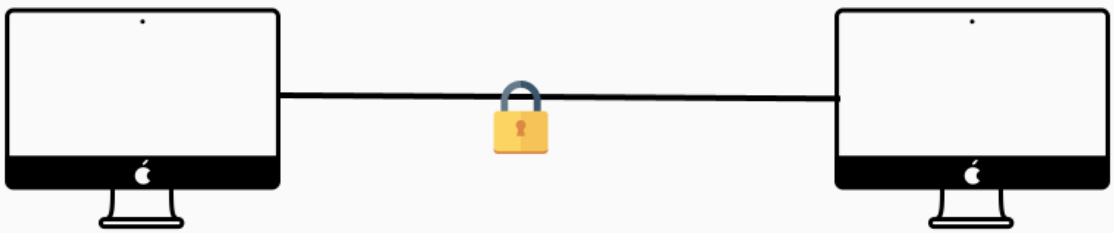
What a JWT is made of?

let's decode it!

antra verma

JWT which stands for JSON Web Token, is a way by which we can securely exchange information between two parties.



Here is an example of JWT:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.*eyJpZCI6MTIzNDU2Nzg5LCJuYW1lIjoiSm9zZXBoIn0*.*OpOSSw7e485LOP5PrzScxHb7SR6sAOMRckfFwi4rp7o*

As you can see, the above token consists of three different parts, separated by two dots.

Theses three parts are named as:

HEADER

PAYLOAD

SIGNATURE

antra verma

HEADER

The Header is basically a JSON object that consists of two things:

- Type of token
- Encryption algorithm that is being used
- e.g

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

PAYLOAD

The Payload is the part which contains information about the user identity, in other words **claims**.

- Claims can be further categorized as - registered, public and private
- e.g

```
{
    "userId": "765",
    "name": "john doe",
     "exp":  156790
 }
```

SIGNATURE

The Signature part is just what its name says. It is used to verify that the sender who claims this jwt token is the actual owner of it, or if its an information that's being exchanged, was not changed along its way.

- for our example, the signature would be created something like this:

```
HS256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret)
```

At the end, we get the result like this:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTIzNDU2Nzg5LCJuYW1lIjoiSm9zZXBoIn0.OpOSSw7e485LOP5PrzScxHb7SR6sAOMRckfFwi4rp7o

somethings you need to keep in mind regarding jwt:

- As you remember the header part consists of the “alg” property which basically describes what type of algorithm will be used while signing the algorithm, i.e. HS256, RS256 etc.

- But do note here that, **some JWT’s can also be created without a signature or encryption**. Such a token is referred to as unsecured and its header should have the value of the alg object key assigned to as ‘none’.

- You also need to be careful about the information that you put in the payload part of the jwt.

- If your jwt is not encrypted you might want to **avoid putting any sensitive information** there, since it can be read by anyone.

We made it till the end!

Was it helpful?