

# Assignment 04

## Information Security

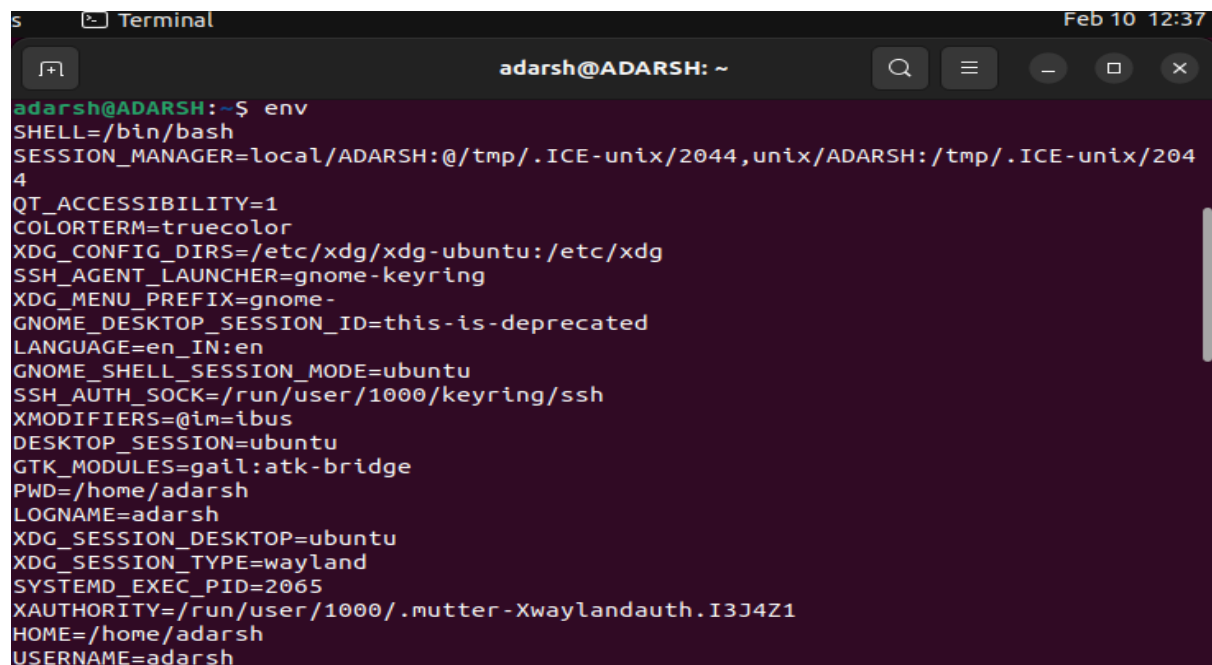
ADARSH

2022pis0026

11 February 2023

## 1. Manipulating Environment Variables

### Showing Environment Variables

A terminal window titled 'Terminal' with a dark background and light text. The window shows the output of the 'env' command, listing various environment variables such as SHELL, SESSION\_MANAGER, QT\_ACCESSIBILITY, and USERNAME. The user 'adarsh' is logged in at 'ADARSH' on 'Feb 10 12:37'.

```
s Terminal Feb 10 12:37
adarsh@ADARSH: ~
adarsh@ADARSH:~$ env
SHELL=/bin/bash
SESSION_MANAGER=local/ADARSH:@/tmp/.ICE-unix/2044,unix/ADARSH:/tmp/.ICE-unix/2044
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
LANGUAGE=en_IN:en
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
GTK_MODULES=gail:atk-bridge
PWD=/home/adarsh
LOGNAME=adarsh
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=2065
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.I3J4Z1
HOME=/home/adarsh
USERNAME=adarsh
```

```
Terminal Feb 10 12:38
adarsh@ADARSH: ~
USER_NAME=adarsh
IM_CONFIG_PHASE=1
LANG=en_IN
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;4
4: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:*.t7
z=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;3
1:*.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:*.j
pg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=0
1;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.t
iff=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;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:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cg
h=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=0
0;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
```

```
Terminal Feb 10 12:39
adarsh@ADARSH: ~
VTE_VERSION=6800
WAYLAND_DISPLAY=wayland-0
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/46f14c98_d087_4b60_81b7_26ae830
75718
GNOME_SETUP_DISPLAY=:1
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=adarsh
GNOME_TERMINAL_SERVICE=:1.99
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/local/share:/usr/share:/var/lib/snapd/des
ktop
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
r/local/games:/snap/bin:/snap/bin
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/adarsh/Desktop
_=/usr/bin/env
adarsh@ADARSH:~$
```

## 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  [icon]
pcprocess.c
1 #include <unistd.h>
2 #include <stdio.h>
3 #include <stdlib.h>
4 extern char **environ;
5 void printenv()
6 {
7     int i = 0;
8     while (environ[i] != NULL) {
9         printf("%s\n", environ[i]);
10        i++;
11    }
12 }
13 void main()
14 {
15     pid_t childPid;
16     switch(childPid = fork()) {
17     case 0: /* child process */
18         printenv();
19         exit(0);
20     default: /* parent process */
21         printenv();
22         exit(0);
23     }
24 }
```

```
es  Text Editor  Feb 11 23:09
Open  [icon]
pcprocess.c
1 #include <unistd.h>
2 #include <stdio.h>
3 #include <stdlib.h>
4 extern char **environ;
5 void printenv()
6 {
7     int i = 0;
8     while (environ[i] != NULL) {
9         printf("%s\n", environ[i]);
10        i++;
11    }
12 }
13 void main()
14 {
15     pid_t childPid;
16     switch(childPid = fork()) {
17     case 0: /* child process */
18         printenv();
19         exit(0);
20     default: /* parent process */
21         printenv();
22         exit(0);
23     }
24 }
```

```
es  Terminal  Feb 11 23:09
adarsh@ADARSH: ~/Desktop
adarsh@ADARSH: ~/Desktop
adarsh@ADARSH: ~/Desktop$ gedit cporcess.c
adarsh@ADARSH: ~/Desktop$ gcc pcprocess.c
adarsh@ADARSH: ~/Desktop$ ./a.out > pr.txt
adarsh@ADARSH: ~/Desktop$ gcc cprocess.c
cc1: fatal error: cprocess.c: No such file or directory
compilation terminated.
adarsh@ADARSH: ~/Desktop$ gcc cprocess.c
adarsh@ADARSH: ~/Desktop$ ./a.out > ch.txt
adarsh@ADARSH: ~/Desktop$ diff pr.txt ch.txt
adarsh@ADARSH: ~/Desktop$
```

**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.



```
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, NULL);
10    return 0 ;
11 }
```

The screenshot shows a text editor window titled "Text Editor" with a timestamp of "Feb 12 11:05". The editor contains a C program named "evex.c" located at "~/Desktop". The code is as follows:

```
ities 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-funct
ion-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
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 }
```

```
es  Terminal Feb 12 11:09
adarsh@ADARSH: ~/Desktop

adarsh@ADARSH:~/Desktop$ gcc -o evex2 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, environ);
      |   ^~~~~~
[1]+  Killed                  gedit evex.c
adarsh@ADARSH:~/Desktop$ ./evex2
SHELL=/bin/bash
SESSION_MANAGER=local/ADARSH:@/tmp/.ICE-unix/2060,unix/ADARSH:/tmp/.ICE-unix/2060
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
LANGUAGE=en_IN:en
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
GTK_MODULES=gail:atk-bridge
PWD=/home/adarsh/Desktop
LOGNAME=adarsh
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=2085
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.56FD01
HOME=/home/adarsh
USERNAME=adarsh
IM_CONFIG_PHASE=1
LANG=en_IN
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:*.tztst=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:*.wlm=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
```

```
es  Terminal Feb 12 11:10
adarsh@ADARSH: ~/Desktop

XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
GTK_MODULES=gail:atk-bridge
PWD=/home/adarsh/Desktop
LOGNAME=adarsh
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=2085
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.56FD01
HOME=/home/adarsh
USERNAME=adarsh
IM_CONFIG_PHASE=1
LANG=en_IN
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:*.tztst=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:*.wlm=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/78890362_9ceb_4062_8768_708b9302ac19
GNOME_SETUP_DISPLAY=:1
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=adarsh
GNOME_TERMINAL_SERVICE=:1.100
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
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
GNOME_SESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
_=./evex2
```

## 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
IN_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
XAUTORITY=/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: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:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.b2=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:*.pgn=01;35:*.ppn=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
```



```
es Terminal Feb 12 11:28
adarsh@ADARSH: ~/Desktop

COLORTERM=truecolor
IM_CONFIG_PHASE=1
WAYLAND_DISPLAY=wayland-0
LOGNAME=adarsh
_=/usr/bin/su
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:pl=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:*.lzm=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=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:*.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:
GNOME_TERMINAL_SERVICE=:1.100
SSH_AGENT_LAUNCHER=gnome-keyring
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
SHELL=/bin/bash
QT_ACCESSIBILITY=1
GDMSESSION=ubuntu
LESSCLOSE=/usr/bin/lesspipe %s %s
QT_IM_MODULE=ibus
PWD=/home/adarsh/Desktop
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=6800
```

## 5. Environment Variable and Set-UID Programs

```
ies Text Editor Feb 12 11:05
adarsh@ADARSH: ~/Desktop
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, NULL);
10    return 0;
11 }
```

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.

```
adarsh@ADARSH:~/Desktop$ sudo chmod 4755 ./foo
adarsh@ADARSH:~/Desktop$ sudo chown root ./foo
adarsh@ADARSH:~/Desktop$
```

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



```
s Terminal Feb 12 11:57
adarsh@ADARSH: ~/Desktop
adarsh@ADARSH: ~/Desktop$ sudo chown root ./foo
adarsh@ADARSH: ~/Desktop$ sudo chmod 4755 ./foo
adarsh@ADARSH: ~/Desktop$ ./foo
SHELL=/bin/bash
SESSION_MANAGER=local/ADARSH:@/tmp/.ICE-unix/2060,unix/ADARSH:/tmp/.ICE-unix/2060
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
LANGUAGE=en_IN:en
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
GTK_MODULES=gail:atk-bridge
PWD=/home/adarsh/Desktop
LOGNAME=adarsh
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=wayland
SYSTEMD_EXEC_PID=2085
XAUTHORITY=/run/user/1000/.mutter-Xwaylandauth.56FD01
HOME=/home/adarsh
USERNAME=adarsh
IM_CONFIG_PHASE=1
LANG=en_IN
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pl=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:*.lzh=01;31:*.lzm=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:*.wln=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:*.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:*.enf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.f
lac=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=0
0;36:*.xspf=00;36:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6800
WAYLAND_DISPLAY=wayland-0
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/78890362_9ceb_4062_8768_708b9302ac19
GNOME_SETUP_DISPLAY=:1
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
```

```
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=adarsh
GNOME_TERMINAL_SERVICE=:1.100
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
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
= ./foo
```

## 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:

```
s Text Editor Feb 12 12:20
set.c
~/Desktop

1 int main()
2
3 system("ls");
4 return 0;
5
```

```
adarsh@ADARSH:~/Desktop$ gcc -o set set.c
set.c: In function 'main':
set.c:3:1: warning: implicit declaration of function 'system' [-Wimplicit-function-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$
```

