**JWT (JSON Web Token)**

The JWT is acquired by exchanging the username and password.

You need to login using Basic Authentication by providing username and password. On success of Basic Authentication, you will get a JSON web token.

JSON Web Token contains three distinctive parts.

1. Header

2. Payload

3. Signature

This information is encoded using Base64. If we decode, we will see something like this.

**header**

{

"typ": "JWT”, # Type of the token

"alg": "HS256" # Algorithm used for encoding the information.

}

**payload**

{

"token\_type": "access", # Type of the token(access/refresh)

"exp": 1543828431, # Expire time for the token

"jti": "7f5997b7150d46579dc2b49167097e7b", # Actual Token

"user\_id": 1 # User\_id of the token issued.

}

**signature**

The signature is issued by the JWT backend, using the **header base64 encode** + **payload base64 encode** + **SECRET\_KEY**. Upon each request this signature is verified.

If any information in the header or in the payload was changed by the client it will invalidate the signature.

The only way of checking and validating the signature is by using your application’s SECRET\_KEY. That’s why you should always keep your SECRET\_KEY **secret**!