Question
Muhammad Awan · Apr 18, 2019

How to add Access token (JWT) on Client Web Server Side instead of Browser's local storage.

Hi Team,

I am using Angular 7 with angular material for my client application that connects and obtains Access token from IRIS Authorization Server (OAUTH 2.0).
The problem that I am facing right now is regarding this access token being exposed to browser and stores in the local storage of the browser.

Right now, I am having hard time finding an alternative but secure option to store access token on the server side (client WEB SERVER) instead of browser ’ s local storage.

Following are the suggestions that I have googled recently, not sure if there is any better way that I need to explore.

- A WEB Server-side session that maintains sensitive data User IDs, Session IDs,,JWTs, API keys, etc.
- Store in cookies with “ httpOnly ” option which also less vulnerable to XSS attacks
- indexedDB solution which also has some caveats

Please let me know if anyone has implemented a better and secure way of storing token information on the server side (Client Web server) and incorporated the information in client application to send token inside the HTTP (Header) request for consuming REST APIs.

Please share some code if you have them handy to understand and implement the expected concept properly.

Any guidelines or lead would be really appreciated.

#InterSystems IRIS

Source URL:https://community.intersystems.com/post/how-add-access-token-jwt-client-web-server-side-instead-browserslocal-storage