Programowanie Back-End

Uwierzytelnienie i autoryzacja w REST API

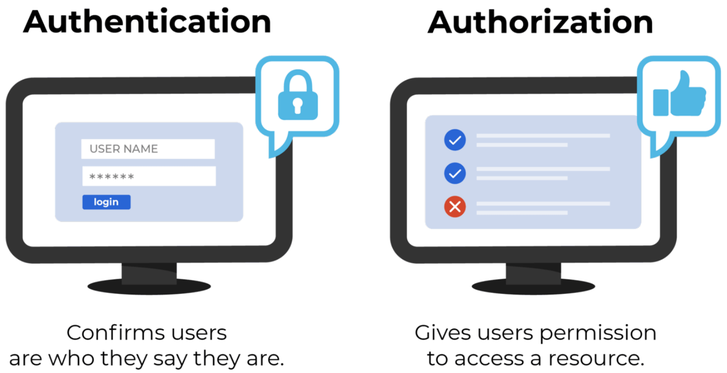
mgr inż. Jakub Gogola

Uwierzytelnienie vs autoryzacja

Jaka jest różnica?

Te dwa pojęcia często (błędnie) są używane zamiennie, ale oznaczają zupełnie różne rzeczy:

- **Uwierzytelnianie** (*Authentication*) → sprawdza, **kim jesteś**
- **Autoryzacja** (*Authorization*) → sprawdza, **do czego masz dostęp**



Metody uwierzytelnienia

Sesje

- Użytkownik podaje login i hasło.
- Serwer sprawdza dane i zapisuje informację o sesji w bazie danych.
- Klient otrzymuje **identyfikator sesji** (np. w ciasteczku).
- Przy każdym żądaniu do API serwer sprawdza, czy sesja jest ważna.

Metody uwierzytelnienia

Sesje

Zalety

✅ Wbudowane w wiele frameworków (np. Django, Flask).

✅ Możliwość łatwego unieważniania sesji (np. po wylogowaniu).

Wady

❌ Wymaga przechowywania sesji na serwerze.

❌ Nie działa dobrze w aplikacjach rozproszonych (np. gdy API działa na wielu serwerach).

Metody uwierzytelnienia

Tokeny

Jak działa?

- Użytkownik podaje login i hasło.
- Serwer generuje **token** (np. JWT – JSON Web Token).
- Klient przechowuje token i przesyła go w nagłówku Authorization w kolejnych żądaniach.
- Serwer weryfikuje token, ale nie musi przechowywać informacji o sesji.

Metody uwierzytelnienia

Tokeny

Zalety

✅ Skalowalne – nie wymaga przechowywania sesji.

✅ Można łatwo korzystać w aplikacjach mobilnych i frontendowych.

Wady

❌ Trudniej unieważnić tokeny (np. po wylogowaniu).

❌ Jeśli token wycieknie, może zostać wykorzystany przez innego użytkownika.

JSON Web Token

Jak działa?

JWT (JSON Web Token) to **zaszyfrowany token**, który pozwala na uwierzytelnianie użytkowników **bez przechowywania sesji na serwerze**.

JSON Web Token

Budowa

Struktura JWT składa się z trzech części:

```
header.payload.signature
```

- **Header** – zawiera informacje o algorytmie szyfrowania
- **Payload** – zawiera dane użytkownika (np. ID, role)
- **Signature** – zabezpiecza token przed manipulacją

Przykład

- https://github.com/JakubGogola/dsw-backend-programming/tree/main/lectures/lecture-4/auth

Dziękuję za uwagę!