

TEMA 1 – DATC

Datorită *same-origin policy*, browser-ele web nu permit resurselor din domenii diferite să interacționeze, asigurând astfel securitatea.

CORS (*Cross-origin resource sharing*) este un standard care permite accesarea de resurse din alte domenii decât cel original, pentru a realiza o integrare mai bună între serviciile web. Acesta adaugă headere HTTP care permit browser-ului să decidă dacă acceptă sau nu conținutul din alte domenii.

Cereri CORS simple:

Clientul face o cerere pentru o resursă de pe server, aceasta conținând un header *Origin*, care indică originea codului de pe client. Dacă serverul acceptă cererea, trimite resursa și un header *Access-Control-Allow-Origin*. Se verifică dacă originea precizată în header-ul *Origin* al cererii se regăsește în originile acceptate trimise de server, iar în caz afirmativ, browser-ul acceptă resursa. Când header-ul *Access-Control-Allow-Origin* este setat pe „*”, toate originile vor fi acceptate. Dacă originea nu este acceptată, serverul răspunde cu eroare.

Cereri CORS pre-flight:

O cerere pre-flight este trimisă înaintea cererii efective. Aceasta conține headere care permit server-ului să verifice dacă cererea este validă. De exemplu, în cererea pre-flight poate apărea header-ul *Access-Control-Request-Method*. Dacă în header-ul *Access-Control-Allow-Methods* trimisă ca răspuns de către server apare metoda din cererea clientului, acesta va putea trimite o cerere prin care să apeleze acea metodă.

Se recurge la o cerere pre-flight dacă cererea efectivă folosește o altă metodă în afară de *GET* și *POST*, dacă sunt setate headere *custom* sau dacă în corpul cererii apar tipuri *MIME* altele decât *text/plain*.

Headere pentru cereri HTTP:

- Origin
- Access-Control-Request-Method
- Access-Control-Request-Headers

Headere pentru răspunsuri HTTP:

- Access-Control-Allow-Origin
- Access-Control-Allow-Credentials
- Access-Control-Expose-Headers
- Access-Control-Max-Age
- Access-Control-Allow-Methods
- Access-Control-Allow-Headers

CORS este foarte util, deoarece minimizează riscurile de securitate, în timp ce permite accesarea resurselor din domenii diferite.