Web-Server: Bilder/Dateien schützen

Problem:

Viele 'Content-Diebe' binden auf ihren Homepages Bilder oder Download-Dateien von fremden Servern ein ohne auf die Quelle hinzuweisen.
Nachteil für den Server-Betreiber:
Er hat den Traffic an der Backe.

Weitere Infos: www.trafficklau.de

Lösungen:

1.) per mod_rewrite:

Hier entscheidet mod_rewrite anhand des Referers, ob das Bild von der aktuellen Domain geladen wird oder nicht:

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www.)?huschi.net(/.*)?$ [NC]
RewriteRule .(gif|jpg)$ - [F]
```

Das sorgt dafür, daß deutliche verminderter Traffic entsteht. Wenn man auf den Datenklau hinweisen will, kann man eine passende dazu Grafik erstellen und die letzte Zeile austauschen:

```
RewriteRule .(gif|jpg)$ http://www.huschi.net/images/bloed.gif [R,L]
```

2a) per PHP-/Perl-Script (ohne Server-Zugriff):

Ein nutzt ein PHP- oder Perl-Script um die Bilder aus einem geschützten Verzeichnis (z.B. cgi-bin, .htaccess-Schutz oder ausserhalb des DocumentRoots). Alle Bilder werden ausschließlich über die URL des Scriptes in HTML eingebunden. Das Script kann dann anhand verschiedener Kriterien Unterscheiden, ob es das Bild ausliefern darf/soll oder eben nicht:

- Referer

- Cookie

- Session-ID

2b) per PHP-/Perl-Script: (mit Server-Zugriff)

Man setzte in der Server-Config (VirtualHost / Directory) einen Action-Handler für die MIME-Types:

```
Action image/gif /cgi-bin/images.cgi
Action image/jpg /cgi-bin/images.cgi
Action image/png /cgi-bin/images.cgi
```


(c) 2024 huschi <huschi@huschi.net>

Web-Server: Bilder/Dateien schützen

(siehe: Apache 2.0 Documentation)

Eindeutige ID: #1057
huschi
2006-01-20 09:25

(c) 2024 huschi <huschi@huschi.net>
URL: https://www.huschi.net/index.php?action=artikel&cat=10&id=58&artlang=de