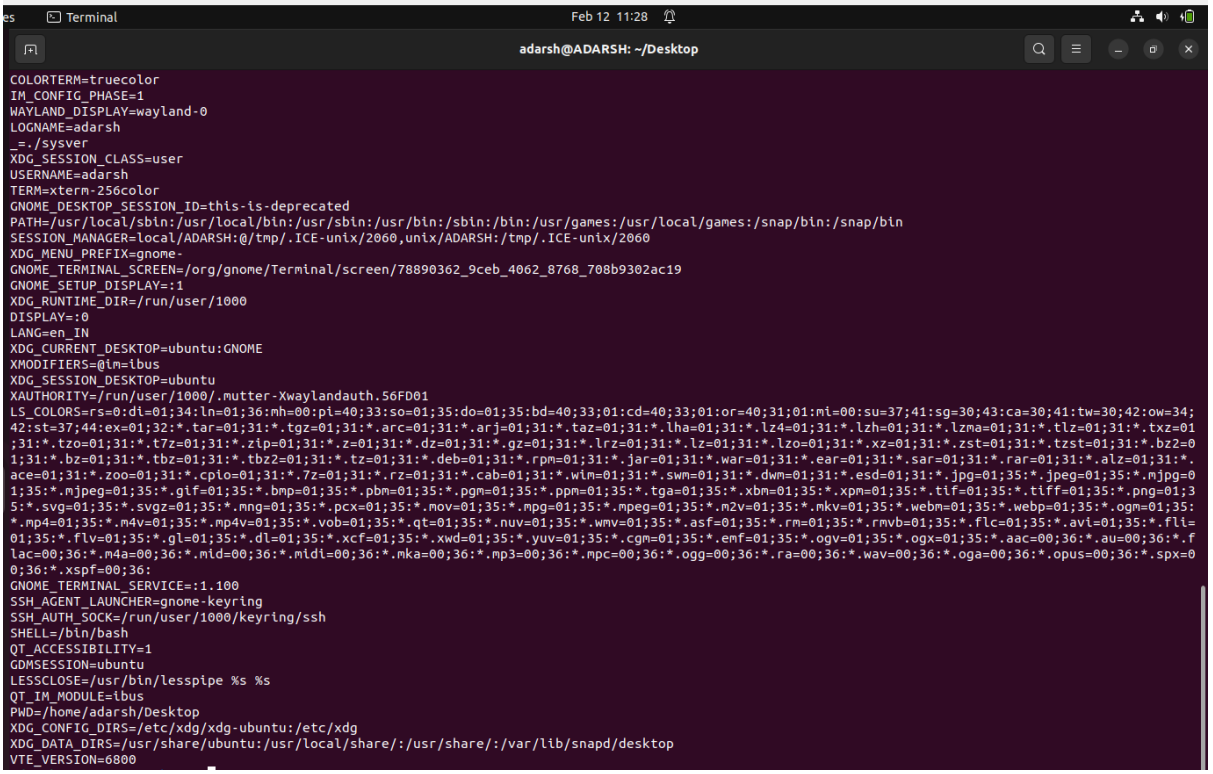


4.Environment Variables and *system()*

1. system() by default passes Environment Variables to the child process. 2. Verified this by running the program (*sysver.c*)

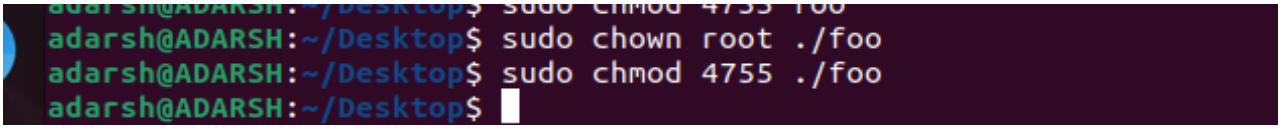

ies
Text Editor
Feb 12 11:22
Open
sysver.c
~/Desktop
1 #include <stdio.h>
2 #include <stdlib.h>
3 int main()
4 {
5 system("/usr/bin/env");
6 return 0 ;
7 }


ies
Terminal
Feb 12 11:26
adarsh@ADARSH: ~/Desktop
adarsh@ADARSH:~/Desktop$ gcc -o sysver sysver.c
[2]+ Killed gedit sysver.c
adarsh@ADARSH:~/Desktop$ gcc -o sysver sysver.c
adarsh@ADARSH:~/Desktop$ ./sysver
LESSOPEN=| /usr/bin/lesspipe %s
LANGUAGE=en_IN:en
USER=adarsh
XDG_SESSION_TYPE=wayland
SHLVL=1
HOME=/home/adarsh
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gail:atk-bridge
SYSTEMD_EXEC_PID=2085
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
COLORTERM=truecolor
IM_CONFIG_PHASE=1
WAYLAND_DISPLAY=wayland-0
LOGNAME=adarsh
_=./sysver
XDG_SESSION_CLASS=user
USERNAME=adarsh
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/ADARSH:@/tmp/.ICE-unix/2060,unix/ADARSH:/tmp/.ICE-unix/2060
XDG_MENU_PREFIX=gnome-
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/78890362_9ceb_4062_8768_708b9302ac19
GNOME_SETUP_DISPLAY=:1
XDG_RUNTIME_DIR=/run/user/1000
DISPLAY=:0
LANG=en_IN
XDG_CURRENT_DESKTOP=ubuntu:GNOME
XMODIFIERS=@im=ibus
XDG_SESSION_DESKTOP=ubuntu
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.56FD01
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:*.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:*.f

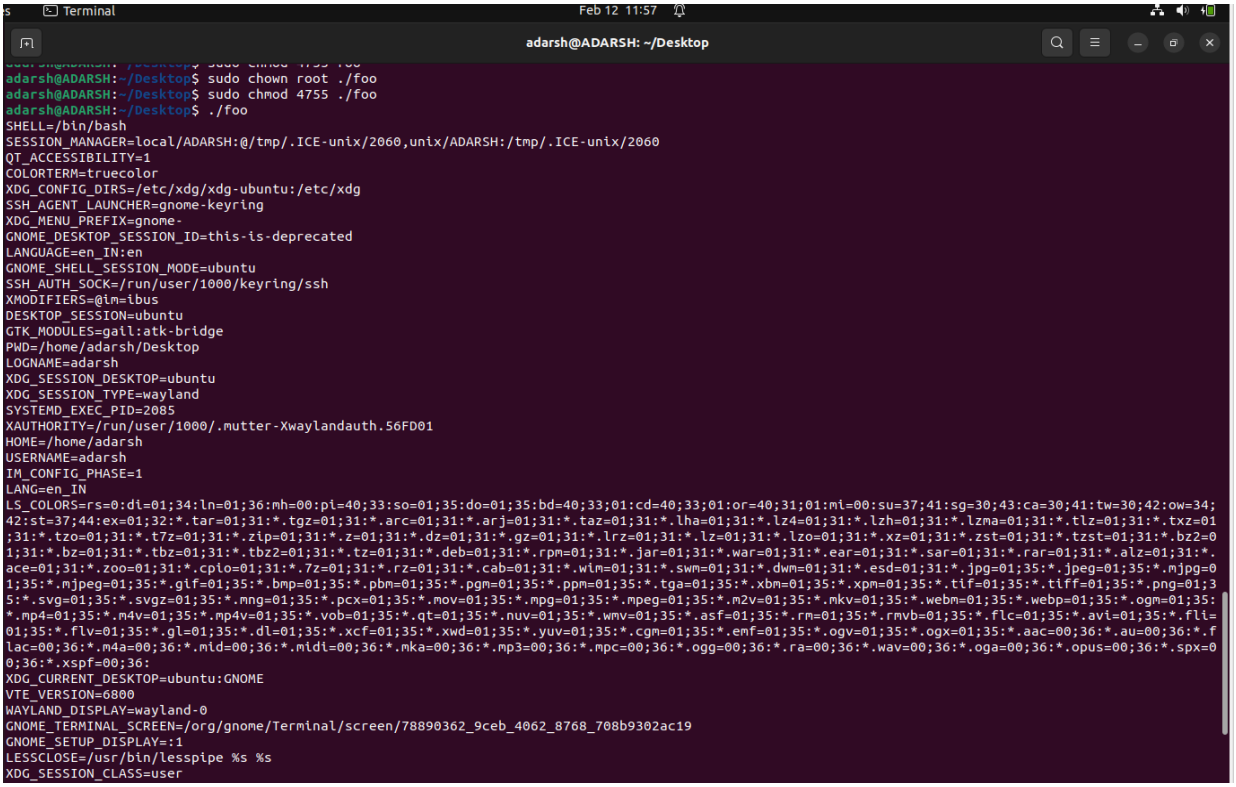


5. Environment Variable and Set-UID Programs

1. Compile the program (*foo.c*), change its (*foo*) ownership to root, and make it a Set-UID program and set Environment Variables in user level.



2. Running the program we can see the Environment Variables (rootenv.txt) are not changed in root level, new variables are also not added.



6.The PATH Environment Variable and Set-UID Programs

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

```
adarsh@ADARSH:~/Desktop$ gcc -o set set.c
set.c: In function ‘main’:
set.c:3:1: warning: implicit declaration of function ‘system’ [-Wimplicit-functi
on-declaration]
    3 | system("ls");
      | ^~~~~~
adarsh@ADARSH:~/Desktop$ ./set
 adarsh.txt   evex1            foo.c          set.c
 a.out        evex2            pcprocess.c   'Sniffing and spoofing files'
 ch.txt       evex.c           pr.txt         sysver
 cporcess.c   fifthquest.txt   rootenv.txt    sysver.c
 cprocess.c   foo              set            typescript
adarsh@ADARSH:~/Desktop$
```