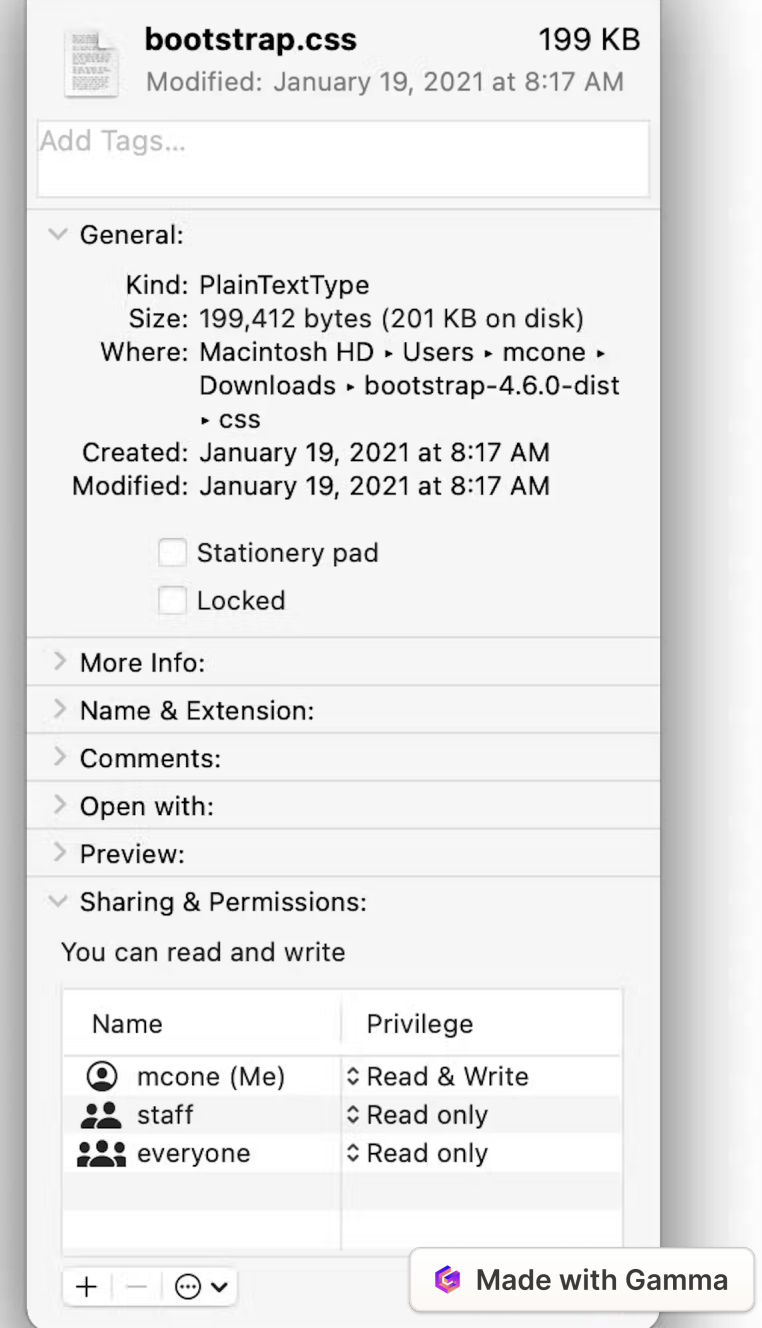


# Security by File Permission

Absolutely, managing file permissions is crucial for maintaining security on a Unix/Linux system.

 by Hema V



# chmod

The chmod command is used to change the permissions of a file. For example, "chmod 755 file\_name" grants read, write, and execute permissions to the owner, and read and execute permissions to group and others.





# chown

The chown command changes the owner and/or group of a file. To change the owner and group, use the command "chown user\_name:group\_name file\_name" and replace user\_name and group\_name with the desired owner and group.

# chgrp

The chgrp command changes the group ownership of a file. Use the command "chgrp group\_name file\_name" to specify the desired group.





# ls

The `ls -l` command lists detailed information about files, including their permissions, owner, group, and other attributes.



# umask

The umask command sets the default permissions for newly created files. For example, "umask 027" ensures that the group has no permissions and others have no write or execute permissions.

An abstract background on the left side of the slide. It features a light beige background with a large, stylized hand silhouette in a darker beige color. The hand is positioned with fingers spread, reaching towards the right. There are also some darker, wavy shapes in the upper left corner.

# passwd

The passwd command changes the password for a specific user. Use the command "passwd user\_name" to change the password for the desired user.