Task1:

1)

```
/bin/bash
/bin/bash 80x24
e[09/09/19]seed@VM:~$ env
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:3992a4e4-96aa-4f54-ac9c-2675366c491a
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2753
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
XDG_MENU_PREFIX=gnome-
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=14680068
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1499
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
```

2)

```
[09/09/19]seed@VM:~$ export
declare -x ANDROID_HOME="/home/seed/android/android-sdk-linux"
declare -x CLUTTER_IM_MODULE="xim"
declare -x COLORTERM="gnome-terminal"
declare -x COMPIZ_BIN_PATH="/usr/bin/"
declare -x COMPIZ_CONFIG_PROFILE="ubuntu-lowgfx"
declare -x DBUS_SESSION_BUS_ADDRESS="unix:abstract=/tmp/dbus-6IIjZB9jor"
declare -x DEFAULTS_PATH="/usr/share/gconf/ubuntu.default.path"
declare -x DERBY_HOME="/usr/lib/jvm/java-8-oracle/db"
declare -x DESKTOP_SESSION="ubuntu"
declare -x DISPLAY=":0"
declare -x GDMSESSION="ubuntu"
declare -x GDM_LANG="en_US"
declare -x GIO_LAUNCHED_DESKTOP_FILE="/usr/share/applications/terminator.desktop
"
declare -x GIO_LAUNCHED_DESKTOP_FILE_PID="2753"
declare -x GNOME_DESKTOP_SESSION_ID="this-is-deprecated"
declare -x GNOME_KEYRING_CONTROL=""
declare -x GNOME_KEYRING_PID=""
declare -x GPG_AGENT_INFO="/home/seed/.gnupg/S.gpg-agent:0:1"
declare -x GTK2_MODULES="overlay-scrollbar"
declare -x GTK_IM_MODULE="ibus"
declare -x GTK_MODULES="gail:atk-bridge:unity-gtk-module"
declare -x HOME="/home/seed"
```

/bin/bash

/bin/bash 80x24

```
declare -x UPSTART_EVENTS="xsession started"
declare -x UPSTART_INSTANCE=""
declare -x UPSTART_JOB="unity7"
declare -x UPSTART_SESSION="unix:abstract=/com/ubuntu/upstart-session/1000/1499"
declare -x USER="seed"
declare -x WINDOWID="14680068"
declare -x XAUTHORITY="/home/seed/.Xauthority"
declare -x XDG_CONFIG_DIRS="/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg"
declare -x XDG_CURRENT_DESKTOP="Unity"
declare -x XDG_DATA_DIRS="/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/
usr/share/:/var/lib/snapd/desktop"
declare -x XDG_GREETER_DATA_DIR="/var/lib/lightdm-data/seed"
declare -x XDG_MENU_PREFIX="gnome-"
declare -x XDG_RUNTIME_DIR="/run/user/1000"
declare -x XDG_SEAT="seat0"
declare -x XDG_SEAT_PATH="/org/freedesktop/DisplayManager/Seat0"
declare -x XDG_SESSION_DESKTOP="ubuntu"
declare -x XDG_SESSION_ID="c1"
declare -x XDG_SESSION_PATH="/org/freedesktop/DisplayManager/Session0"
declare -x XDG_SESSION_TYPE="x11"
declare -x XDG_VTNR="7"
declare -x XMODIFIERS="@im=ibus"
[09/09/19]seed@VM:~$ unset
[09/09/19]seed@VM:~$
```

Task2:

```
[09/09/19]seed@VM:~$ gcc task2.c -o task2
[09/09/19]seed@VM:~$ task2 > child
[09/09/19]seed@VM:~$ gcc task2.c -o task2
[09/09/19]seed@VM:~$ task2 > parent
[09/09/19]seed@VM:~$ diff child parent
[09/09/19]seed@VM:~$
```

parent × | task2.c × | child

```
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:3992a4e4-96aa-4f54-ac9c-2675366c491a
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2753
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
XDG_MENU_PREFIX=gnome-
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/lib/boost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
WINDOWID=14680068
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1499
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;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;
QT_ACCESSIBILITY=1
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
DESKTOP_SESSION=ubuntu
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:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
QT_IM_MODULE=ibus
QT_QPA_PLATFORMTHEME=appmenu-qt5
XDG_SESSION_TYPE=x11
PWD=/home/seed
JOB=unity-settings-daemon
XMODIFIERS=@im=ibus
JAVA_HOME=/usr/lib/jvm/java-8-oracle
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
GDM_LANG=en_US
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
```

Parent's environment variables are inherited by the child process.

Task3:

```
task3
#include <stdio.h>
#include <stdlib.h>

extern char **environ;

int main() {
        char *argv[2];
        argv[0] = "/usr/bin/env";
        argv[1] = NULL;
        //execve("/usr/bin/env", argv, NULL);
        execve("/usr/bin/env", argv, environ);
        return 0;
}
```

```
[09/09/19]seed@VM:~$ gcc task3.c -o task3
task3.c: In function 'main':
task3.c:10:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve("/usr/bin/env", argv, NULL);
  ^
[09/09/19]seed@VM:~$ task3 > res1
[09/09/19]seed@VM:~$ gcc task3.c -o task3
task3.c: In function 'main':
task3.c:11:2: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  execve("/usr/bin/env", argv, environ);
  ^
[09/09/19]seed@VM:~$ task3 > res2
[09/09/19]seed@VM:~$ diff res1 res2
0a1,76
> XDG_VTNR=7
> ORBIT_SOCKETDIR=/tmp/orbit-seed
> XDG_SESSION_ID=c1
> XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
> IBUS_DISABLE_SNOOPER=1
> TERMINATOR_UUID=urn:uuid:3992a4e4-96aa-4f54-ac9c-2675366c491a
> CLUTTER_IM_MODULE=xim
> SESSION=ubuntu
> GIO_LAUNCHED_DESKTOP_FILE_PID=2753
> ANDROID_HOME=/home/seed/android/android-sdk-linux
> GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
> TERM=xterm
```

The new program environment variable is empty, the old program has lots of environment variable They are not inherited by new program.

Task4:

```c
#include <stdio.h>
#include <stdlib.h>

int main() {
        system("/usr/bin/env");
        return 0;
}
```

```
/bin/bash 82x40

[09/09/19]seed@VM:~$ gcc task4.c -o task4
[09/09/19]seed@VM:~$ ./task4
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
UPSTART_INSTANCE=
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
ORBIT_SOCKETDIR=/tmp/orbit-seed
LD_LIBRARY_PATH=/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_
_64_0/stage/lib:
SHLVL=1
LIBGL_ALWAYS_SOFTWARE=1
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
HOME=/home/seed
QT4_IM_MODULE=xim
DESKTOP_SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
GTK_MODULES=gail:atk-bridge:unity-gtk-module
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
INSTANCE=
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-6IIjZB9jor
GIO_LAUNCHED_DESKTOP_FILE_PID=2753
COLORTERM=gnome-terminal
GNOME_KEYRING_CONTROL=
QT_QPA_PLATFORMTHEME=appmenu-qt5
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
IM_CONFIG_PHASE=1
SESSIONTYPE=gnome-session
UPSTART_JOB=unity7
LOGNAME=seed
GTK_IM_MODULE=ibus
WINDOWID=14680068
 =./task4
```

Unlike command execve(), using system(), the environment variable of the calling process is passed to the new program /bin/sh

Task5:

1)

```c
#include <stdio.h>
#include <stdlib.h>

extern char **environ;

void main() {
        int i = 0;
        while (environ[i] != NULL) {
                printf("%s\n", environ[i]);
                i++;
        }
}
```

2)

```
[09/09/19]seed@VM:~$ gcc task5.c -o task5
[09/09/19]seed@VM:~$ sudo chown root task5
[09/09/19]seed@VM:~$ sudo chmod 4755 task5
```

3)

```
[09/09/19]seed@VM:~$ export PATH=/home/seed:$PATH
[09/09/19]seed@VM:~$ export LD_LIBRARY_PATH=/home/seed/source
[09/09/19]seed@VM:~$ export YI=TIANXIANG
[09/09/19]seed@VM:~$ export
declare -x ANDROID_HOME="/home/seed/android/android-sdk-linux"
declare -x CLUTTER_IM_MODULE="xim"
declare -x COLORTERM="gnome-terminal"
declare -x COMPIZ_BIN_PATH="/usr/bin/"
declare -x COMPIZ_CONFIG_PROFILE="ubuntu-lowgfx"
declare -x DBUS_SESSION_BUS_ADDRESS="unix:abstract=/tmp/dbus-6IIjZB9jor"
declare -x DEFAULTS_PATH="/usr/share/gconf/ubuntu.default.path"
declare -x DERBY_HOME="/usr/lib/jvm/java-8-oracle/db"
declare -x DESKTOP_SESSION="ubuntu"
declare -x DISPLAY=":0"
declare -x GDMSESSION="ubuntu"
declare -x GDM_LANG="en_US"
declare -x GIO_LAUNCHED_DESKTOP_FILE="/usr/share/applications/terminator.desktop
"
declare -x GIO_LAUNCHED_DESKTOP_FILE_PID="5817"
declare -x GNOME_DESKTOP_SESSION_ID="this-is-deprecated"
declare -x GNOME_KEYRING_CONTROL=""
declare -x GNOME_KEYRING_PID=""
declare -x GPG_AGENT_INFO="/home/seed/.gnupg/S.gpg-agent:0:1"
declare -x GTK2_MODULES="overlay-scrollbar"
```

After running program:

```
PATH=/home/seed:/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bi
:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/b
in:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/se
ed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform
-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin
```

Environment variable are passed from parent to child process.

Task6:

1)

```c
#include <stdio.h>
#include <stdlib.h>

extern char **environ;

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

2)

```
[09/09/19]seed@VM:~$ gcc task6.c -o task6
[09/09/19]seed@VM:~$ ./task6
android         Documents         lib       prog    source   task4    task6.c
bin             Downloads         Music     prog.c  task2    task4.c  Templates
child           examples.desktop  myfile    Public  task2.c  task5    Test
Customization   gcc               parent    res1    task3    task5.c  Videos
Desktop         get-pip.py        Pictures  res2    task3.c  task6
[09/09/19]seed@VM:~$ gcc ls.c -o ls
[09/09/19]seed@VM:~$ ./ls
hackerls[09/09/19]seed@VM:~$ gcc ls.c -o ls
```

```
[09/09/19]seed@VM:~$ sudo chown root task6
[09/09/19]seed@VM:~$ sudo chmod 4755 task6
```

```
[09/09/19]seed@VM:~$ export PATH=.:$PATH
```

```
[09/09/19]seed@VM:~$ ./task6
hackerls
[09/09/19]seed@VM:~$
```

Task7:

1)

Mylib.c:

```
#include <stdio.h>
void sleep(int s) {
        printf("I am not sleeping!\n");
}
```

Myprog.c:

```
#include<stdio.h>
int main() {
        sleep(1);
        return 0;
}
```

```
[09/09/19]seed@VM:~$ gcc -fPIC -g -c mylib.c
[09/09/19]seed@VM:~$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
[09/09/19]seed@VM:~$ export LD_PRELOAD=./libmylib.so.101
ERROR: ld.so: object './libmylib.so.101' from LD_PRELOAD cannot be preloaded (ca
nnot open shared object file): ignored.
[09/09/19]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/09/19]seed@VM:~$ gcc myprog.c -o myprog
myprog.c: In function 'main':
myprog.c:3:2: warning: implicit declaration of function 'sleep' [-Wimplicit-func
tion-declaration]
  sleep(1);
  ^
[09/09/19]seed@VM:~$
```

2)

```
[09/09/19]seed@VM:~$ ./myprog
I am not sleeping!
[09/09/19]seed@VM:~$ sudo chown myprog root
chown: invalid user: 'myprog'
[09/09/19]seed@VM:~$ sudo chown root myprog
[09/09/19]seed@VM:~$ sudo chmod 4755 myprog
[09/09/19]seed@VM:~$ ./myprog
[09/09/19]seed@VM:~$ ./myprog
[09/09/19]seed@VM:~$
```

```
[09/09/19]seed@VM:~$ su root
Password:
root@VM:/home/seed# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed# ./myprog
I am not sleeping!
root@VM:/home/seed#
```

```
[09/09/19]seed@VM:~$ sudo chown bob myprog
[09/09/19]seed@VM:~$ sudo chmod 4755 myprog
[09/09/19]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/09/19]seed@VM:~$ ./myprog
[09/09/19]seed@VM:~$
```

First not sleeping
Second sleep
Third not sleeping
Fourth sleep

3)
The LD_PRELOAD environment variable contains a list of shared libraries, which will be searched first by the dynamic linker.
Using LD_PRELOAD environment variable, we can get the linker to link the sleep() function to our code, instead of the one in the standard libc library.
Result is different, due to the countermeasure implemented by the dynamic linker, which ignores the LD_PRELOAD environment variable when the process's real and effective UID differ.
This is the experiment:

```
[09/09/19]seed@VM:~$ cp /usr/bin/env ./myenv
[09/09/19]seed@VM:~$ sudo chown root myenv
[09/09/19]seed@VM:~$ sudo chmod 4755 myenv
[09/09/19]seed@VM:~$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/09/19]seed@VM:~$ export LD_LIBRARY_PATH=.
[09/09/19]seed@VM:~$ export LD_MYOWN="my own value"
[09/09/19]seed@VM:~$ env | grep LD_
LD_PRELOAD=./libmylib.so.1.0.1
LD_LIBRARY_PATH=.
LD_MYOWN=my own value
[09/09/19]seed@VM:~$ myenv | grep LD_
LD_MYOWN=my own value
[09/09/19]seed@VM:~$
```

From the above experiment, we can see that even though myenv and env are identical programs in terms of executables, when they are executed, the process running my env does not even have those two EV. The LD_MYOWN EV serves a control of the experiment: it is defined by us, not used by dynamic linker, and thus poses no threat to Set-UID programs. That is why variable is not removed from either process.

Task8:

1)

```c
#include <string.h>
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char *argv[]) {
        char *v[3];
        char *command;

        if (argc < 2) {
                printf("Please type a file name.\n");
                return 1;
        }

        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]);

        system(command);
        //execve(v[0], v, NULL);

        return 0;
}
```

```
[09/09/19]seed@VM:~$ gcc task8.c -o task8
[09/09/19]seed@VM:~$ sudo chown root task8
[09/09/19]seed@VM:~$ sudo chmod 4755 task8
[09/09/19]seed@VM:~$
```

I can compromise the integrity of the system by change the environment variable “PATH”. And I could make my own program mycat to do this.

2)

```c
#include <string.h>
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char *argv[]) {
        char *v[3];
        char *command;

        if (argc < 2) {
                printf("Please type a file name.\n");
                return 1;
        }

        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]);

        //system(command);
        execve(v[0], v, NULL);

        return 0;
}
```

```
[09/09/19]seed@VM:~$ gcc task8.c -o task8
task8.c: In function 'main':
task8.c:21:2: warning: implicit declaration of function 'execve' [-Wimplicit-fun
ction-declaration]
  execve(v[0], v, NULL);
  ^
[09/09/19]seed@VM:~$ sudo chown root task8
[09/09/19]seed@VM:~$ sudo chmod 4755 task8
[09/09/19]seed@VM:~$
```

No, it won't work. Execve() doesn't invoke shell, so it do nothing with the environment variable.

Task9:

```c
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>

void main()
{
        int fd;
        fd = open("/etc/zzz", O_RDWR | O_APPEND);
        if (fd == -1) {
                printf("Cannot open /etc/zzz\n");
                exit(0);
        }

        sleep(1);

        setuid(getuid());

        if (fork()) {
                close(fd);
                exit(0);
        }
        else {
                write(fd, "Malicious Data\n", 15);
                close(fd);
        }
}
```

```
[09/09/19]seed@VM:~$ gcc task8.c -o task8
task8.c: In function ‘main’:
task8.c:21:2: warning: implicit declaration of function ‘execve’ [-Wimplicit-fun
ction-declaration]
  execve(v[0], v, NULL);
  ^
[09/09/19]seed@VM:~$ sudo chown root task8
[09/09/19]seed@VM:~$ sudo chmod 4755 task8
[09/09/19]seed@VM:~$ gcc task9.c -o task9
task9.c: In function ‘main’:
task9.c:14:2: warning: implicit declaration of function ‘sleep’ [-Wimplicit-func
tion-declaration]
  sleep(1);
  ^
task9.c:16:2: warning: implicit declaration of function ‘setuid’ [-Wimplicit-fun
ction-declaration]
  setuid(getuid());
  ^
task9.c:16:9: warning: implicit declaration of function ‘getuid’ [-Wimplicit-fun
ction-declaration]
  setuid(getuid());
         ^
task9.c:18:6: warning: implicit declaration of function ‘fork’ [-Wimplicit-funct
ion-declaration]
  if (fork()) {
      ^
task9.c:19:3: warning: implicit declaration of function ‘close’ [-Wimplicit-func
tion-declaration]
   close(fd);
   ^
task9.c:23:3: warning: implicit declaration of function ‘write’ [-Wimplicit-func
tion-declaration]
   write(fd, "Malicious Data\n", 15);
   ^
[09/09/19]seed@VM:~$ sudo chown root task9
[09/09/19]seed@VM:~$ sudo chmod 4755 task9
[09/09/19]seed@VM:~$
```

```
[09/09/19]seed@VM:~$ su
Password:
root@VM:/home/seed# touch /etc/zzz
root@VM:/home/seed# ll /etc/zzz
-rw-r--r-- 1 root root 0 Sep  9 23:25 /etc/zzz
root@VM:/home/seed# cat /etc/zzz
root@VM:/home/seed# exit
exit
[09/09/19]seed@VM:~$ ./task9
[09/09/19]seed@VM:~$ su
Password:
root@VM:/home/seed# cat /etc/zzz
Malicious Data
root@VM:/home/seed# ll /etc/zzz
-rw-r--r-- 1 root root 15 Sep  9 23:26 /etc/zzz
root@VM:/home/seed#
```

Yes. It is in child process and it will be modified.
Because it forget to close the file after degrade the priviledge. And it exist the Capability Leaking.