

```
# BULLETPROOF . 52. 8 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 Custom Code to modify/edit/change this code and to save it permanently.
# To be able to view the install.php file 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.

# BEGIN BPS WPADMIN DENY ACCESS TO FILES
<FilesMatch "^(install\.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>
# 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.
# CCWTOP
# 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.
```

```

# 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 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 RewriteRules.
# 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]
..

```



```

RewriteCond %{QUERY_STRING} (<| %3C). *script. *(>| %3E) [NC, OR]
RewriteCond %{QUERY_STRING} (<| %3C)([^\s]*s)+cript. *(>| %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} ^. *(<| \| \| | <| >). * [NC, OR]
RewriteCond %{QUERY_STRING} (NULL| outfile| load_file) [OR]
RewriteCond %{QUERY_STRING} (&| %26, %2F)+(<| %3C| %3E| %0A| %0D| %00) [NC, OR]
RewriteCond %{QUERY_STRING} (<| %3C| %3E| %0A| %0D| %00) [NC, OR]
RewriteCond %{QUERY_STRING} concat[^\[]*\[^\]]*&) [NC, OR]
RewriteCond %{QUERY_STRING} union([^\s]*s)+elect [NC, OR]
RewriteCond %{QUERY_STRING} union([^\a]*a)+11([^\s]*s)+elect [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

```