

# Introduction to **JWT** as an **Absolute Beginner**



**Vikas Rajput**  
**@vikasrajputin**



# 1. JWT stands for **JSON Web Token**

- It's a token that is used to authenticate and authorize users in an application.
- "authenticate" means who they're.
- "authorize" means what they can access.
- The token itself contains, all the necessary information about the user, like user ID and role, etc, in a JSON.





- JWT tokens are typically generated by the server and sent to the client after a successful login.
- The client can then use the JWT token (with each request) to authenticate and authorize itself to the server.
- Typically the token looks like this:

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.  
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4  
gRG91IiwiaXNTb2NpYWwiOnRydWV9.  
4pcPyMD09olPSyXnrXCjTwXyr4BsezdI1AVTmud2fU4
```



## 2. JWT has three parts:

- ◆ Header (highlighted in red below)
  - ◆ Payload (highlighted in pink below)
  - ◆ Signature (highlighted in blue below)
- On left you can see the encoded token, on right we can see decoded JSON object with 3 parts.

The screenshot displays a JWT decoding interface. On the left, under the 'Encoded' tab, a token is shown with its three parts highlighted: the header in red, the payload in pink, and the signature in blue. On the right, under the 'Decoded' tab, the token is broken down into its constituent parts:

- HEADER: ALGORITHM & TOKEN TYPE:** A JSON object with `"alg": "HS256"` and `"typ": "JWT"`.
- PAYLOAD: DATA:** A JSON object with `"sub": "1234567890"`, `"name": "John Doe"`, and `"iat": 1516239022`.
- VERIFY SIGNATURE:** A section showing the HMACSHA256 algorithm and the base64-encoded header and payload, followed by a text input for the secret key.

Red arrows point from the highlighted parts of the encoded token to their corresponding decoded JSON objects.





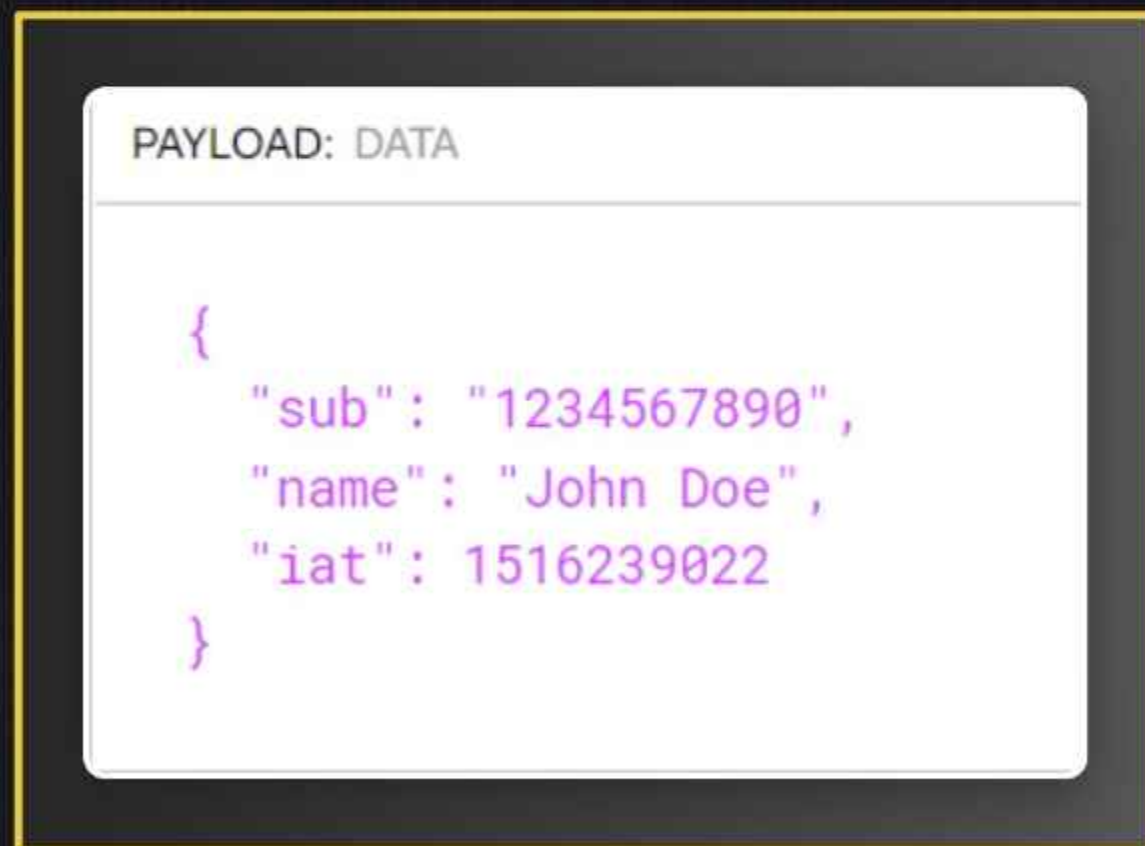
- The header typically consists of two parts: the type of the token, which is usually JWT, and the signing algorithm being used, such as HMAC SHA256 or RSA.

```
HEADER: ALGORITHM & TOKEN TYPE

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

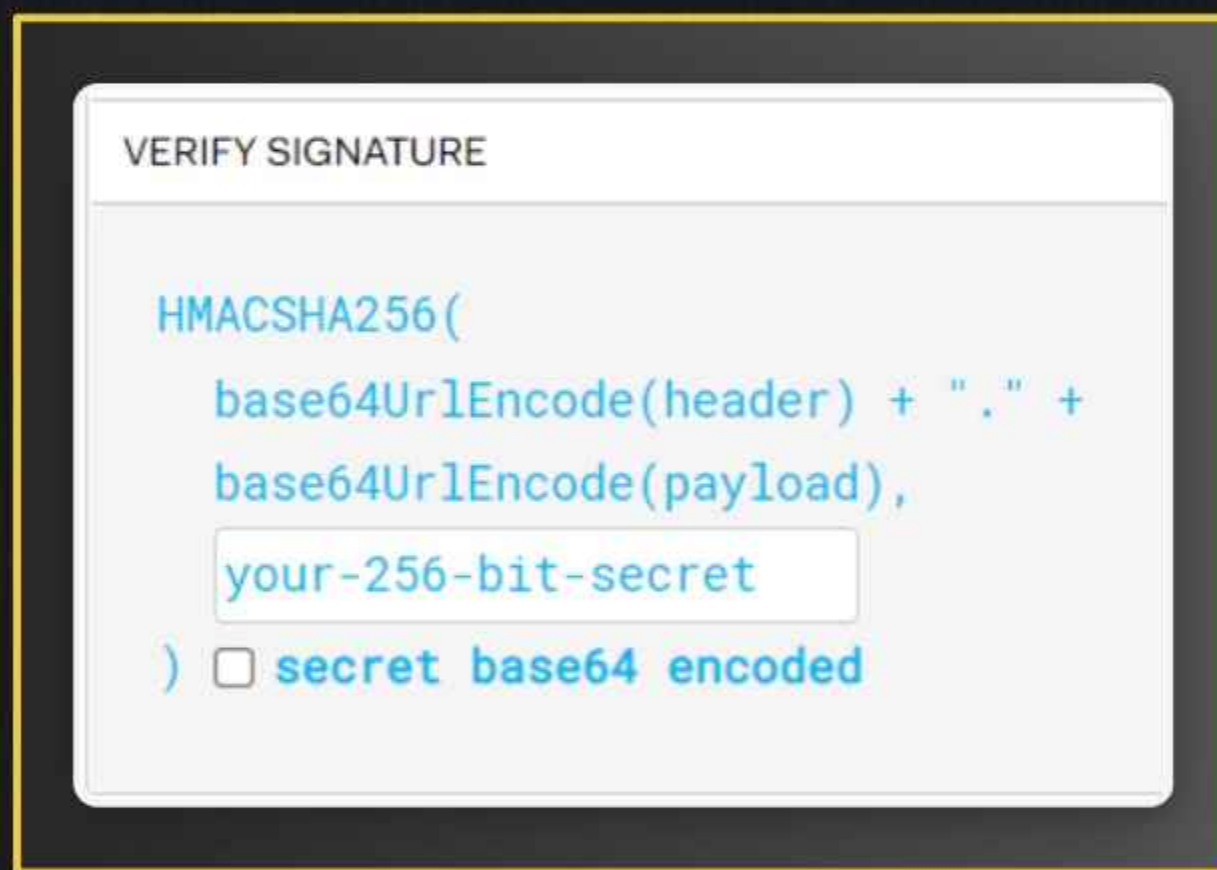


- The payload contains the claims, which are statements about an entity (typically, the user) and additional metadata.
- Claims are typically represented as key-value pairs and can include information such as the user's ID, name, email, and roles.





- The signature is used to verify that the sender of the JWT is who it says it is and to ensure that the message has not been tampered with.



- That's a quick introduction to JWT!
- We will see more in-depth concepts of JWT in the upcoming posts.



❤️ **Thanks** for reading !

For more content on  
**Java & Backend** Development,  
follow me on below handles



**Vikas Rajput**  
**@vikasrajputin**

