11 Autorisierung und Security

Thema

Rollen, Berechtigungen und zentrale Sicherheitsmassnahmen.

Auftrag

Erweitere die API um mindestens zwei Rollen und eine funktionsbasierte Berechtigung. Prüfe ausserdem Eingaben, Secrets, CORS und die Unterscheidung von `401` und `403`.

Abgabe

- Rollen- oder Berechtigungskonzept;
- mindestens zwei geschützte Funktionen;
- Testfälle für erlaubten und verweigerten Zugriff;
- Security-Checkliste.

Lernzielkontrolle

1. Was ist der Unterschied zwischen Authentifizierung und Autorisierung?
2. Wann antwortet eine API mit `401` und wann mit `403`?
3. Was ist der Unterschied zwischen rollen- und funktionsbasierter Autorisierung?
4. Welche Backend-Sicherheitsmassnahmen gehören zu jeder API?

Zeitbudget

Zeit: ca. 5 Stunden