

# File permissions in Linux

## Project description

My organization needed to ensure proper file permissions on the research team's project directory. The lab environment that would normally allow me to practice these commands returned a 404 error, but based on the scenario and current permissions documentation provided, here's how I would examine and modify file permissions in the /home/researcher2/projects directory to secure the system and remove unauthorized access.

## Check file and directory details

To check permissions for all files and subdirectories in the projects directory, including hidden files, I would use:

bash

ls -la

## Describe the permissions string

Looking at `project_t.txt` with permissions `-rw-rw-r--`, here's how the 10-character string breaks down:

The first character indicates file type. A hyphen (-) means regular file, while d indicates a directory. The next nine characters split into three groups of three, representing user, group, and other permissions respectively. For `project_t.txt`: characters 2-4 (`rw-`) show the user can read and write but not execute, characters 5-7 (`rw-`) show the group can read and write, and characters 8-10 (`r--`) show others can only read. Each position shows r (read), w (write), x (execute), or a hyphen when that permission isn't granted.

## Change file permissions

The organization doesn't allow others to have write access to any files. From the permissions check, `project_k.txt` showed `-rw-rw-rw-`, giving others write access that needs to be removed.

bash

```
chmod o-w project_k.txt
```

## Change file permissions on a hidden file

The archived file `.project_x.txt` shouldn't have write permissions for anyone, but user and group should be able to read it. Current permissions `-rw--w----` give the user write access and the group only write without read.

bash

```
chmod u-w,g-w,g+r .project_x.txt
```

## Change directory permissions

The `drafts` directory should only be accessible by `researcher2`. Current permissions `drwx--x---` show the group has execute access, which lets them enter the directory and view contents.

bash

```
chmod g-x drafts
```

## Summary

I would have checked permissions using `ls -la` to display all files including hidden ones in the `projects` directory. After identifying where permissions didn't match security requirements, I would use `chmod` commands to fix them. The changes include removing write access for others on `project_k.txt`, making `.project_x.txt` read-only for user and group, and removing group access from the `drafts` directory.