.htaccess Security and Blacklist Control

BRUCE JACKSON

WEBSICHERHEIT

Protect specific folders

Secure “uploads” or other “777” directory from unwanted file types

```
<FilesMatch "\.(php|php3|php4|php5|sh)$">
    Deny from All
</FilesMatch>
```

Password protect a directory – create .htaccess in the directory with:

```
AuthType Basic
AuthName “Restricted area"
AuthUserFile .htpasswd
require valid-user
```

Block all Proxies – use with care!

```
RewriteCond %{HTTP:VIA}                    !^$ [OR]
RewriteCond %{HTTP:FORWARDED}              !^$ [OR]
RewriteCond %{HTTP:USERAGENT_VIA}          !^$ [OR]
RewriteCond %{HTTP:X_FORWARDED_FOR}        !^$ [OR]
RewriteCond %{HTTP:PROXY_CONNECTION}       !^$ [OR]
RewriteCond %{HTTP:XPROXY_CONNECTION}      !^$ [OR]
RewriteCond %{HTTP:XROXY_CONNECTION}       !^$ [OR]
RewriteCond %{HTTP:HTTP_PC_REMOTE_ADDR}    !^$ [OR]
RewriteCond %{HTTP:HTTP_CLIENT_IP}         !^$ [OR]
RewriteCond %{HTTP:HTTP_PROXY_CONNECTION} !^$
RewriteRule ^(.*)$ - [F]
```

Trap most automated SPAM bots

If they are requesting resources, then they're probably not bots.

```
RewriteCond %{REQUEST_FILENAME} (mytheme\.css|\.jpg)$ [NC]
RewriteRule .* - [L,co=human:abides:%{HTTP:Host}:86400]
```

Second, check incoming POST Requests to see if they have that cookie set,

Check if this is a POST request, the human cookie must be set..

```
RewriteCond %{REQUEST_METHOD} =POST
RewriteCond %{REQUEST_URI} !=/index.php [NC]
RewriteCond %{HTTP_COOKIE} !^.*human.*$ [NC]
RewriteRule .* - [F]
```

Block Referrer Spam

Block referrer spam such as Semalt

```
RewriteCond %{HTTP_REFERER} ^http://.*youtubedownload\.org/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*soundfrost\.org/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*joingames\.org/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*videofrost\.net/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*feedouble\.com/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*fbfreegifts\.com/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*savetubevideo\.com/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*kambasoft\.com/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*buttons\-for\-website\.com/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*7makemoneyonline\.com/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*darodar\.com/ [NC,OR]
RewriteCond %{HTTP_REFERER} ^http://.*semalt\.com/ [NC]
RewriteRule ^(.*)$ - [F,L]
```

Useful Information

- Control Website for Blacklisting / Malware
  - http://www.websicherheit.at/web-security-check/
  - https://www.virustotal.com/
  - http://perishablepress.com/5g-blacklist-2013/
  - http://winginx.com/en/htaccess

    For nginx Server, convert Apache htaccess commands into nginx compatible commands

Thanks for your attention

DOWNLOAD SLIDES:

WEBSICHERHEIT.AT/2015/CMS-SECURITY-TALK-WIEN

WEBSICHERHEIT