Task 1:

Env:

```
[09/01/20]seed@VM:~$ env
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
TERMINATOR_UUID=urn:uuid:16b50cad-a319-45c5-bd71-34571217ba5a
IBUS_DISABLE_SNOOPER=1
CLUTTER_IM_MODULE=xim
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
LD_PRELOAD=/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/li
b/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.
64.0
WINDOWID=25165828
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1484
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
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:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;4
4:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;
31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7
z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=0
1;31:*.lzo=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:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;3
1:*.cab=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=0
1;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:*.o
gv=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=0
0;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
QT_ACCESSIBILITY=1
```

PWD:

```
[09/01/20]seed@VM:~$ env | grep PWD
PWD=/home/seed
```

Export unset:

```
[09/01/20]seed@VM:~$ export hbw=0325
[09/01/20]seed@VM:~$ env | grep hbw
hbw=0325
[09/01/20]seed@VM:~$ unset hbw
[09/01/20]seed@VM:~$ env | grep hbw
```

Task 2:

父进程与子进程环境变量没有区别：

```
[09/01/20]seed@VM:~$ gcc test.c && a.out > child
[09/01/20]seed@VM:~$ vim test.c
[09/01/20]seed@VM:~$ gcc test.c && a.out > child
[09/01/20]seed@VM:~$ vim test.c
[09/01/20]seed@VM:~$ gcc test.c && a.out > parent
[09/01/20]seed@VM:~$ diff parent child
[09/01/20]seed@VM:~$
```

说明子进程自动继承了父进程的环境变量。

Task 3:

```
[09/01/20]seed@VM:~$ gcc test.c && a.out>env1
test.c: In function ‘main’:
test.c:9:5: warning: implicit declaration of function ‘execve’ [-Wimplicit-funct
ion-declaration]
     execve("/usr/bin/env", argv, NULL);
     ^
[09/01/20]seed@VM:~$ vim test.c
[09/01/20]seed@VM:~$ gcc test.c && a.out>env2
test.c: In function ‘main’:
test.c:9:5: warning: implicit declaration of function ‘execve’ [-Wimplicit-funct
ion-declaration]
     execve("/usr/bin/env", argv, environ);
     ^
[09/01/20]seed@VM:~$ diff env1 env2
0a1,71
> XDG_VTNR=7
> ORBIT_SOCKETDIR=/tmp/orbit-seed
> XDG_SESSION_ID=c1
```

两个环境变量的值完全不相同，execve 的第三个参数为 NULL 时，环境变量也为空，只有指定 environ 时才会完全继承该进程的环境变量。

Task 4:

```
[09/01/20]seed@VM:~$ vim test.c
[09/01/20]seed@VM:~$ gcc test.c && a.out | sort > env1
test.c: In function ‘main’:
test.c:9:5: warning: implicit declaration of function ‘execve’ [-Wimplicit-funct
ion-declaration]
     execve("/usr/bin/env", argv, environ);
     ^
[09/01/20]seed@VM:~$ vim test.c
[09/01/20]seed@VM:~$ gcc test.c && a.out | sort > env2
[09/01/20]seed@VM:~$ diff env1 env2
[09/01/20]seed@VM:~$
```

两个环境变量的值完全相同

Task 5:

```
[09/01/20]seed@VM:~$ echo $PATH
/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr
/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/
java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/andro
id-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/see
d/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
[09/01/20]seed@VM:~$ a.out | grep PATH=/home
PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib
/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/
android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/hom
e/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
```

PATH 相同

```
[09/01/20]seed@VM:~$ echo $LD_LIBRARY_PATH
/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/li
b:
[09/01/20]seed@VM:~$ a.out | grep LD_LIBRARY_PATH
```

子进程没有继承 LD_LIBRARY_PATH 环境变量

```
[09/01/20]seed@VM:~$ echo $bwhe
0325
[09/01/20]seed@VM:~$ a.out | grep bwhe
bwhe=0325
```

继承了自定义环境变量 bwhe

Task 6:

```
[09/01/20]seed@VM:~$ vim ls.c
[09/01/20]seed@VM:~$ gcc ls.c -o ls
[09/01/20]seed@VM:~$ vim test.c
[09/01/20]seed@VM:~$ gcc test.c
test.c: In function ‘main’:
test.c:3:5: warning: implicit declaration of function ‘system’ [-Wimplicit-funct
ion-declaration]
     system("ls");
     ^
[09/01/20]seed@VM:~$ a.out
hello world[09/01/20]seed@VM:~$
```

成功让 ls 变成输出”hello world”

Task 7:

```
[09/01/20]seed@VM:~$ vim mylib.c
[09/01/20]seed@VM:~$ gcc -fPIC -g -c mylib.c
[09/01/20]seed@VM:~$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[09/01/20]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~$ vim myprog.c
[09/01/20]seed@VM:~$ gcc my
mylib.c   mylib.o   myprog.c
[09/01/20]seed@VM:~$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:4:5: warning: implicit declaration of function 'sleep' [-Wimplicit-func
tion-declaration]
     sleep(1);
     ^
[09/01/20]seed@VM:~$ ./myprog
I am not sleeping!
[09/01/20]seed@VM:~$ sudo chown root myprog
[09/01/20]seed@VM:~$ sudo chmod 4755 myprog
[09/01/20]seed@VM:~$ ./myprog
```

Make myprog a regular program, and run it as a normal user:

说明目录修改成功

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

说明超级用户权限下的目录并未得到修改

```
[09/01/20]seed@VM:~$ su
Password:
root@VM:/home/seed# echo $LD_PRELOAD
/home/seed/lib/boost/libboost_program_options.so.1.64.0:/home/seed/lib/boost/lib
boost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# echo $LD_PRELOAD
./libmylib.so.1.0.1
root@VM:/home/seed# ./myprog
I am not sleeping!
```

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

说明超级用户权限下的目录已经修改成功

```
[09/01/20]seed@VM:~$ sudo chown user1 myprog
[09/01/20]seed@VM:~$ sudo chmod 4755 myprog
[09/01/20]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~$ ./myprog
[09/01/20]seed@VM:~$
```

说明 user1 用户下的对应目录没有被修改

设置 test.c 文件生成 a.out 来输出环境变量

```
[09/01/20]seed@VM:~$ sudo chown seed myprog
[09/01/20]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~$ a.out | grep LD_PRELOAD
LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~$
```

Make myprog a regular program, and run it as a normal user:

说明在 seed 用户中对应目录修改成功

```
[09/01/20]seed@VM:~$ sudo ./a.out | grep LD_PRELOAD
[09/01/20]seed@VM:~$
```

说明超级用户下对应的目录没有受到修改

说明只有在修改了指定目录的用户权限下运行该程序才能修改 sleep 函数。

Task 8:

```
[09/02/20]seed@VM:~/lab$ echo 1 > a
[09/02/20]seed@VM:~/lab$ ls
a  a.out  Bobfile.c  rm  rm.c  test
[09/02/20]seed@VM:~/lab$ a.out "aa;rm a;ls"
/bin/cat: aa: No such file or directory
a.out  Bobfile.c  rm  rm.c  test
[09/02/20]seed@VM:~/lab$
```

其中 a.out 是编译后生成的可执行文件，看到通过分号直接删除了文件 a，实现了删除文件的权限。

```
[09/02/20]seed@VM:~/lab$ vim Bobfile.c
[09/02/20]seed@VM:~/lab$ gcc Bobfile.c
Bobfile.c: In function ‘main’:
Bobfile.c:18:5: warning: implicit declaration of function ‘execve’ [-Wimplicit-f
unction-declaration]
     execve(v[0], v, NULL);
     ^
[09/02/20]seed@VM:~/lab$ a.out "aa;rm test"
/bin/cat: 'aa;rm test': No such file or directory
```

Execve 会将参数作为整个指令的参数，所以会直接显示没有这个文件。

Task 9:

```
[09/02/20]seed@VM:~/lab$ sudo chown root test
[09/02/20]seed@VM:~/lab$ sudo chmod 4755 test
[09/02/20]seed@VM:~/lab$ ./test
Cannot open /etc/zzz
[09/02/20]seed@VM:~/lab$ ll
total 24
-rwxrwxr-x 1 seed seed 7328 Sep  2 20:26 a.out
-rw-rw-r-- 1 seed seed  479 Sep  2 11:02 Bobfile.c
-rwsr-xr-x 1 root seed 7640 Sep  2 21:48 test
-rw-rw-r-- 1 seed seed 1061 Sep  2 21:48 test.c
[09/02/20]seed@VM:~/lab$ vim test.c
[09/02/20]seed@VM:~/lab$ ./test
[09/02/20]seed@VM:~/lab$ cat /etc/zzz
Malicious Data
```

由于在 setuid 之前用户没有关闭文件描述符 fd，导致用户在降级之后仍然有权限将相关内容写入/etc/zzz

学号：57117127
姓名：贺博文