```
# this disallows direct access to the folder listing
# and disallows access to any executables files (that users may upload)
# the script allows only .jpg/.png uploads, but we never know...
Options -Indexes
Options -ExecCGI
AddHandler cgi-script .php .php3 .php4 .phtml .pl .py .jsp .asp .htm .shtml .sh .cgi
# completely disable the PHP engine inside THIS folder, so what ever an attacker will do,
PHP code will never run here
# more info on this: http://www.electrictoolbox.com/disable-php-apache-htaccess/
php_flag engine off
```