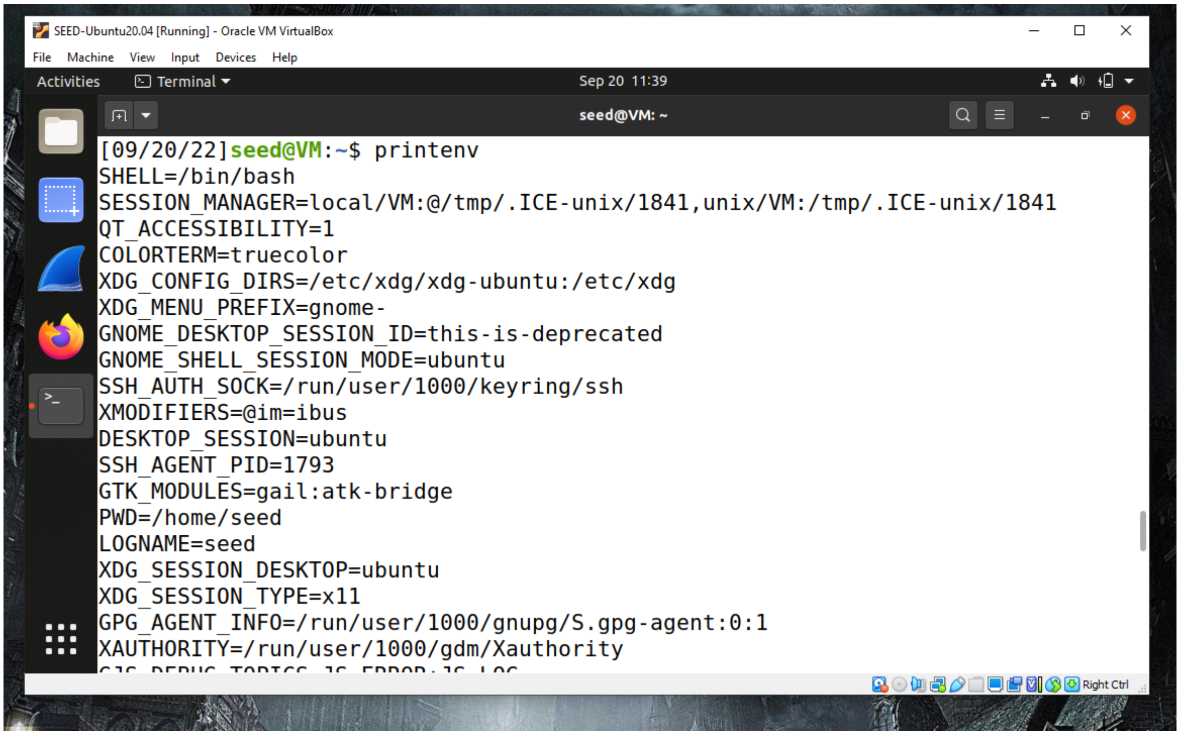
[redacted]

Environment Variable and Set-UID Program Lab

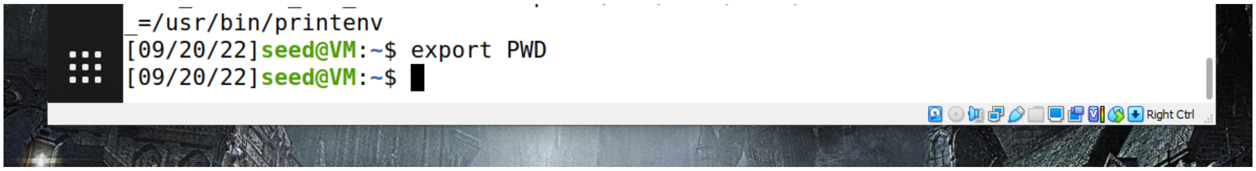
Overview — The purpose of this lab is to understand, and be able to control environment variables to affect program and system behaviors. This also aided in describing the vulnerabilities that can be exploited by abusing environment variables.

Task 1 — Manipulating Environment Variables

In this task, we study the commands that can be used to set and unset environment variables.



```
[09/20/22]seed@VM:~$ printenv
SHELL=/bin/bash
SESSION_MANAGER=local/VM:@/tmp/.ICE-unix/1841,unix/VM:/tmp/.ICE-unix/1841
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=1793
GTK_MODULES=gail:atk-bridge
PWD=/home/seed
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
```

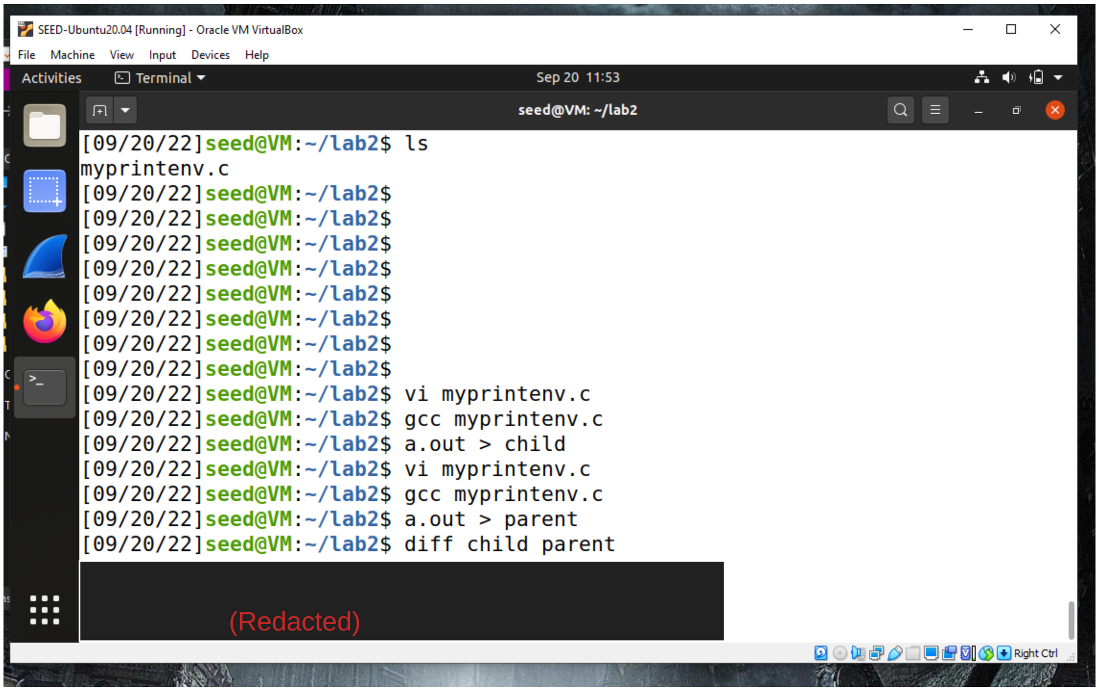


```
_=/usr/bin/printenv
[09/20/22]seed@VM:~$ export PWD
[09/20/22]seed@VM:~$ 
```

Observation(s) and conclusion — Environment variables are readily viewable by any user and can be set using $ export.

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

In this task, we study how a child process gets its environment variables from its parent.


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Sep 20 11:53
seed@VM: ~/lab2
Right Ctrl

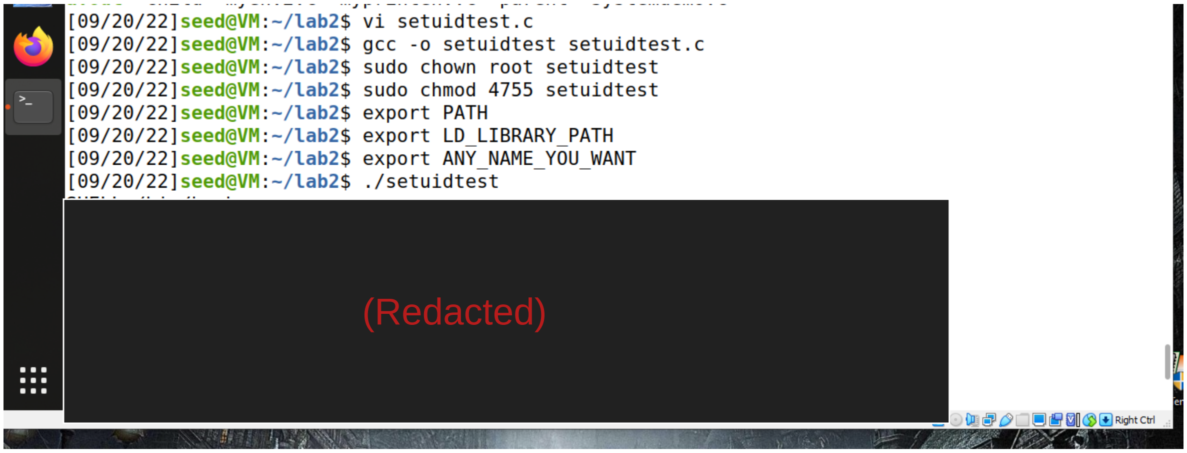
```
[09/20/22]seed@VM:~/lab2$ ls
myprintenv.c
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$ vi myprintenv.c
[09/20/22]seed@VM:~/lab2$ gcc myprintenv.c
[09/20/22]seed@VM:~/lab2$ a.out > child
[09/20/22]seed@VM:~/lab2$ vi myprintenv.c
[09/20/22]seed@VM:~/lab2$ gcc myprintenv.c
[09/20/22]seed@VM:~/lab2$ a.out > parent
[09/20/22]seed@VM:~/lab2$ diff child parent
```

(Redacted)

Observation(s) and conclusion —

(Redacted)

Task 3 — Environment Variable and Set-UID Programs



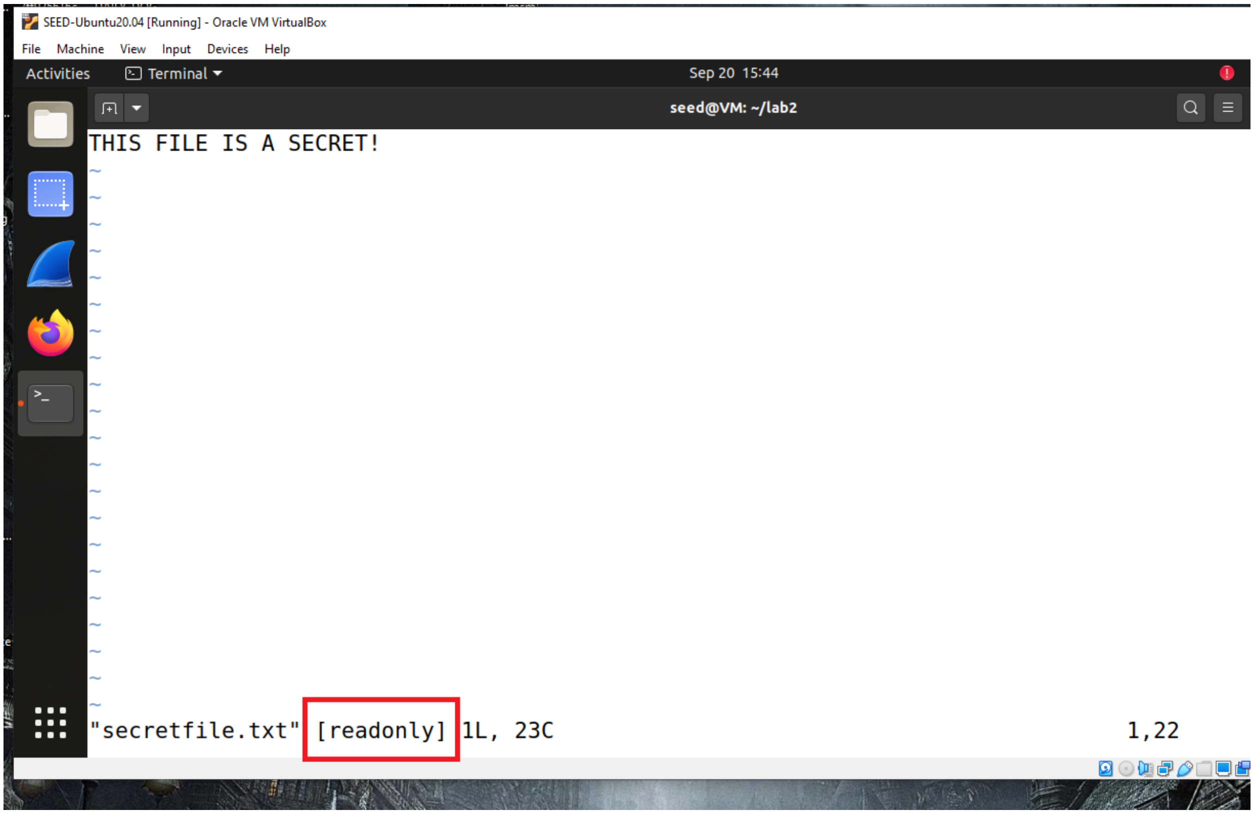
```
[09/20/22]seed@VM:~/lab2$ vi setuidtest.c
[09/20/22]seed@VM:~/lab2$ gcc -o setuidtest setuidtest.c
[09/20/22]seed@VM:~/lab2$ sudo chown root setuidtest
[09/20/22]seed@VM:~/lab2$ sudo chmod 4755 setuidtest
[09/20/22]seed@VM:~/lab2$ export PATH
[09/20/22]seed@VM:~/lab2$ export LD_LIBRARY_PATH
[09/20/22]seed@VM:~/lab2$ export ANY_NAME_YOU_WANT
[09/20/22]seed@VM:~/lab2$ ./setuidtest
```

(Redacted)

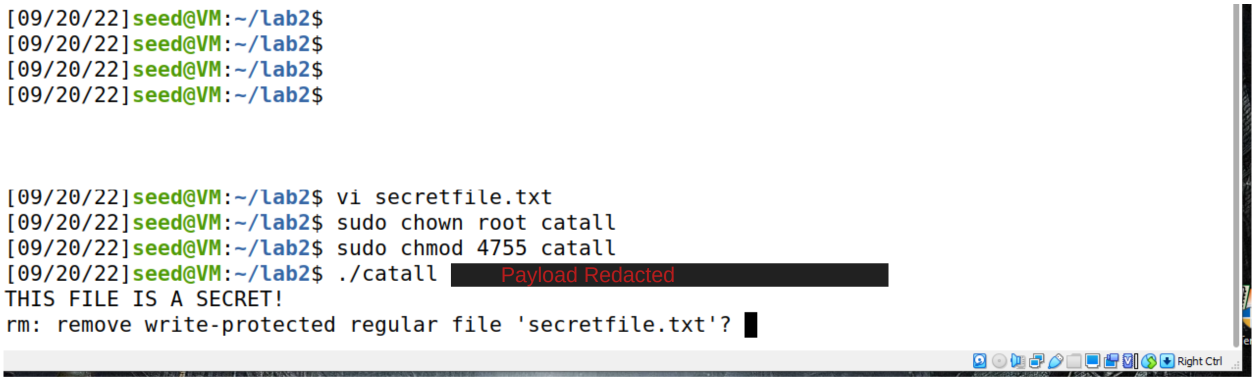
Observation(s) and conclusion — [redacted]

(Redacted)

Task 4 - Exploiting the Audit Set-UID Program


SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Sep 20 15:44
seed@VM: ~/lab2

```
THIS FILE IS A SECRET!
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"secretfile.txt" [readonly] 1L, 23C                                   1,22
```



```
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$
[09/20/22]seed@VM:~/lab2$



[09/20/22]seed@VM:~/lab2$ vi secretfile.txt
[09/20/22]seed@VM:~/lab2$ sudo chown root catall
[09/20/22]seed@VM:~/lab2$ sudo chmod 4755 catall
[09/20/22]seed@VM:~/lab2$ ./catall     Payload Redacted
THIS FILE IS A SECRET!
rm: remove write-protected regular file 'secretfile.txt'?
```

Observation(s) and conclusion — [redacted]

(Redacted, but here is where they explain how they exploited the program and got a file to be deleted)