# File permissions in Linux

## Project description

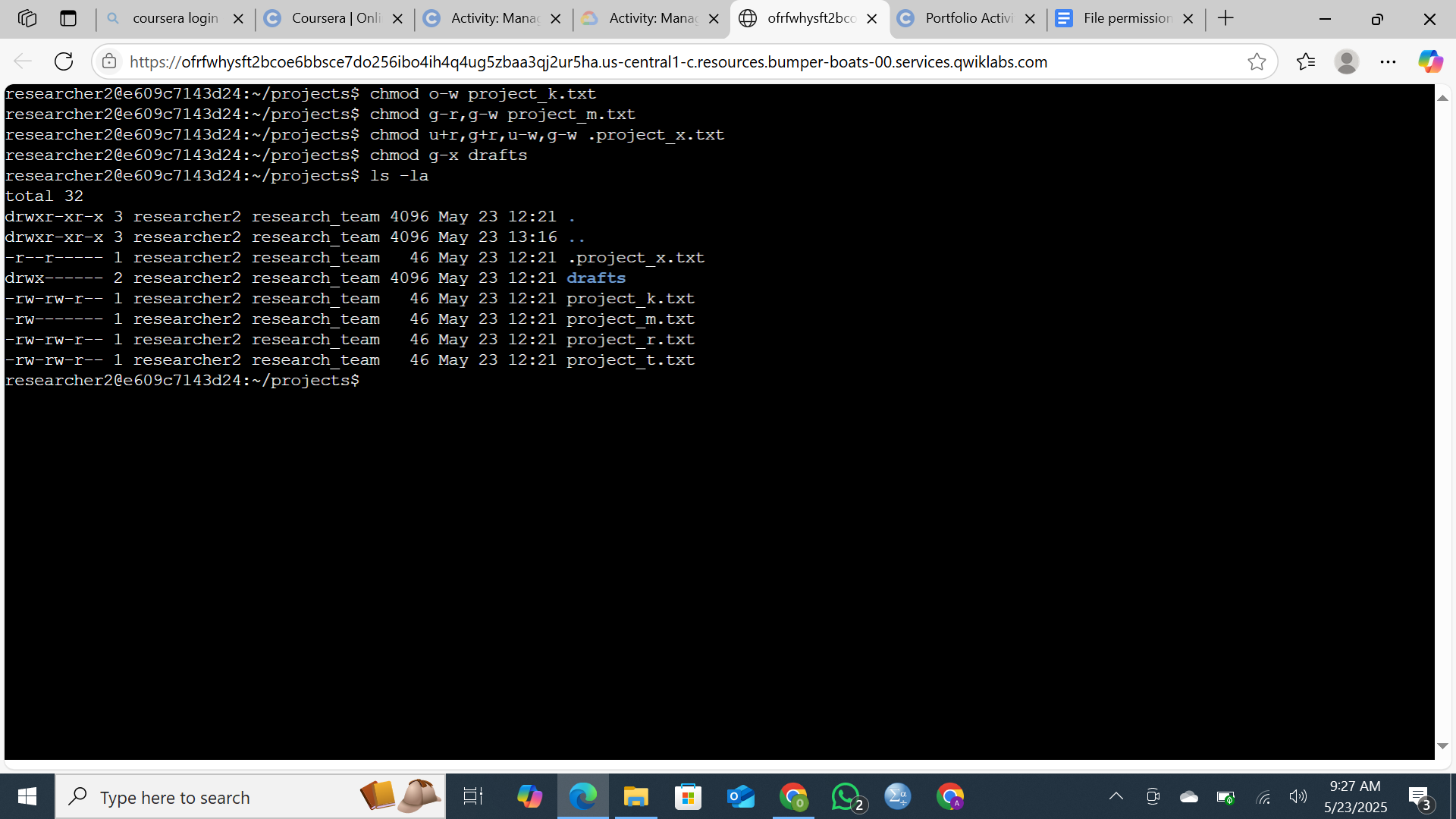
As a Security Professional at a large organization, I work closely with our research team, supporting their operations by ensuring that access to digital resources is both secure and appropriate.

One of my core responsibilities is to manage and audit user permissions on the file system. This means I routinely inspect current access controls to ensure that only authorized team members have the right level of access to sensitive research data and tools.

When I conduct these audits, I look for mismatches between assigned permissions and actual user roles. If I find that a user has access they shouldn’t, or is missing necessary permissions, I take immediate action to correct it. This involves modifying the file system permissions—granting access to legitimate users and revoking it from unauthorized individuals.

.

## Check file and directory details



I began by verifying my current working directory using the pwd command. Next, I listed the subdirectories within my directory to review the folder structure. I navigated to the **"projects"** directory using the cd command, then listed the files it contains. To perform a detailed review of file permissions—including both hidden and visible files—I used the ls -la command. This allowed me to examine ownership and access rights for all files within the directory.

## Describe the permissions string

**project\_x.txt**: The user has **read and write** permissions. The group has **write-only** permission. No permissions are granted to others.

**drafts/** directory: The user has **full access** (read, write, execute). The group has **execute-only** permission. Others have **no access**.

**project\_k.txt**: The user, group, and others all have **read and write** permissions. **Execute** permission is not granted to any party.

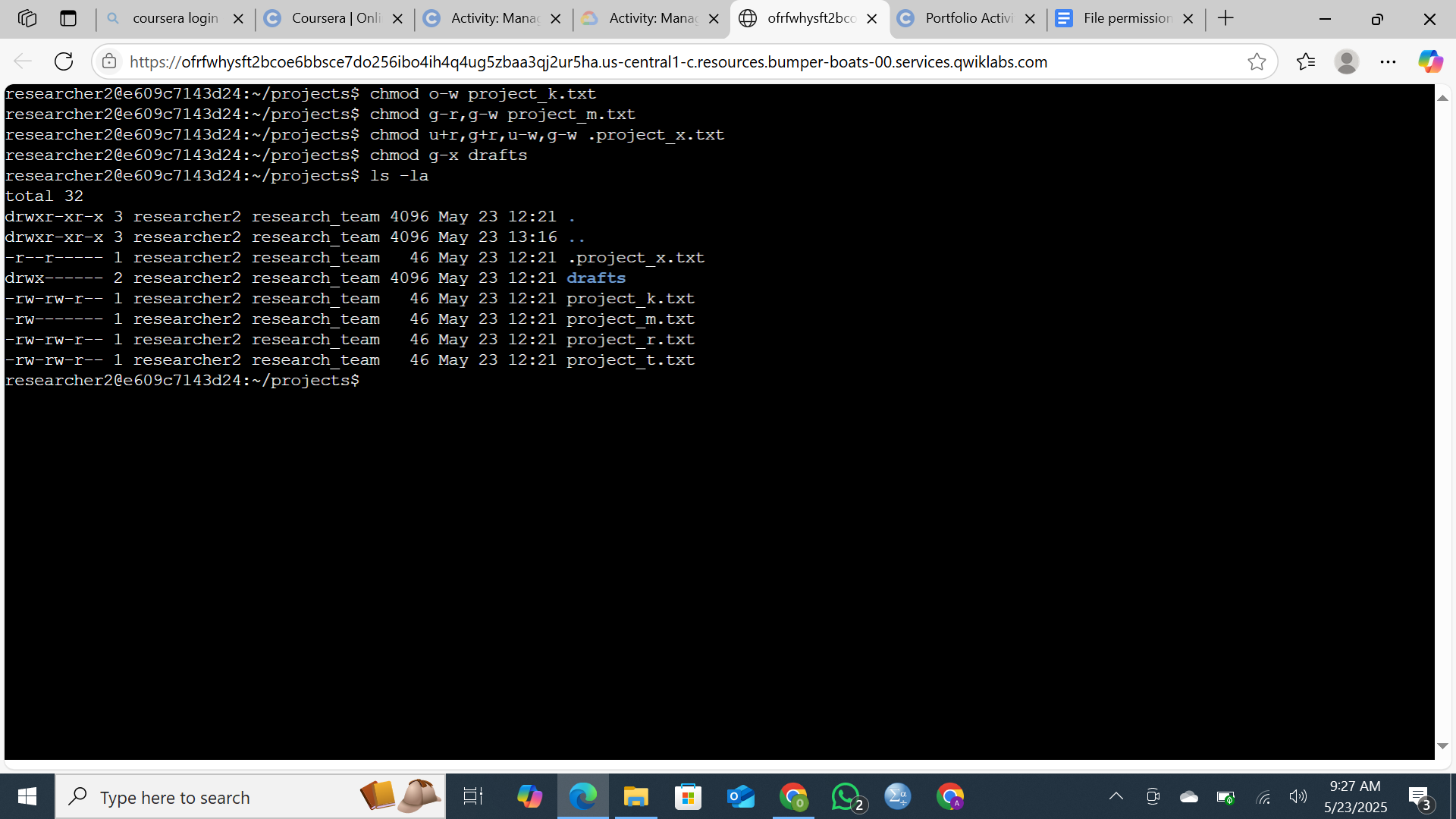
**project\_m.txt**: The user has **read and write** permissions. The group has **read-only** access. Others have **no access**.

**project\_r.txt**: Both the user and group have **read and write** permissions. Others have **read-only** access.

**project\_t.txt**: The user and group are granted **read and write** permissions. Others have **read-only** access.

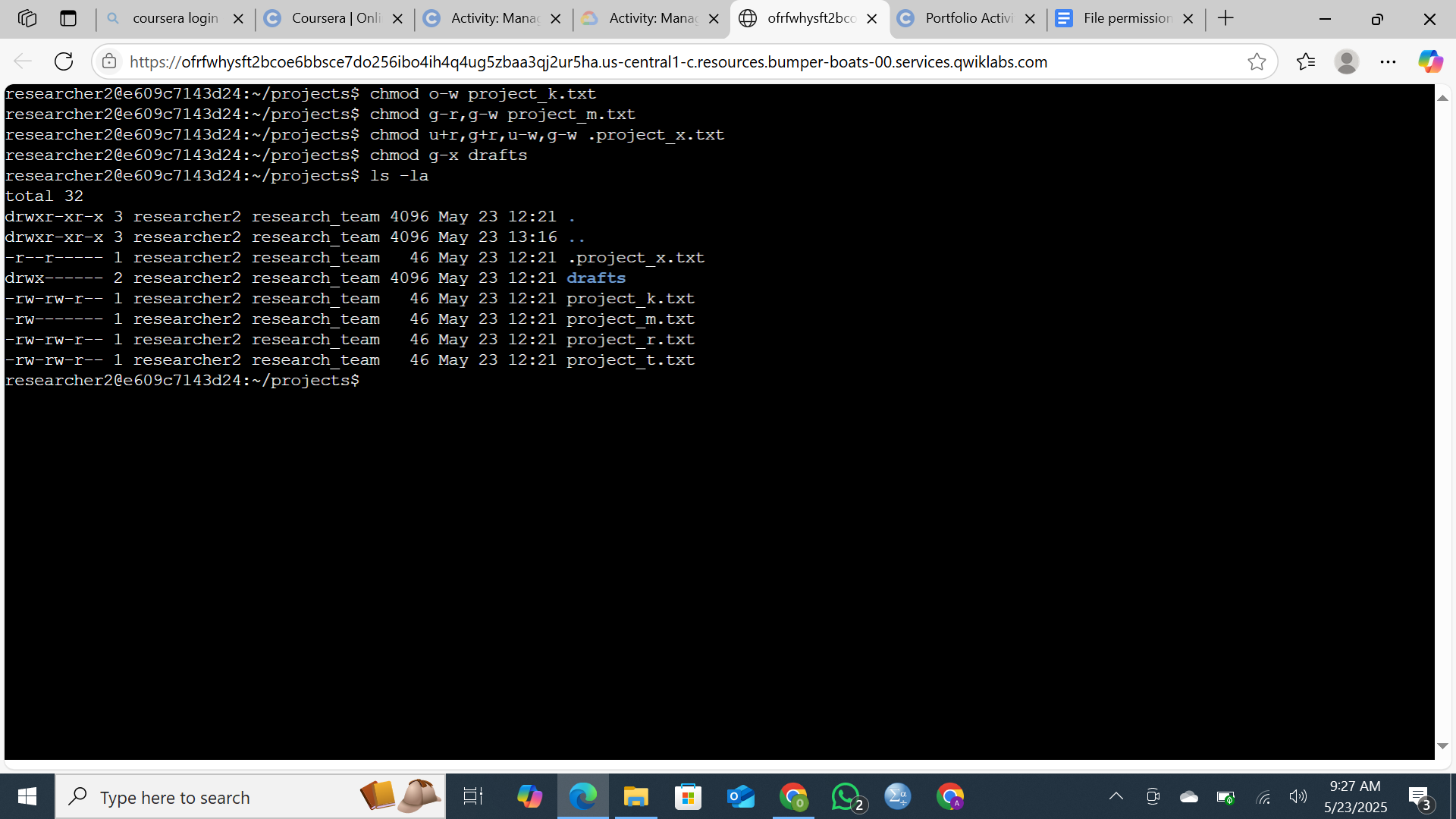
## Change file permissions on a hidden file

I modified the permissions of the hidden file .project\_x.txt to allow both the user and the group to **read** the file, while restricting **write** access. The leading dot in the filename indicates that it is a hidden file in Unix-based systems.(chmod u+r,g+r,u-w,g-w .project\_x.txt)



## Change directory permissions

I removed the executive permission for the group in the draft directory.(chmod g-x drafts)



## Summary

As a Security Analyst responsible for managing and auditing user permissions on the file system, I successfully modified the access permissions of several files and a directory to align with security policies.This proactive approach helps maintain the integrity and confidentiality of our systems, protects our research data, and supports overall compliance with our security policies