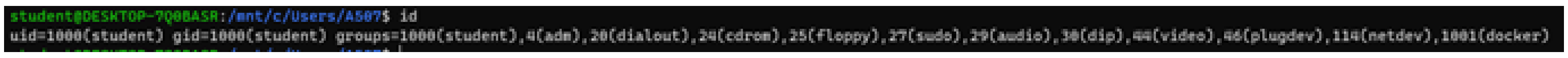
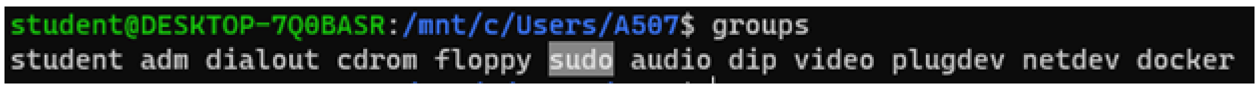
Vježba 6: Linux permissions and ACLs

id komandom saznajemo :

- korisnički ID (**uid**)
- ID korisničke primarne grupe (**gid**)
- ID naknadnih grupa (**groups**) kojima korisnik pripada

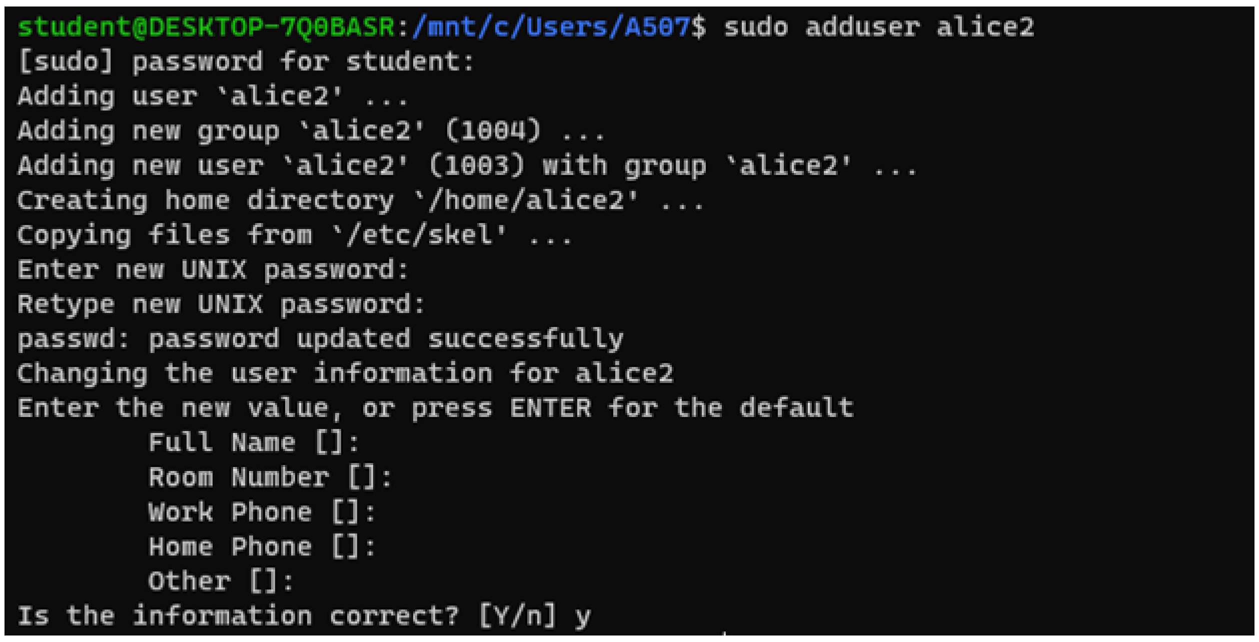


```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ id
uid=1000(student) gid=1000(student) groups=1000(student),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),114(netdev),1001(docker)
```

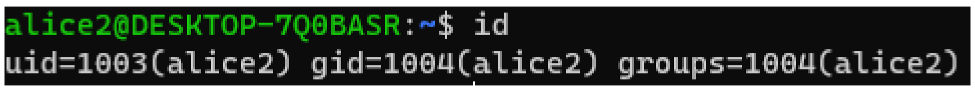


```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ groups
student adm dialout cdrom floppy sudo audio dip video plugdev netdev docker
```

S obzirom da korisnik student ima **administratorska/superuserska (sudo)** prava može kreirati novog koristnika → **alice2**.

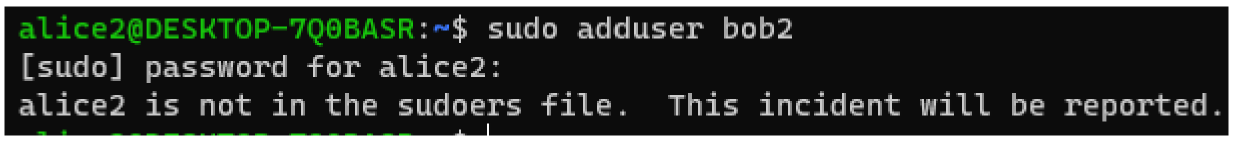


```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ sudo adduser alice2
[sudo] password for student:
Adding user `alice2' ...
Adding new group `alice2' (1004) ...
Adding new user `alice2' (1003) with group `alice2' ...
Creating home directory `/home/alice2' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for alice2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```



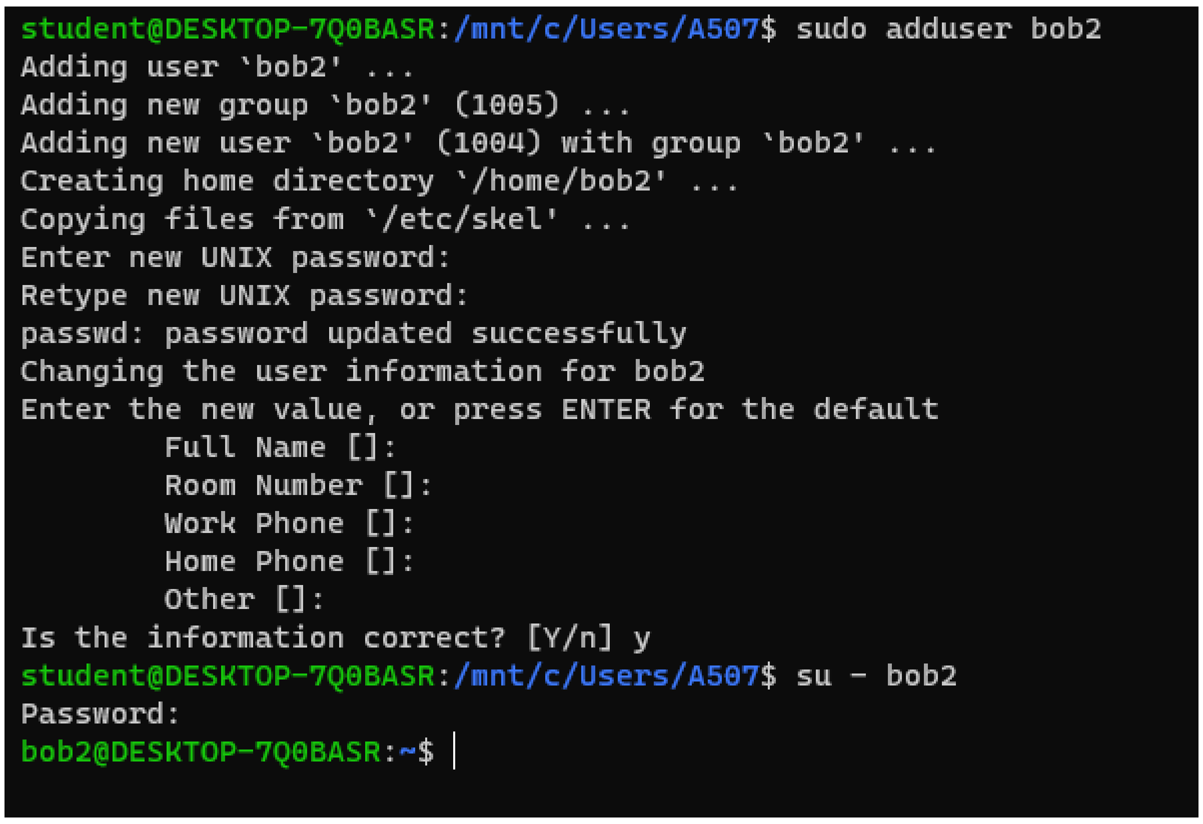
```
alice2@DESKTOP-7Q0BASR:~$ id
uid=1003(alice2) gid=1004(alice2) groups=1004(alice2)
```

Pokušaj kreiranja korisnika **bob2.** S obzirom da alice2 nema **sudo** dozvole, ne može kreirati novog korisnika.



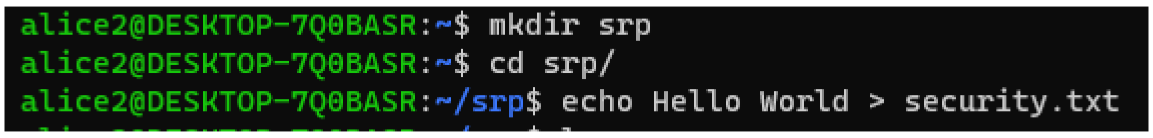
```
alice2@DESKTOP-7Q0BASR:~$ sudo adduser bob2
[sudo] password for alice2:
alice2 is not in the sudoers file.  This incident will be reported.
```

Zato smo ga morali kreirati s korisnikom **student**.



```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ sudo adduser bob2
Adding user `bob2' ...
Adding new group `bob2' (1005) ...
Adding new user `bob2' (1004) with group `bob2' ...
Creating home directory `/home/bob2' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for bob2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ su - bob2
Password:
bob2@DESKTOP-7Q0BASR:~$
```

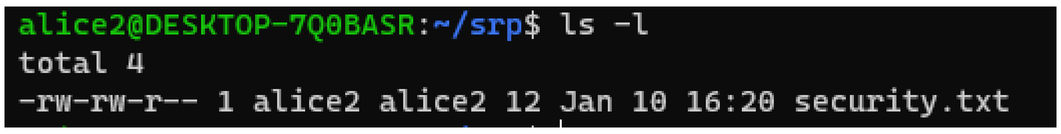
Kreiranje datoteke **srp** i upisivanje texta u novo kreirarni **security.txt** file.



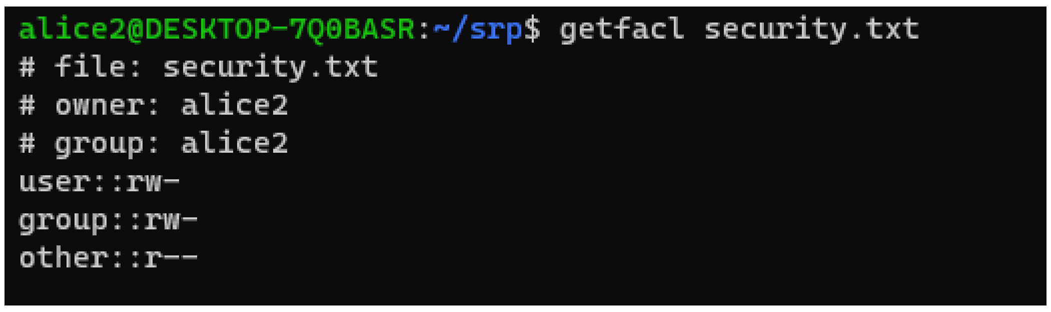
```
alice2@DESKTOP-7Q0BASR:~$ mkdir srp
alice2@DESKTOP-7Q0BASR:~$ cd srp/
alice2@DESKTOP-7Q0BASR:~/srp$ echo Hello World > security.txt
```

Ispisivanje korisničkih dozvola za korisnike, grupe i ostale:

- r → read, čitanje .txt filea
- w → write, upisivanje .txt u file
- x → execute, promjena .txt filea u executable file



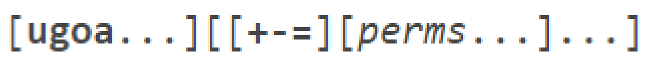
```
alice2@DESKTOP-7Q0BASR:~/srp$ ls -l
total 4
-rw-rw-r-- 1 alice2 alice2 12 Jan 10 16:20 security.txt
```



```
alice2@DESKTOP-7Q0BASR:~/srp$ getfacl security.txt
# file: security.txt
# owner: alice2
# group: alice2
user::rw-
group::rw-
other::r--
```

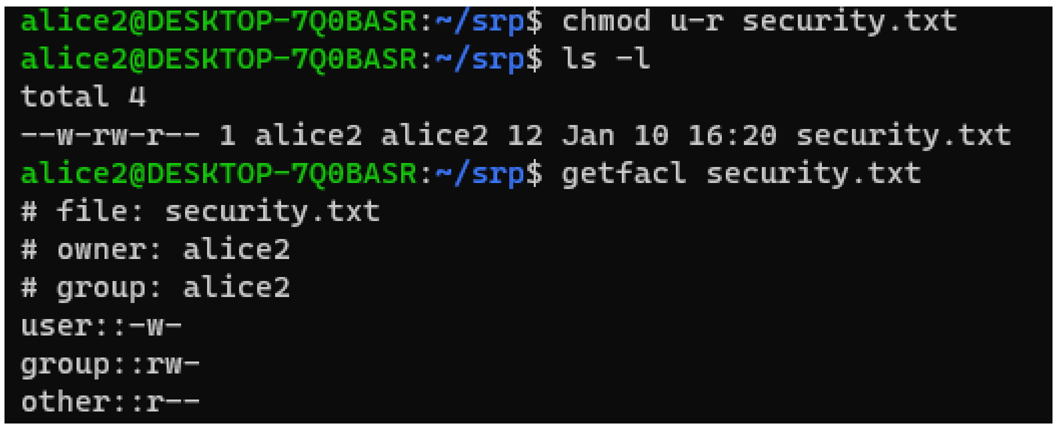
Komanda **chmod** služi za uređivanje, odnosno promjenu dozvola korisnika/grupe/ostalih.

1. Odaberemo kome mijenjamo dozvole:
   user **(u)**, group**(g)**, others**(o),** everyone**(a)**
2. Dodajemo dozvolu**(+)**,
   oduzimamo dozvoulu**(-)**,
   postavljamo određena dozvole**(=)**
3. Odaberemo tip dozvole**(r, w ,x)**



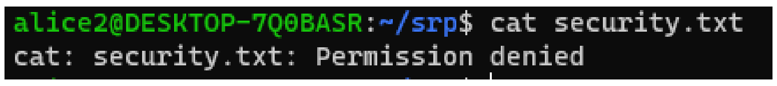
```
[ugoa...][[+-=][perms...]...]
```

U sljedećem primjeru smo korisniku prvo oduzeli dozvolu za čitanje sadržaja **security.txt**.



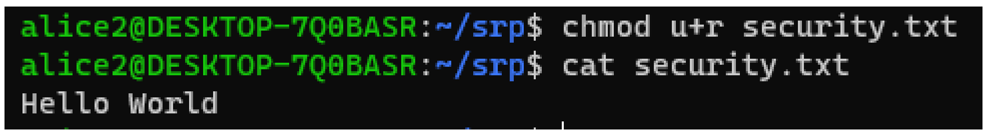
```
alice2@DESKTOP-7Q0BASR:~/srp$ chmod u-r security.txt
alice2@DESKTOP-7Q0BASR:~/srp$ ls -l
total 4
--w-rw-r-- 1 alice2 alice2 12 Jan 10 16:20 security.txt
alice2@DESKTOP-7Q0BASR:~/srp$ getfacl security.txt
# file: security.txt
# owner: alice2
# group: alice2
user::-w-
group::rw-
other::r--
```

alice2 nema pravo pročitati .txt file.



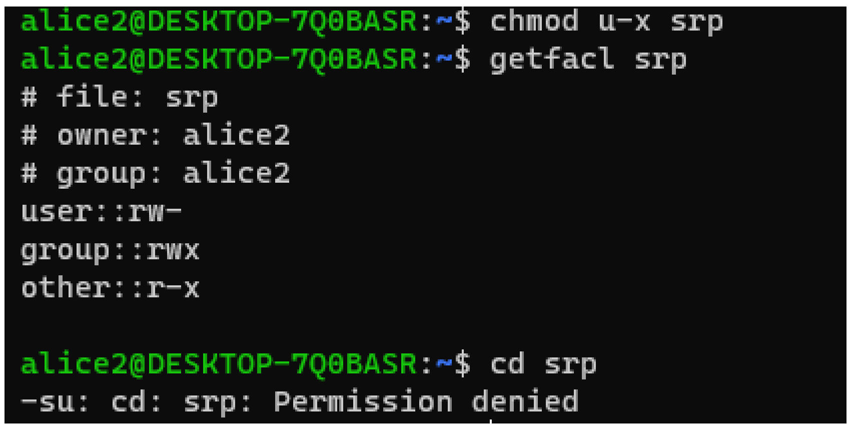
```
alice2@DESKTOP-7Q0BASR:~/srp$ cat security.txt
cat: security.txt: Permission denied
```

Nakon toga smo vratili dozvolu i uspjeli pročitati sadržaj.



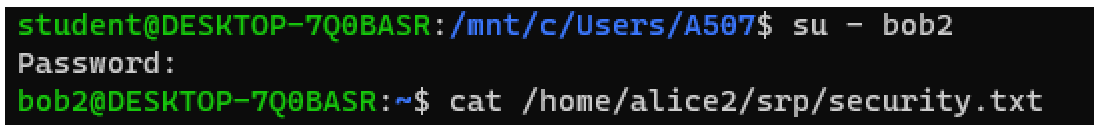
```
alice2@DESKTOP-7Q0BASR:~/srp$ chmod u+r security.txt
alice2@DESKTOP-7Q0BASR:~/srp$ cat security.txt
Hello World
```

Istu stvar možemo napraviti i za datoteku **srp**.
Korisniku **alice2** brišemo execute pravo za datoteku srp.



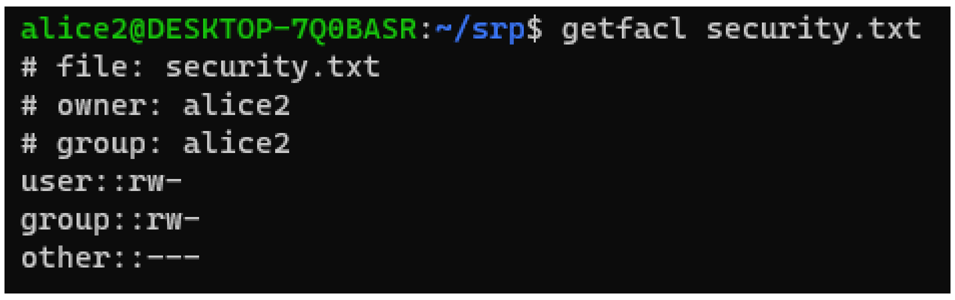
```
alice2@DESKTOP-7Q0BASR:~$ chmod u-x srp
alice2@DESKTOP-7Q0BASR:~$ getfacl srp
# file: srp
# owner: alice2
# group: alice2
user::rw-
group::rwx
other::r-x

alice2@DESKTOP-7Q0BASR:~$ cd srp
-su: cd: srp: Permission denied
```

Ako **bob2** pokuša pročitati sadržaj .txt filea, uspijet će iz razloga što pripada grupi **other**, koja ima dozvolu čitanja.

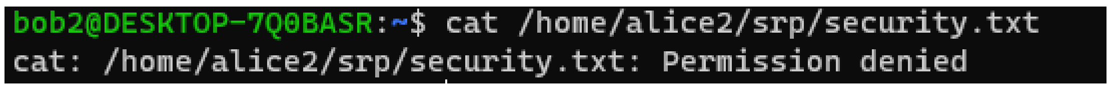


```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ su - bob2
Password:
bob2@DESKTOP-7Q0BASR:~$ cat /home/alice2/srp/security.txt
```

Ako grupi **other** oduzmemo tu dozvolu, **bob2** ga također izgubi.

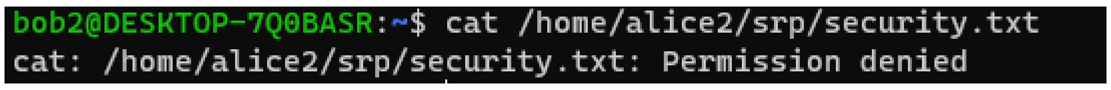


```
alice2@DESKTOP-7Q0BASR:~/srp$ getfacl security.txt
# file: security.txt
# owner: alice2
# group: alice2
user::rw-
group::rw-
other::---
```

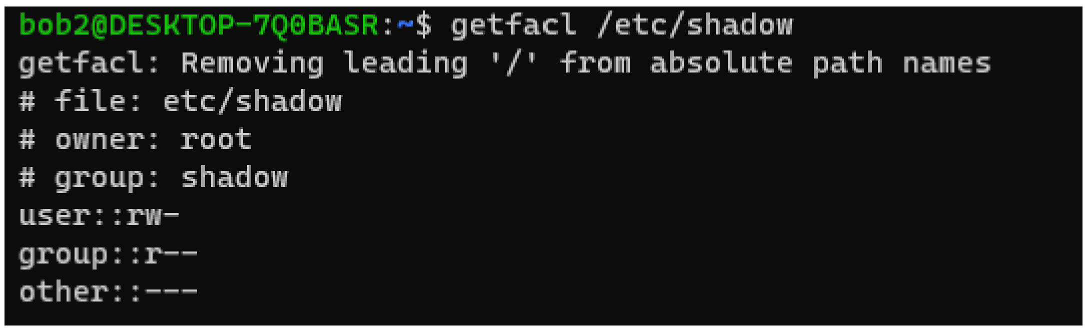


```
bob2@DESKTOP-7Q0BASR:~$ cat /home/alice2/srp/security.txt
cat: /home/alice2/srp/security.txt: Permission denied
```

Korisnika **bob2** dodajemo grupi **alice2**.

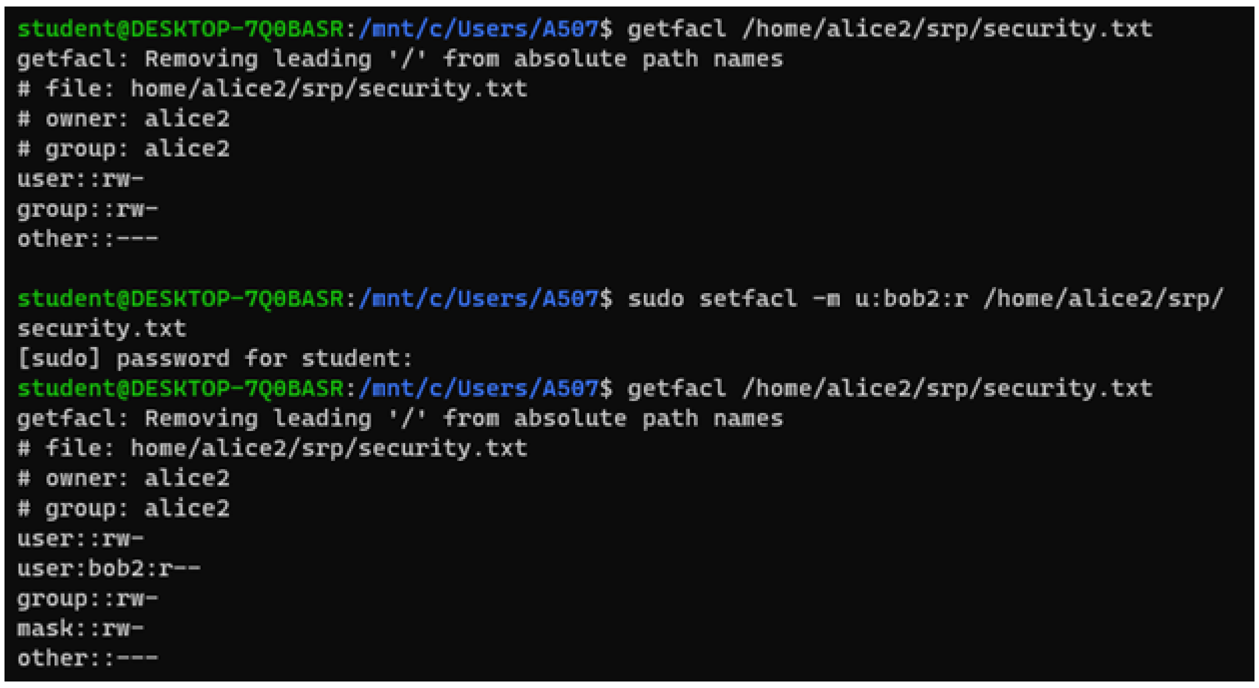


```
bob2@DESKTOP-7Q0BASR:~$ cat /home/alice2/srp/security.txt
cat: /home/alice2/srp/security.txt: Permission denied
```



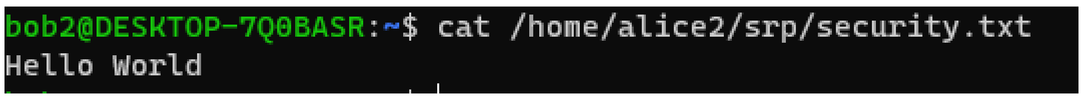
```
bob2@DESKTOP-7Q0BASR:~$ getfacl /etc/shadow
getfacl: Removing leading '/' from absolute path names
# file: etc/shadow
# owner: root
# group: shadow
user::rw-
group::r--
other::---
```

Pomoću naredbe **setfacl** (promjeni ACL) smo dali dozvole korisniku bob2 da čita podatke **security.txt** filea.



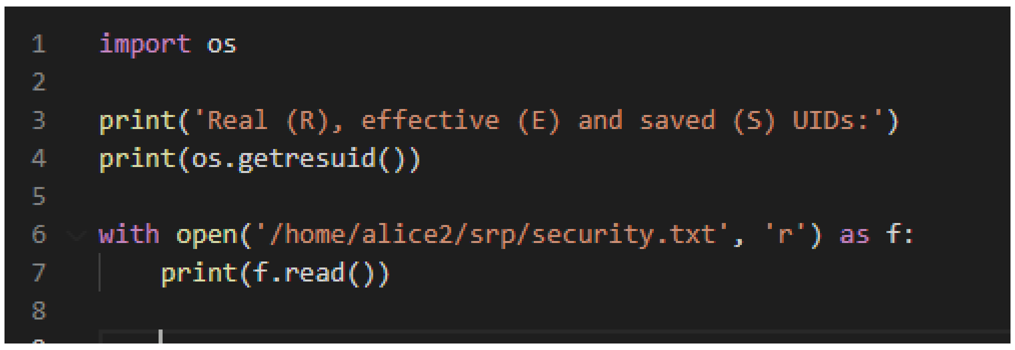
```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ getfacl /home/alice2/srp/security.txt
getfacl: Removing leading '/' from absolute path names
# file: home/alice2/srp/security.txt
# owner: alice2
# group: alice2
user::rw-
group::rw-
other::---

student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ sudo setfacl -m u:bob2:r /home/alice2/srp/
security.txt
[sudo] password for student:
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507$ getfacl /home/alice2/srp/security.txt
getfacl: Removing leading '/' from absolute path names
# file: home/alice2/srp/security.txt
# owner: alice2
# group: alice2
user::rw-
user:bob2:r--
group::rw-
mask::rw-
other::---
```

bob2 sada ima pravo čitati sadržaj.

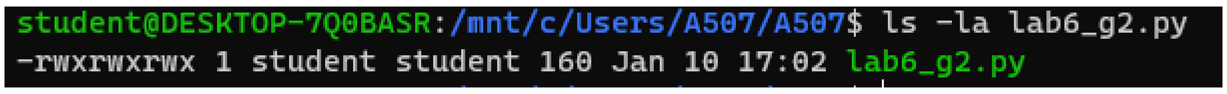


```
bob2@DESKTOP-7Q0BASR:~$ cat /home/alice2/srp/security.txt
Hello World
```

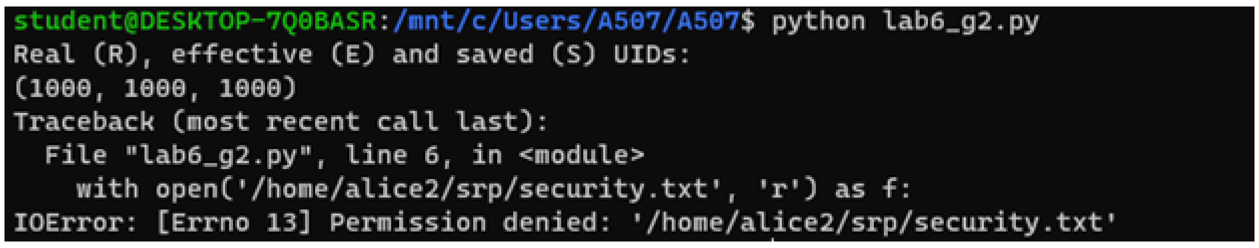
lab6_g2.py kod



```python
import os

print('Real (R), effective (E) and saved (S) UIDs:')
print(os.getresuid())

with open('/home/alice2/srp/security.txt', 'r') as f:
    print(f.read())
```

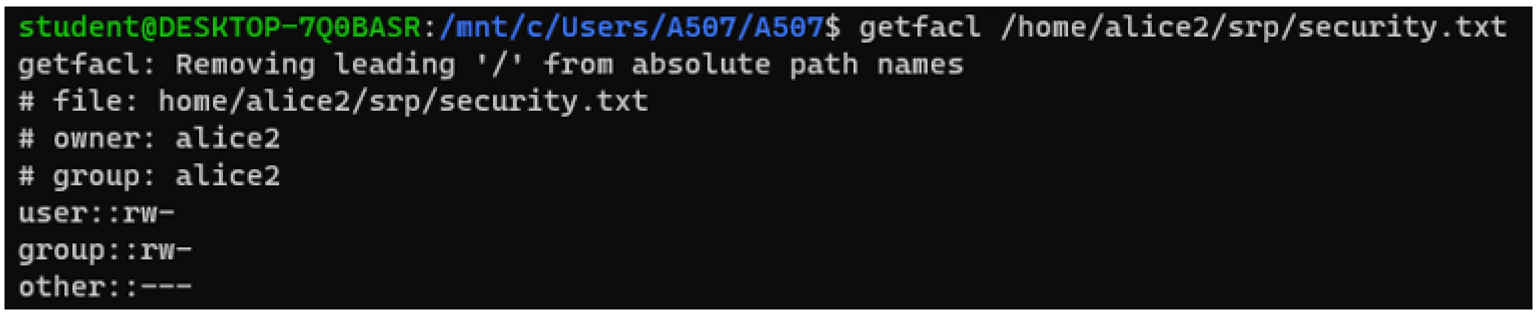


```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/A507$ ls -la lab6_g2.py
-rwxrwxrwx 1 student student 160 Jan 10 17:02 lab6_g2.py
```



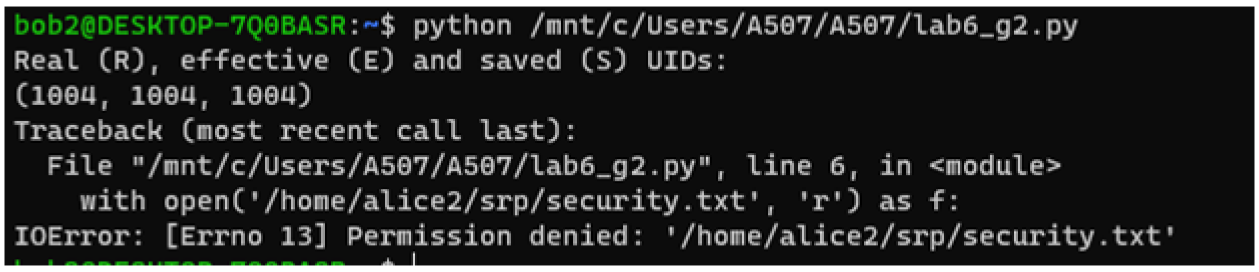
```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/A507$ python lab6_g2.py
Real (R), effective (E) and saved (S) UIDs:
(1000, 1000, 1000)
Traceback (most recent call last):
  File "lab6_g2.py", line 6, in <module>
    with open('/home/alice2/srp/security.txt', 'r') as f:
IOError: [Errno 13] Permission denied: '/home/alice2/srp/security.txt'
```

Ne možemo pokrenuti program jer nismo ni u **grupi** ni **alice2**.



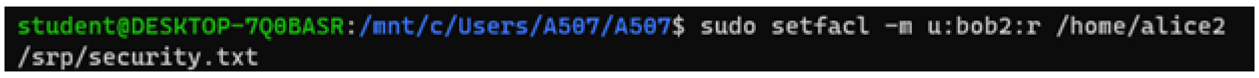
```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/A507$ getfacl /home/alice2/srp/security.txt
getfacl: Removing leading '/' from absolute path names
# file: home/alice2/srp/security.txt
# owner: alice2
# group: alice2
user::rw-
group::rw-
other::---
```

Korisnik **bob2** ne može pristupiti **security.txt** datoteci.



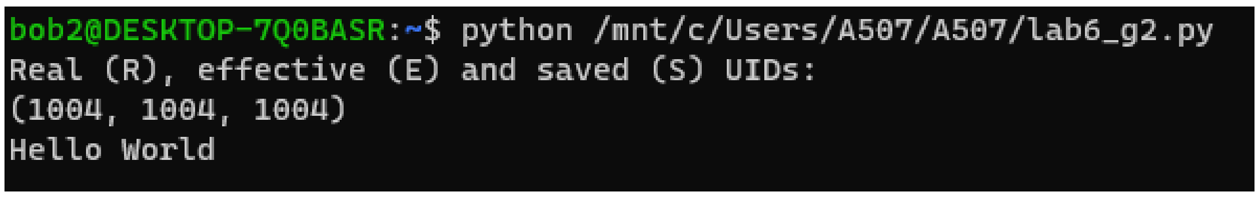
```
bob2@DESKTOP-7Q0BASR:~$ python /mnt/c/Users/A507/A507/lab6_g2.py
Real (R), effective (E) and saved (S) UIDs:
(1004, 1004, 1004)
Traceback (most recent call last):
  File "/mnt/c/Users/A507/A507/lab6_g2.py", line 6, in <module>
    with open('/home/alice2/srp/security.txt', 'r') as f:
IOError: [Errno 13] Permission denied: '/home/alice2/srp/security.txt'
```

Dajemo korisniku **bob2** prava čitanja.



```
student@DESKTOP-7Q0BASR:/mnt/c/Users/A507/A507$ sudo setfacl -m u:bob2:r /home/alice2
/srp/security.txt
```

Uspjeh:



```
bob2@DESKTOP-7Q0BASR:~$ python /mnt/c/Users/A507/A507/lab6_g2.py
Real (R), effective (E) and saved (S) UIDs:
(1004, 1004, 1004)
Hello World
```