Question
Jack Huser · Oct 25, 2022

Security on TrakCare's Apache for CORS Policy

Hi everyone,

I have an issue when calling Trakcare's webservices using a web application.

The issue is that, the browser is blocking the queries because of the CORS Policy.

In fact, the browser is sending a first HTTP query OPTIONS called "preflight" (in Chrome's developers tools) and Apache server answers with no CORS Control Origin in Header (CORS header ‘ Access-Control-Allow-Origin ’ missing). So the query is blocked and does not reach the Webservices server (IRIS Interoperability).

We were advice to add those configuration in Apache:

```
SetEnvIf REQUEST_METHOD OPTIONS options
Header onsuccess unset ACCESS-CONTROL-ALLOW-ORIGIN
Header always set ACCESS-CONTROL-ALLOW-ORIGIN "http://localhost:4200"
Header always set ACCESS-CONTROL-ALLOW-METHODS "POST, OPTIONS" env=options
Header always set ACCESS-CONTROL-ALLOW-HEADERS "authorization" env=options
RewriteEngine On
RewriteCond %{REQUEST_METHOD} OPTIONS
RewriteRule ^(.*)$ $1 [R=204,L]
```

I'm reluctant in modifying the TrakCare's Apache with command I'm not sure to understand.

And my concern is about security. What if one of those command, which change Apache redirection behaviour, introduce a lack of security?

And what if another web application with another url wants to request access to the webservice too?

Apache with allow CORS Query only for http://localhost:4200. Since "ACCESS-CONTROL-ALLOW-ORIGIN" can't be set to "*" for Basic Authentication.

If anyone has some system knowledge about Apache and Security, I'd be glad to have some comments and advices.

Thank you very much for your help.

regards,

Jacques

#Red Hat Enterprise Linux (RHEL) #System Administration #TrakCare
Product version: IRIS 2020.1
$ZV: IRIS for UNIX (Red Hat Enterprise Linux for x86-64) 2020.1 (Build 215021670U) Fri Jun 17 2022 17:37:24 EDT

Source URL:https://community.intersystems.com/post/security-trakcares-apache-cors-policy