Question
Sean Connelly · May 17, 2017

How to handle pre-flight checks in CSP?

From a browser, an XMLHttpRequest to a CSP page on a different server will obviously hit the CORS security check.

To get around this I can set the Access-Control-Allow-Origin header on that particular CSP class.

However, setting any request headers on the XMLHttpRequest object will trigger a pre-flight OPTIONS request.

This OPTIONS request is not handled by the target CSP page and the Access-Control-Allow-Origin header is never set, triggering a CORS error.

I can see in the new REST class that it can get a handle on the OPTIONS request but standard CSP pages don't seem to get them.

Are there any solutions for doing this in standard CSP such that it will work with older versions of Caché?

It currently feels like the answer is no, so I am looking at JSONP as an alternative, but would appreciate if anyone has managed to solve this without a hack. I also want to avoid using a proxy which is what I normally always use.

Sean.

#CSP #Caché