What is Same Origin Policy?

Same Origin Policy (SOP) is an important concept in the web application security model. As per this policy, it permits scripts running on pages originating from the same site which can be a combination of the following:

- Domain
- Protocol
- Port

Example

The reason behind this behaviour is security. If you have try.com in one window and gmail.com in another window, then you DONOT want a script from try.com to access or modify the contents of gmail.com or run actions in context of gmail on your behalf.

Below are webpages from the same origin. As explained before, the same origin takes domain/protocol/port into consideration.

- http://website.com
- http://website.com/
- http://website.com/my/contact.html

Below are webpages from a different origin.

- http://www.site.co.uk anotheadomain
- http://site.org anotheadomain
- https://site.com anotheerprotocol
- http://site.com:8080 anotheerport

Same Origin policy Exceptions for IE

Internet Explorer has two major exceptions to SOP:

- The first one is related to 'Trusted Zones'. If both domains are in highly trusted zone then the Same Origin policy is not applicable completely.

- The second exception in IE is related to port. IE doesn't include port into Same Origin policy, hence the http://website.com and http://wesite.com:4444 are considered from the same origin and no restrictions are applied.

Loading [MathJax]/jax/output/HTML-CSS/fonts/TeX/fontdata.js