JWT (JSON Web Token)

JSON Web Token (JWT) je otevřený standard (RFC 7519), který definuje kompaktní a samostatný způsob pro bezpečný přenos informací mezi stranami jako objekt JSON. Tyto informace mohou být ověřeny a důvěryhodné, protože jsou digitálně podepsány.

V moderním webovém vývoji se JWT používá především pro **autentizaci** a **výměnu informací**.

Struktura JWT

JWT se skládá ze tří částí oddělených tečkou (`node.js`): **Header**, **Payload** a **Signature**. Výsledný token vypadá následovně: `xxxxx.yyyyy.zzzzz`.

1. Header (Hlavička)

Obsahuje informace o typu tokenu a použitém algoritmu digitálního podpisu (např. HMAC SHA256 nebo RSA).

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

2. Payload (Obsah/Nároky)

Obsahuje samotná data, tzv. **claims** (nároky). Jsou to informace o uživateli (např. ID, jméno, role) a metadata (např. čas expirace).

```
{
  "sub": "1234567890",
  "name": "Jan Novák",
  "admin": true,
  "iat": 1516239022
}
```

3. Signature (Podpis)

Vytváří se vzetím zakódované hlavičky, zakódovaného payloadu, tajného klíče (secret) a algoritmu určeného v hlavičce. Podpis zajišťuje, že s tokenem nebylo po cestě manipulováno.

Jak JWT funguje v praxi

```
1. **Login:** Uživatel pošle přihlašovací údaje (např. jméno a heslo) na
server.
2. **Vytvoření:** Server ověří údaje a vygeneruje JWT podepsaný tajným
klíčem.
3. **Uložení:** Server pošle JWT zpět klientovi (prohlížeči), který si ho
uloží (např. v LocalStorage nebo Cookies).
4. **Autorizace:** Při každém dalším požadavku klient přiloží JWT do HTTP
hlavičky (''Authorization: Bearer <token>'').
5. **Ověření:** Server pouze ověří podpis tokenu. Pokud je platný, uživatele
obslouží bez nutnosti dotazovat se znovu do databáze.
```

Výhody a nevýhody

Vlastnost	Výhoda / Nevýhoda	Popis
Bezstavovost	Výhoda	Server nemusí držet relaci (session) v paměti. Skvělé pro škálování.
Samostatnost	Výhoda	Token obsahuje všechna potřebná data o uživateli.
Bezpečnost	Výhoda	Digitální podpis brání podvržení dat v payloadu.
Expirace	Nevýhoda	Token nelze snadno zneplatnit před jeho expirací (pokud není použit blacklist).
Velikost	Nevýhoda	Token může narůst, pokud do něj vložíte příliš mnoho dat.

Bezpečnostní doporučení

- **Nikdy nevkládejte citlivá data:** Payload je pouze zakódován (Base64), nikoliv šifrován. Kdokoliv jej může přečíst.
- **Používejte HTTPS:** Bez šifrovaného spojení může útočník token zachytit (tzv. *Token Theft*).
- **Krátká expirace (exp):** Nastavujte TTL tokenu na co nejkratší dobu (minuty) a pro obnovu používejte tzv. **Refresh Tokens**.
- **Silný tajný klíč:** Podpis je jen tak silný, jak silný je klíč použitý k jeho vytvoření.

> **Nástroj:** Pro ladění a dekódování tokenů můžete použít oficiální webový debugger na **jwt.io**.

Zpět na Data