**Lez4 16/09/2024**

**RESTful API**

**Autenticazione e Autorizzazione RESTful API**

*definizioni introduttive*

prima autentichi poi vedi autorizzazioni (base dei ruoli…)

metodi di **autenticazione**

http basic authentication (login, non sicuro),

token-based(codice univoco con tante info) authentication,

es json web token(JWT), Oauth

Oauth: servizi terzi per autenticazione(es accedi con google),

<https://www.proofpoint.com/it/threat-reference/oauth>

OpenID connect (uso di servizi centralizzati, spid….)(molto complesso ed esterno)

estensione oauth

<https://www.cybersecurity360.it/soluzioni-aziendali/openid-connect-cose-a-cosa-serve-e-perche-e-importante/>

utilizzando oauth è molto + sicuro nel comune

***autorizzazione***

ciò che fornisce ruoli agli utenti per svolgere azioni

caso eliminazione dato importante da parte di user

*eliminazione* logica: il superamministratore non perde controllo del dato cancellato, fa un update/POST che impedirà di visualizzare il dato all’user che l’avrà “cancellato”

Quindi Nella cancellazione logica, il record rimane fisicamente nel file, ma il suo contenuto informativo non ha più alcun valore per l'archivio. Nella cancellazione fisica, il record viene materialmente eliminato dall'archivio.

*controllo basato su ruoli(admin…)*

*controllo basato su risorse*

*controllo basato su attributi*(etichette )

JWT

<https://jwt.io/>