X-Frame-Options

X-Frame-Options

Introduction

X-Frame-Options is HTTP response header used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe> or <objects>. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

X-Frame-Options MODES:

1) DENY
2) SAMEORIGIN
3) ALLOW-FROM “URI”’ /”SERIALIZED-ORIGIN” (A serialized-origin include only scheme,host and port of the uri)

X-Frame-Options : DENY

This secures the page from getting displayed in any frame, irrespective of the site accessing it. A browser receiving the content with this response header set will not display content in any frame.

X-Frame-Options : SAMEORIGIN

The page can only be displayed in a frame on the same origin as the page. This does not support displaying the page in the subdomain page as well.

X-Frame-Options : ALLOW-FROM

The page can only be displayed in a frame on the specified origin. On receiving a page with ALLOW-FROM set, the browser makes a decision whether to display the response in the iframe based on the scheme, host and port values. If any one of the property doesn’t match, browser blocks the iframe from displaying data. It doesn’t take path value into consideration.

One drawback of ALLOW-FROM is that it doesn’t give the provision to configure multiple hosts.
Not all the browsers support this mode. Chrome doesn’t support this mode at all.

X-Frame-Options

One alternative for sending multiple hosts is to use Content-Security-Policy header, which along many other policies can white-list what URLs are allowed to host your page in a frame, using the frame-ancestors directive. More info about CSP can be found here.

Syntax for adding X-Frame-Options response header:

DENY AND SAMEORIGIN

response.addHeader(“X-Frame-Options”,”DENY/SAMEORIGIN”);

ALLOW-FROM

response.addHeader(“X-Frame-Options”,”ALLOW-FROM”+” “+URI);

Browser Support for X-Frame-Options :

Browser	DENY/SAMEORIGIN SUPPORT	ALLOW-FROM SUPPORT
Chrome	4.1.249.1042	Won’t support - Supports CSP frame-ancestors
Firefox	3.6.9 (1.9.2.9)	
IE	8.0	9.0
Safari	10.50	
Opera	4.0	Won’t support - Supports CSP frame-ancestors

X-Frame-Options

X-Frame-Options in WaveMaker :

Existing

X-Frame-Option of every request made to wavemaker is set to **SAMEORIGIN** by default. There wasn’t a provision to set a different X-Frame-Option mode.

From now, users can set any one of the X-Frame-Option mode through profile properties.

Back-End Changes to support X-Frame-Options

general-options.json

New property xFrameOptions is added to general-options.

```
"xFrameOptions" : {
                     "mode" : "SAMEORIGIN",
                    "allowFromUrl" : null
          }
```

Default value of mode is set to ‘SAMEORIGIN’.

Profile properties

Two new properties got added to development and deployment profiles.

```
          security.general.xFrameOptions.allowFromUrl=
          security.general.xFrameOptions.mode=SAMEORIGIN
```

Project-security.xml

Two new properties “xFrameOptionsMode” and “allowFromUrl” are added to “WMXFrameOptionsHeaderFIlter” bean.

```
 <bean class="com.wavemaker.runtime.security.filter.WMXFrameOptionsHeaderFilter"
id="wmXFrameOptionsFilter">
       <property name="xFrameOptionsMode" value="${general.xFrameOptions.mode}"/>
       <property name="allowFromUrl" value="${general.xFrameOptions.allowFromUrl}"/>
   </bean>
```