Đây là một file thường nằm trong thư mục root của hosting. Các web server như Apache sử dụng nó để cấu hình bảo mật các thư mục trên host. Khi truy cập một thư mục có chứa file .htaccess thường là thư mục root sẽ có một hộp thoại yêu cầu nhập username và password, chỉ khi nào bạn nhập đúng mật khẩu mới có thể xem được trong thư mục root có gì.

Tại sao file này có dấu chấm “ .” đó là do các web server qui định những file có dấu “.” Đằng trước là file cấu hình , và các file này sẽ bị ẩn đi khi bạn duyệt các thư mục được bảo vệ bằng file .htacces. Nó có thể điều khiển, cấu hình được nhiều việc hữu ích bằng cách thay đổi các thông số mặc định do apache quản lý. File .htaccess có tác dụng trên thư mục chứa nó và toàn bộ các thư mục con chính vì thế .htaccess thường được lưu trữ trên thư mục root nhằm bảo mật thông tin cho website của bạn. Chính vì liên quan tới vấn đề bảo mật nên .htaccess phải có sự bảo mật riêng để tránh sự truy cập trái phép từ bên ngoài và thông thường nó được chmod 644.

.htaccess là một công cụ rất mạnh trong việc quản lí website. Một lỗi cú pháp nhỏ (thậm chí là một khoảng trắng) cũng khiến website của bạn hoạt động không được bình thường như trước. Sau khi áp dụng .htaccess, bạn nên kiểm tra một lượt website của mình xem .htaccess có gây ra lỗi ở phần, trang con nào không? Do vậy trước khi làm việc với .htaccess, bạn nên backup cẩn thận dữ liệu của mình, nếu có trục trặc xảy ra, việc khôi phục trở nên đơn giản.

.htaccess cho phép bạn cấu hình mà không cần động chạm vào cấu hình chính của Apache. Tuy nhiên, về mặt hiệu năng và bảo mật, nếu có thể, bạn nên sử dụng httpd.conf hơn là sử dụng .htaccess. Cụ thể, khi được cấu hình để sử dụng .htaccess, thì Apache sẽ tìm kiếm tất cả những folder có chứa .htaccess để thực thi, và nó sẽ thực thi tất cả những file .htaccess tìm được. Do vậy, sẽ làm website của bạn trở nên ì ạch một cách không cần thiết. Nếu website của bạn là website cá nhân, hoặc ít người truy cập, thì đó là chuyện nhỏ. Nhưng nếu là một website đại chúng (báo điện tử, trang nhạc, film..) thì đây là một vấn đề rất lón. Do vậy .htaccess chỉ có tác dụng trong trường hợp bạn không có quyền cấu hình trên httpd.conf của Apache.

Những vấn đề thường gặp có thể xử lý bằng .htaccess.

1. Bỏ hoặc thêm www cho domain

Bạn nghĩ rằng domain website dạng www.domain.com và http://domain.com là 1? Nhưng Searrch Engine không nghĩ như vậy họ xem 2 URL trên là 2 cái khác nhau chính vì thế khi làm SEO cho web bạn phải chú ý vấn đề này. Phải thực hiện redirect về một trang 2 dang URL trên.

# Thêm WWW vào URL  
RewriteEngine On  
RewriteBase /  
RewriteCond %{HTTP\_HOST} !^www.taka.com.vn$ [NC]  
RewriteRule ^(.\*)$ http://www.taka.com.vn/$1 [L,R=301]

# Không thêm WWW vào URL  
RewriteEngine On  
RewriteBase /  
RewriteCond %{HTTP\_HOST} !^taka.com.vn$ [NC]  
RewriteRule ^(.\*)$ http://taka.com.vn/$1 [L,R=301]

Bạn có thể tìm hiểu thêm về các loại [**301 redirect**](http://taka.com.vn/redirect-301-chuyen-huong-301-la-gi/) với file .htaccess

2. Cấm truy cập với 1 ip hoặc dải ip cụ thể

Đôi khi để hạn chế truy cập từ 1 ip hoặc dải ip nào đó vì lí do spam bạn có thể sử dụng những dòng lệnh sau:

allow from all  
deny from 124.90.94.138  
deny from 124.90

Dòng thứ 2 dùng để chặn 1 ip còn dòng thứ 3 là chặn luôn một dải ip. bạn có thể thay địa chỉ ip tương ứng vào đoạn code phía trên.

3. Bỏ “category” trong URL của wordpress

khi bạn [**thiết kế website**](http://taka.com.vn/) bằng wordpress thì mặc định URL của một bài post thuộc category nào đó sẽ có dạng như: http://taka.com.vn/category/bai-post.html. Để đảm bảo tính sạch sẽ cho URL của website bạn sẽ muốn bỏ chữ category này đi. Lúc này bạn sử dụng đoạn code:

RewriteRule ^category/(.+)$ http://taka.com.vn/$1 [R=301,L]

4. Thêm dấu “/” vào cuối URL

#Thêm / vào cuối URL  
RewriteBase /  
RewriteCond %{REQUEST\_FILENAME} !-f  
RewriteCond %{REQUEST\_URI} !#  
RewriteCond %{REQUEST\_URI} !(.\*)/$  
RewriteRule ^(.\*)$ http://taka.com.vn/$1/ [L,R=301]

5. Chống hotlink

Nhiều người copy bài viết của bạn và copy luôn cả link ảnh gây hao tốn băng thông của website để ngăn chặn việc này bạn sử dụng đoạn lệnh sau:

Options +FollowSymlinks  
#No hotlink  
RewriteEngine On  
RewriteCond %{HTTP\_REFERER}!^$  
RewriteCond %{HTTP\_REFERER}!^http://(www.)?taka.com.vn/[nc]  
RewriteRule .\*.(gif|jpg|png)$ http://taka.com.vn/images/nohotlink.gif[nc]

6. Không cho truy cập file wp-config.php của WordPress

Rất nhiều người sử dụng wordpress để [**thiết kế web**](http://taka.com.vn/thiet-ke-website) và đã quá quen thuộc với file wp-config.php, đây là file rất quan trọng vì nó chứa thông tin username và password database chính vì thế cần có chế độ bảo vệ thích hợp với những dòng lệnh sau:

# Bảo mật file wpconfig.php  
  
order allow,deny  
deny from all

7. Bật tính năng nén file Gzip

Với tính năng này các file trên server được nén giúp cho website tải nhanh hơn

AddOutputFilterByType DEFLATE text/html text/plain text/xml application/xml application/xhtml+xml text/javascript text/css application/x-javascript  
BrowserMatch ^Mozilla/4 gzip-only-text/html  
BrowserMatch ^Mozilla/4.0[678] no-gzip  
BrowserMatch bMSIE !no-gzip !gzip-only-text/html

8. Giới hạn kích thước file upload

Cấp phép cho người dùng upload lên host với một kích thước nhất định sẽ hạn chế được hao tốn tài nguyên. đoạn lệnh dưới đây giới hạn upload là 10MB

# Giới hạn đến 10mb  
LimitRequestBody 10240000

9. Bỏ phần mở rộng của file có đuôi .php

khi bạn lập trình web bằng php thì URL thường có phần mở rộng là .php. Vì lý do nào đó bạn muốn URL trong sạch sẽ không có đuôi .php ở sau lúc đó bạn sử dụng đoạn code dưới đây.

RewriteRule ^(([^/]+/)\*[^.]+)$ /$1.php [L]