

```
# BULLETPROOF .48.2 >>>>>> SECURE .HTACCESS
```

```
# If you edit the BULLETPROOF .48.2 >>>>>> SECURE .HTACCESS text above  
# you will see error messages on the BPS Security Status page  
# BPS is reading the version number in the htaccess file to validate checks  
# If you would like to change what is displayed above you  
# will need to edit the BPS /includes/functions.php file to match your changes  
# If you update your WordPress Permalinks the code between BEGIN WordPress and  
# END WordPress is replaced by WP htaccess code.  
# This removes all of the BPS security code and replaces it with just the default WP htacce:  
# To restore this file use BPS Restore or activate BulletProof Mode for your Root folder ag
```

```
# BEGIN WordPress
```

```
# IMPORTANT!!! DO NOT DELETE!!! - B E G I N Wordpress above or E N D WordPress - text in thi  
# They are reference points for WP, BPS and other plugins to write to this htaccess file.  
# IMPORTANT!!! DO NOT DELETE!!! - BPSQSE BPS QUERY STRING EXPLOITS - text  
# BPS needs to find the - BPSQSE - text string in this file to validate that your security ;
```

```
# TURN OFF YOUR SERVER SIGNATURE
```

```
ServerSignature Off
```

```
# ADD A PHP HANDLER
```

```
# If you are using a PHP Handler add your web hosts PHP Handler below
```

```
# DO NOT SHOW DIRECTORY LISTING
```

```
# If you are getting 500 Errors when activating BPS then comment out Options -Indexes  
# by adding a # sign in front of it. If there is a typo anywhere in this file you will also  
Options -Indexes
```

```
# DIRECTORY INDEX FORCE INDEX.PHP
```

```
# Use index.php as default directory index file
```

```
# index.html will be ignored will not load.
```

```
DirectoryIndex index.php index.html /index.php
```

```
# BPS ERROR LOGGING AND TRACKING
```

```
# BPS has premade 403 Forbidden, 400 Bad Request and 404 Not Found files that are used  
# to track and log 403, 400 and 404 errors that occur on your website. When a hacker attempt  
# 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 at:  
# All BPS log files are htaccess protected so that only you can view them.  
# The 403.php, 400.php and 404.php files are located in the context /includes/bulletproof/err
```

```
# The 400.php, 403.php and 404.php files are located in /wp-content/plugins/bulletproof-security/
# The 400 and 403 Error logging files are already set up and will automatically start logging
# 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.php
# to your Theme's 404.php template file. Simple instructions are included in the BPS 404.php file.
# 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 template file.
```

```
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 - .htaccess, .htpasswd and all file names starting with .
RedirectMatch 403 /\..*$
```

```
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.(php)$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
```

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

#### # REQUEST METHODS FILTERED

```
# This filter is for blocking junk bots and spam bots from making a HEAD request, but may allow a
# HEAD request from bots that you want to allow in certain cases. This is not a security filter,
# a nuisance filter. This filter will not block any important bots like the google bot. If you want
# all bots to make a HEAD request then remove HEAD from the Request Method filter.
# The TRACE, DELETE, TRACK and DEBUG request methods should never be allowed against your website.
```

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK|DEBUG) [NC]
RewriteRule ^(.*)$ - [F,L]
```

#### # PLUGINS AND VARIOUS EXPLOIT FILTER SKIP RULES

```
# IMPORTANT!!! If you add or remove a skip rule you must change S= to the new skip number
# Example: If RewriteRule S=5 is deleted than change S=6 to S=5, S=7 to S=6, etc.
```

```

# 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 By Host Name But Allow Internal Requests
RewriteCond %{QUERY_STRING} ^.*(http|https|ftp)(%3A|:)(%2F|/)(%2F|/)(w){0,3}?(
(blogger|picasa|blogspot|tsunami|petapolitiki|photobucket|imgur|imageshack|wordpress\|com|im|
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|im|
thegame).*$ [NC]
RewriteRule .* index.php [F,L]
RewriteCond %{REQUEST_URI} (timthumb\.php|phpthumb\.php|thumb\.php|thumbs\.php) [NC]

```

```
RewriteCond %{HTTP_REFERER} ^.*demo5.local.*
RewriteRule . - [S=1]
```

### # 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.*

*# Add or remove user agents temporarily or permanently from the first User Agent filter below  
# If you want a list of bad bots / User Agents to block then scroll to the end of this file.*

```
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|archiver|loader|email|harvest|
```

```
RewriteCond %{THE_REQUEST} \?\ HTTP/ [NC,OR]
```

```
RewriteCond %{THE_REQUEST} \\*\ HTTP/ [NC,OR]
```

```
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:// [OR]
```

```
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=(\\.\./?)+ [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} (\\.\./|\\.\.) [OR]
```

```
RewriteCond %{QUERY_STRING} ftp\ [NC,OR]
```

```
RewriteCond %{QUERY_STRING} http\ [NC,OR]
```

```
RewriteCond %{QUERY_STRING} https\ [NC,OR]
```

```
RewriteCond %{QUERY_STRING} \\=\\u\\ [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} (\.\/|\/\.\.\/|\/\.\.\.\/)+(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_includel allow_url_fopenl safe_model_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,L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]

```

```
# DENY BROWSER ACCESS TO THESE FILES
```

```
# wp-config.php, bb-config.php, php.ini, php5.ini, readme.html
```

```
# Replace Allow from 88.77.66.55 with your current IP address and remove the  
# pound sign # from in front of the Allow from line of code below to access 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>
```

```
# IMPORTANT!!! DO NOT DELETE!!! the END WordPress text below
```

```
# END WordPress
```

```
# BLOCK HOTLINKING TO IMAGES
```

```
# To Test that your Hotlinking protection is working visit http://altlab.com/htaccess_tutorial
```

```
#RewriteEngine On
```

```
#RewriteCond %{HTTP_REFERER} !^https?://(www\.)?add-your-domain-here\.com [NC]
```

```
#RewriteCond %{HTTP_REFERER} !^$
```

```
#RewriteRule . *\. (\.jpeg|\.jpg|\.gif|\.bmp|\.png)$ - [F]
```

```
# FORBID COMMENT SPAMMERS ACCESS TO YOUR wp-comments-post. php FILE  
# This is a better approach to blocking Comment Spammers so that you do not  
# accidentally block good traffic to your website. You can add additional  
# Comment Spammer IP addresses on a case by case basis below.  
# Searchable Database of known Comment Spammers http://www.stopforumspam.com/
```

```
<FilesMatch "^(wp-comments-post\. php)">
```

```
Order Allow,Deny
```

```
Deny from 46.119.35.
```

```
Deny from 46.119.45.
```

```
Deny from 91.236.74.
```

```
Deny from 93.182.147.
```

```
Deny from 93.182.187.
```

```
Deny from 94.27.72.
```

```
Deny from 94.27.75.
```

```
Deny from 94.27.76.
```

```
Deny from 193.105.210.
```

```
Deny from 195.43.128.
```

```
Deny from 198.144.105.
```

```
Deny from 199.15.234.
```

```
Allow from all
```

```
</FilesMatch>
```

```
# BLOCK MORE BAD BOTS RIPPERS AND OFFLINE BROWSERS
```

```
# If you would like to block more bad bots you can get a blacklist from
```

```
# http://perishablepress.com/press/2007/06/28/ultimate-htaccess-blacklist/
```

```
# You should monitor your site very closely for at least a week if you add a bad bots list
```

```
# to see if any website traffic problems or other problems occur.
```

```
# Copy and paste your bad bots user agent code list directly below.
```