

```
# BULLETPROOF . 50.1 >>>>>> SECURE . HTACCESS
```

```
# If you edit the BULLETPROOF . 50.1 >>>>>> 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.
```

```
# BEGIN WordPress
```

```
<IfModule mod_rewrite.c>  
RewriteEngine On  
RewriteBase /kaona/  
RewriteRule ^index\.php$ - [L]  
RewriteCond %{REQUEST_FILENAME} !-f  
RewriteCond %{REQUEST_FILENAME} !-d  
RewriteRule . /kaona/index.php [L]  
</IfModule>
```

```
# END WordPress
```

```
# BEGIN WordPress
```

```
<IfModule mod_rewrite.c>  
RewriteEngine On  
RewriteBase /kaona/  
RewriteRule ^index\.php$ - [L]  
RewriteCond %{REQUEST_FILENAME} !-f  
RewriteCond %{REQUEST_FILENAME} !-d  
RewriteRule . /kaona/index.php [L]  
</IfModule>
```

```
# END WordPress
```

```
# BEGIN WordPress
```

```
<IfModule mod_rewrite.c>  
RewriteEngine On  
RewriteBase /kaona/  
RewriteRule ^index\.php$ - [L]  
RewriteCond %{REQUEST_FILENAME} !-f  
RewriteCond %{REQUEST_FILENAME} !-d  
RewriteRule . /kaona/index.php [L]  
</IfModule>
```

```
# END WordPress
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /kaona/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /kaona/index.php [L]
</IfModule>
```

```
# END WordPress
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /kaona/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /kaona/index.php [L]
</IfModule>
```

```
# END WordPress
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /kaona/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /kaona/index.php [L]
</IfModule>
```

```
# END WordPress
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /kaona/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
```

```
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /kaona/index.php [L]
</IfModule>

# END WordPress
# This removes all of the BPS security code and replaces it with just the default WP
htaccess code
# To restore this file use BPS Restore or activate BulletProof Mode for your Root folder
again.

# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /kaona/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /kaona/index.php [L]
</IfModule>

# END WordPress

# BLOCK HOTLINKING TO IMAGES
# To Test that your Hotlinking protection is working visit
http://alt1ab.com/htaccess_tutorial.html
#RewriteEngine On
#RewriteCond %{HTTP_REFERER} !^https?://(www\.)?add-your-domain-here\.com [NC]
#RewriteCond %{HTTP_REFERER} !^$
#RewriteRule .*\. (jpegl jpgl gifl bml 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.
```