Mohammad Arshad

U00304676

NCS 531-11

ASSIGNMENT 2

Task 1: Manipulating environment variables

In this task I played around creating, deleting and printing environment variables.

```
[01/24/2018 19:23] seed@ubuntu:~$
[01/24/2018 19:23] seed@ubuntu:~$
[01/24/2018 19:23] seed@ubuntu:~$ export Library=1234567
[01/24/2018 19:25] seed@ubuntu:~$ env | grep Library
Library=1234567
[01/24/2018 19:25] seed@ubuntu:~$ unset Library
[01/24/2018 19:26] seed@ubuntu:~$ env | grep Library
[01/24/2018 19:26] seed@ubuntu:~$
[01/24/2018 19:26] seed@ubuntu:~$
```

Fig 1: Export and unset command

```
[01/24/2018 19:23] seed@ubuntu:~$
[01/24/2018 19:23] seed@ubuntu:~$ env | grep PATH
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
DEFAULTS_PATH=/usr/share/gconf/ubuntu-2d.default.path
PATH=.:/usr/lib/lightdm/lightdm:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
MANDATORY_PATH=/usr/share/gconf/ubuntu-2d.mandatory.path
[01/24/2018 19:23] seed@ubuntu:~$
[01/24/2018 19:23] seed@ubuntu:~$
```

Fig 2: Viewing a particular environment variable

```
[01/24/2018 19:22] seed@ubuntu:~$
[01/24/2018 19:22] seed@ubuntu:~$ printenv
SSH_AGENT_PID=2721
GPG_AGENT_INFO=/tmp/keyring-GkpH7w/gpg:0:1
TERM=xterm
SHELL=/bin/bash
XDG_SESSION_COOKIE=6da3e071019f67095bc4c5e900000002-1516850415.316870-726398189
WINDOWID=58720261
GNOME_KEYRING_CONTROL=/tmp/keyring-GkpH7w
USER=seed
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: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:*.arj=01;31:*.taz=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.zip=01;31:*.z=01;31:*.Z=
01;31:*.dz=01;31:*.gz=01;31:*.lz=01;31:*.xz=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:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35
:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;
35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=
01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01
;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.axv=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;3
6:*.flac=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:*.axa=00;36:*.oga=00;36:*.spx=00;
36:*.xspf=00;36:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/tmp/keyring-GkpH7w/ssh
SESSION_MANAGER=local/ubuntu:@/tmp/.ICE-unix/2668,unix/ubuntu:/tmp/.ICE-unix/2668
DEFAULTS_PATH=/usr/share/gconf/ubuntu-2d.default.path
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu-2d:/etc/xdg
PATH=.:/usr/lib/lightdm/lightdm:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
DESKTOP_SESSION=ubuntu-2d
PWD=/home/seed
GNOME_KEYRING_PID=2657
LANG=en_US.UTF-8
MANDATORY_PATH=/usr/share/gconf/ubuntu-2d.mandatory.path
UBUNTU_MENUPROXY=libappmenu.so
GDMSESSION=ubuntu-2d
SHLVL=1
HOME=/home/seed
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LOGNAME=seed
XDG_DATA_DIRS=/usr/share/ubuntu-2d:/usr/share/gnome:/usr/local/share/:/usr/share/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-Ve4DAYr0LT,guid=df493930d26f030f0486c9db0000003e
LESSOPEN=| /usr/bin/lesspipe %s
```

Fig 3: Viewing all the environment variable

Task 2: Inheriting environment variables from parents

For this task I compiled and run the program provided in the task description. In the first step we collected the output of child process using the fork().

```
[01/24/2018 19:29] seed@ubuntu:~$ gcc -o Task1 Task1.c
[01/24/2018 19:30] seed@ubuntu:~$ Task1 > child
[01/24/2018 19:31] seed@ubuntu:~$ ./Task1
SSH_AGENT_PID=2721
GPG_AGENT_INFO=/tmp/keyring-GkpH7w/gpg:0:1
TERM=xterm
SHELL=/bin/bash
XDG_SESSION_COOKIE=6da3e071019f67095bc4c5e900000002-1516850415.316870-726398189
WINDOWID=58720261
GNOME_KEYRING_CONTROL=/tmp/keyring-GkpH7w
USER=seed
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: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:*.arj=01;31:*.taz=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz
=01;31:*.txz=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lz=01;
31:*.xz=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:*.ace
=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.jpg=01;35:*.jpeg=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;3
5:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=0
1;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:*.axv=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.a
ac=00;36:*.au=00;36:*.flac=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:*.axa=00;36:*.oga=00;36:*.spx=00;
36:*.xspf=00;36:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/tmp/keyring-GkpH7w/ssh
SESSION_MANAGER=local/ubuntu:@/tmp/.ICE-unix/2668,unix/ubuntu:/tmp/.ICE-unix/2668
DEFAULTS_PATH=/usr/share/gconf/ubuntu-2d.default.path
Library=1234567
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu-2d:/etc/xdg
PATH=.:/usr/lib/lightdm/lightdm:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
:/sbin:/bin:/usr/games
DESKTOP_SESSION=ubuntu-2d
PWD=/home/seed
GNOME_KEYRING_PID=2657
LANG=en_US.UTF-8
```

Fig 4: Output of the program in Task2

Then changed the program to get the parent process and compared both the output.

```
[01/24/2018 20:00] seed@ubuntu:~$
[01/24/2018 20:00] seed@ubuntu:~$
[01/24/2018 20:00] seed@ubuntu:~$ gcc -o Task1 Task1.c
[01/24/2018 20:01] seed@ubuntu:~$ ./Task1 > Task1.parent
[01/24/2018 20:01] seed@ubuntu:~$ diff Task1.child Task1.parent
[01/24/2018 20:01] seed@ubuntu:~$
```

Fig 5: Comparing parent and child process

There was no difference both of the file. This is because child process inherit most of the character of the parent process. One of such character is the environment variables. **By doing this test I came to a conclusion that environment variables are inherited by the child process from the parent process.**

Task 3: Environment variables and execve()

For this task I compiled and run the program provided in the task description.

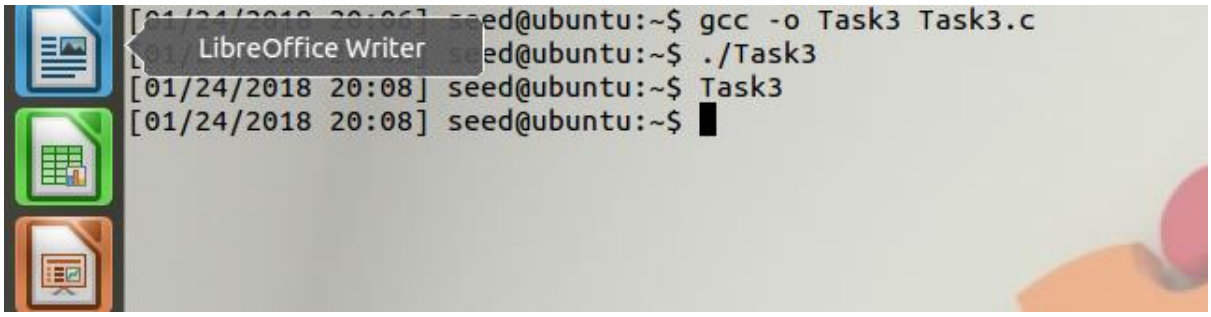


Fig 6: Program with - execve("/usr/bin/env", argv, NULL);

When I run the program with - **execve("/usr/bin/env", argv, NULL);** there was no output generated. This is because the argument was a “NULL”.

Now I changed the “NULL” argument to “environ” variable, compiled and run the program to get the output of “/usr/bin/env”.

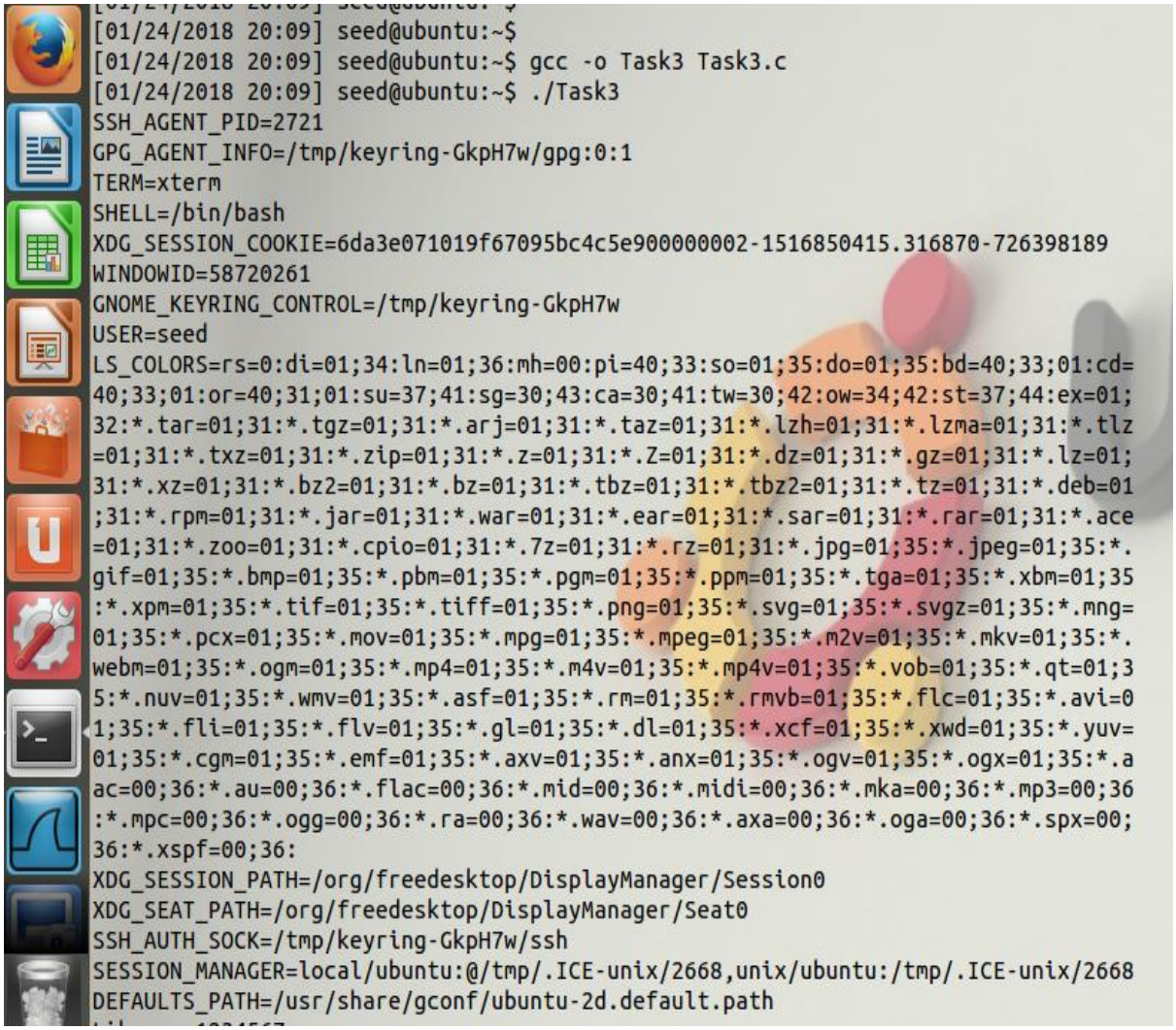


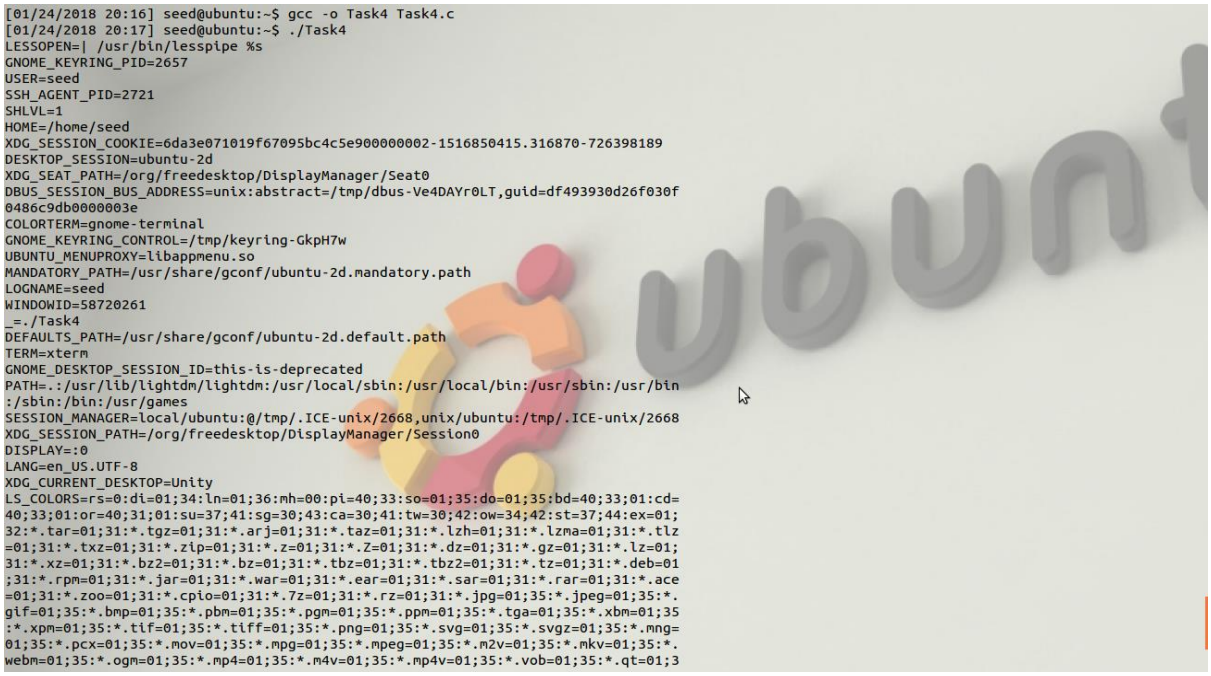
Fig 7: Program with - execve("/usr/bin/env", argv, environ);

This is because of replacing the "NULL" argument with the "environ" variable. Environ is a variable that points to an array of pointers to strings called the "environment". The last pointer in this array has the value NULL.

Task 4: Environment variables and system()

System() executes **/bin/sh**, and asks the shell to execute the command. Using the program provided in the task I was able to understand the problem with using system().

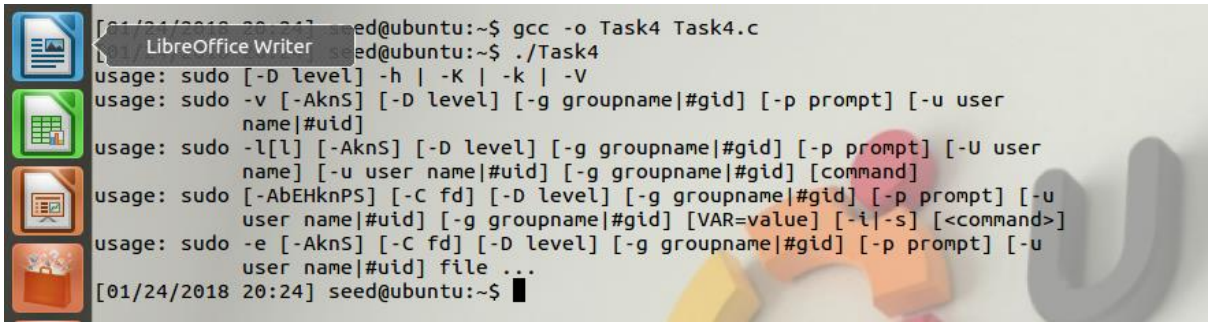
First I compiled and run the program with **system("/usr/bin/env");**



```
[01/24/2018 20:16] seed@ubuntu:~$ gcc -o Task4 Task4.c
[01/24/2018 20:17] seed@ubuntu:~$ ./Task4
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=2657
USER=seed
SSH_AGENT_PID=2721
SHLVL=1
HOME=/home/seed
XDG_SESSION_COOKIE=6da3e071019f67095bc4c5e900000002-1516850415.316870-726398189
DESKTOP_SESSION=ubuntu-2d
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-Ve4DAYr0LT,guid=df493930d26f030f
0486c9db0000003e
COLORTERM=gnome-terminal
GNOME_KEYRING_CONTROL=/tmp/keyring-GkpH7w
UBUNTU_MENUPROXY=libappmenu.so
MANDATORY_PATH=/usr/share/gconf/ubuntu-2d.mandatory.path
LOGNAME=seed
WINDOWID=58720261
_=./Task4
DEFAULTS_PATH=/usr/share/gconf/ubuntu-2d.default.path
TERM=xterm
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
PATH=.:/usr/lib/lightdm/lightdm:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
:/sbin:/bin:/usr/games
SESSION_MANAGER=local/ubuntu:@/tmp/.ICE-unix/2668,unix/ubuntu:/tmp/.ICE-unix/2668
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
DISPLAY=:0
LANG=en_US.UTF-8
XDG_CURRENT_DESKTOP=Unity
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: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:*.arj=01;31:*.taz=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz
=01;31:*.txz=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lz=01;
31:*.xz=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:*.ace
=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.jpg=01;35:*.jpeg=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;3
```

Fig 8: Output of system("/usr/bin/env");

Then I changed the command in system function to "**sudo**" which is shell command. Interestingly I was able to run the command.



```
LibreOffice Writer
[01/24/2018 20:24] seed@ubuntu:~$ gcc -o Task4 Task4.c
[01/24/2018 20:24] seed@ubuntu:~$ ./Task4
usage: sudo [-D level] -h | -K | -k | -V
usage: sudo -v [-AknS] [-D level] [-g groupname|#gid] [-p prompt] [-u user
            name|#uid]
usage: sudo -l[l] [-AknS] [-D level] [-g groupname|#gid] [-p prompt] [-U user
            name] [-u user name|#uid] [-g groupname|#gid] [command]
usage: sudo [-AbEHknPS] [-C fd] [-D level] [-g groupname|#gid] [-p prompt] [-u
            user name|#uid] [-g groupname|#gid] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-C fd] [-D level] [-g groupname|#gid] [-p prompt] [-u
            user name|#uid] file ...
[01/24/2018 20:24] seed@ubuntu:~$
```

Fig 9: Output of system("sudo")

The reason for this command to get processed is that system() executes a command specified in the function by calling **/bin/sh –c <u>command</u>**

Task 5: Environment variable and Set-UID Programs

In this task we are going through inheritance of environment variables by the process of SETUID program.

I complied the program and changed the ownership to root and set the UID.

```
[01/25/2018 09:56] seed@ubuntu:~$ gcc -o Task5 Task5.c
[01/25/2018 09:57] seed@ubuntu:~$ sudo chown root Task5
[sudo] password for seed:
[01/25/2018 09:57] seed@ubuntu:~$ chmod u+s Task5
chmod: changing permissions of `Task5': Operation not permitted
[01/25/2018 09:58] seed@ubuntu:~$ sudo chmod u+s Task5
[01/25/2018 09:59] seed@ubuntu:~$ ls -l
total 9944
-rw-rw-r--  1 seed seed    2627 Jan 24 19:39 child
drwxr-xr-x  4 seed seed    4096 Dec  9  2015 Desktop
drwxr-xr-x  3 seed seed    4096 Dec  9  2015 Documents
drwxr-xr-x  2 seed seed    4096 Sep 17  2014 Downloads
drwxrwxr-x  6 seed seed    4096 Sep 16  2014 elggData
-rw-r--r--  1 seed seed    8445 Aug 13  2013 examples.desktop
-rw-rw-r--  1 seed seed     341 Jan 21 19:11 hello.c~
drwxr-xr-x  5 root root    4096 Jan 18 20:02 john-1.8.0
-rw-r--r--  1 root root 5450412 May 29  2013 john-1.8.0.tar.gz
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Music
-rw-rw-r--  1 seed seed     181 Jan 21 20:44 new.c~
drwxr-xr-x 24 root root    4096 Jan  9  2014 openssl-1.0.1
-rw-r--r--  1 root root  132483 Jan  9  2014 openssl_1.0.1-4ubuntu5.11.debian.tar
.gz
-rw-r--r--  1 root root 4453920 Mar 22  2012 openssl_1.0.1.orig.tar.gz
drwxr-xr-x  2 seed seed    4096 Jan 24 20:29 Pictures
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Public
-rwxrwxr-x  1 seed seed    7328 Jan 24 20:01 Task1
-rw-rw-r--  1 seed seed     341 Jan 24 20:00 Task1.c
-rw-rw-r--  1 seed seed     341 Jan 24 19:59 Task1.c~
-rw-rw-r--  1 seed seed    2627 Jan 24 19:59 Task1.child
-rw-rw-r--  1 seed seed    2627 Jan 24 20:01 Task1.parent
-rwxrwxr-x  1 seed seed    7233 Jan 24 20:29 Task3
-rw-rw-r--  1 seed seed     184 Jan 24 20:29 Task3.c
-rw-rw-r--  1 seed seed     174 Jan 24 20:28 Task3.c~
-rwxrwxr-x  1 seed seed    7161 Jan 24 20:24 Task4
-rw-rw-r--  1 seed seed      81 Jan 24 20:24 Task4.c
-rw-rw-r--  1 seed seed      89 Jan 24 20:16 Task4.c~
-rwsrwxr-x  1 root seed    7231 Jan 25 09:57 Task5
-rw-rw-r--  1 seed seed     153 Jan 25 09:55 Task5.c
drwxr-xr-x  2 seed seed    4096 Aug 13  2013 Templates
-rw-rw-r--  1 seed seed       0 Jan 24 19:29 Untitled Document
```

Fig 9: Changing ownership and setting UID

Then I created few environment variables and run the program.

```
[01/25/2018 10:07] seed@ubuntu:~$ export PATH=/home/seed:$PATH
[01/25/2018 10:09] seed@ubuntu:~$ export LD_LIBRARY_PATH=/usr/local/lib
[01/25/2018 10:14] seed@ubuntu:~$ export Task5=/home/seed
[01/25/2018 10:15] seed@ubuntu:~$
[01/25/2018 10:15] seed@ubuntu:~$
[01/25/2018 10:15] seed@ubuntu:~$ ./Task5
Task5=/home/seed
SSH_AGENT_PID=2721
GPG_AGENT_INFO=/tmp/keyring-GkpH7w/gpg:0:1
TERM=xterm
SHELL=/bin/bash
XDG_SESSION_COOKIE=6da3e071019f67095bc4c5e900000002-1516850415.316870-726398189
WINDOWID=44040197
GNOME_KEYRING_CONTROL=/tmp/keyring-GkpH7w
USER=seed
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: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:*.arj=01;31:*.taz=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz
=01;31:*.txz=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lz=01;
31:*.xz=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:*.ace
=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.jpg=01;35:*.jpeg=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;3
5:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=0
1;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:*.axv=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.a
ac=00;36:*.au=00;36:*.flac=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:*.axa=00;36:*.oga=00;36:*.spx=00;
36:*.xspf=00;36:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/tmp/keyring-GkpH7w/ssh
SESSION_MANAGER=local/ubuntu:@/tmp/.ICE-unix/2668,unix/ubuntu:/tmp/.ICE-unix/2668
DEFAULTS_PATH=/usr/share/gconf/ubuntu-2d.default.path
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu-2d:/etc/xdg
PATH=/home/seed:.:/usr/lib/lightdm/lightdm:/usr/local/sbin:/usr/local/bin:/usr/sb
in:/usr/bin:/sbin:/bin:/usr/games
DESKTOP_SESSION=ubuntu-2d
```

Fig 10: After creating env variables.

Here we can see that two of the variable we exported are in the output file. (Task5=/home/seed, PATH=/home/seed). The LD_LIBRARY_PATH=/usr/local/lib variable is not present. This is because when we type the program name in the shell a child process is invoked and this child process runs the program. The LD_LIBRARY_PATH variable is not inherited by the child process from the parent shell process because of the security.

The LD_LIBRARY_PATH cannot be used with setuid. This is a security feature in linux. To confirm this I recompiled the program and ran it without making it a setuid root program and I was able to get all the env variables I set.

```
[01/25/2018 10:16] seed@ubuntu:~$ gcc -o Task5 Task5.c
[01/25/2018 10:17] seed@ubuntu:~$ ./Task5
Task5=/home/seed
SSH_AGENT_PID=2721
GPG_AGENT_INFO=/tmp/keyring-GkpH7w/gpg:0:1
TERM=xterm
SHELL=/bin/bash
XDG_SESSION_COOKIE=6da3e071019f67095bc4c5e900000002-1516850415.316870-726398189
WINDOWID=44040197
GNOME_KEYRING_CONTROL=/tmp/keyring-GkpH7w
USER=seed
LD_LIBRARY_PATH=/usr/local/lib
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: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:*.arj=01;31:*.taz=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz
=01;31:*.txz=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lz=01;
31:*.xz=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:*.ace
=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.jpg=01;35:*.jpeg=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;3
5:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=0
1;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:*.axv=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.a
ac=00;36:*.au=00;36:*.flac=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:*.axa=00;36:*.oga=00;36:*.spx=00;
36:*.xspf=00;36:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/tmp/keyring-GkpH7w/ssh
SESSION_MANAGER=local/ubuntu:@/tmp/.ICE-unix/2668,unix/ubuntu:/tmp/.ICE-unix/2668
DEFAULTS_PATH=/usr/share/gconf/ubuntu-2d.default.path
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu-2d:/etc/xdg
PATH=/home/seed:.:/usr/lib/lightdm/lightdm:/usr/local/sbin:/usr/local/bin:/usr/sb
in:/usr/bin:/sbin:/bin:/usr/games
DESKTOP_SESSION=ubuntu-2d
PWD=/home/seed
GNOME_KEYRING_PID=2657
LANG=en_US.UTF-8
```

Fig 11: Program without the SETUID.

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

Compiled the program, and changed its owner to root, and made it a Set-UID program.

```
[01/25/2018 11:06] seed@ubuntu:~$ sudo chown root Task6
[sudo] password for seed:
[01/25/2018 11:07] seed@ubuntu:~$ sudo chmod u+s Task6
[01/25/2018 11:08] seed@ubuntu:~$ ./Task6
child               openssl_1.0.1-4ubuntu5.11.debian.tar.gz  Task4
Desktop             openssl_1.0.1.orig.tar.gz                Task4.c
Documents           Pictures                                 Task4.c~
Downloads           Public                                   Task5
elggData            Task1                                    Task5.c
examples.desktop    Task1.c                                  Task6
hello.c~            Task1.c~                                 Task6.c
john-1.8.0          Task1.child                              Task6.c~
john-1.8.0.tar.gz   Task1.parent                             Templates
Music               Task3                                    Untitled Document
new.c~              Task3.c                                  Untitled Document~
openssl-1.0.1       Task3.c~                                 Videos
```

Fig 12: Output of system("ls")

I was able to run this setuid program instead of running the command /bin/ls. The code was not running with root privilege. The reason I was able to get the output of /bin/ls using "ls" is that the system() executes /bin/sh –c first and then execute the command. So the command was run in the shell.

Task 7: The LD PRELOAD environment variable and Set-UID Programs

In this task we are studying how the SETUID program deals with the LD_PRELOAD environment variable.

Following step 1, I compiled the program and created the LD_PRELOAD variable.

Given below are my observations on different setups:

• Make Task7 a regular program, and run it as a normal user.

```
[01/26/2018 08:23] seed@ubuntu:~$ gcc -fPIC -g -c mylib.c
[01/26/2018 08:27] seed@ubuntu:~$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[01/26/2018 08:28] seed@ubuntu:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[01/26/2018 08:29] seed@ubuntu:~$ gcc -o Task7 Task7.c
[01/26/2018 08:33] seed@ubuntu:~$
[01/26/2018 08:33] seed@ubuntu:~$
[01/26/2018 08:33] seed@ubuntu:~$ ./Task7
I am not sleeping!
[01/26/2018 08:33] seed@ubuntu:~$
```

Fig 12: Task7 as a regular program

"Task7" program was able to load and link "mylib.o ", using the dynamic loader/linker.

• Make Task7 a Set-UID root program, and run it as a normal user.

```
[01/26/2018 08:33] seed@ubuntu:~$
[01/26/2018 08:33] seed@ubuntu:~$ sudo chown root Task7
[sudo] password for seed:
[01/26/2018 08:34] seed@ubuntu:~$ sudo chmod u+s Task7
[01/26/2018 08:34] seed@ubuntu:~$
[01/26/2018 08:34] seed@ubuntu:~$ ./Task7
[01/26/2018 08:34] seed@ubuntu:~$
[01/26/2018 08:34] seed@ubuntu:~$
```

Fig 13: Task7 as a SETUID root program

The program didn't give any output, as it is run as s SETUID root program.

• Make Task7 a Set-UID root program, export the LD PRELOAD environment variable again in the root account and run it

```
[01/26/2018 08:38] seed@ubuntu:~$
[01/26/2018 08:38] seed@ubuntu:~$ su
Password:
[01/26/2018 08:38] root@ubuntu:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
[01/26/2018 08:39] root@ubuntu:/home/seed# exit
exit
[01/26/2018 08:39] seed@ubuntu:~$ ./Task7
[01/26/2018 08:39] seed@ubuntu:~$
[01/26/2018 08:40] seed@ubuntu:~$
[01/26/2018 08:40] seed@ubuntu:~$ su
Password:
[01/26/2018 08:40] root@ubuntu:/home/seed# ./Task7
[01/26/2018 08:40] root@ubuntu:/home/seed# env
```

Fig 13: Task7 after exporting LD_PRELOAD in root.

The program didn't give any output even after exporting LD_PRELOAD in root.

• Make task7 a Set-UID user1 program (i.e., the owner is user1, which is another user account), export the LD PRELOAD environment variable again in a different user's account (not-root user) and run it.

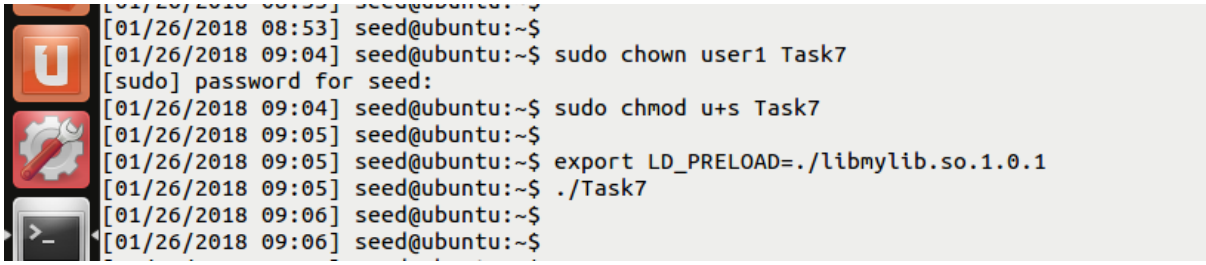


Fig 14: Task7 as a SETUID user1 program.

The program didn't give any output.

The reason for the different behaviors is because LD_PRELOAD cannot be used with setuid. This is a security feature in linux. Since function interposition lets you make a program do almost anything you want it to, Linux prevents you from modifying the behavior of a program running on behalf of another user or group. Also the The LD* variables are not inherited by the child process from the parent shell process because of the security.

A similar experiment we did in Task5,where the LD_LIBRARY_PATH was not inherited as the program was run as a SETUID root program.

Task 8: Invoking external programs using system() versus execve()

This task helps as to understand the benefits of using execve() over system().

Compiled the given program, made root its owner, and changed it to a Set-UID program. This program uses the system() to invoke the commands.

Fig 15: Running of program with system() and exploiting the vulnerability

Here I made a test file “Task8test”. When running the program I provided the filename and the content was printed. Next time I run the program, along with the filename I added the shell command ls – **./Task8 “Task8test; ls”.** This made the program to print the test file and also the list of files. After that I tried to remove file “Task6” which is a root file. I did this using the command **./Task8 “Task8test; rm Task6”.** I was able to delete a root file without having the access to root.

To check the working of execve() , changed the system() command with execve() and the compiled the program.

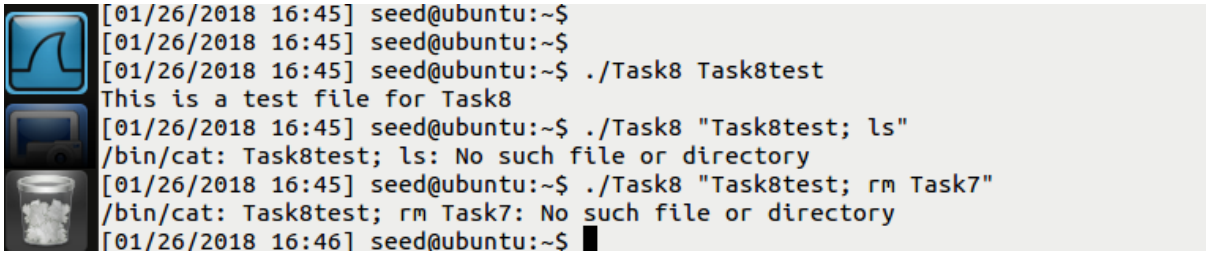


Fig 16: program with execve()

Here I was not able to perform any activity that used the shell command. I was just able to print the test file.

The reason for the above observation is that system() executes a command specified in the function by calling /bin/sh –c command. This will invoke the shell. But execve() does not invoke the shell and directly execute the command.

Task 9: Capability Leaking

This task is for testing the capability leaking vulnerability. When revoking the privilege, one of the common mistakes is capability leaking. The process may have gained some privileged capabilities when it was still privileged; when the privileged is downgraded, if the program does not clean up those capabilities, they may still be accessible by the non-privileged process. In other words, although the effective user ID of the process becomes non-privileged, the process is still privileged because it possesses privileged capabilities.

Created a test file /etc/zzz.txt with permission 0644.

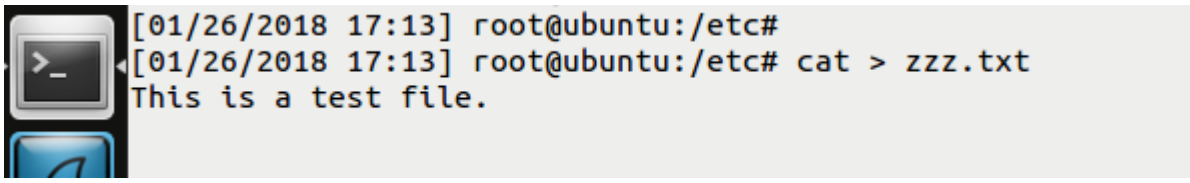


Fig 17: Test file /etc/zzz.txt

Compiled the given program and changed its owner to root, and made it a Set-UID program. This program will open the file and using the capability leaking vulnerability, it will edit the file.

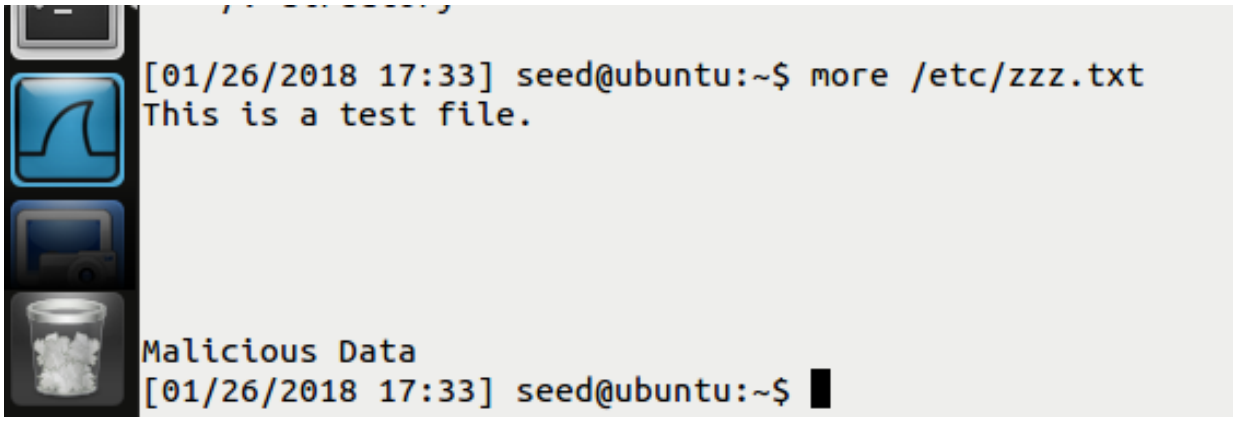


Fig 18: Edited file after running the program.