CSP Extension for Magento 2

Sprinix CSP (Content Security Policy) Extension helps to manage and whitelist to any host or external sources through configurations.

By Default, in Magento CSP module helps to detect and mitigate Cross-Site Scripting (XSS) and related data injection attacks, It can restrict browser content to allow only whitelisted resources to appear, whenever we had to add any external source, we had to manually upgrade and deploy it after adding it to the whitelist. Now with the help of Sprinix CSP extension , we just have to add our host or any external source in the config settings and it will already be whitelisted.

You can also add or manage the policies in csp_whitelist.xml which already exist in Sprinix CSP on path: app/code/Sprinix/CSP/etc/csp_whitelist.xml.

Installation Instructions

- Download 'Sprinix CSP Extension.zip' file .

- Extract 'Sprinix_CSP.zip' file to 'app/code/Sprinix/CSP'. You should create a folder path 'app/code/Sprinix/CSP' if not exist.

- Download '.overrides.zip' file .

- Extract '.overrides.zip' file to 'src'.

- Go to Magento root folder and run : bin/composer require kub-at/php-simple-html-dom-parser.

- bin/magento setup:upgrade;
- bin/magento setup:di:compile;
- bin/magento setup:static-content:deploy -f
- Add the below code in your src/composer.json file.

```
"extra": {
    "magento-force": "override",
    "no-git-submodules": true,
    "composer-exit-on-patch-failure": true
    },
    "scripts": {
        "composer-overrides": "cp -rf .overrides/*/ ./",
        "post-install-cmd": [
        "@composer-overrides"
        ]
      },
      "scripts-descriptions": {
        "composer-overrides": "Override folders in project root with those i
      n .overrides/ directory"
      }
```

- Then go to the root folder and run command : bin/composer install .
- Go to Magento root folder and run upgrade command line to install 'Sprinix_CSP'.
- bin/magento setup:upgrade
- bin/magento setup:di:compile
- bin/magento setup:static-content:deploy-f

Admin Store Configuration

To Configure the Sprinix CSP Extension for your stores follow the path given below:

STORES -> Configuration -> SPRINIX -> CSP

CSP Frontend Configuration

⊘ General Settings		
Enable [store view	Yes	•
Report Only [store view	Yes	•
	Setting to Enable/Disable Report only on Frontend.	
CSP Policie: [store view	<pre>5 <policies> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"> <policy id="style-src"></policy></policy></policy></policy></policy></policy></policy></policy></policy></policy></policy></policy></policy></policy></policy></policy></policies></pre>	-
		11

For the field, 'Enable', select Yes to enable the extension.

There are two modes in CSP; "Reports_Only" and "Restrict Mode". Ideally, Magento is always running with "Restrict Mode".

Restrict Mode:

In this mode, Magento acts on any policy violations. The browser will refuse to load nonwhitelisted content and report a CSP Error in the browser console.

	Eleme	nts	Console	Sources	Network	Performance	Memory	Application	Security	Lighthouse	Recorder 🗸	Performance insights ₫	◎ 1 ■ 1	® :	×
00	top 🔻	0	Filter									Default levels 🔻	2 Issues: 🗖	1 🗖 1	۲
 ▶ :::: @ ▶ ::: @ ▶ ::: @ ▶ :: @ ▶ :: @ ▶ :: @ 	1 message No user m 1 error No warnin No info No verbos	 95 > 2	Refused t following widgets.ma analytics fpdbs.san assets.br	o load the Content S agentocomu .google.co dbox.paypa aintreegat	image ' <u>ht</u> ecurity Po ecre.com d m <u>www.goog</u> 1.com *.vi eway.com c	tps://media.wi licy directive letagmanager.c letagmanager.c ,paypal.com i.y	red.com/phd "img-src addservices om *.ftcdn. timg.com *. cckout.payp	<pre>>rtos/593261c assets.adobec .com www.goo net * .behancu youtube.com yal.com *.payp al.com *.payp</pre>	/master/w 25 fm.com amcgi le-analytic e.net t.payp validator.sw al.com goog	60%2Cc limit// lobal.sc.omtro s.com googlead al.com www.pay agger.io www.pay agger.io wata:	<u>85120553.jpg</u> 't dc.net dpm.dem ds.g.doubleclit y <u>pal.com yww.pg</u> <u>sandbox,paypal</u> 'self' 'unsafe-	because it violates the <u>lo</u> dex.net <u>cm.everesttech.net</u> *.at <u>xpalobjects.com</u> fpdbs.paypal.e <u>com</u> b.stats.paypal.com dub.sta inline'".	al.magento obe.com bleclick.net om ts.paypal.cc	<u>com/:117</u> ; ; ;m	2

For Example, In the image attached above, CSP Refuses to load a image from "wired.com" as it is not on the CSP list.

Report Only:

Magento reports policy violations but doesn't block. By default, CSP violations are written to the browser console.

- 6		Elemen	ts	Console	Sources	Network	Performance	Memory	Application	Security	Lighthouse	Recorder 🗸	Performance insights 🛽	<mark>©</mark> 1	2		×
Œ	0	top 🔻	0	Filter									Defa	ult levels 🔻	2 Issue	es: 🗖 2	۲
2		1 message No user m 1 error No warnings No info No verbose	○ 5 5	[Report 0 violates widgets.n analytics fpdbs.sar assets.bu	bnly] Refus the follow angentocommunity .google.cc udbox.paypara caintreegat	ed to load ing Conten erce.com d m <u>www.goog</u> 1.com *.vw eway.com c	the image <u>int</u> t Security Pol- letagmanger.cc peocdm.com i.y .paypal.com cho	tps://media lcy directi addservices m *.ftcdn. img.com *. eckout.payp	wired.com/ph ve: "img-src com whw.goog net * behance youtube.com *.payp	hotos/593261 assets.ado 1 <u>e-analytic</u> .net t.payp aildator.so bal.com goog	<pre>c/master/w 2: edim.com ancgj s.com googleac al.com wiwi.pay agger.io wiwi.pay agger.io wiwi.pay le.com data: '</pre>	560%2Cc limit/8 lobal sc.omtrdc Sg.doubleclic (pal.com www.pa andbox.paypal. 'self' 'unsafe-	<pre>is120553.jpg' because it .net dpm.demdex.net cm.e upogle.com bid ypalobjects.com fpdbs.pa com b.stats.paypal.com d inline'".</pre>	local.m: veresttech. g.d.oublecl ypal.com ub.stats.pa	<u>gento.c</u> net *.a ick.net ypal.co	<u>com/:117</u> dobe.com	9

For the field, **'Reports Only'**, select No, if you want enable the "Restrict mode". By default it contains "Report Only" mode. So you can prepare the list of violated policies from browser console.

CSP Frontend Configuration

⊘ General Settings

Enable [store view]	Yes	•
Report Only [store view]	Yes K	*
	Some to Feadlan Icable Report Abill on France	
CCD Delision	Setting to chable/bisable report only on thoritend.	
CSP Policies [store view]	<policies> <policy id="style-src"> <values></values></policy></policies>	Î
CSP Policies [store view]	<pre><policies> <policy id="style-src"> <policy id="style-src"> <values> <value id="fonts-google-style" type="host">google.com</value></values></policy></policy></policies></pre>	*

Earlier, we had to add our policies in magento csp_whitelist.xml. But now, With the help of given field named '**CSP Policies**' we can directly add the policies in our configuration setting. As we used to add policies in csp_whitelist.xml with the same format as followed to add policies in this. And, the CSP policies that is written in csp_whitelist.xml by default and policies added here through provided configuration will be merged.

CSP Frontend Configuration		
⊖ General Settings		
Enable [store view]	Yes	•
Report Only [store view]	Yes Setting to Enable/Disable Report only on Frontend.	•
CSP Policies [store view]	<policies> <policy id="style-src"> <values> <value <br="" id="fonts-google-style">type="host">google.com</value> </values></policy></policies>	•

Auto Fix Inline Style:

Select "Yes" for the "Auto Fix Inline Style" field to autofix all the inline css.

CSP Frontend Configuration		
⊘ General Settings		
Enable [store view]	Ye	
Auto Fix Inline Script [store view]	Ye	
Auto Fix Inline Style [store view]	Yes 🔹	
Report Only [store view]	No Setting to Enable/Disable Report only on Frontend.	
CSP Policies [store view]	<policies></policies>	

Auto Fix Inline Script:

CSP Frontend Configuration

Select "Yes" for the "Auto Fix Inline Script" field to autofix all the inline script.

Yes
Yes
Yes
No
Setting to Enable/Disable Report only on Frontend.
<policies></policies>

To Configure the Magento CSP module for your stores follow the path given below:

STORES -> Configuration -> SECURITY -> Content Security Policy(CSP)

Report Only:

Stores -> Configuration -> Security -> Content Security Policy(CSP) -> Mode -> Storefront Default -> Report Only Select "No".

~	Mode	G	9
~	\odot Admin Default		
^	 ⊘ Storefront Default 		
	Report URI [store view]	URI to r yort CSP violations on storefront. Used for all storefro t pages that don't have own URI configured above.	
iel	Report Only [store view]	No Setting to Enable/Disable Report only on Frontend.	

Auto Fix Inline style:

Stores -> Configuration -> Security -> Content Security Policy(CSP) -> CSP Policies -> General Settings -> Styles -> Auto Fix Inline Style Select "No".

~	CSP Policies		$\overline{\bigcirc}$
~			
	🔗 General Settings		
~		1	
~			
	Auto Fix Inline Style [store view]	No	
	Auto Fix Inline Script [store view]	No	

Auto Fix Inline Script:

Stores -> Configuration -> Security -> Content Security Policy(CSP) -> CSP Policies -> General Settings -> Scripts -> Auto Fix Inline Script Select "No" .

Y		0
	CSP Policies	(\bigcirc)
~		
	⊘ General Settings	
~		
~	0	
	Auto Fix Inline Style [store view] No	
	⊖ Scripts	
	Auto Fix Inline Script	
	[store view]	