RecipeFilePermissions

File and Directory Permissions and Security

In a Linux/Unix environment you can set file ownership and permission to optimize security in a production environment or to provide flexibility in a developement enviroment.

In a production environment, you want most of the files in your Tiki install to be read only.

However, Tiki requires read/write access to certain directories and the files they store:

backups dump img/wiki img/wiki_up modules/cache temp temp/cache templates_c templates styles maps whelp static static/styles

In addition, during the usual installation process (tiki-install.php), Tiki requires read/write access to the db directory.

Examples of production and development permissions:

To be continued...

Some wise words from Damian 😊 : Once installed the templates/ and styles/ directly can be set to read only, these only need to be writable by Apache if your going to use the built in TPL or CSS editors.