JWT vs OAuth –

JWT –

- JSON Web Token

– It is tokenization format.

- Content is also wrapped as token

- One of the most secured way

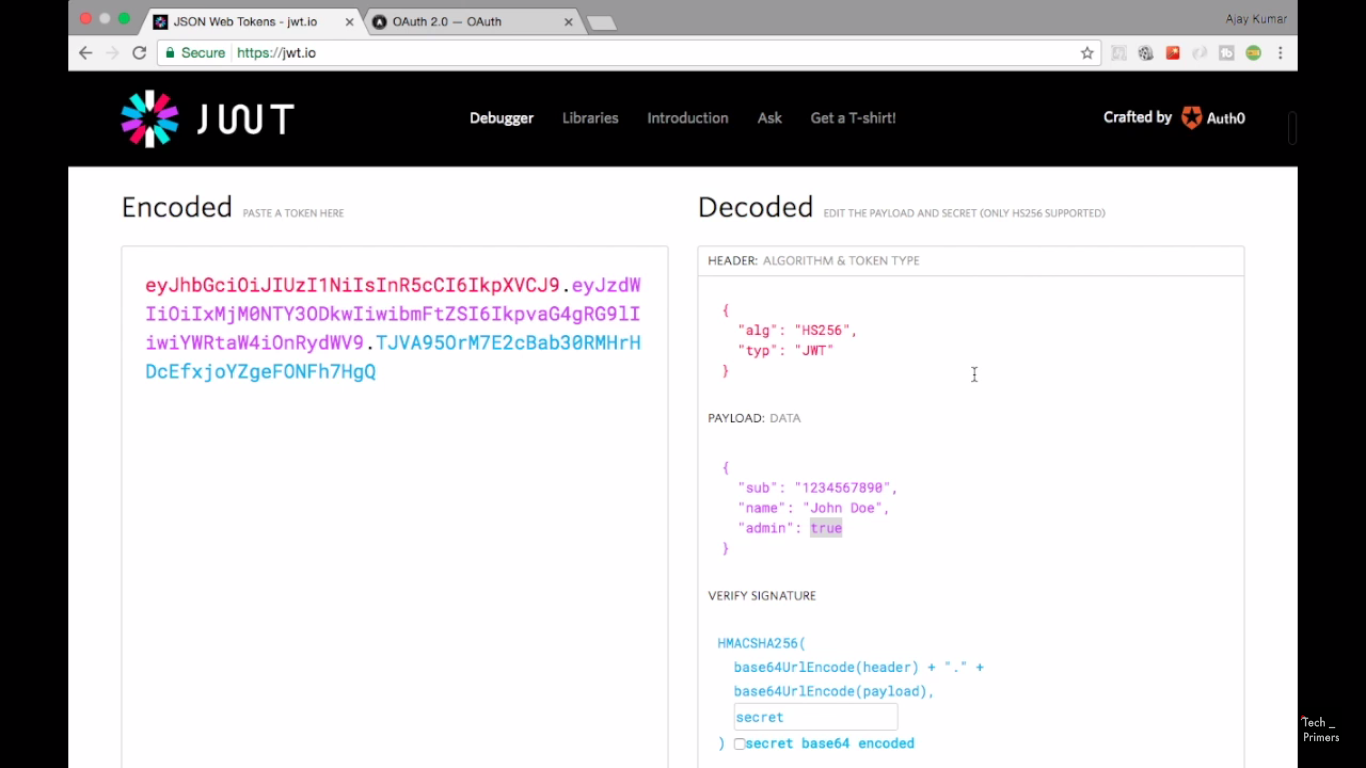
- Split into 3 parts –

Header – Algorithm (Hashing 256) that we are using to encode our message and type = JWT

Payload – Real message

Signature - encoded header and payload; then merge that along with secret.

Real encoded, secure message looks like below (left side). Two dots (separating three parts).



- JWT is NOT completely secure because anyone can see this message which we are passing in header.

- It is just a way to ship packets from client to server.

**OAuth** –

- Every time a request is made, an access token (within its valid time) is sent to the service which both client and server knows.

- It is a standard, a protocol for authorization. Used to communicate between 2 processes (client/ server) using authentication mechanism.

- We then decide whether we are authorized to it (that resource).

- E.g. – Google oauth (like android mobile). When you try installing any app from play store, it asks users whether you allow these permissions (to the people/ app) to third party – that is what oauth is i.e. taking the end user consent to perform some operation.

One more example could be spending (deducting) some money on any website (like amazon) with users permission to deduct money from his bank account.

- Authorization is easily achieved using OAuth.

- Authentication is not needed for each request. Instead tokens (access tokens) are passed with each request.

