

BULLETPROOF . 51. 4 WP-ADMIN SECURE . HTACCESS

DO NOT ADD URL REWRITING IN THIS FILE OR WORDPRESS WILL BREAK

RewriteRule ^(.*)*\$ - [F] works in /wp-admin without breaking WordPress

RewriteRule . /index.php [L] will break WordPress

WPADMIN DENY BROWSER ACCESS TO FILES

Deny Browser access to /wp-admin/install.php

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

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

the /wp-admin/install.php file directly from your Browser.

BEGIN BPS WPADMIN DENY ACCESS TO FILES

```
<FilesMatch "^(install\.php)">
```

```
Order Allow,Deny
```

```
Deny from all
```

```
#Allow from 88. 77. 66. 55
```

```
</FilesMatch>
```

END BPS WPADMIN DENY ACCESS TO FILES

BEGIN OPTIONAL WP-ADMIN ADDITIONAL SECURITY MEASURES:

BEGIN CUSTOM CODE WPADMIN TOP

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

END CUSTOM CODE WPADMIN TOP

BEGIN EXAMPLE OF OPTIONAL/ADDITIONAL SECURITY MEASURES

EXAMPLE WP-ADMIN DIRECTORY PASSWORD PROTECTION - .htpasswd

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

This code example from BEGIN EXAMPLE to END EXAMPLE is just an example of optional

code that you could add to your wp-admin htaccess file in the CUSTOM CODE WPADMIN TOP text

IMPORTANT: To setup Directory Password Protection use your web host control panel.

This example code is just showing you what the code will look like after you setup

Directory Password Protection using your web host control panel.

NOTES: Adding Directory Password Protection creates an additional password login

to gain access to your wp-admin folder/WordPress Login page.

Users / visitors to your site will not be able to register or login to your site

unless you give them the Directory Password Protection username and password.

You can modify a single example here or use valid users to allow all valid

```

# you can specify a single specific user or use valid-user to allow all valid
# user accounts to be able to login to your site.

# EXAMPLE:
#AuthType basic
#AuthGroupFile /dev/null
#AuthUserFile /path/to/protected/server/directory/.htpasswd
#AuthName "Password Protected Area"
#require user JohnDoe
#require valid-user
# END EXAMPLE OF OPTIONAL/ADDITIONAL SECURITY MEASURES

# END OPTIONAL WP-ADMIN ADDITIONAL SECURITY MEASURES

# REQUEST METHODS FILTERED
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^(TRACE|DELETE|TRACK|DEBUG) [NC]
RewriteRule ^(.*)$ - [F]

# BEGIN CUSTOM CODE WPADMIN PLUGIN/FILE SKIP RULES
# To add wp-admin plugin skip/bypass rules use BPS wp-admin Custom Code.
# If a plugin is calling a wp-admin file in a way that it is being blocked/forbidden
# by BPS you can whitelist that file name by creating a skip rule for that file.
#
# Example: skip/bypass rule for the admin-ajax.php file and post.php file
# RewriteCond %{REQUEST_URI} (admin-ajax\.php|post\.php) [NC]
# RewriteRule . - [S=2]
#
# The [S] flag is used to skip following rules. Skip rule [S=2] will skip 2 following Rewri
# The skip rules MUST be in descending consecutive number order: 4, 3, 2...
# If you add a new skip rule above skip rule 2 it will be skip rule 3: [S=3]
#
# Example: Multiple skip rules in descending consecutive number order.
# Yoast Facebook OpenGraph wp-admin plugin skip/bypass rule
# RewriteCond %{QUERY_STRING} page=wpseo_social&key=(.*) [NC]
# RewriteRule . - [S=3]
# skip/bypass rule for the admin-ajax.php file and post.php file
# RewriteCond %{REQUEST_URI} (admin-ajax\.php|post\.php) [NC]
# RewriteRule . - [S=2]
#
" END CUSTOM CODE WPADMIN PLUGIN/FILE SKIP RULES

```

END CUSTOM CODE WPADMIN PLUGIN/FILE SKIP RULES

DEFAULT WHITELIST SKIP RULE FOR WP PRESS THIS

RewriteCond %{REQUEST_URI} (press-this\.php) [NC]

RewriteRule . - [S=1]

BEGIN BPSQSE-check BPS QUERY STRING EXPLOITS AND FILTERS

WORDPRESS WILL BREAK IF ALL THE BPSQSE FILTERS ARE DELETED

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

RewriteCond %{HTTP_USER_AGENT} (%0A|%0D|%27|%3C|%3E|%00) [NC, OR]

RewriteCond %{HTTP_USER_AGENT} (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) [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} \\=PHPI[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]*)script\\.(>|%3E) [NC, OR]

RewriteCond %{QUERY_STRING} (<|%3C)\\.iframe\\.(>|%3E) [NC, OR]

RewriteCond %{QUERY_STRING} (<|%3C)([^\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} ^\\.*(\\(|\\)|<|>\\.)* [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} (;|<|>|'|"|\)| %0A| %0D| %22| %27| %3C| %3E| %00). *
</\*| union| select| insert| drop| delete| update| cast| create| char| convert| alter| declare| order| scr
[NC, OR]
RewriteCond %{QUERY_STRING} (sp_executesql) [NC]
RewriteRule ^(.*)$ - [F]
# END BPSQSE-check BPS QUERY STRING EXPLOITS AND FILTERS
```