**JWT – JSON WEB TOKEN**

**Introduction:**

JSON Web Token (JWT) is an open standard that defines a compact and self-contained way for **securely transmitting information** between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the **HMAC** algorithm) or a public/private key pair using **RSA** or **ECDSA**.

**Advantages of using JWT:**

* **Authorization:** Once the user is logged in, each subsequent request will include the JWT, allowing the user to access routes, services, and resources that are permitted with that token.
* **Information Exchange:** JSON Web Tokens are a good way of securely transmitting information between parties. Because JWTs can be signed using public/private key pairs. Additionally, as the signature is calculated using the header and the payload, that also verifies that the content hasn't been tampered with.

**Structure**:

JSON Web Tokens consist of **three parts** separated by dots (.), which are:

* Header
* Payload
* Signature

Example of a JWT

xxxxx.yyyyy.zzzzz

**Header**

The header typically consists of two parts: the **type of** the token, which is JWT, and the **signing algorithm** being used, such as HMAC SHA256 or RSA.



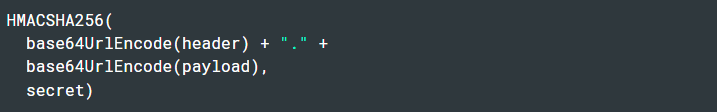
**Payload**

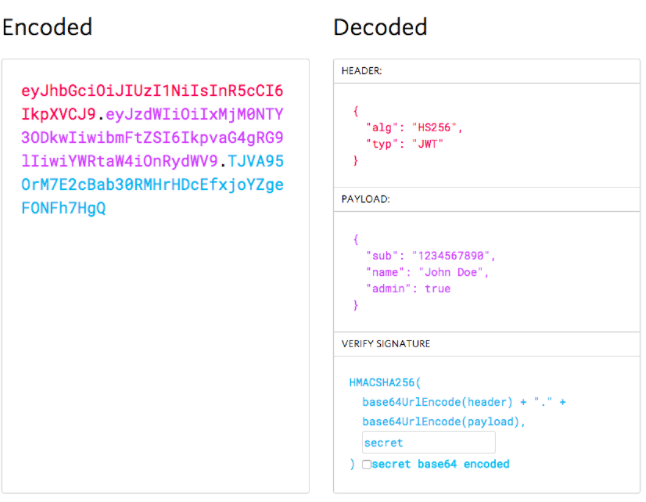
The second part of the token is the payload, which contains the claims. Claims are statements about an **entity** (typically, the user) and additional data.



### Signature

The signature is used to **verify the message** wasn't changed along the way, and, in the case of tokens signed with a private key, it can also verify that the sender of the JWT is who it says it is.





**Working of JWT:**

In authentication, when the user successfully logs in using their credentials, a JSON Web Token will be returned. Since tokens are credentials, great care must be taken to prevent security issues.

The server's protected routes will check for a valid JWT in the Authorization header, and if it's present, the user will be allowed to access protected resources. If the JWT contains the necessary data, the need to query the database for certain operations may be reduced, though this may not always be the case.

