By default, the pages of Kentico Portal Engine websites cannot be embedded into frames rendered on external sites. This framing restriction is achieved by including the X-Frame-Options header in the HTTP response:

```
X-Frame-Options: SAMEORIGIN
```

The header ensures that pages can only be displayed in frames if they **originate on the same host name and server** as the parent page. Otherwise browsers do not render them.

The same-origin policy can help protect against clickjacking attacks that use framing. Clickjacking is a type of attack where the attacker tricks website users into clicking something different than what they see, thus performing an action that for example reveals confidential data or has another negative effect on the user or website. In a typical clickjacking scenario, the attacker places a transparent frame within a page, that contains a button or a link, over another element on a website. The underlying element can be an image or a video, which the users expect to play when they click it. Instead, they click the concealed link or button. This way the attacker can make the users perform unintended actions, usually on websites where the users are authenticated.

If you need to intentionally display your site's pages within a frame on another domain, you can disable the same-origin policy for specific pages or website sections. To do that, add the **CMSXFrameOptionsExcluded** key into the *appSettings* section of your web.config file:

```
<add key="CMSXFrameOptionsExcluded" value="/Services;/Products;/Partners" />
```

The system excludes all pages under the specified paths from the clickjacking protection.

- You can enter any alias path as a value.
- To exclude multiple paths, enter values separated by semicolons (;).
- Entering "/" disables the protection completely.

Special cases where the X-Frame-Options header is not included

There are a few special cases where the clickjacking protection is disabled by the system.

These cases include preview modes of objects (for example, transformations) which can be displayed in the context of different websites and different domains. To display the previews of these objects properly, Kentico does not include the X-Frame-Options header in such pages. Therefore, to maintain the security protection against clickjacking, Kentico adds a special **clickjacking hash** to the URL of the particular frame. The content of the frame is displayed only if hash validation is successful.