# File permissions in Linux

## Project description

In this task, I am responsible for checking and updating file and directory permissions on a Linux system to make sure user access matches the organization’s security guidelines. The main goal is to strengthen file system security by properly managing access rights.

## Check file and directory details

ls -la /home/researcher2/projects

## Describe the permissions string

The permissions string is a 10-character code that shows the type of file and the access rights for different users.

The first character tells you the file type: a dash (-) means it’s a regular file, d indicates a directory, and l stands for a symbolic link.

The next three characters, positions 2–4 show what the owner can do, read (r), write (w), or execute (x).

Characters 5 to 7 indicate the group’s permissions.

The last three characters, 8–10 represent the permissions for all other users, also using r, w, and x.

For example, -rw-r--r-- indicates a regular file where the owner can read and write, while the group and others can only read it.

## Change file permissions

chmod o-w /home/researcher2/projects/project\_m.txt

## Change file permissions on a hidden file

chmod o-w /home/researcher2/projects/.project\_x.txt

## Change directory permissions

chmod 700 /home/researcher2/projects/drafts

## Summary

As part of this assignment, I reviewed and updated file and directory permissions within a Linux environment. Using the ls -la command, I checked the current permission settings to verify they followed the organization’s access control policies. I then applied the chmod command to adjust permissions as needed for specific files, including hidden ones, and various directories. These actions support a more secure and well-managed file system, aligning user access with organizational security standards.