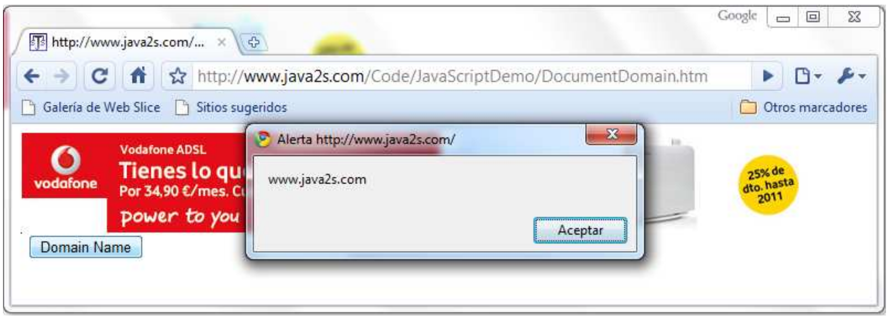
Bypassing Google Chrome 4 Javascript Filter

Google Chrome 4 included a new Javascript Filter which allows users to disallow javascript in websites. This filter doesn´t allow to web sites to execute any Javascript code if the web site is accessed directly.

This protection, can be easily bypassed since it only is applied when the web site is accessed as the main page. This means, if the blocked domain site is used in an iframe object, then the Javascript filter doesn´t block any Javascript code.

POC

To see this method in action, firstly we block http://www.java2s.com/ domain. This site has a page to test, using Javascript, its domain name. It is just a test page for Javascript.



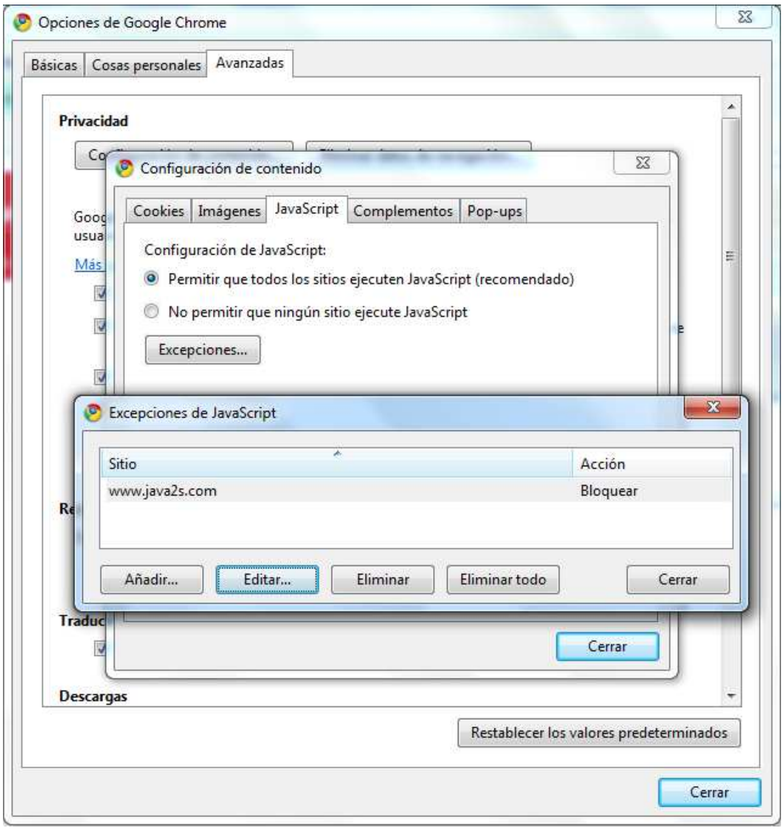
http://www.java2s.com/Code/JavaScriptDemo/DocumentDomain.htm

Alerta http://www.java2s.com/

www.java2s.com

Aceptar

Then, this domain is set to be Javascript blocked using the filter in the Advance settings configuration panel.



Configuración de JavaScript:

● Permitir que todos los sitios ejecuten JavaScript (recomendado)

○ No permitir que ningún sitio ejecute JavaScript

Sitio	Acción
www.java2s.com	Bloquear

If this web site is accessed directly, then Javascript is disabled and the button doesn´t work.

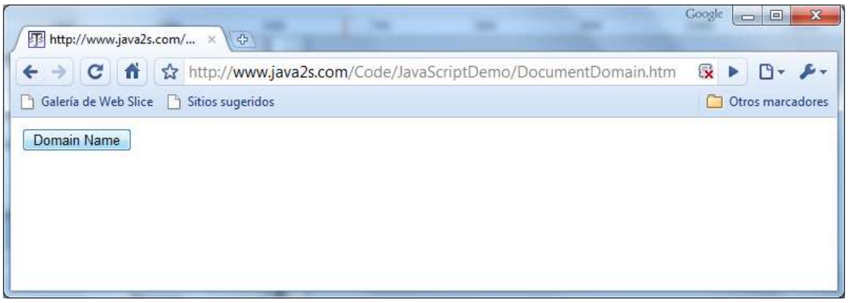
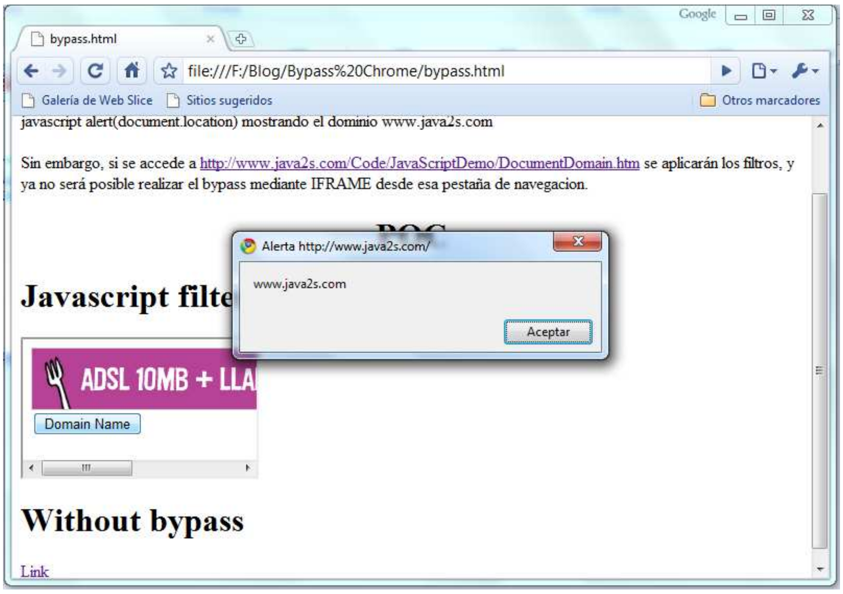

http://www.java2s.com/...
http://www.java2s.com/Code/JavaScriptDemo/DocumentDomain.htm
Galería de Web Slice
Sitios sugeridos
Otros marcadores
Domain Name
Google

Figure 3: Javascript blocked

Then, close Google Chrome and open a new page in which the page in the blocked domain is configured within an iframe object, therefore the filter is not checking the domain and Javascript can be executed.



javascript alert(document.location) mostrando el dominio www.java2s.com

Sin embargo, si se accede a http://www.java2s.com/Code/JavaScriptDemo/DocumentDomain.htm se aplicarán los filtros, y ya no será posible realizar el bypass mediante IFRAME desde esa pestaña de navegacion.

Javascript filte

www.java2s.com

Without bypass

Link

Best regards,