BULLETPROOF .52 >>>>>>>> SECURE .HTACCESS

CUSTOM CODE TOP PHP/PHP.INI HANDLER/CACHE CODE
BEGIN WEBSITE SPEED BOOST
Time cheat sheet in seconds
A86400 = 1 day
A172800 = 2 days
A2419200 = 1 month
A4838400 = 2 months
A29030400 = 1 year

Test which ETag setting works best on your Host/Server/Website
with Firefox Firebug, Firephp and Yslow benchmark tests.

Create the ETag (entity tag) response header field
FileETag MTime Size

Remove the ETag (entity tag) response header field
Header unset ETag
FileETag none

<IfModule mod_expires.c>
ExpiresActive on
ExpiresByType image/jpg A4838400
ExpiresByType image/gif A4838400
ExpiresByType image/jpeg A4838400
ExpiresByType image/png A4838400
ExpiresByType video/webm A4838400
ExpiresByType application/x-shockwave-flash A4838400
ExpiresByType application/x-javascript A4838400
ExpiresByType application/javascript A4838400
ExpiresByType text/javascript A4838400
ExpiresByType text/css A4838400
#ExpiresByType text/html A86400
Default is 2 days below so the line above is not needed / commented out
ExpiresDefault A172800
</IfModule>

<IfModule mod_headers.c>
<FileMatch "\.(js|css|f|v|ico|pdf|avi|mov|ppt|doc|mp3|wmv|wav|gif|jpg|jpeg|png|swf|webm)$">
Header send Cache-Control "public"
</FileMatch>

# END WEBSITE SPEED BOOST
<?php

header append Cache-Control "proxy-revalidate"
</FilesMatch>

Header set Cache-Control "private, no-cache, no-store, proxy-revalidate, no-transform"
Header set Pragma "no-cache"
</FilesMatch>
</IfModule>

<IfModule mod_deflate.c>

# Insert filters
AddOutputFilterByType DEFLATE text/plain
AddOutputFilterByType DEFLATE text/html
AddOutputFilterByType DEFLATE text/xml
AddOutputFilterByType DEFLATE text/css
AddOutputFilterByType DEFLATE application/xml
AddOutputFilterByType DEFLATE application/xhtml+xml
AddOutputFilterByType DEFLATE application/rss+xml
AddOutputFilterByType DEFLATE application/javascript
AddOutputFilterByType DEFLATE application/x-javascript
AddOutputFilterByType DEFLATE application/x-httpd-php
AddOutputFilterByType DEFLATE application/x-httpd-fastphp
AddOutputFilterByType DEFLATE image/svg+xml

# Drop problematic browsers
BrowserMatch ^Mozilla/4 gzip-only-text/html
BrowserMatch ^Mozilla/4\.[0-9]* gzip-only-text/html
BrowserMatch \bMSIE\b gzip-only-text/html

# Make sure proxies don't deliver the wrong content
Header append Vary User-Agent env=! dont-vary
</IfModule>

# END WEBSITE SPEED BOOST

<IfModule mod_headers.c>

# Protects against Drive-by Download attacks
# Protects against MIME/Content-Type-sniffing
Header set X-Content-Type-Options nosniff
</IfModule>
# Block other sites from displaying your website in iFrames
# Protects against Clickjacking
<IfModule mod_headers.c>
# Using DENY will block all iFrames including iFrames on your own website
# Header set X-Frame-Options DENY
# Recommended: iFrames from the same site are allowed – other sites are blocked
Header always append X-Frame-Options SAMEORIGIN
</IfModule>

# TURN OFF YOUR SERVER SIGNATURE
# Suppresses the footer line server version number and ServerName of the serving virtual host.
ServerSignature Off

# DO NOT SHOW DIRECTORY LISTING
# Disallow mod_autoindex from displaying a directory listing
# If a 500 Internal Server Error occurs when activating Root BulletProof Mode
# copy the entire DO NOT SHOW DIRECTORY LISTING and DIRECTORY INDEX sections of code
# and paste it into BPS Custom Code and comment out Options -Indexes
# by adding a # sign in front of it.
# Example: #Options -Indexes
Options -Indexes

# DIRECTORY INDEX FORCE INDEX.PHP
# Use index.php as default directory index file. index.html will be ignored.
# If a 500 Internal Server Error occurs when activating Root BulletProof Mode
# copy the entire DO NOT SHOW DIRECTORY LISTING and DIRECTORY INDEX sections of code
# and paste it into BPS Custom Code and comment out DirectoryIndex
# by adding a # sign in front of it.
# Example: #DirectoryIndex index.php index.html /index.php
DirectoryIndex index.php index.html /index.php

# CUSTOM CODE BRUTE FORCE LOGIN PAGE PROTECTION
# Protect wp-login.php from Brute Force Login Attacks based on IP Address
<FFilesMatch "^\(wp-login\\.php\)"
Order Allow,Deny
# Add your website domain name
Allow from example.com
# Add your website/Server IP Address
Allow from 69.200.95.1
# Add your Public IP Address using 2 or 3 octets so that if/when
# your IP address changes it will still be in your subnet range. If you
# have a static IP address then use all 4 octets.
# Examples: 2 octets: 65.100. 3 octets: 65.100.50. 4 octets: 65.100.50.1
Allow from 65.100.50.
</FilesMatch>

# BPS ERROR LOGGING AND TRACKING
# Use BPS Custom Code to modify/edit/change this code and to save it permanently.
# BPS has premade 403 Forbidden, 400 Bad Request, 410 Gone and 404 Not Found files that are
# to track and log 403, 400, 410 and 404 errors that occur on your website. When a hacker at
# hack your website the hackers IP address, Host name, Request Method, Refering link, the
# requested resource, the user agent of the hacker and the query string used in the hack at
# All BPS log files are htaccess protected so that only you can view them.
# The 400, php, 403, php, 404, php and 410, php files are located in /wp-content/plugins/bullet
# The 400, 410 and 403 Error logging files are already set up and will automatically start i
# after you install BPS and have activated BulletProof Mode for your Root folder.
# If you would like to log 404 errors you will need to copy the logging code in the BPS 404,
# to your Theme’s 404.php template file. Simple instructions are included in the BPS 404.ph
# You can open the BPS 404.php file using the WP Plugins Editor.
# NOTE: By default WordPress automatically looks in your Theme’s folder for a 404.php Theme

ErrorDocument 400 /wp-content/plugins/bulletproof-security/400.php
ErrorDocument 401 default
ErrorDocument 403 /wp-content/plugins/bulletproof-security/403.php
ErrorDocument 404 /404.php

# DENY ACCESS TO PROTECTED SERVER FILES AND FOLDERS
# Use BPS Custom Code to modify/edit/change this code and to save it permanently.
# Files and folders starting with a dot: .htaccess, .htpasswd, .errordocs, .logs
RedirectMatch 403 \.(htaccess|htpasswd|errordocs|logs)$

# WP-ADMIN/INCLUDES
# Use BPS Custom Code to remove this code permanently.
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.php$ - [F]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F]
RewriteRule ^wp-includes/theme-compat/ - [F]
# WP REWRITE LOOP START

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

# REQUEST METHODS FILTERED
# If you want to allow HEAD Requests use BPS Custom Code and
# remove/delete HEAD from the Request Method filter.
# Example: RewriteCond %{REQUEST_METHOD} ^<\(TRACE|DELETE|TRACKI|DEBUG\) [NC]
# The TRACE, DELETE, TRACK and DEBUG Request methods should never be removed.
RewriteCond %{REQUEST_METHOD} ^<\(HEAD\|TRACE\|DELETE\|TRACK\|DEBUG\) [NC]
RewriteRule ^\.(.*)$ - [F]

# PLUGINS/ THEMES AND VARIOUS EXPLOIT FILTER SKIP RULES
# To add plugin/theme skip/bypass rules use BPS Custom Code.
# The [S] flag is used to skip following rules. Skip rule [S=12] will skip 12 following Rew
# The skip rules MUST be in descending consecutive number order: 12, 11, 10, 9...
# If you delete a skip rule, change the other skip rule numbers accordingly.
# Examples: If RewriteRule [S=5] is deleted then change [S=6] to [S=5], [S=7] to [S=6], etc.
# If you add a new skip rule above skip rule 12 it will be skip rule 13: [S=13]

# Adminer MySQL management tool data populate
RewriteCond %{REQUEST_URI} ^/wp-content/plugins/adminer/ [NC]
RewriteRule . - [S=12]

# Comment Spam Pack MU Plugin - CAPTCHA images not displaying
RewriteCond %{REQUEST_URI} ^/wp-content/mu-plugins/custom-anti-spam/ [NC]
RewriteRule . - [S=11]

# Peters Custom Anti-Spam display CAPTCHA Image
RewriteCond %{REQUEST_URI} ^/wp-content/plugins/peters-custom-anti-spam-image/ [NC]
RewriteRule . - [S=10]

# Status Updater plugin fb connect
RewriteCond %{REQUEST_URI} ^/wp-content/plugins/fb-status-updater/ [NC]
RewriteRule . - [S=9]

# Stream Video Player - Adding FLV Videos Blocked
RewriteCond %{REQUEST_URI} ^/wp-content/plugins/stream-video-player/ [NC]
RewriteRule . - [S=8]

# XCloner 404 or 403 error when updating settings
RewriteCond %{REQUEST_URI} ^/wp-content/plugins/xcloner-backup-and-restore/ [NC]
RewriteRule . - [S=7]

# BuddyPress Logout Redirect
RewriteCond %{QUERY_STRING} (sp_executesql) [NC]
RewriteRule ^(.*)$ - [F]
# END BPSQSE BPS QUERY STRING EXPLOITS
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
# WP REWRITE LOOP END

# DENY BROWSER ACCESS TO THESE FILES
# Use BPS Custom Code to modify/edit/change this code and to save it permanently.
# wp-config.php, bb-config.php, php.ini, php5.ini, readme.html
# Replace 88.77.66.55 with your current IP address and remove the
# pound sign # in front of the Allow from line of code below to be able to access
# any of these files directly from your Browser.

<FilesMatch "^(wp-config\.php|php\.*\.ini|php5\.ini|readme\.html|bb-config\.php)">
Order Allow,Deny
Deny from all
#Allow from 88.77.66.55
</FilesMatch>

# CUSTOM CODE BOTTOM HOTLINKING/FORBID COMMENT SPAMMERS/BLOCK BOTS/BLOCK IP/REDIRECT CODE
# WP AUTHOR ENUMERATION BOT PROBE PROTECTION
# Rewrites to author=999999 that does not actually exist
# which results in a standard 404 error. To the hacker bot
# it appears that this author does not exist without giving
# any clues that the author does actually exist.

RewriteCond %{QUERY_STRING} ^author=(\[0-9]\{1,\})$ [NC]
RewriteRule ^(.*)$ $1?author=999999 [L]

# XML-RPC DDoS PROTECTION
# You can whitelist your IP address if you use A Weblog Client
# or want to whitelist your IP address for any other reasons.
# Example: uncomment #Allow from x.x.x. by deleting the # sign and
# replace the x's with your actual IP address. Allow from 99.88.77.
# Note: It is recommended that you use 3 octets x.x.x. of your IP address
# instead of 4 octets x.x.x.x of your IP address.

<FilesMatch "^\(xmlrpc\.[^\s]*\)?>
Order Deny,Allow
# Whitelist Jetpack/ Automattic CIDR IP Address Blocks
Allow from 192.0.64.0/18
Allow from 209.15.0.0/16
Allow from 66.155.0.0/17
Deny from all
</FilesMatch>

# Block/Forbid Referer Spammers/Referer Phishing
RewriteCond %{HTTP_REFERER} ^.*(ranksonic\.semalt\.kambasoftware\.buttons-for-website\.buttons\.com|best-seo-offer\.com|best-seo-solution\.com).*$ [NC]
RewriteRule ^(.*)$ - [F]