HotLink Protection - x3

For cPanel & WHM version 58

(Home >> Security >> HotLink Protection)

Warning:
This document describes functionality from cPanel's **deprecated** x3 theme. We **strongly** recommend that you use cPanel's current theme (Paper Lantern) instead.

- We **removed** the deprecated x3 theme from new installations in cPanel & WHM version 60.
  - Make **certain** that you read the appropriate documentation for your version of cPanel & WHM.
  - For more information, read our What's My Version Number documentation.
- cPanel's Paper Lantern theme does **not** include certain x3 theme-specific features.
  - For a complete list of Paper Lantern features, read our cPanel Features List documentation.
  - If you need a feature that the Paper Lantern theme does not include, submit a feature request.

Overview

A hotlink occurs when someone embeds content from your site in another site and uses your bandwidth to serve the files. You can use this interface to prevent this issue.

Notes:
- When you disable hotlinks, make certain that you allow hotlinks for any necessary domains. For example, your website's subdomains and the URL that you use to access your cPanel account.
- If the URL that you use to access your cPanel account does not appear in the *List the URLs to which you wish to allow access* list, you may not see embedded images in the *HTML Editor - x3* in the *File Manager - x3* interface (*Home* >> *Files* >> *File Manager*).

Enable hotlink protection

To enable hotlink protection, perform the following steps:

1. Click *Enable.*
2. To allow specific sites to hotlink to your site, add their URLs to the *List the URLs to which you wish to allow access* list.
3. To block direct access to files of specific types, add those file extensions to the *Block direct access for the following extensions* list.
   - For example, to block all `.jpg` images, add `.jpg` to the *Block direct access for the following extensions* list.
   - When you block these file types, others **cannot** hotlink those types of files from your website, regardless of any other settings.
4. To allow visitors access to specific content through the URL, select the *Allow direct requests* option.
   - For example, if you enable this option, a visitor could enter `http://www.example.com/folder/example.jpg` as a URL to access the `example.jpg` file.
5. To redirect requests for certain content, enter the URL to which you want to redirect your visitor in the *Redirect the request to the following URL* text box.
6. Click *Submit*.

Disable hotlink protection

To disable hotlink protection, click *Disable*.

Note:
When you click *Disable*, the system deletes the entries in the *List the URLs to which you wish to allow access* list. We **strongly** recommend that you save the list locally before you disable hotlink protection.