Iriza Andrea-Cassiana

Anul IV-IS

Tema1 DATC

OAuth este un protocol sau un cadru de autorizare standard deschis care descrie modul in care serverele si serviciile fara legatura pot permite in mod sigur accesul autentificat la resursele lor fara a imparti efectiv acreditarile initiale, legate de un singur login.

OAuth permite utilizatorului, printr-un furnizor de autentificare cu care a fost autentificat anterior cu succes, sa ofere unui alt site/serviciu un token autentic cu acces limitat pentru accesul resurselor suplimentare.

OAuth 1.0 vs. OAuth 2.0: Modificarile sunt atat de importante incat versiunea 2.0 nu este compatibila cu versiunea 1.0, si chiar implementari diferite ale versiunii 2.0 ar putea sa nu functioneze perfect intre ele. OAuth 2.0 este mai putin sigur, mai complex si mai putin prescriptiv decat versiunea 1.0.

Una dintre cele mai mari critici ale OAuth 2.0 este ca standardul nu intentioneaza in mod direct sa defineasca sau sa sustina criptarea, semnarea, verificarea clientului sau legarea canalelor (legand o anumita sesiune sau tranzactie unui anumit client si server). In schimb, OAuth se asteapta ca utilizatorii sa foloseasca un protocol de protectie externa cum ar fi TLS(Transport Layer Security).

Cross-Origin Sharing Resource(CORS) este un mecanism care utilizeaza antete HTTP suplimentare pentru ca un browser sa permita unei aplicatii web sa poata accesa resursele selectate dintr-un server de origine diferita. O aplicatie web face o cerere HTTP cross-origin atunci cand solicita o resursa care are o origine diferita(domeniu, protocol si port) decat propria origine.

CORS este utilizat pentru a permite solicitari HTTP cross-site pentru:

- Invocarea API-urilor XMLHttpRequest sau Fetch
- Fonturi Web
- WebGl texte
- Imagini/cadre video desenate folosind drawImage()

Standardul CORS este necesar pentru ca le permite serverelor sa specifice nu doar cine poate accesa resursele, ci si cum ele pot fi accesate.

Cererile cross-origin sunt facute utilizand metodele standard HTTP. Cele mai multe servere vor permite cererile GET ceea ce inseamna ca vor permite resurselor externe sa le citeasca proprile resurse. Metodele standard HTTP ca si PATCH, PUT sau DELETE pot fi respinse pentru a preveni comportamentul premeditat. De exemplu, este posibil ca serverul A sa nu vrea ca serverele B, C sau D sa-i editeze sau sa ii stearga resursele.