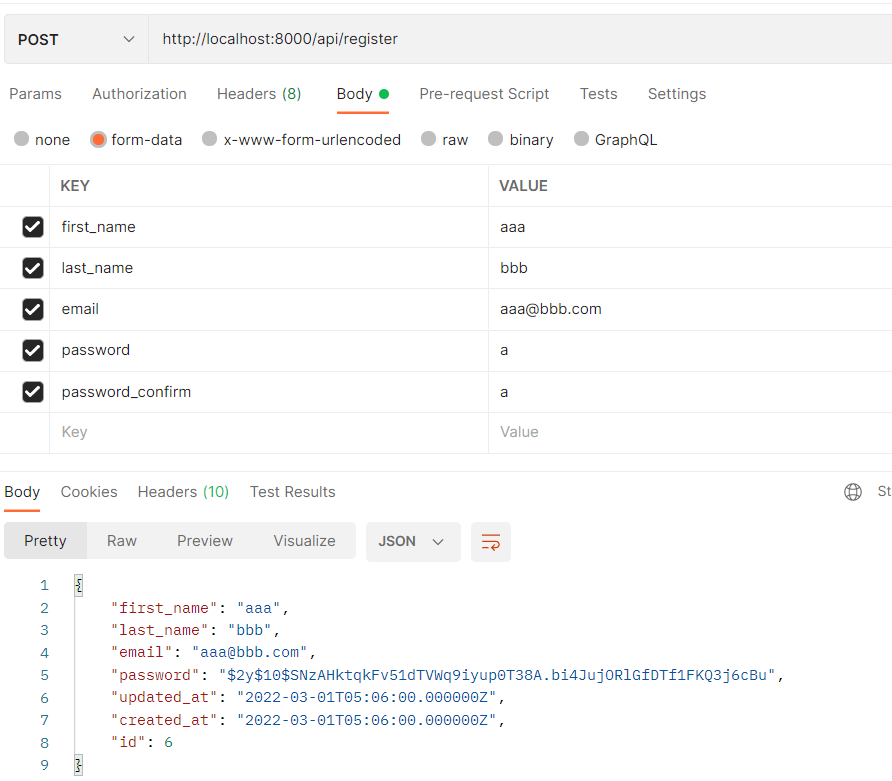
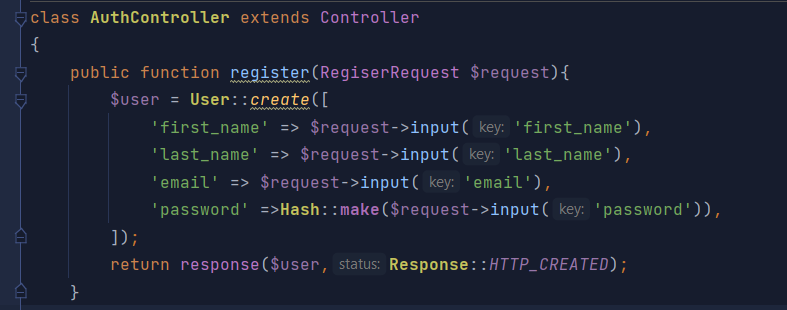
Login

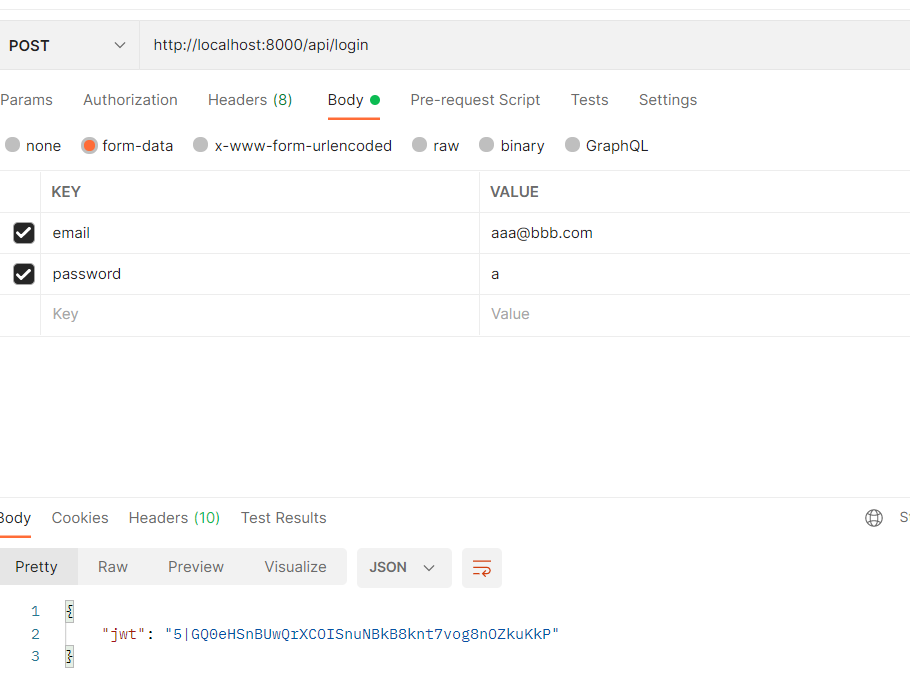
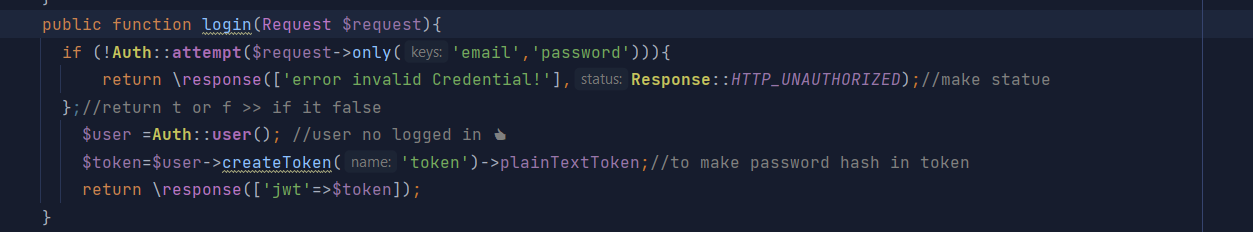
# Postman

## Register

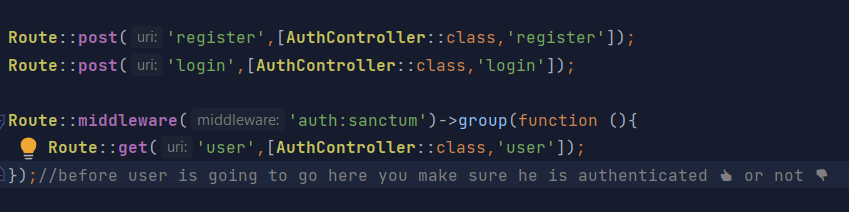


## Login

### Making JSON Web Token(JWT)



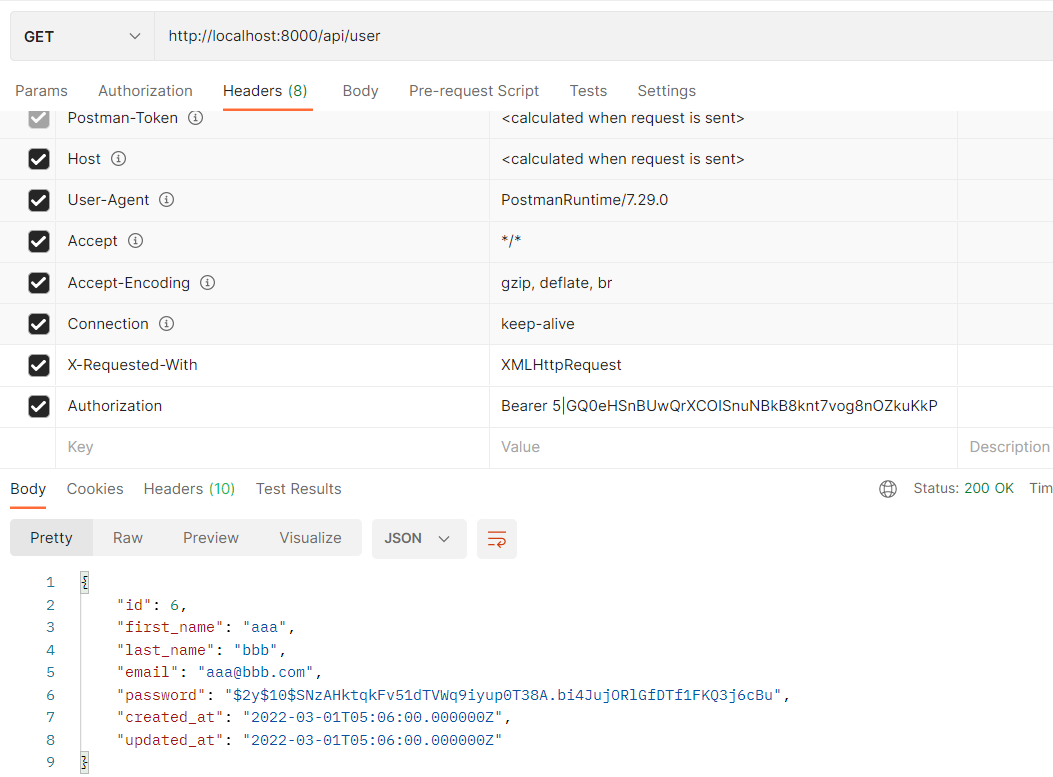
## API Routes



## Authorize Rules

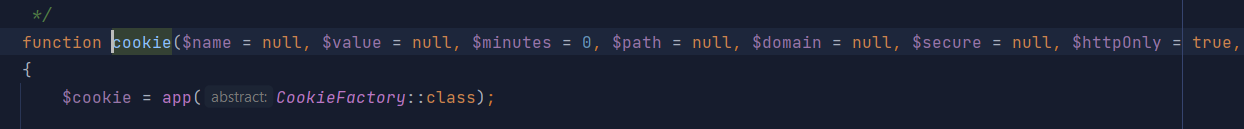
## Authorization

### NOTICE :The authorization key has same JWT of user "aaa" that's make him authenticate



# Login with cookie 🍪..

## Now the response when we log in will get also a JWT cookie with it and the front end cannot access because it is http only



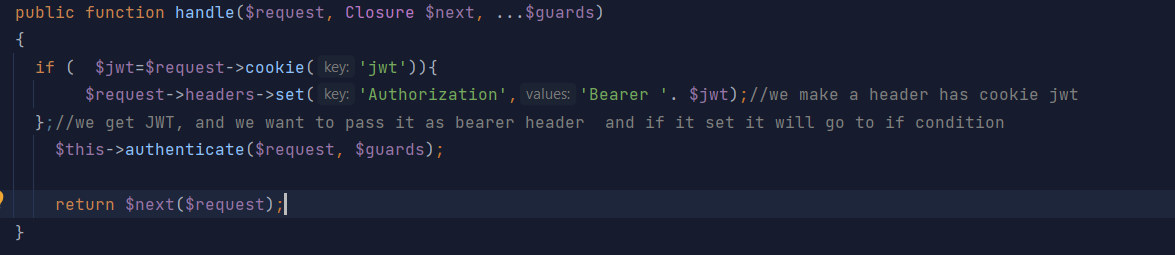
## Get JWT from cookie so we can get it

### In config cons : we must set it true



## we make a header has cookie JWT

### we get JWT, and we want to pass it as bearer header and if it set it will go to if condition

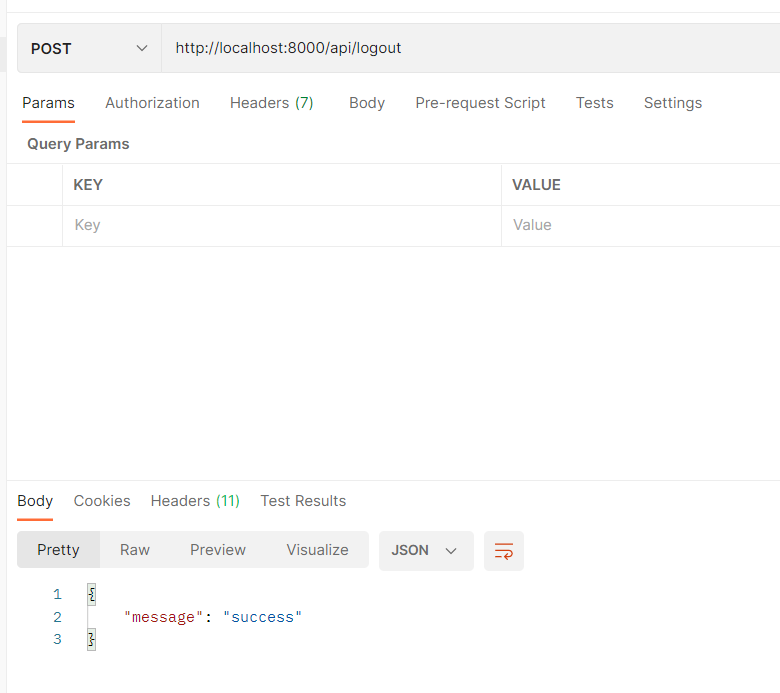


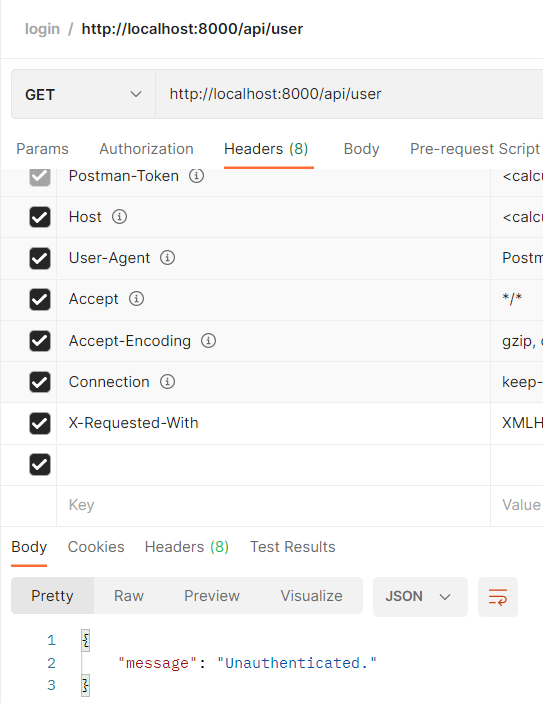
## Now we log in cookie and without add Authorization

## 

# Logout

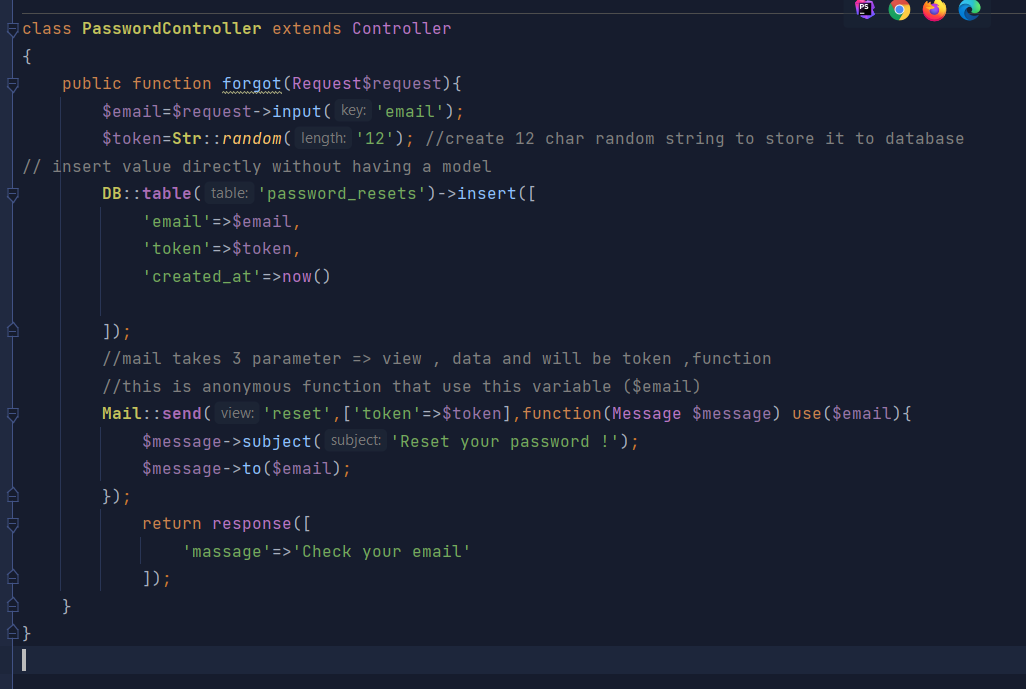
### Look out and this will be a post request for logout needs to the user to be write authenticated to remove the cookie And that said, basically with this we forget the cookie, we said another cookie, which, like we cannot delete cookies, we just set a cookie in the past to delete the previous cookie.



Now user is logout and gives unauthenticated 

# Sending email went forget password

## First will create controller called PasswordController



## create it's routes



## Also create mail server to test it's work by using mailhog

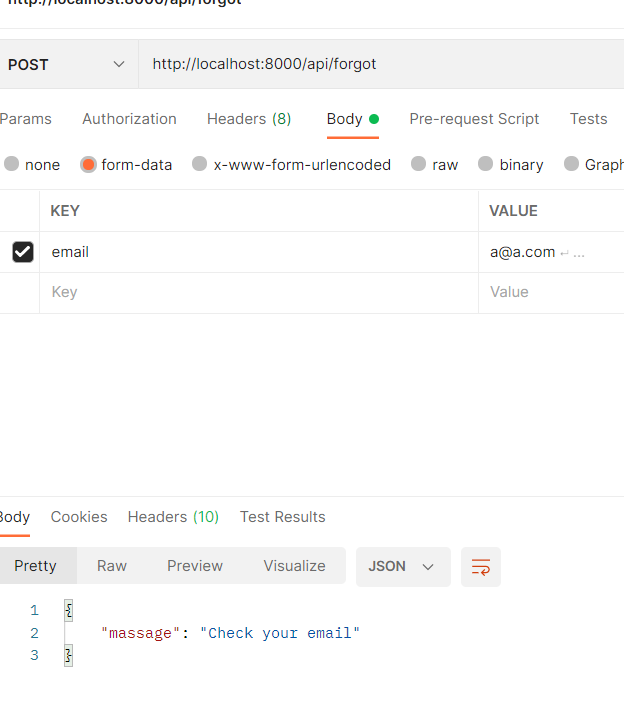
### Has in .env

MAIL\_HOST=localhost  
MAIL\_PORT=1025

### And also make reset page

Click <a href="localhost:3000/reset/{{$token}}}">here</a>to reset your password  
{{--//port 3000 because react app--}}

## Finally when send email



when email is send