File Permissions Audit Report: /home/researcher2/projects

Date: July 31, 2024

Summary:

An audit of file and directory permissions was conducted within the `/home/researcher2/projects` directory. The following observations and actions were taken to enhance security and align permissions with the principle of least privilege:

Findings:

A comprehensive examination of file permissions within the `/home/researcher2/projects` directory was conducted using the `ls -la` command. This analysis revealed a series of permissions configurations across files and the 'drafts' subdirectory, with implications for data security and access control.

The user 'researcher2', who is also a member of the 'research_team' group, is the primary owner of all items within the directory. As such, 'researcher2' maintains full control (read, write, and execute) over all files and the 'drafts' subdirectory, aligning with expected ownership privileges.

The 'research_team' group exhibits varying levels of access to the files. For `project_k.txt`, `project_r.txt`, and `project_t.txt`, the group enjoys both read and write privileges. In contrast, for `project_m.txt`, group access is limited to read-only. The hidden file `.project_x.txt` presents an atypical scenario where the group possesses the unusual and potentially risky write-only access, warranting further investigation to ensure it's intentional and not a potential security misconfiguration. Furthermore, the 'research_team' group is granted execute permission on the 'drafts' subdirectory, allowing them to navigate its contents even without explicit read or write access to the files within.

An area of concern was identified in the permissions for `project_k.txt`, which currently grants 'other' users (those outside the owner and group) both read and write permissions. This level of access might be excessive depending on the sensitivity of the file's content and could pose a security risk. In contrast, `project_m.txt` and `.project_x.txt` appropriately restrict access for 'other' users.

Actions Taken:

- **`project_k.txt`:** Removed write access for 'other' users (`chmod o-w project_k.txt`).
- **`project_m.txt`:** Removed read and write permissions for the group (`chmod g-rw project_m.txt`).

- **`.project_x.txt`:** Set read-only permissions for both the user and the group (`chmod ug=r .project_x.txt`).
- **`drafts`:** Removed execute permission for the group (`chmod g-x drafts`).

Recommendations:

- Periodically review file and directory permissions to ensure they align with the principle of least privilege.
- Investigate the unusual write-only access on `.project_x.txt` to determine if it's intentional or a potential security issue.
- Consider further restricting group access to the `drafts` directory if even viewing file names is deemed sensitive.

Conclusion:

This audit and subsequent actions have improved the security posture of the `/home/researcher2/projects` directory by mitigating potential vulnerabilities and enforcing appropriate access controls. Continued vigilance and regular permission reviews are recommended to maintain a secure environment.

Submitted by: Junaid Shakoor

Date of Submission: July 31, 2024