Nexcess

Content Security Policy Extension

USER MANUAL

Supported Version

Magento CE 1.9 & EE 1.14

Document Version 1.0

TABLE OF CONTENT

INTRODUCTION

WHAT IS CSP

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware.

To enable CSP, you need to configure your web server to return the Content-Security-Policy HTTP header (sometimes you will see mentions of the X-Content-Security-Policy header, but that's an older version and you don't need to specify it anymore).

USING CSP

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page. For example, a page that uploads and displays images could allow images from anywhere, but restrict a form action to a specific endpoint. A properly designed Content Security Policy helps protect a page against a cross site scripting attack. This article explains how to construct such headers properly, and provides examples.

Examples: Common use cases

Ex: 1 : Content-Security-Policy: default-src 'self' ;

Ex: 2 : Content-Security-Policy: default-src 'self' *.trusted.com

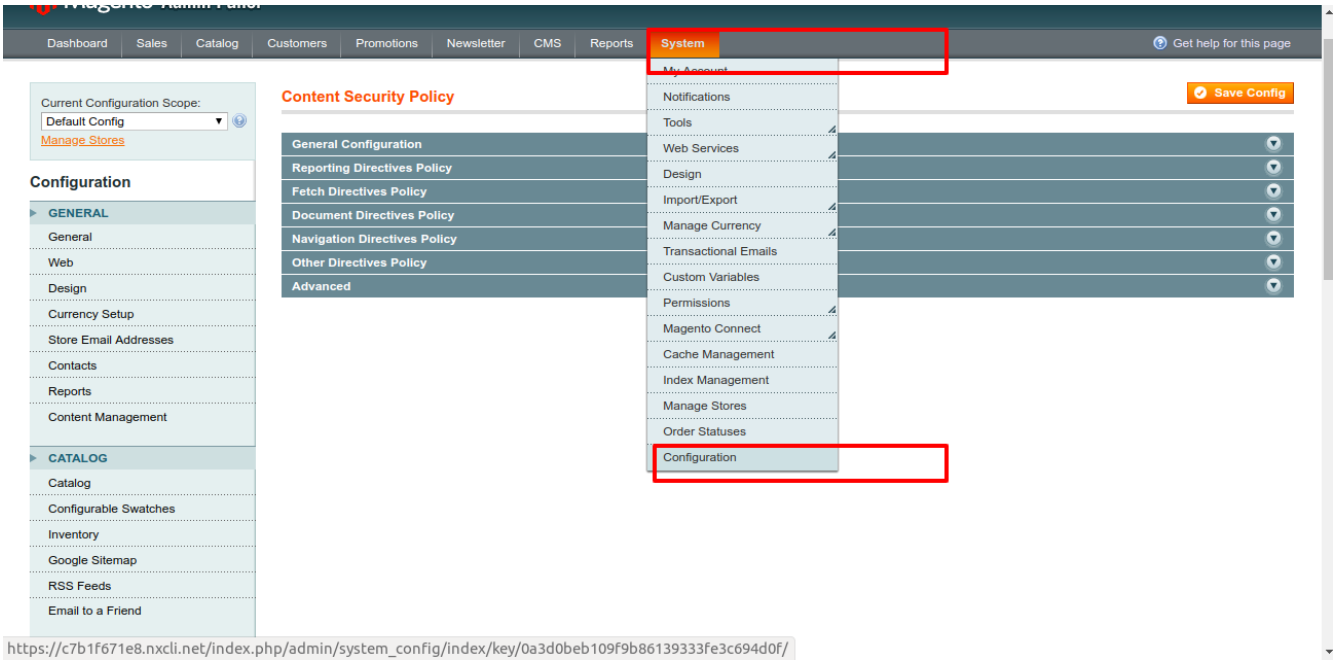
Ex: 3 : Content-Security-Policy: default-src 'self'; img-src *; media-src media1.com media2.com; script-src userscripts.example.com

MODULE CONFIGURATION

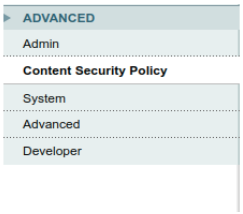
WHERE IS CSP MODULE ?

1. Login to Magento admin.

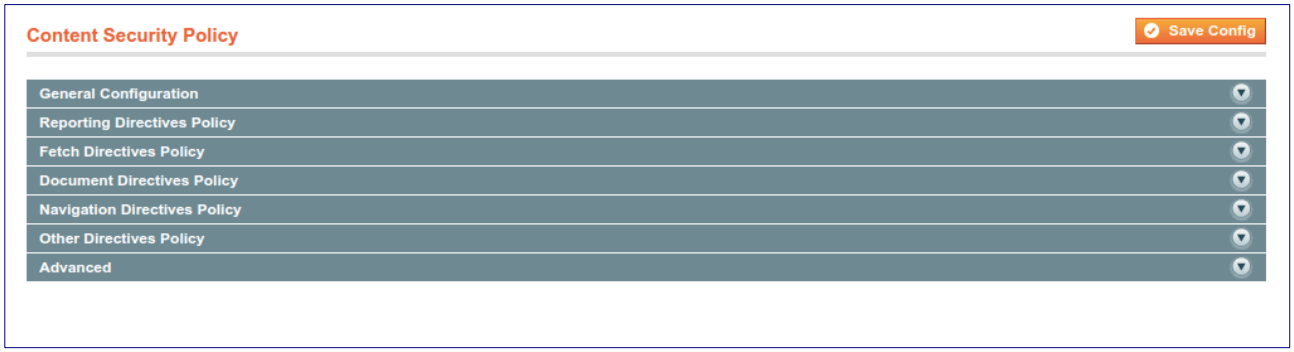
2. Navigate to **System > Configuration**.



3. Navigate to **Advanced** section which resides in last of all left options.



4 . Click on **Content Security Policy** menu



HOW DOES IT WORKS ?

All Policies are listed with some default sources . If you want to apply another source, override it in ADVANCE > POLICY section.

Steps for policy enable :

1. Enable Directives which required for trigger.
2. Select those you want to exclude (Optional).
3. If you want to add more source in any policy, exclude it from multi select and rewrite it in Advance section.
   (Because you can add policy only single time with one or many sources.)

CONFIGURATION

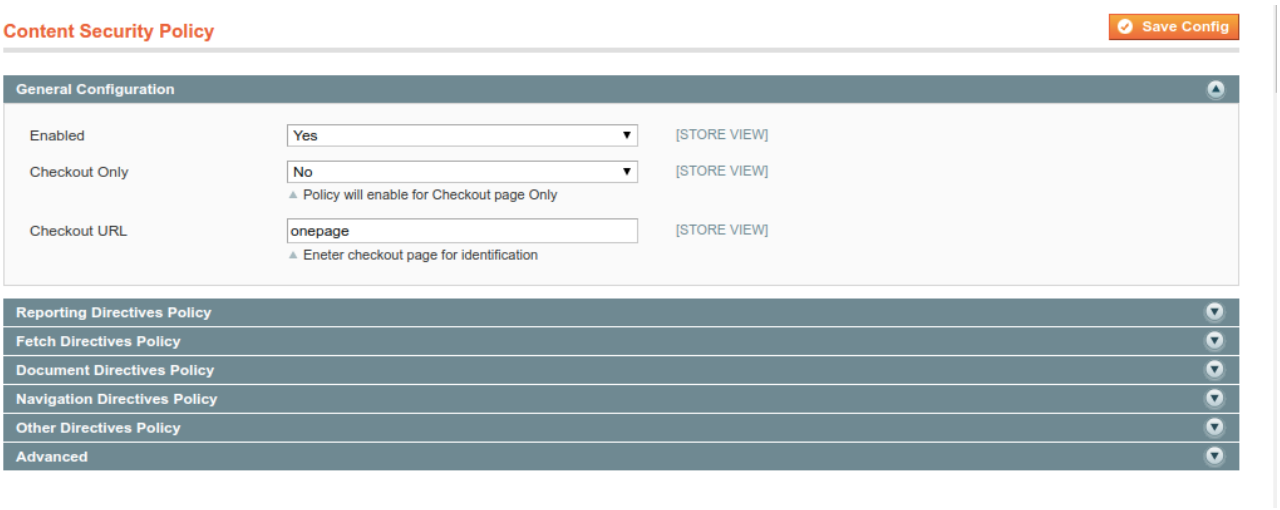
GENERAL SETTINGS

1. **Enabled** (Required) : This is a module configuration input for enable and disable. If you do not enable it, module would not work.

   Enable module by “Enable to Yes”.

2. **Checkout Only :** If you want to trigger policies in checkout page only, enable it by yes. If you keep it “No” policies will trigger on all pages (default case).

3. **Checkout URL** : Put checkout page URI in textbox



REPORTING DIRECTIVE POLICY

This section is for reporting and Monitoring information of website on third party reporting tool. Here we have given steps for https://report-uri.com/

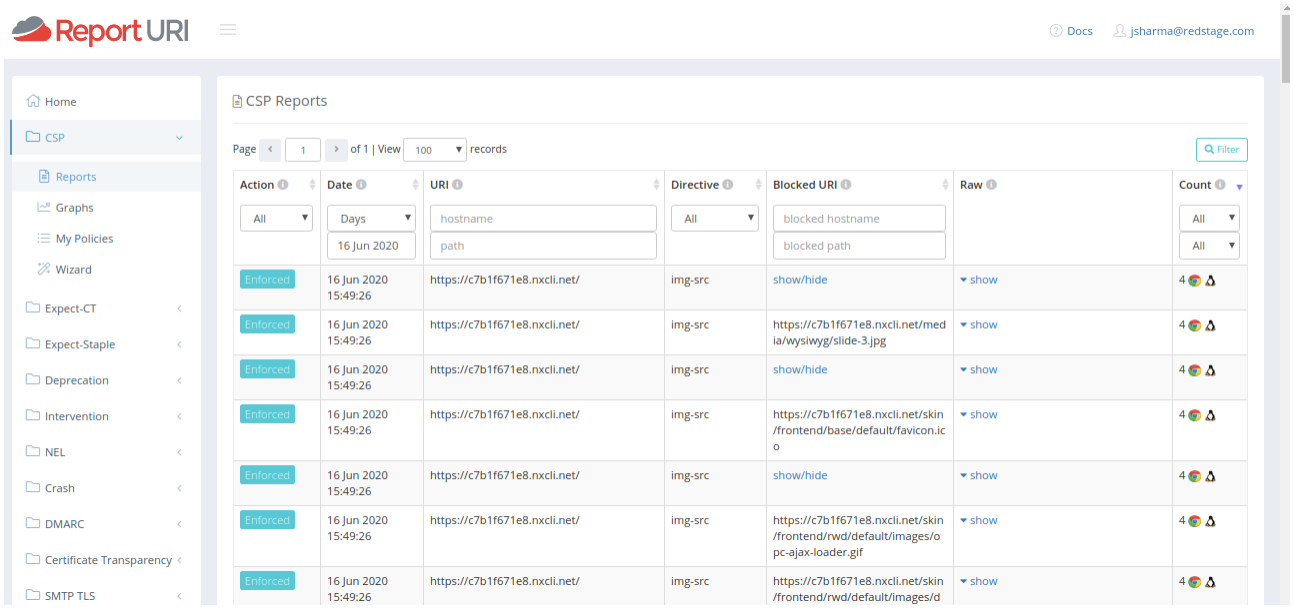
1. **Reporting Directives Policy :** Enable Reporting policy to 'Yes' if you want to add third party tool for monitoring policy status.
Set 'No' will not add any tool for reporting and monitoring.

2. **Report URI Subdomain :** Get URI subdomain by below steps and put it in textbox.
   - Go to https://report-uri.com/register/ and register for a free account.
   - Go to CSP->Wizard.
   - Click "Create your Wizard reporting address."
   - Copy your current subdomain.

For more information of configuration refer : https://docs.report-uri.com/

3. **Reporting Mode :** Select mode you want to trigger.
   - For maximum security, change the Reporting Mode to enforce.
   - Alternatively, you can set the Reporting Mode to Reporting Only (but if you do that on your live site, you'll probably surpass the free limit of Report-Uri.com).
   - I recommend you at least enable Checkout Lockdown which enforces your CSP on the checkout, which is the most vulnerable part of the site for js infections.

Result after connecting with Reporting tool :



FETCH DIRECTIVE POLICY

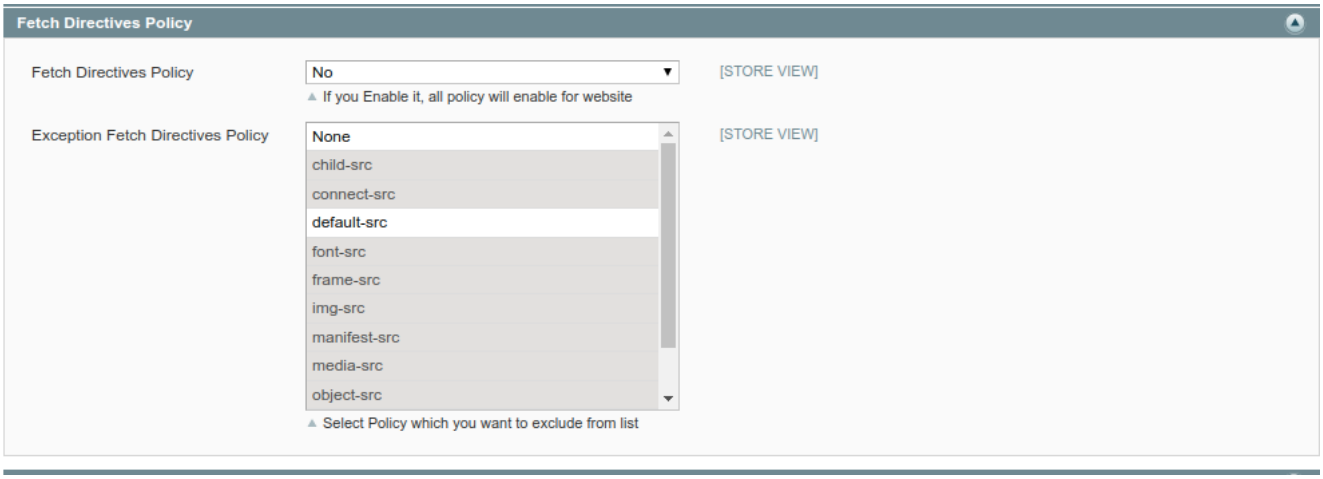
This directive has below policies listed :

1. child-src
2. connect-src
3. default-src
4. font-src
5. frame-src
6. img-src
7. manifest-src
8. media-src
9. object-src
10. script-src
11. style-src

** Default Source for all policies is **'self'**

Fetch Directives Policy : This configuration will enable all the policies listed above.

Exception Fetch Directives Policy : This will exclude selected policies for not being triggered.



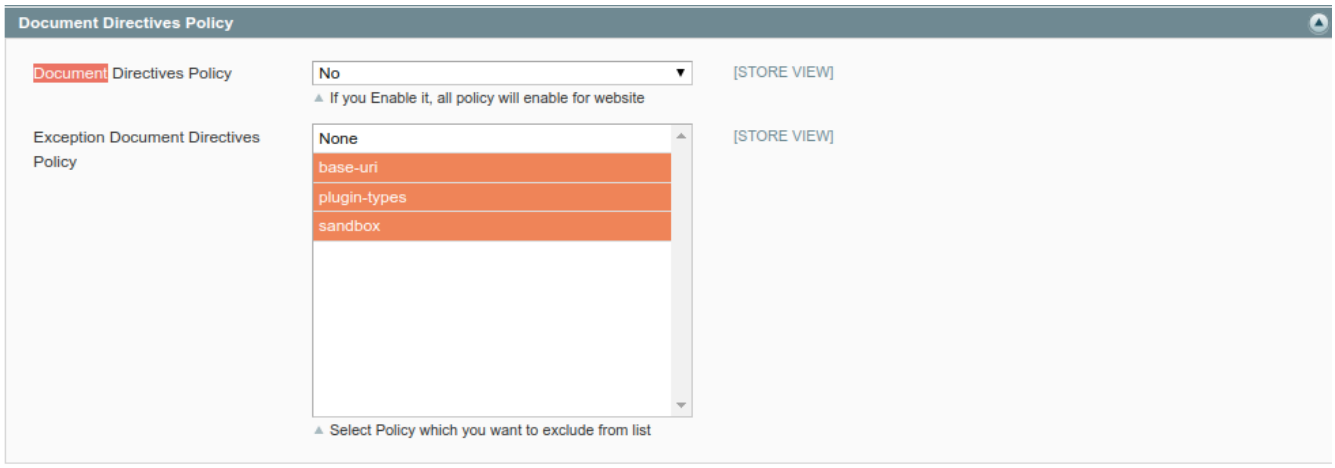
DOCUMENT DIRECTIVE POLICY

This directive has below policies listed :
1. base-uri
2. plugin-types
3. sandbox

** Default Source for **base-uri** policy is **'self'** , for **plugin-types** and **sandbox** is blank/empty.

Document Directives Policy : This configuration will enable all the policies listed above.

Exception Document Directives Policy : This will exclude selected policies for not being triggered.



NAVIGATION DIRECTIVE POLICY

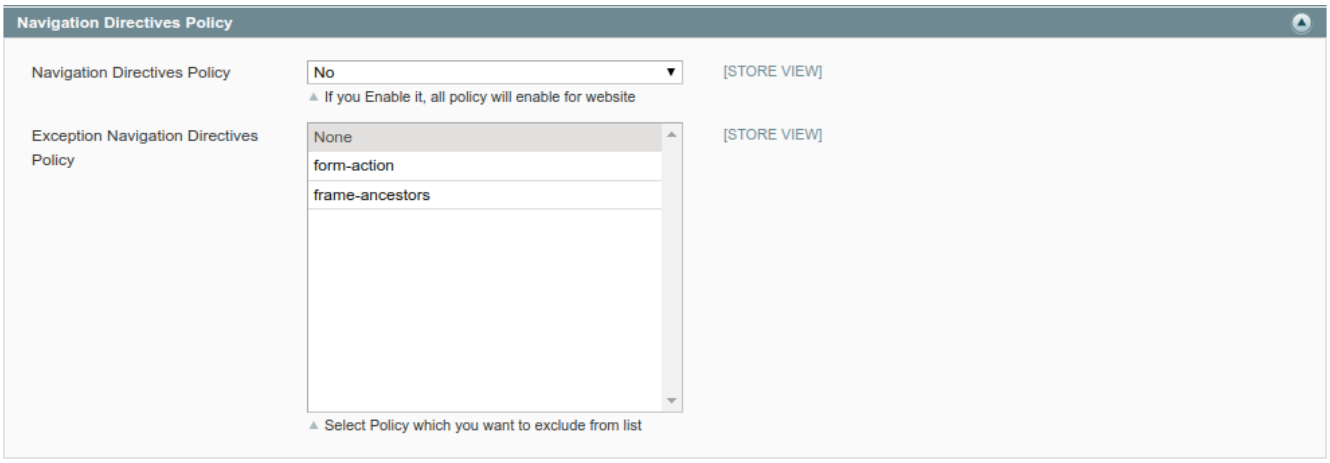
This directive has below policies listed :

1. form-action
2. frame-ancestors

** Default Source for all policies is **'self'**

Navigation Directives Policy : This configuration will enable all the policies listed above.

Exception Navigation Directives Policy : This will exclude selected policies for not being triggered.



OTHER DIRECTIVE POLICY

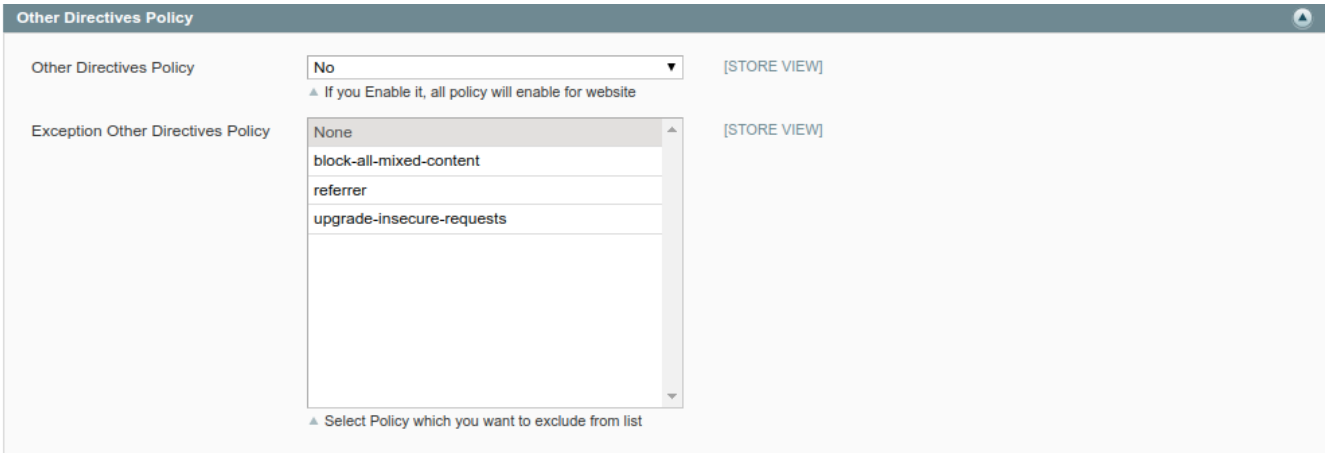
This directive has below policies listed :

1. block-all-mixed-content
2. referrer
3. upgrade-insecure-requests

** Default Source for **block-all-mixed-content** is **blank/empty**, for **referrer** is **'none'** and for upgrade-insecure-requests **'self'** .

Other Directives Policy : This configuration will enable all the policies listed above.

Exception Other Directives Policy : This will exclude selected policies for not being triggered.



ADVANCED SETTINGS

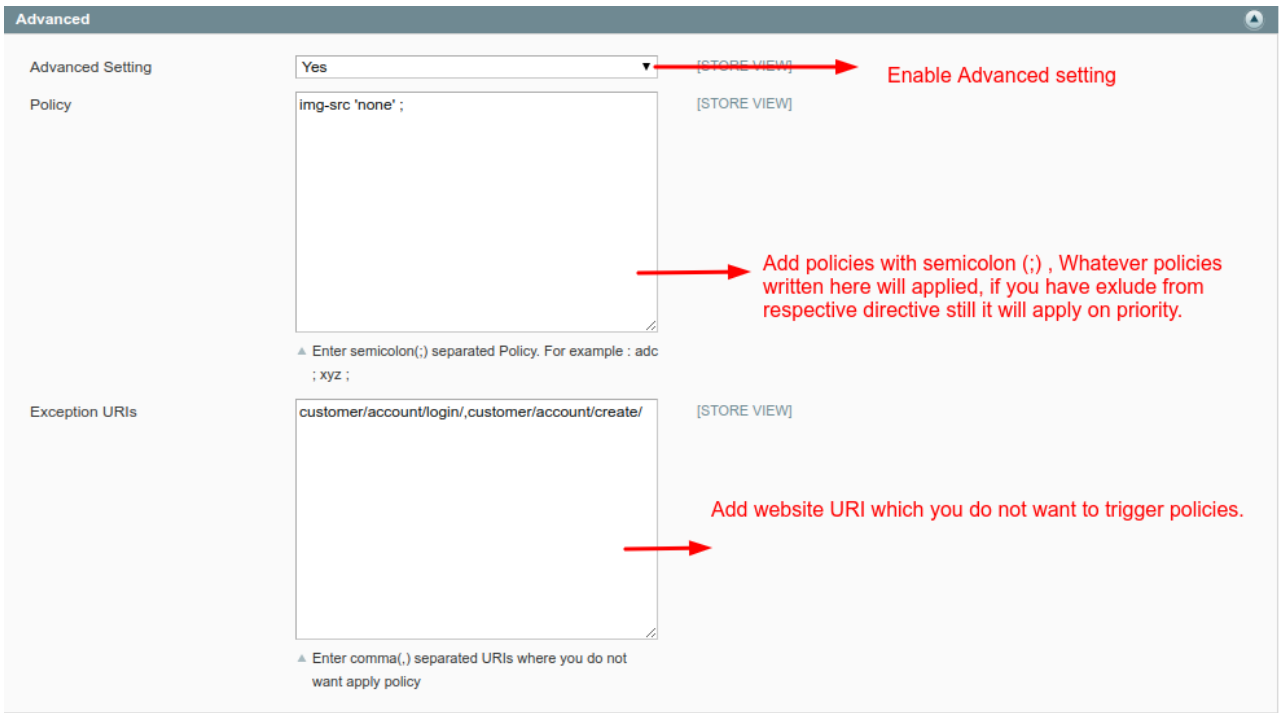
1. **Advanced Setting :** Enable Advanced setting to “YES” for action done by this section. If set “NO” then it won’t work for the module.

2. **Policy Section** (optional) **:** If you want add extra sources other than default you can add policies in this section.
Define policies with semicolon (;) separated. Policies will triggered on priority which define in advanced section and default will get ignored.

For example : img-src: ‘none’; default-src: ‘none’ ;

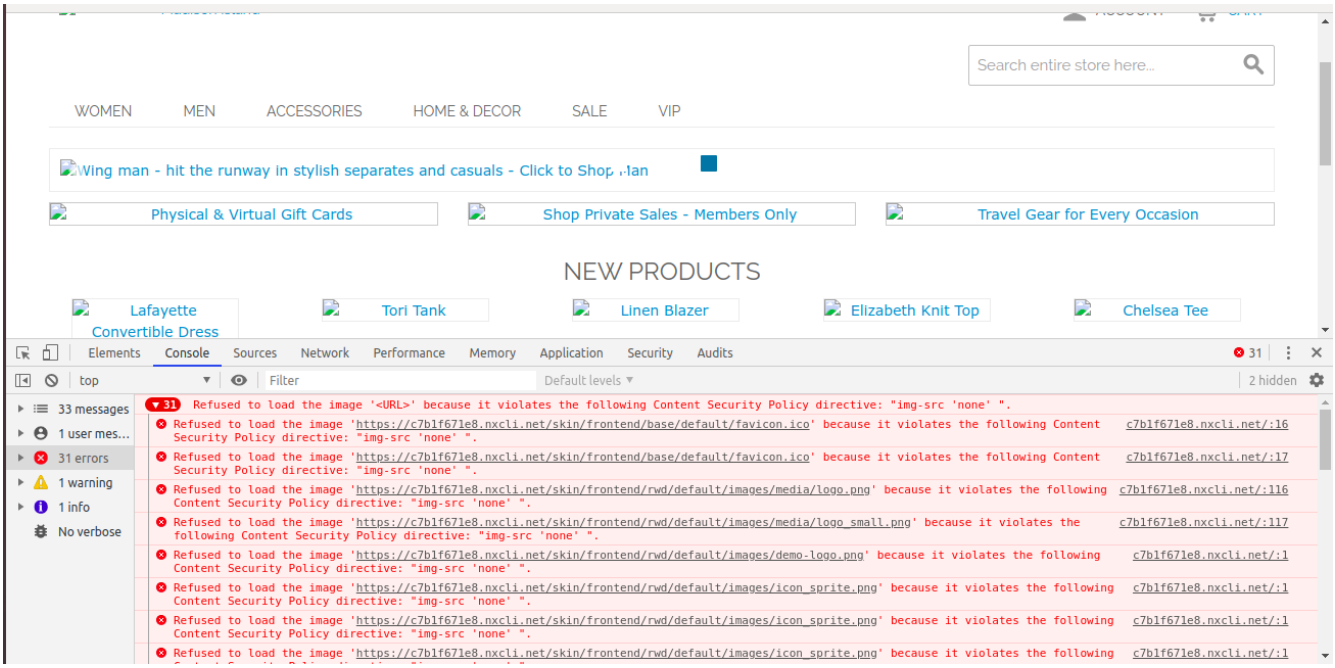
Note : While adding **img-src: ‘none’** from advanced section will ignore **img-src ‘self’** which was applying by default if you have enabled **fetch directives**.

3. Exception URI’s (optional) **:** Define pages where you do not want to trigger policy.
For example : customer/account/login/ , customer/account/create/
Make it comma(,) separated.



POLICIES ON FRONTEND

1. We wrote policy in advanced setting for images. **img-src : none;** Its output would be like this :



2. Policy is not triggering on **Login** and **Register** page as we have exclude them.