HK2

CSP (Content Security Policy)

Basant Mandal

15th July, 2023

Introduction

This Module **HK2 CSP Whitelisting** is for Magento version 2.3.5 or above & It whitelist some of the major urls like *Cloudflare, Google Analytics, Google Fonts, Fontawesome, Addthis, Googleapis, Facebook Graph, Pinterest, Vimeo, Twitter, Trust Pilot* & ContentSquare.

One can disable Magento 2 CSP. However, Disabling results in more possibilities of attacks on the Magento store. (CSP) are a powerful tool to mitigate against **Cross Site Scripting (XSS)** and related attacks.

When does this type of error occur?

- If you have added any external JS Script Link in your theme/module.
- If you added an external Stylesheet Link in your theme/module.
- If you added an external Iframe in your theme/module.

If you face these types of CSP Errors or the error mentioned in the screenshot?

Errors Like :-

- **Refused to Frame** https://demosite.com
- **Refused to Load the Script** https://demosite.com
- **Etc, CSP Policy Issues**
- **Violate Content Security Policy Directive**

The above errors can be sorted out by using this module. But don't forget to check whether the problematic url is listed below on the Whitelist URLs Section. If not, Please Check the **Section - How Does The Extension Work** else this module won't work in your case. This Module does not disable the CSP Policy, rather it whitelists some of the common urls which are mentioned below.

Installation Guide

1. Setup :- Extract the zip folder in app/code
2. Run :- **php bin/magento module:enable HK2_Csp**
3. Run :- **php bin/magento setup:upgrade** from your magento directory

Once Installed, You can check in **Magento Frontend - Browser Console**, Whether you are facing any more CSP Policy Issues.

Note:- Please check the URLs which are whitelisted below. This Module does not disable the CSP Policy, rather it whitelists some of the common urls which are mentioned below.

How Does The Extension Work?

You can add a domain to the whitelist for a policy (like script-src, style-src, font-src and others) by updating the csp_whitelist.xml present in **/app/code/HK2/Csp/etc/csp_whitelist.xml.** Please only create rules for URLs that you have verified as safe & safe for your Magento Store. Ensure that you use a unique "id" (e.g. the URL) for each entry within its group.

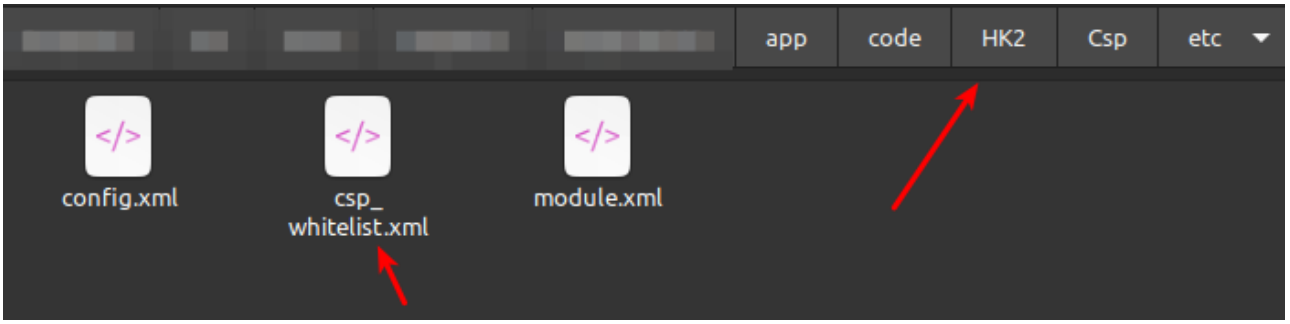
Below screenshot describes Policy Name & Description.

POLICY NAME	DESCRIPTION
`default-src`	The default policy.
`base-uri`	Defines which URLs can appear in a page's `<base>` element.
`child-src`	Defines the sources for workers and embedded frame contents.
`connect-src`	Defines the sources that can be loaded using script interfaces.
`font-src`	Defines which sources can serve fonts.
`form-action`	Defines valid endpoints for submission from `<form>` tags.
`frame-ancestors`	Defines the sources that can embed the current page.
`frame-src`	Defines the sources for elements such as `<frame>` and `<iframe>`.
`img-src`	Defines the sources from which images can be loaded.
`manifest-src`	Defines the allowable contents of web app manifests.
`media-src`	Defines the sources from which images can be loaded.
`object-src`	Defines the sources for the `<object>`, `<embed>`, and `<applet>` elements.
`script-src`	Defines the sources for JavaScript `<script>` elements.
`style-src`	Defines the sources for stylesheets.

How to add your own URL for Whitelisting in CSP?

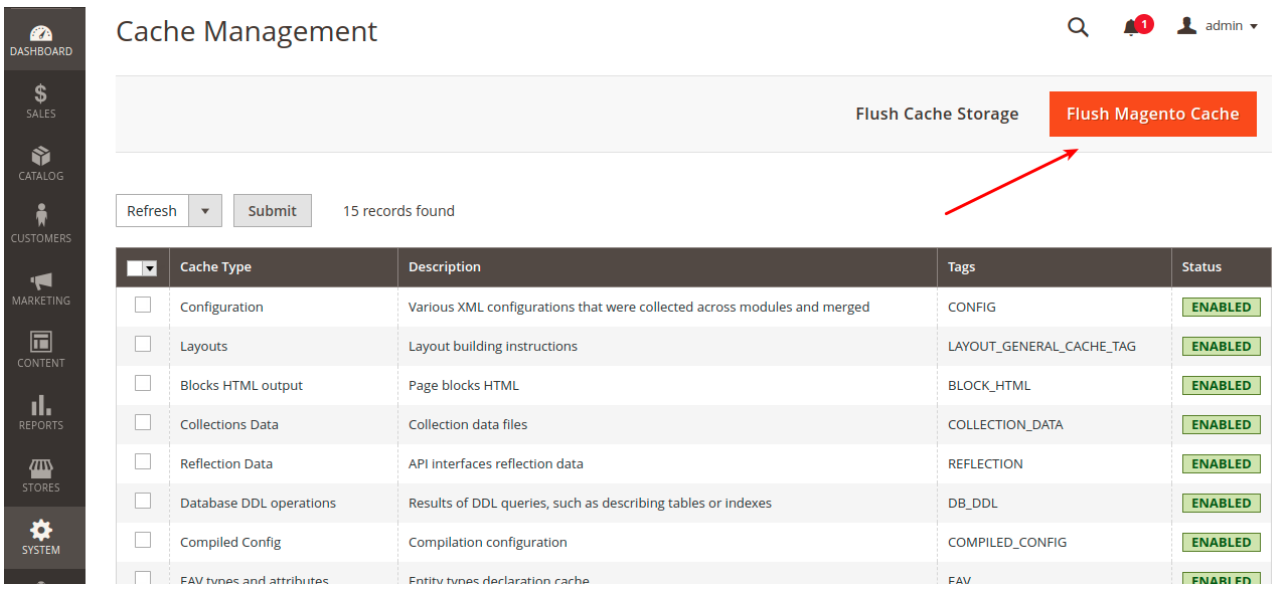
1. How to add your own URL for Whitelisting? -

   Step-1 Open *<magento_root>app/code/HK2/Csp/etc/csp_whitelist.xml* from your editor.



2. Now you have to add the url which you want to be whitelisted. Add the URL in the specific Policy, else it wont work. For Example:- Add your script url to be whitelisted in **script-src** & Stylesheet Src in **style-src**. For complete policy list you can visit this link :- https://developer.adobe.com/commerce/php/development/security/content-security-policies/#configure-csps-for-your-custom-codeextensiontheme

3. Once done, Save the file and Clean the Cache from Admin - System - Tools - Cache Management



Once done, You can see your url has been whitelisted. In case of any error, try checking in a private tab or start from Step-1

For more information you can check the following link on how to add links to whitelist

- **How to Add Domain in Whitelisting**:- https://developer.adobe.com/commerce/php/development/security/content-security-policies/#add-a-domain-to-the-whitelist
- **Complete Information on CSP**:- https://developer.adobe.com/commerce/php/development/security/content-security-policies
- **Types of CSP & Policy Name & Description:-** https://developer.adobe.com/commerce/php/development/security/content-security-policies/#configure-csps-for-your-custom-codeextensiontheme

Screenshot of the *app/code/HK2/Csp/etc/csp_whitelist.xml*. Where you can add your whitelist urls.

```xml
<?xml version="1.0"?>
<!--
/**
 * @Info        Whitelisting CSP
 * @author      Basant Mandal - HK2
 * @copyright   Copyright (c) 2022 Basant Mandal - HK2
 * @package     HK2_Csp
 * @version     1.0.0
 */
-->
<csp_whitelist xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="urn:magento:module:Magento_Csp/etc/csp_whitelist.xsd">
    <policies>
        <policy id="script-src">
            <values>
                <value id="addthis.com" type="host">*.addthis.com</value>
                <value id="ajaxgoogleapis" type="host">*.googleapis.com</value>
                <value id="cloudflare" type="host">*.cloudflare.com</value>
                <value id="fontawesome" type="host">*.fontawesome.com</value>
                <value id="google" type="host">*.google.com</value>
                <value id="google-analytics" type="host">*.google-analytics.com</value>
                <value id="googletagmanager.com" type="host">googletagmanager.com</value>
                <value id="graph-facebook" type="host">graph.facebook.com</value>
                <value id="gstatic" type="host">*.gstatic.com</value>
                <value id="addthis.moatads.com" type="host">*.moatads.com</value>
                <value id="trustpilot" type="host">*.trustpilot.com</value>
                <value id="vimeo" type="host">*.vimeo.com</value>
                <value id="widgets-pinterest" type="host">widgets.pinterest.com</value>
            </values>
        </policy>
        <policy id="style-src">
            <values>
                <value id="cloudflare" type="host">*.cloudflare.com</value>
                <value id="fontawesome" type="host">*.fontawesome.com</value>
                <value id="googleapis" type="host">*.googleapis.com</value>
                <value id="gstatic" type="host">*.gstatic.com</value>
                <value id="twitter.com" type="host">*.twitter.com</value>
            </values>
        </policy>
        <policy id="img-src">
            <values>
                <value id="cloudflare" type="host">*.cloudflare.com</value>
                <value id="data" type="host">data:</value>
                <value id="google-analytics" type="host">*.google-analytics.com</value>
                <value id="paypal" type="host">*.paypal.com</value>
                <value id="twitter.com" type="host">*.twitter.com</value>
                <value id="vimeocdn" type="host">*.vimeocdn.com</value>
            </values>
        </policy>
        <policy id="connect-src">
            <values>
                <value id="cloudflare" type="host">*.cloudflare.com</value>
                <value id="paypal" type="host">*.paypal.com</value>
                <value id="twitter.com" type="host">*.twitter.com</value>
            </values>
        </policy>
        <policy id="font-src">
            <values>
                <value id="cloudflare" type="host">*.cloudflare.com</value>
                <value id="fontawesome" type="host">*.fontawesome.com</value>
                <value id="fontawesomecdn" type="host">*.bootstrapcdn.com</value>
                <value id="googleapis" type="host">*.googleapis.com</value>
                <value id="gstatic" type="host">*.gstatic.com</value>
                <value id="twitter.com" type="host">*.twitter.com</value>
            </values>
        </policy>

        <policy id="frame-src">
            <values>
                <value id="addthis.com" type="host">*.addthis.com</value>
                <value id="google.com" type="host">*.google.com</value>
                <value id="trustpilot" type="host">*.trustpilot.com</value>
                <value id="twitter.com" type="host">*.twitter.com</value>
                <value id="vimeo" type="host">*.vimeo.com</value>
            </values>
        </policy>

    </policies>
</csp_whitelist>
```

Features

1. Fully Customizable as per your Store needs. Please read the above documentation on how to add your own URL for CSP Whitelisting.
2. Simple, 100% Open Source & Free.
3. CSP is not disabled rather specific listed urls are whitelisted, keeping your Magento Store Safe.

Disclaimer

1. **Basant Mandal (HK2 - Hash Tag Kitto)** does not make any warranties about the completeness, reliability and accuracy of this image or its related products. Any action you take upon the information you find here is strictly at your own risk.
2. **Basant Mandal (HK2 - Hash Tag Kitto)** will not be liable for any losses and/or damages in connection with the use of our website.

Support - Bug Reporting

For Bug reporting, Please open an issue at https://github.com/basantmandal/HK2-ScrollTop/issues on GitHub. When filing a bug remember that the better written the bug is, the more likely it is to be fixed.

In case of any feedback or any feature additions feel free to contact at support@hashtagkitto.co.in

Whitelisted Urls

Some of the Default URL Whitelisted in module HK2 CSP

- Addthis (moatads is a part of Addthis)
- Cloudflare
- Facebook Graph
- Fontawesome
- Google Analytics, Google Fonts, Gstatic, Google Tag Manager & Googleapis
- Pinterest
- Trust Pilot
- Twitter
- Vimeo
- ContentSquare

Complete List of URL Whitelisted

scripts-src whitelisted

- *.addthis.com
- *.googleapis.com
- *.cloudflare.com
- *.fontawesome.com
- *.google.com
- *.google-analytics.com
- googletagmanager.com
- graph.facebook.com
- *.gstatic.com
- *.moatads.com
- *.trustpilot.com
- *.vimeo.com
- Widgets.pinterest.com
- *.contentsquare.net

style-src whitelisted

- *.cloudflare.com
- *.fontawesome.com
- *.googleapis.com
- *.gstatic.com
- *.twitter.com

img-src whitelisted

- *.cloudflare.com
- data:
- *.google-analytics.com
- *.paypal.com
- *.twitter.com
- *.vimeocdn.com
- *.contentsquare.net

connect-src whitelisted

- *.cloudflare.com
- *.paypal.com
- *.twitter.com

font-src whitelisted

- *.cloudflare.com
- *.fontawesome.com
- *.googleapis.com</value>
- *.gstatic.com
- *.twitter.com

frame-src whitelisted

- *.addthis.com
- *.google.com
- *.trustpilot.com
- *.twitter.com
- *.vimeo.com