htaccess File Configuration - Best Practices

This document contains various .htaccess file configurations and their explanations. These configurations help improve your website's security, performance, SEO, and user experience. Make sure to use them based on your website's requirements.

# 1. Disable Directory Listing

Code:  
Options -Indexes  
  
Explanation:  
- Disables directory listing, which prevents visitors from seeing files in a folder if no index file exists. This enhances security by protecting your files from being exposed to the public.

# 2. Redirect HTTP to HTTPS

Code:  
RewriteEngine On  
RewriteCond %{HTTPS} off  
RewriteRule ^ https://%{HTTP\_HOST}%{REQUEST\_URI} [L,R=301]  
  
Explanation:  
- Forces the website to always redirect from HTTP to HTTPS for enhanced security. This ensures that all traffic between users and the server is encrypted.

# 3. Block Hotlinking

Code:  
RewriteEngine On  
RewriteCond %{HTTP\_REFERER} !^$  
RewriteCond %{HTTP\_REFERER} !^https://(www\.)?yourdomain.com [NC]  
RewriteRule \.(jpg|jpeg|png|gif|pdf)$ - [F,NC]  
  
Explanation:  
- Blocks other websites from hotlinking to your images or media files, preventing unauthorized use of your resources. This helps save bandwidth and improves security.

# 4. Prevent Image Hotlinking with Custom Image

Code:  
RewriteEngine On  
RewriteCond %{HTTP\_REFERER} !^$  
RewriteCond %{HTTP\_REFERER} !^https://(www\.)?yourdomain.com [NC]  
RewriteRule \.(jpg|jpeg|png|gif)$ /path/to/custom-image.jpg [L]  
  
Explanation:  
- If hotlinking is detected, it redirects to a custom image instead of the blocked media. This maintains your bandwidth.

# 5. Block Access to Specific IPs

Code:  
Order Deny,Allow  
Deny from 192.168.1.100  
Allow from all  
  
Explanation:  
- Blocks specific IP addresses from accessing the website, useful for blocking unwanted or malicious visitors.

# 6. Password Protect Directories (Basic Authentication)

Code:  
<Directory "/path/to/protected-directory">  
 AuthType Basic  
 AuthName "Restricted Area"  
 AuthUserFile /path/to/.htpasswd  
 Require valid-user  
</Directory>  
  
Explanation:  
- Adds basic authentication to a directory, requiring a username and password to access the resources.

# 7. Set Up Custom Error Pages

Code:  
ErrorDocument 404 /404.html  
ErrorDocument 403 /403.html  
ErrorDocument 500 /500.html  
  
Explanation:  
- Specifies custom error pages for different error codes, enhancing user experience by guiding users when they encounter an error.

# 8. Leverage Browser Caching for Performance

Code:  
<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 text/css "access plus 1 month"  
 ExpiresByType application/javascript "access plus 1 month"  
</IfModule>  
  
Explanation:  
- Sets expiration dates for files, enabling browser caching to improve website loading time and performance.

# 9. Rewrite URLs for Clean and SEO-friendly Links

Code:  
RewriteEngine On  
RewriteRule ^about-us$ /about.html [L]  
RewriteRule ^services$ /services.html [L]  
  
Explanation:  
- Rewrites URLs for clean, descriptive, and SEO-friendly URLs, which improve search engine rankings.

# 10. Allow Only Specific File Types for Uploads

Code:  
<FilesMatch "\.(jpg|jpeg|png|gif|pdf)$">  
 Order Allow,Deny  
 Allow from all  
</FilesMatch>  
  
Explanation:  
- Restricts the file types that users can upload to only a specified list, such as images or PDFs.