

```
# BULLETPROOF . 52. 9 >>>>>> SECURE . HTACCESS

# PHP/PHP. INI HANDLER/CACHE CODE
# Use BPS Custom Code to add php/php.ini Handler and Cache htaccess code and to save it permi
# Most Hosts do not have/use/require php/php.ini Handler htaccess code

# 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
# 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

# BRUTE FORCE LOGIN PAGE PROTECTION
# PLACEHOLDER ONLY
# Use BPS Custom Code to add Brute Force Login protection code and to save it permanently.
# See this link: http://forum.ait-pro.com/forums/topic/protect-login-page-from-brute-force-1
# for more information.

# 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, Referering link, the
# requested resource, the user agent of the hacker and the query string used in the hack at:
# 011 BPS has files for htaccess protected so that only you can view them
```

```
# All BPS log files are ntaccess 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-security/
# The 400, 410 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
# 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]
```

```
Redirect 403 ^.*$
```

```
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 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|imgurl|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|imgurl|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} ^.*demo2.local.*
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|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} \=\\|\\| [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)/self/(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)cPath=http://(.*)$ [NC,OR]
RewriteCond %{QUERY_SCRIPT} (<|>|%) .*script.*(<|>|%) [NC,OR]
RewriteCond %{QUERY_SCRIPT} (<|>|%) ([^s]*)+cript.*(<|>|%) [NC,OR]
RewriteCond %{QUERY_SCRIPT} (<|>|%) .*embed.*(<|>|%) [NC,OR]
RewriteCond %{QUERY_SCRIPT} (<|>|%) ([^e]*)+mbed.*(<|>|%) [NC,OR]
RewriteCond %{QUERY_SCRIPT} (<|>|%) .*object.*(<|>|%) [NC,OR]
RewriteCond %{QUERY_SCRIPT} (<|>|%) ([^o]*)+bject.*(<|>|%) [NC,OR]
RewriteCond %{QUERY_SCRIPT} (<|>|%) .*iframe.*(<|>|%) [NC,OR]
RewriteCond %{QUERY_SCRIPT} (<|>|%) ([^i]*)+frame.*(<|>|%) [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]*)+select [NC,OR]
RewriteCond %{QUERY_STRING} union([^\a]*a)+11([^\s]*)+select [NC,OR]
RewriteCond %{QUERY_STRING} \-[sdcrl].*(allow_url_includel allow_url_fopenl safe_model_disable_1
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
# To be able to view these files from a Browser, replace 127.0.0.1 with your actual

```

```
# current IP address. Comment out: #Require all denied and Uncomment: Require ip 127.0.0.1
# Comment out: #Deny from all and Uncomment: Allow from 127.0.0.1
# Note: The BPS System Info page displays which modules are loaded on your server.

<FilesMatch "^(wp-config\.php|php\.(ini|php5\.(ini|readme\.(html|bb-config\.php))>
<IfModule mod_authz_core.c>
Require all denied
#Require ip 127.0.0.1
</IfModule>

<IfModule !mod_authz_core.c>
<IfModule mod_access_compat.c>
Order Allow,Deny
Deny from all
#Allow from 127.0.0.1
</IfModule>
</IfModule>
</FilesMatch>

# HOTLINKING/FORBID COMMENT SPAMMERS/BLOCK BOTS/BLOCK IP/REDIRECT CODE
# PLACEHOLDER ONLY
# Use BPS Custom Code to add custom code and save it permanently here.
```