

```

# 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>
<FilesMatch "\.(js|css|flv|ico|pdf|avi|mov|ppt|doc|mp3|wmv|wav|gif|jpg|jpeg|png|swf|webm)$">
Header append Cache-Control "public"

```

```

Header append Cache-Control public
</FilesMatch>
<FilesMatch "\.(txt|html)$">
Header append Cache-Control "proxy-revalidate"
</FilesMatch>
<FilesMatch "\.(php|cgi|pl|html|xml)$">
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[678] no-gzip
BrowserMatch \bMSIE[ ] !no-gzip !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

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

# DO NOT SHOW DIRECTORY LISTING
# If you are having trouble with your server, you may want to turn on the following

```

```
# 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
```

```
<FilesMatch "^(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 attacks
# hack your website the hackers IP address, Host name, Request Method, Referering link, the
# requested resource, the user agent of the hacker and the query string used in the hack attack
# 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/bulletproof/wp-content/
```

```
# The 400, 410 and 403 Error logging files are already set up and will automatically start logging errors
```

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.php
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
ErrorDocument 410 /wp-content/plugins/bulletproof-security/410.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|TRACK|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 RewriteRule
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 than 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} action=logout&redirect_to=http%3A%2F%2F(.*) [NC]

RewriteRule . - [S=6]

redirect_to=

RewriteCond %{QUERY_STRING} redirect_to=(.*) [NC]

RewriteRule . - [S=5]

Login Plugins Password Reset And Redirect 1

RewriteCond %{QUERY_STRING} action=resetpass&key=(.*) [NC]

RewriteRule . - [S=4]

Login Plugins Password Reset And Redirect 2

RewriteCond %{QUERY_STRING} action=rp&key=(.*) [NC]

RewriteRule . - [S=3]

TIMTHUMB FORBID RFI and MISC FILE SKIP/BYPASS RULE

Use BPS Custom Code to modify/edit/change this code and to save it permanently.

Remote File Inclusion (RFI) security rules

```

# Note: Only whitelist your additional domains or files if needed - do not whitelist hacker
RewriteCond %{QUERY_STRING} ^.*(http|https|ftp)(%3A|:)(%2F|/)(%2F|/)(w){0,3}.?
(blogger|picasa|blogspot|tsunami|petapolitiki|photobucket|imgur|imageshack|wordpress\.com|img
thegame).*$ [NC,OR]
RewriteCond %{THE_REQUEST} ^.*(http|https|ftp)(%3A|:)(%2F|/)(%2F|/)(w){0,3}.?
(blogger|picasa|blogspot|tsunami|petapolitiki|photobucket|imgur|imageshack|wordpress\.com|img
thegame).*$ [NC]
RewriteRule .* index.php [F]
#
# Example: Whitelist additional misc files: (example\.php|another-file\.php|phpthumb\.php|ti
RewriteCond %{REQUEST_URI} (timthumb\.php|phpthumb\.php|thumb\.php|thumbs\.php) [NC]
# Example: Whitelist additional website domains: RewriteCond %{HTTP_REFERER} ^.*(YourWebsite
RewriteCond %{HTTP_REFERER} ^.*dove.121texas.com.*
RewriteRule . - [S=1]

# BEGIN BPSQSE BPS QUERY STRING EXPLOITS
# The libwww-perl User Agent is forbidden - Many bad bots use libwww-perl modules, but some
# Good sites such as W3C use it for their W3C-LinkChecker.
# Use BPS Custom Code to add or remove user agents temporarily or permanently from the
# User Agent filters directly below or to modify/edit/change any of the other security code
RewriteCond %{HTTP_USER_AGENT} (havi|libwww-perl|wget|python|nikto|curl|scan|java|winhttp|
RewriteCond %{HTTP_USER_AGENT} (%0A|%0D|%27|%3C|%3E|%00) [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (;|<|>|'|!|\)|\(|%0A|%0D|%22|%27|%28|%3C|%3E|%00).*(libwww-
perl|wget|python|nikto|curl|scan|java|winhttp|HTTrack|clsh|http|archiver|loader|email|harvest|
RewriteCond %{THE_REQUEST} (\?|&|%2a)+(.%20+\\s+.%20+\\s+\\s+.%20+\\s+)%20+\\s+HTTP(:|/|/)
RewriteCond %{THE_REQUEST} etc/passwd [NC,OR]
RewriteCond %{THE_REQUEST} cgi-bin [NC,OR]
RewriteCond %{THE_REQUEST} (%0A|%0D|\\r|\\n) [NC,OR]
RewriteCond %{REQUEST_URI} owssvr\.dll [NC,OR]
RewriteCond %{HTTP_REFERER} (%0A|%0D|%27|%3C|%3E|%00) [NC,OR]
RewriteCond %{HTTP_REFERER} \.opendirviewer\. [NC,OR]
RewriteCond %{HTTP_REFERER} users\.skynet\.be.* [NC,OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=http:// [NC,OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=(\\.\.//?)+ [NC,OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=/([a-z0-9_ ]//?)+ [NC,OR]
RewriteCond %{QUERY_STRING} \=PHP([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{1
RewriteCond %{QUERY_STRING} (\\.\\. /| %2e%2e%2f| %2e%2e/| \.\\. %2f| %2e\\. %2f| %2e\\. /| \. %2e%2f| \. %2e/
RewriteCond %{QUERY_STRING} ftp\.: [NC,OR]
RewriteCond %{QUERY_STRING} http\.: [NC,OR]
RewriteCond %{QUERY_STRING} https\.: [NC,OR]
RewriteCond %{QUERY_STRING} \=\\|w\\ [NC,OR]

```

```

RewriteCond %{QUERY_STRING} ^(.*)/self/(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)cPath=http://(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} (\<| %3C). *script. *(\>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (<| %3C)([^\s]*s)+cript. *(>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (\<| %3C). *embed. *(\>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (<| %3C)([^\e]*e)+mbed. *(>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (\<| %3C). *object. *(\>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (<| %3C)([^\o]*o)+bject. *(>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (\<| %3C). *iframe. *(\>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (<| %3C)([^\i]*i)+frame. *(>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} base64_encode.*\(. *\) [NC,OR]
RewriteCond %{QUERY_STRING} base64_(en|de)code[^]*\([^\)]*\) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=| \[| \)%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=| \[| \)%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} ^.*(\(|\)| <|>| %3c| %3e). * [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(\\x00| \\x04| \\x08| \\x0d| \\x1b| \\x20| \\x3c| \\x3e| \\x7f). * [NC,OR]
RewriteCond %{QUERY_STRING} (NULL|OUTFILE|LOAD_FILE) [OR]
RewriteCond %{QUERY_STRING} (\.(1,|/)+)(motd|etc|bin) [NC,OR]
RewriteCond %{QUERY_STRING} (localhost|loopback|127\. 0\.. 0\.. 1) [NC,OR]
RewriteCond %{QUERY_STRING} (<|>|'| %0A| %0D| %27| %3C| %3E| %00) [NC,OR]
RewriteCond %{QUERY_STRING} concat[^\(]*\([NC,OR]
RewriteCond %{QUERY_STRING} union([^\s]*s)+select [NC,OR]
RewriteCond %{QUERY_STRING} union([^\a]*a)+11([^\s]*s)+select [NC,OR]
RewriteCond %{QUERY_STRING} \-[sdcrl]. *(allow_url_include|allow_url_fopen|safe_mode_disable_f
RewriteCond %{QUERY_STRING} (;|<|>|'|"|\)| %0A| %0D| %22| %27| %3C| %3E| %00). *
(</\>| union| select| insert| drop| delete| update| cast| create| char| convert| alter| declare| order| scr
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]
```