Insecure Frame (External)

205541608 HASSAN SANUSI BAYERO.

Summary

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing   properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as http://site.com :

http://site.com  
http://site.com/  
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as http://site.com :

http://www.site.com  (a sub domain)  
http://site.org            (different top level domain)  
https://site.com         (different protocol)  
http://site.com:8080  (different port)

When the sandbox attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

* Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
* Forms are disabled. The hosted content is not allowed to make forms post back to any target.
* Scripts are disabled. JavaScript is disabled and will not execute.
* Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
* Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the sandbox attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

* It might trick the user into supplying a username and password to the site loaded inside the iframe.
* It might navigate the parent window to a phishing page.
* It might execute untrusted code.
* It could show a popup, appearing to come from the parent site.

Sandbox containing a value of :

* allow-same-origin will not treat it as a unique origin.
* allow-top-navigation will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
* allow-forms will allow form submissions from inside the iframe.
* allow-popups will allow popups.
* allow-scripts will allow malicious script execution however it won't allow to create popups.

Remediation

* Apply sandboxing in inline frame <iframe sandbox src="framed-page-url"></iframe>