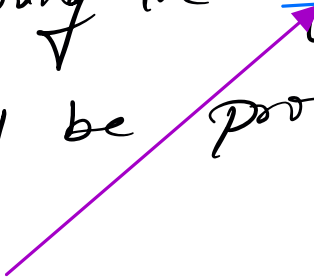


## Authentication:


Step where user needs to verify the identity. for this application, the user needs to provide the email and password which it created during the registration process. The user will be provided a token after Auth process.



what after it?

## Authorization :-

Once the user authenticates, he is provided a token. Now to access a resource, the user needs to show a token that was sent during authentication. This ensures that the user is entitled to a resource.



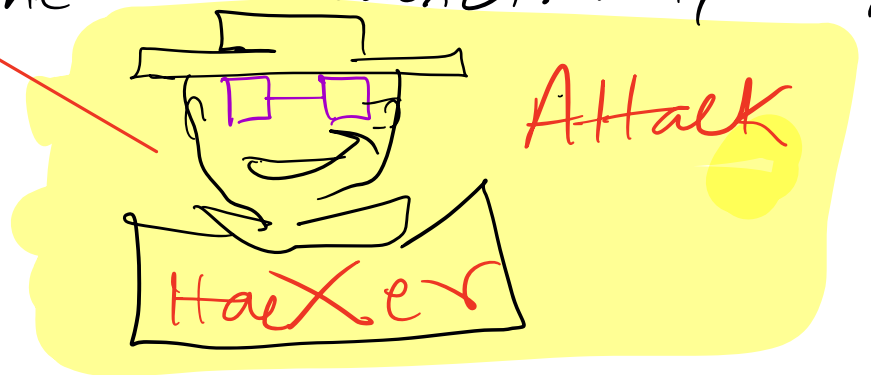
JWT:

JSON web token, is used to Encrypt a payload into a Signed token that has the permissions or Authorities of the user.

we will be sending the token to user by http Cookies.

this cant be accessed.

Http cookies are type of web cookies that come with a special security attribute that restrict cookies from being accessed by javascript in the web-browser. This prevents XSS attacks.

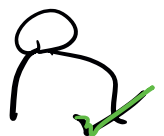


Auth process:-

user  
authenticated



Sends http  
only Signed  
cookies with JWT  
token



# Accessing protected resource



User send  
back the  
same cookie



if the cookie  
matches and  
token is valid



process  
the  
request



if the cookie  
doesn't match  
or token is invalid



Abort  
the  
operation