What to shove up your .htaccess

Simon Bragg
http://sibra.co.uk

Cambridge Wordpress Meetup August 2018

The .htaccess file

.htaccess files enable:

- Configuration changes to directory and sub-directory;

- Without accessing httpd.conf,
  - Usually allowed;

- Short commands:
  - key value pair.

If you screw it up syntax, you get:

Error 500 internal server error

What you can do

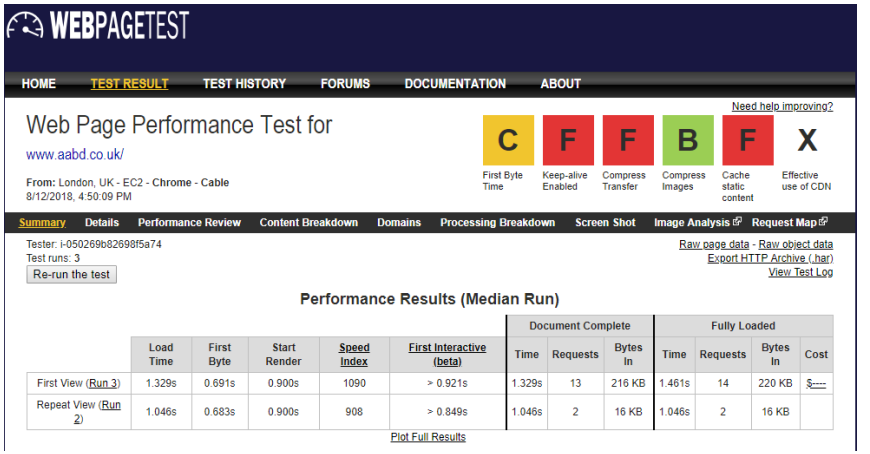
Can:

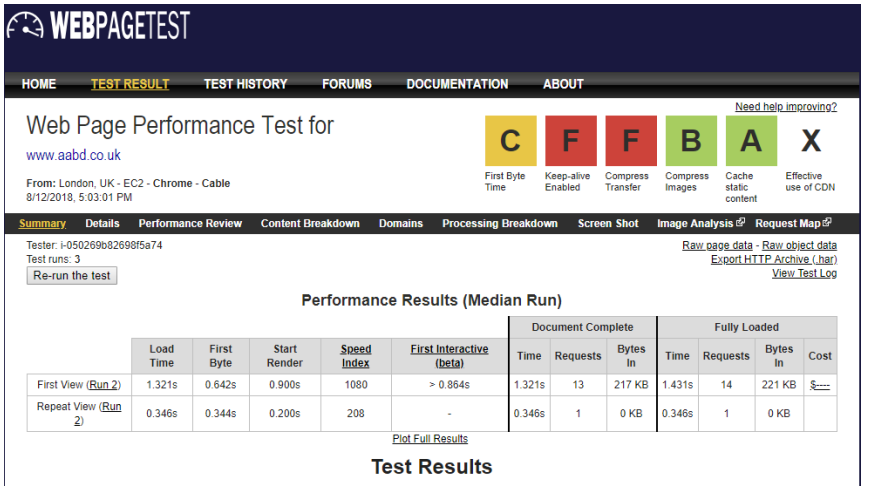
- Browser caching
- gzip compression for file transfer
- Keep alive
- Regex for redirects
- Security enhancements

Browser caching

```
## EXPIRES CACHING ##
<IfModule mod_expires.c>
ExpiresActive On
ExpiresByType image/jpg "access plus 1 year"
ExpiresByType image/jpeg "access plus 1 year"
ExpiresByType image/gif "access plus 1 year"
ExpiresByType image/png "access plus 1 year"
ExpiresByType text/css "access plus 1 year"
ExpiresByType application/pdf "access plus 1 month"
ExpiresByType application/x-shockwave-flash "access
plus 1 month"
ExpiresByType image/x-icon "access plus 1 year"
ExpiresByType text/javascript "access 1 month"
ExpiresByType text/x-javascript "access 1 month"
ExpiresByType application/javascript "access 1 month"
ExpiresByType application/x-javascript "access 1 month"
ExpiresByType application/json "access 1 month"
ExpiresByType application/vnd.ms-fontobject "access
plus 1 year"
ExpiresByType application/x-font-ttf "access plus 1
year"
ExpiresByType application/x-font-opentype "access plus
1 year"
ExpiresByType application/x-font-woff "access plus 1
year"
ExpiresByType image/svg+xml "access plus 1 year"


ExpiresDefault "access plus 2 days"
</IfModule>
## EXPIRES CACHING ##
```



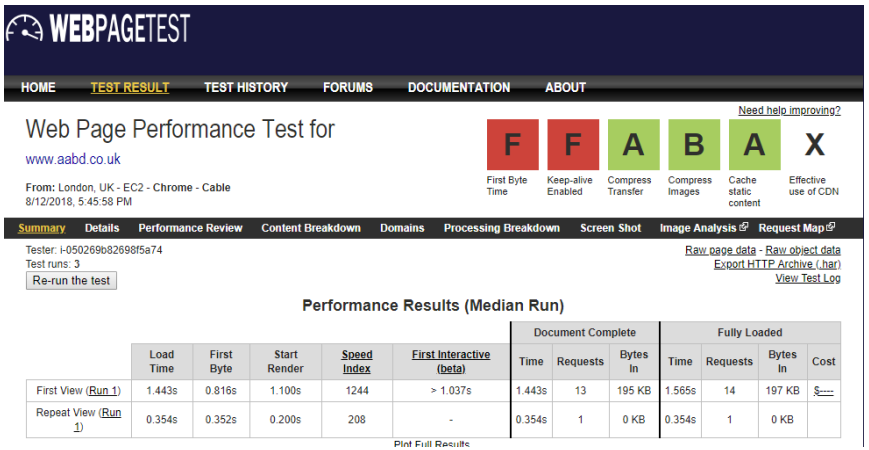


Compress transfer: gzip

After Wordpress stuff

```
<IfModule mod_filter.c>
    AddOutputFilterByType DEFLATE "application/atom+xml" \
                                  "application/javascript" \
                                  "application/json" \
                                  "application/ld+json" \
                                  "application/manifest+json" \
                                  "application/rdf+xml" \
                                  "application/rss+xml" \
                                  "application/schema+json" \
                                  "application/vnd.geo+json" \
                                  "application/vnd.ms-fontobject" \
                                  "application/x-font-ttf" \
                                  "application/x-javascript" \
                                  "application/x-web-app-manifest+json" \
                                  "application/xhtml+xml" \
                                  "application/xml" \
                                  "font/eot" \
                                  "font/opentype" \
                                  "image/bmp" \
                                  "image/svg+xml" \
                                  "image/vnd.microsoft.icon" \
                                  "image/x-icon" \
                                  "text/cache-manifest" \
                                  "text/css" \
                                  "text/html" \
                                  "text/javascript" \
                                  "text/plain" \
                                  "text/vcard" \
                                  "text/vnd.rim.location.xloc" \
                                  "text/vtt" \
                                  "text/x-component" \
                                  "text/x-cross-domain-policy" \
                                  "text/xml"

</IfModule>
```



Keep alive, if allowed by host

At end of .htaccess file

```
 ## KEEP ALIVE ##
<ifModule mod_headers.c>
    Header set Connection keep-alive
</ifModule>
## END ENABLE KEEP ALIVE ##
```

But cheapo host doesn't allow this.

RedirectMatch for Regex redirects

Have mod_rewrite.c enabled for #Begin Wordpress stuff.

So can use Regex to redirect multiple pages in one line. Some Examples:

Perhaps for tweaking URL structure:
.* means anything, (.*) means whatever, and repeat in $1

```
RedirectMatch 301 .*/employment/employee-shares/(.*)
http://www.website.co.uk/employee-shares/$1
```

^ means start of string, (/D) means 1 non digit character.

```
RedirectMatch 301 ^/share(\D)options$
http://www.website.co.uk/employee-shares/
```

Use of OR for multiple redirects to one page:

```
RedirectMatch 301 ((/introducing-the-
pod/)|(/products/pod/)|(/about-us/the-vision/)|(/cambridge-
pod/)) https://website.co.uk/pod/
```

http to https

When have http site and converting to https, add in bold

```
 <IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /

RewriteCond %{HTTPS} !=on
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

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

Bits of code

1. Protect important files, deny access to them:

```
<FilesMatch "^.*(error_log|wp
config\.php|php.ini|\.[hH][tT][aApP].*)$">
Order deny,allow
Deny from all
</FilesMatch>
```

Check php.ini, is php.ini

2. Prevent directory browsing /wp-content/uploads/

```
Options All -Indexes
```

3. Block unauthorized execution of PHP files.

Most hackers upload backdoors to /uploads folder

```
<Directory "/var/www/wp-content/uploads/">
<Files "*.php">
Order Deny,Allow
Deny from All
</Files>
</Directory>
```

4. Protect against Script injections

Hackers change Wordpress GLOBALS & REQUEST variables, so:

```
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (<|%3C).*script.*(>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|[|%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|[|%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]
```

Bits of code 2

5. Secure wp-includes directory

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
</IfModule>
```

6. Prevent username enumeration

Visitor who enters `your-site.com/?author=1` finds username. One less thing to guess. Just needs the password. So:

```
RewriteCond %{QUERY_STRING} author=d
RewriteRule ^ /? [L,R=301]
```

7. Prevent hot linking

Most hackers upload backdoors to /uploads folder

```
RewriteEngine On RewriteCond %{HTTP_REFERER} !^$ RewriteCond %{HTTP_REFERER}
!^http://(www\.)?your-site.com/.*$ [NC] RewriteRule \.(gif|jpg)$
http://www.your-site.com/hotlink.gif [R,L]Directory "/var/www/wp-
content/uploads/">
```

And replace `http://www.your-site.com/hotlink.gif` with image url you want to protect

xmlrpc.php blocking?

Xmlrpc : remote procedure call using XML to encode, and http for transport

Enables you to:
Post using weblog clients e.g. Windows Live Writer, IFTTT

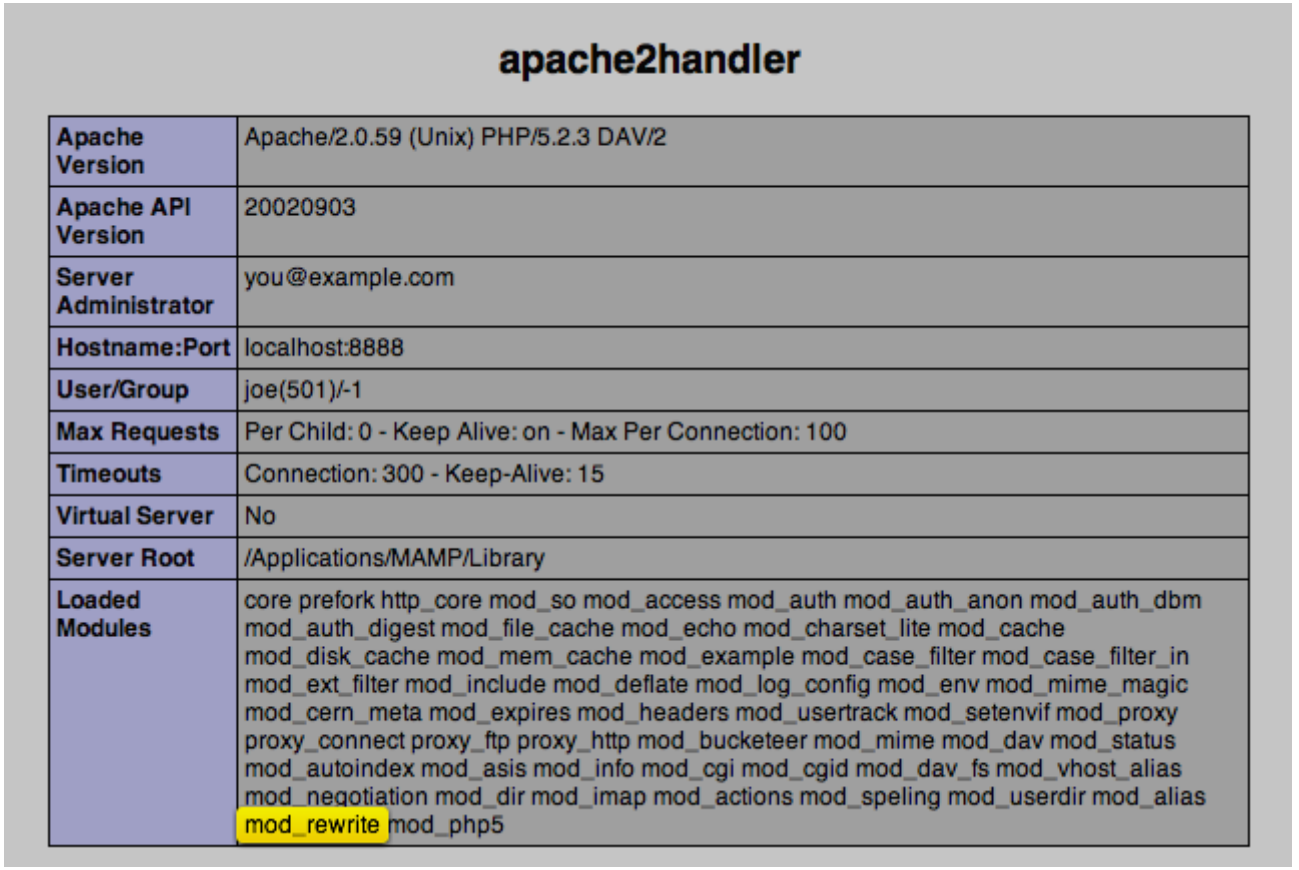
Was a security concern, although not any more.

If want to block:

```
# Block WordPress xmlrpc.php requests
<Files xmlrpc.php>
order deny,allow
deny from all
allow from 123.123.123.123
</Files>
```

What is available

- Set up page with:
  - `<?php phpinfo(); ?>`



apache2handler

Apache Version	Apache/2.0.59 (Unix) PHP/5.2.3 DAV/2
Apache API Version	20020903
Server Administrator	you@example.com
Hostname:Port	localhost:8888
User/Group	joe(501)/-1
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 15
Virtual Server	No
Server Root	/Applications/MAMP/Library
Loaded Modules	core prefork http_core mod_so mod_access mod_auth mod_auth_anon mod_auth_dbm mod_auth_digest mod_file_cache mod_echo mod_charset_lite mod_cache mod_disk_cache mod_mem_cache mod_example mod_case_filter mod_case_filter_in mod_ext_filter mod_include mod_deflate mod_log_config mod_env mod_mime_magic mod_cern_meta mod_expires mod_headers mod_usertrack mod_setenvif mod_proxy proxy_connect proxy_ftp proxy_http mod_bucketeer mod_mime mod_dav mod_status mod_autoindex mod_asis mod_info mod_cgi mod_cgid mod_dav_fs mod_vhost_alias mod_negotiation mod_dir mod_imap mod_actions mod_speling mod_userdir mod_alias mod_rewrite mod_php5

Discussion