creating a model object and saving it, there is another way

**const user = await User.create({email , password})**

creates a document inside the collection, and returns that newly created document as object.

you don't have to create a user object first and then save it in this case.

npm i validator

has many validator functions.

**const {isEmail} = require('validator')**

**isEmail** is a method which you can pass onto the validator in schema.





**const user = await User.create({email , password})**

This is the error thrown when a user is not created in database due to some **invalid input** based on **schema.**

**Unique** is not a validator in mongoose schema. When a duplicate is added in a unique declared field, this error is thrown. You can identify it using **code.**

A screen shot of a computer

Description automatically generated

const handleErrors = (err) => {

  console.log(err.message, err.code);

  // console.log(err);

  let errors = { email: '', password: '' };

  // duplicate email error

  if (err.code === 11000) {

    errors.email = 'that email is already registered';

    return errors;

  }

  // validation errors

  if (err.message.includes('user validation failed')) {

    // console.log(err);

    Object.values(err.errors).forEach(({ properties }) => {

      // console.log(val);

      // console.log(properties);

      errors[properties.path] = properties.message;

    });

  }

  return errors;

}

This is how you can use the **err** object thrown and convert it to a smaller useful error and send it as a response. **errors** which is returned is send. **res.json({errors})**

  catch(err) {

    //This handle error function will return a small usable object containing

    //error information. error object is thrown when user cannot be created.

    const errors = handleErrors(err);

    res.status(400).json({ errors });

  }

**A screen shot of a computer

Description automatically generated**

This error is sended as a response. **errors** contain errors related to **input fields.**

This code belongs to the same file where schema is made and model is exported.

//next() is required to continue because these are middleware,

//also known as pre and post hooks

// read more on doc

// fire a function after doc saved to db.(post)

//doc is the document which is finally saved.

userSchema.post('save', function (doc, next) {

  console.log('new user was created & saved', doc);

  next();

});

// fire a function before doc saved to db(pre)

//We don't receive 'doc' because this is before saving to database.

//use normal function, not arrow function because we want to use 'this'.

//this in this case refers to the instance of 'User' which is about to be saved.

userSchema.pre('save', function (next) {

  console.log('user about to be created & saved', this);

  next();

});

## Cookies

npm i cookie-parser

Parse Cookie header and populate req.cookies with an object keyed by the cookie names.

// cookies

const cookieParser = require('cookie-parser');

app.use(cookieParser());

//middleware, parses cookie to object which we can use.

app.get('/set-cookies', (req, res) => {

  // res.setHeader('Set-Cookie', 'newUser=true');

  //This is the default way of creating a cookie.

  //This is with the help of cookie-parser library.

  res.cookie('newUser', false);//(name , value , {options})

  res.cookie('isEmployee', true, { maxAge: 1000 \* 60 \* 60 \* 24, httpOnly: true });

  //maxAge : time in milliseconds when cookie will expire, cookie remains only till session.

  //httpOnly : bool , if true, you can't acces the cookie using javascript. 'document.cookie'

  //secure : true, only secure connection are alllow, eg https , NOT http

  res.send('you got the cookies!');

});

If you set cookies, they are send along with response.

If cookie already exist, it is replaced. If it does not, a new one is created.

To delete a cookie:

  res.cookie('jwt', '', { maxAge: 1 });

creating maxAge to 1 millisecond.

Login method is defined as static on **User** model itself. You can then call this method by class name is **User.**

**User.login(“**farazgod1234@gmail.com**” , “**nope**”)**

// static method to login user. Defined along schema.

//finds email, checks password.

//returns ‘user’ object, else throw error with some message.

userSchema.statics.login = async function(email, password) {

  const user = await this.findOne({ email });

  if (user) {

    const auth = await bcrypt.compare(password, user.password);

    if (auth) {

      return user;

    }

    throw Error('incorrect password');

  }

  throw Error('incorrect email');

};

//when loging in, create a new token and cookie.

//send \_id as json response.

module.exports.login\_post = async (req, res) => {

  const { email, password } = req.body;

  try {

    const user = await User.login(email, password); //static method

    const token = createToken(user.\_id)

    res.cookie('jwt', token, { httpOnly: true, maxAge: maxAge \* 1000 });

    res.status(200).json({ user: user.\_id });

  } catch (err) {

    const errors = handleErrors(err);

    res.status(400).json({errors});

  }

}

## Jwt tokens

//Token generator

//create json web token

const maxAge = 3 \* 24 \* 60 \* 60;//3 days in seconds

const createToken = (id) => {

  // (string\_to\_make , secret\_string , {options})

  return jwt.sign({ id }, process.env.SECRET, {

    expiresIn: maxAge//seconds

  });

};

Middleware protecting the routes. Check whether the tokes in the cookie is valid or not.

You can decode the token, which gives you access to the payload.

const jwt = require('jsonwebtoken');

const User = require('../models/User')

const requireAuth = (req, res, next) => {

  const token = req.cookies.jwt;

  //taking out the token. Made possible by cookie parser

  // check json web token exists & is verified

  if (token) {

    //jwt.verify(token , secret , func(error , decodedToken))

    jwt.verify(token, process.env.SECRET, (err, decodedToken) => {

      if (err) {

        console.log(err.message);

        res.redirect('/login');

      } else {

        console.log(decodedToken);

        next();

      }

    });

  } else {

    res.redirect('/login');

    //change the URL in the browser.

    //redirects to the given URL.

    //relative to the domain of the server

  }

};

// check current user

const checkUser = (req, res, next) => {

  //This middleware is to inject the data if they are logged in.

  const token = req.cookies.jwt;

  if (token) {

    jwt.verify(token, process.env.SECRET, async (err, decodedToken) => {

      if (err) {

        res.locals.user = null;

        //we're giving it null instead of not creating user in local at all because,

        // we will be accessing the 'user' inside of the views, so if 'user' does not exist,

        // it will throw error as we're accessing a variable which is not there in the first place

        next();

      } else {

        //user is an object fetched from database from

        //id received from decoding token and accesing from payload

        let user = await User.findById(decodedToken.id);

        res.locals.user = user;//user object is now available to views

        next();

      }

    });

  } else {

    res.locals.user = null;

    next();

  }

};

module.exports = { requireAuth, checkUser };