DisableImageHotLinking

Disable Image Hot Linking

In this How-To guide, we will show you how to disable image hot linking using two methods:

1. mod_rewrite 2. SetEnvIfNoCase and FilesMatch

Using mod_rewrite

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !=""
RewriteCond %{HTTP_REFERER} !^https?://([^/]*)?example\.com/ [NC]
RewriteRule \.(jpe?g|gif|png)$ - [F,NC]
```

This rewrite rule will throw a forbidden if the referer isn't your domain. All png, jpeg, and gif images will not be shown in the web page that is hot linking to your images.

Using SetEnvIfNoCase and FilesMatch

```
SetEnvIfNoCase Referer "^https?://([^/]*)?example\.com/" local_ref=1
SetEnvIf Referer ^$ local_ref=1

<FilesMatch "\.(jpe?g|gif|png)$">
  Order Allow,Deny
  Allow from env=local_ref
</FilesMatch>
```

This SetEnvIf checks the referer and sets a local environment variable if the referer contains your domain. The FilesMatch then matches the request for jpeg, png, and gif files. If there's a match in the filename, then access to that resource is only allowed if the local environment variable is set.

In both methods, you might want to add patterns to the referer checks since there might be more ways your site will be accessed by - localhost for localhost testing, IP address, LAN hostname, etc.

The same holds true for the file extension match. For any other kind of resources you would like to protect, add their file extensions to the file extension pattern.

In both cases, requests that do not specify a referer are allowed entry in order to keep the site working for users that disable the referer for privacy reasons. This does not materially affect the usefulness of the recipes, because the people inlining images on their websites cannot control the referer header sent by visiting clients.

Note that the misspelling of referrer above is intentional and necessary due to a spelling error in the original HTTP specification.