

JSON WEB TOKEN (JWT)

JSON web token is an open standard that defines a compact and self-contained way for transmitting information between two parties ex, client-server as JSON object.

usage

JWT mostly used in authorization, but it can be used in information exchange.

structure

JWT consists of three parts header, payload, and signature

the header contains two parts the type of the token which is JWT and the signing algorithm such as SHA256 or RSA.

an example of header:

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

the payload contains information such as user, role and or expiration time. the payload can be customized to include information as needed.

an example of payload:

```
{
  "name": "khaled",
  "role": "customer",
  "exp": "2024-05-09T03:35:15"
}
```

the signature contains the header and payload in a base64url format separated by a dot and a secret

an example of signature:

`SHA256(base64UrlEncode(header).base64UrlEncode(payload),secret)`

then finally the header, payload and signature form three base64url separated by dots

an example of base64url **header.payload.signature**:

`"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxMjMONTYsInVzZXJuYW1lIjoiaXhnbXBsZV91c2VyaWwiczSI6ImFkbWluIn0.CS5QVW9-S8CK3sUH6myE3A6_Cw-fJSIBJiMy2h7tdZg"`

how does JWT works

1-authentication: when a user logs in, the server checks the credentials with database if the user is valid, the server generate a JWT containing information such as their id, name, and role etc. and then signs it with a secret key only known by the server.

2-sending JWT to the client: after the server generated a JWT token it sends back to the user as a respond then the client store the token usually in cookies which is secured by default, or in local storage which considered bad practice.

3-authoraization: when the user perform an action to a protected route they send their token with the request, then the server verifies the token using the secret key, if the token is valid the server can trust request perform the action.