

```
# BULLETPROOF , 48.5 WP-ADMIN SECURE , HTACCESS
```

```
# If you edit the BULLETPROOF , 48.5 WP-ADMIN 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  
# BPS is also checking that the string BPSQSE exists in this file - do not delete it  
# If you would like to change what is displayed above you  
# will need to edit the BPS functions.php file to match your changes  
# For more info see the BPS Guide at AIT-pro.com
```

```
# DO NOT ADD URL REWRITING IN THIS FILE OR WORDPRESS WILL BREAK  
# RewriteRule ^(.*)$ - [F,L] - works in /wp-admin without breaking WordPress  
# RewriteRule . /index.php [L] - will break WordPress
```

```
# ADD WP-ADMIN FILE NAMES TO FILESMATCH MAKING THEM 403 FORBIDDEN  
# DENY BROWSER ACCESS TO WP-ADMIN INSTALL.PHP  
# Add the wp-admin file names to FilesMatch and deny direct browser access to them.  
# This would generate a HTTP 403 Forbidden error message instead of a 404 error.  
# The root .htaccess file already has a security rule that blocks access to all  
# /wp-admin/includes files in the wp-admin folder. Directly trying to access  
# files with a browser in the wp-admin folder results in 404 HTTP errors, which is  
# essentially the same protection that making the files forbidden 403 would achieve.  
# Making /wp-admin/install.php forbidden is not really necessary, but has been  
# added as an additional security measure.  
# To allow yourself browser access to install.php 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.
```

```
<FilesMatch "^(install\.php|example\.php|example2\.php|example3\.php)">  
Order allow,deny  
Deny from all  
#Allow from 88.77.66.55  
</FilesMatch>
```

```
# BEGIN OPTIONAL WP-ADMIN ADDITIONAL SECURITY MEASURES:
```

```
# BEGIN CUSTOM CODE WPADMIN TOP: Add miscellaneous custom code here  
# CCWTOP  
# END CUSTOM CODE WPADMIN TOP
```

```
# WP-ADMIN DIRECTORY PERMISSION PROTECTION - STARTED
```

```
# WP-ADMIN DIRECTORY PASSWORD PROTECTION - .htpasswd
# The BPS root .htaccess file already has a security rule that blocks access to all
# /wp-admin/includes files in the wp-admin folder.
# The wp-admin directory already requires authentication to gain access to your
# wp dashboard. Adding a second layer of authentication is not really necessary.
# Users / visitors to your site will not be able to register or login
# to your site without also having the additional login information.
# htpasswd encrypts passwords using either a version of MD5 modified for Apache,
# or the system's crypt() routine. Files managed by htpasswd may contain both types
# of passwords; some user records may have MD5-encrypted passwords while others in
# the same file may have passwords encrypted with crypt().
# User accounts and passwords can be added in your host Control Panel or directly
# in the .htpasswd file.
# The .htpasswd file should be in a Server protected directory and not in a public
# directory.
# 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 Zippy
#require valid-user
```

```
# ADD YOUR CURRENT IP ADDRESS TO THIS FILE
```

```
# This will then require that you FTP to your site and manually change the IP
# address in this .htaccess file. And users will not be able to register or login
# to your site without having their IP addresses added to this file. It is possible
# to automate this, but unfortunately in order to not lock you out of your own site
# the IP address would have to be removed on exiting your site. This means that if
# you are not currently logged in then no additional security is in effect.
# If you are not going to access or login to your site for a long time and you
# are not allowing additional users to access your site then
# manually adding an IP address may be an option you want to use temporarily.
```

```
# EXAMPLE:
```

```
#AuthUserFile /dev/null
#AuthGroupFile /dev/null
#AuthName "Password Protected Area"
```

```
## END OF FILE ##
```

```

#AuthType Basic
#order deny,allow
#deny from all
# whitelist home IP address
#allow from 64.233.169.99
# whitelist work IP address
#allow from 69.147.114.210
#allow from 199.239.136.200
# IP while in Kentucky; delete when back
#allow from 128.163.2.27

# END OPTIONAL WP-ADMIN ADDITIONAL SECURITY MEASURES

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

# BEGIN CUSTOM CODE WPADMIN PLUGIN FIXES: Add ONLY WPADMIN personal plugin fixes code here
# CCWPF
# END CUSTOM CODE WPADMIN PLUGIN FIXES

# Allow wp-admin files that are called by plugins
# Fix for WP Press This
RewriteCond %{REQUEST_URI} (press-this\.php) [NC]
RewriteRule . - [S=1]

# BPSQSE-check BPS QUERY STRING EXPLOITS AND FILTERS
# WORDPRESS WILL BREAK IF ALL THE BPSQSE FILTERS ARE DELETED
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|clshttp|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) [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]{16} [NC,OR]
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} \= \| \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) .*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} (\. / | \. . / | \. . . /) +(mod|etc|bin) [NC,OR]
RewriteCond %{QUERY_STRING} (localhost|loopback|127\.\.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) +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,L]

```