JWT

JSON Web Token

Ammar Munir

WHAT

JWT is a compact, URL-safe method of representing claims to be transferred between two parties. It is commonly used for **authentication** and **authorization** in web applications, allowing the secure exchange of information. The token is digitally signed using a secret (HMAC) or a public/private key pair (RSA or ECDSA).

Components of a JWT

Header

Payload

Signature

```
header.payload.signature
```

Ammar Munir

Header

Contains metadata about the token, including the **type** of token (JWT) and the signing **algorithm** used (e.g., HMAC SHA256 or RSA).

Payload

Contains the claims. Claims are statements about an entity (typically, the user) and additional **metadata**.
There are three types of claims:

- **Registered claims:** Predefined claims like iss (issuer), exp (expiration), and sub (subject).
- **Public claims:** Custom claims that are not registered, but defined by the user (e.g., user_id, email).
- **Private claims:** Claims agreed upon by both parties (e.g., permissions or roles).

Signature

The result of signing the encoded header, encoded payload, and a secret key. It ensures the integrity of the token and verifies the **authenticity of the sender.**

Ammar Munir

CREATE OWN

JWT

jwt.py

```python
import jwt
import datetime

# Define your secret key (keep this safe)
SECRET_KEY = 'your-secret-key'

# Create the payload (claims)
payload = {
    'social': 'https://linktr.ee/ammar.munirr',
    'name': 'Ammar Munir',
    'exp': datetime.datetime.utcnow() + datetime.timedelta(hours=1)
}

token = jwt.encode(payload, SECRET_KEY, algorithm='HS256')

print(token)
```

```
# eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9. ----> header
# eyJzb2NpYWwiOiJodHRwczovL2xpbmt0ci5lZS9hbW1hci5tdW5pcnIiLCJuYW1lIjoiQ.... ---> payload
# c4gJ73EfDWwM7zBTozULxvaMNgcpyJ2WFiXWIQtY-e4 ---> signature
```

Ammar Munir

Ammar Munir

linktree/ammar.munirr

WAS IT HELPFUL ?

Follow Now