

Forum: [Hack Forums](#)

Thread: [CORS, the new HTML5 vector?](#)

pwntoken - December 16, 2013, 8:53 am

So I recently saw CORS are inevitably being the latest HTML5 vulnerability vector. I am not sure how we really get a POC for Cross Origin Resource Sharing vulnerability. There are better online POC generators tho like:

Code http://attacker-site.com/html5/CORS/cors_tester.php

But the dump it generates (if the site IS vulnerable) is encoded in some special formats. Like below:

[img]<http://img.openfire-security.net/images/2013/12/16/GzC.gif>[img]

I am not really sure how to use this encoded form tho, does anyone has any idea, how we get to use CORS vulnerability on newly HTML5 based sites? or generate POC along with the vulnerability affection details? ?

Thank you.

Gee4rce - December 16, 2013, 3:37 pm

Can't help you on that, (as i don't understand what you are looking for),
but at first you should fix your image, it's not being displayed (well atleast for me)...
Greetings, Gee.

pwntoken - December 17, 2013, 4:17 am

(Dec 16, 2013 04:37 PM)Gee4rce Wrote: [\[CITE\]](#) Can't help you on that, (as i don't understand what you are looking for),
but at first you should fix your image, it's not being displayed (well atleast for me)...
Greetings, Gee.

The image is fine. CORS is the new HTML5 vector for vulnerability, goes to WASC top lists. I have problems understanding this vector too.