

```
# protect the htaccess file
<files .htaccess>
order allow,deny
deny from all
</files>

# disable the server signature
ServerSignature Off

# limit file uploads to 10mb
LimitRequestBody 10240000

# protect wpconfig.php
<files wp-config.php>
order allow,deny
deny from all
</files>

#who has access who doesnt
order allow,deny
#deny from 000.000.000.000
allow from all

#custom error docs
ErrorDocument 404 /notfound.php
ErrorDocument 403 /forbidden.php
ErrorDocument 500 /error.php

# disable directory browsing
Options All -Indexes

#redirect old to new
Redirect 301 /old.php http://www.yourdomain.com/new.php

#block referring domains
RewriteEngine on
RewriteCond %{HTTP_REFERER} digg\.com [NC]
RewriteRule .* - [F]

#disable hotlinking of images with forbidden or custom image option
RewriteEngine on
```

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?yourdomain.com/.*$ [NC]
#RewriteRule \.(gif|jpg)$ - [F]
#RewriteRule \.(gif|jpg)$ http://www.yourdomain.com/stealingisbad.gif [R,L]

# php compression - use with caution
<ifmodule mod_php4.c>
php_value zlib.output_compression 16386
</ifmodule>

# set the canonical url
RewriteEngine On
RewriteCond %{HTTP_HOST} ^yourdomain\.com$ [NC]
RewriteRule ^(.*)$ http://www.yourdomain.com/$1 [R=301,L]

# protect from spam comments
RewriteEngine On
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{REQUEST_URI} .wp-comments-post\.php*
RewriteCond %{HTTP_REFERER} !.*yourdomain.com.* [OR]
RewriteCond %{HTTP_USER_AGENT} ^$
RewriteRule (.*) ^http://%{REMOTE_ADDR}/$ [R=301,L]

#wp multisite
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]

# uploaded files
RewriteRule ^files/(.+)\.wp-includes/ms-files.php?file=$1 [L]

RewriteCond %{REQUEST_FILENAME} -f [OR]
RewriteCond %{REQUEST_FILENAME} -d
RewriteRule ^ - [L]
RewriteRule . index.php [L]
```