```
# BEGIN Far Future Expiration Plugin
<IfModule mod_expires.c>
ExpiresActive on
<FilesMatch "\.(gif|jpeg|jpg|png|ico|js|css|swf)$">
ExpiresDefault "access plus 240 hours"
</FilesMatch>
</IfModule>
# END Far Future Expiration Plugin

# BEGIN All In One WP Security
#AIOWPS_BLOCK_SPAMBOTS_START
<IfModule mod_rewrite.c>
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{REQUEST_URI} ^(.*)?wp-comments-post\.php(.*)$
RewriteCond %{HTTP_REFERER} !^http(s)?://mirens\.com [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^$
RewriteRule .* http://127.0.0.1 [L]
</IfModule>
#AIOWPS_BLOCK_SPAMBOTS_END
# END All In One WP Security

<IfModule mod_headers.c>
<FilesMatch "\.(js|css|xml|gz)$">
Header append Vary: Accept-Encoding
</FilesMatch>
</IfModule>

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

# END WordPress

<Files 403.shtml>
order allow,deny
```

```
order allow,deny
allow from all
</Files>

deny from 115.
deny from 60.
deny from 125.
deny from 175.
deny from 139.
deny from 122.
deny from 221.
deny from 111.
deny from 113.
deny from 119.
```