<?php

remove\_action( .. this .. );

remove\_action( .. that .. );

remove\_action( .. the other .. );

?>

remove\_action('wp\_head', 'rsd\_link' );

remove\_action('wp\_head', 'wlwmanifest\_link' );

remove\_action('wp\_head', 'feed\_links\_extra', 3 );

remove\_action('wp\_head', 'feed\_links', 2 );

remove\_action('wp\_head', 'index\_rel\_link' );

remove\_action('wp\_head', 'parent\_post\_rel\_link', 10, 0 );

remove\_action('wp\_head', 'start\_post\_rel\_link', 10, 0 );

remove\_action('wp\_head', 'adjacent\_posts\_rel\_link\_wp\_head', 10, 0 );

define('WP\_CONTENT\_DIR', '/path/to/not-wp-content');

define('WP\_CONTENT\_URL', '/url/to/not-wp-content');

<?php

function change\_js\_path() {

if (!is\_admin()) {

wp\_deregister\_script('jquery');

wp\_register\_script('jquery',   
 'http://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js',   
 false, '1.3.2');

wp\_enqueue\_script('jquery');

}

}

add\_action('init', 'change\_js\_path');

?>

wp\_deregister\_script('anotherScript');

wp\_register\_script('anotherScript',  
 'http://somesite.com/path/to/anotherFile.js', false, '');

wp\_enqueue\_script('anotherScript');

#kill spam, and swear at it too

RewriteEngine On

RewriteCond %{REQUEST\_METHOD} POST

RewriteCond %{REQUEST\_URI} .wp-comments-post\.php\*

RewriteCond %{HTTP\_REFERER} !.\*somesite.com.\* [OR]

RewriteCond %{HTTP\_USER\_AGENT} ^$

RewriteRule (.\*) ^http://%{REMOTE\_ADDR}/$ [R=301,L]

#limit file size

LimitRequestBody 5012000

#hotlink prevention

RewriteEngine On

RewriteBase /

RewriteCond %{HTTP\_REFERER} !^$

RewriteCond %{HTTP\_REFERER} !^http://(www\.)?somesite.com/.\*$ [NC]

RewriteRule \.(gif|jpg|png|flv|swf)$ http://www.somesite.com/hahaha.gif [R=302,L]

#create access rule for files matching ..

<FilesMatch "\.(htaccess|htpasswd|ini|phps|fla|psd|log|sh)$">

Order Allow,Deny

Deny from all

</FilesMatch>

#create authentication rule for files matching ..

<FilesMatch "^(exec|env|doit|phpinfo|w)\.\*$">

AuthName "Private"

AuthUserFile /\.htpasswd

AuthType basic

Require valid-user

</FilesMatch>

#hush Apache

ServerSignature Off

#look after me please

<Files .htaccess>

Order deny,allow

Deny from all

</Files>

Disallow: /wp-\*

Disallow: /content

Disallow: /some/path/not-today-thank-you

#only do stuff if Apache's rewriting module is activated

<IfModule mod\_rewrite.c>

#wake up the module

RewriteEngine On

#block by user agent (duplicate rule for each bot)

RewriteCond %{HTTP\_USER\_AGENT} ^badbot [NC,OR]

#block by referrer (duplicate rule for each bot)

RewriteCond %{HTTP\_REFERER} ^(http://)?(www\.)?badbot.\*$ [NC,OR]

#block by matching referrer keyword

RewriteCond %{HTTP\_REFERER} ^(http://)?(www\.)?.\*(-|.)badbot(-|.).\*$   
 [NC,OR]

#block by IP

RewriteCond %{REMOTE\_ADDR} ^123\.45\.67\.890 [NC,OR]

#the last statement drops the "OR" ([NC,OR] becomes [NC])

RewriteCond %{HTTP\_REFERER} ^(http://)?(www\.)?.\*(-|.)badbot(-|.).\*$   
 [NC]

#for requests fitting any of the above conditions ..

#.. create a rewrite to a "Forbidden" error page

RewriteRule ^(.\*)$ - [F]

#and let the module know that's the lot.

</IfModule>

<?php

add\_filter('login\_errors',create\_function('$no\_error', "return   
 null;"));

?>

Options All -Indexes