Diario di bordo Progettino Autenticazione

12.11.2022

Creati progetti backend (nodejs express) e frontend (react).

14.11.2022

Installato bootstrap e react-bootstrap. Npn install.

Creati i files componenti login e registration js. Forms presi da react-bootstrap.

<https://react-bootstrap.github.io/forms/overview/>

Uso un hook per decidere se mostrare la pagina di login oppure quella di registrazione; ancora da programmare e testare. È un’idea, successivamente sarà probabilmente da modificare.

* Scrivere i test per login e registration!!!

15.11.2022

Cercato il come testare da

* <https://it.reactjs.org/docs/testing-recipes.html>
* <https://www.youtube.com/watch?v=6wbnwsKrnYU>
* <https://training.fabiobiondi.io/2019/12/28/react-typescript-unit-test-react-testing-library/>

Scritti dei test. Vado a verificare che i componenti vengano renderizzati correttamente ricercandone le parti nello schermo.

‘It’ e ‘test’ sono essenzialmente lo stesso “comando” <https://stackoverflow.com/questions/45778192/what-is-the-difference-between-it-and-test-in-jest> .

Attenzione: getByPlaceholderText() può causare problemi se esistono più placeholder con il medesimo testo o parte di esso (es. ‘Password’ e ‘Confirm password’). Infatti <https://testing-library.com/docs/queries/byplaceholdertext/> suggerisce di usare in alternativa ‘getByLabelText’, o quantomeno indica che ‘getByPlaceholderText’ non ne è un buon sostituto.

Per eseguire i test si impiega il comando **npm test**.

Rifattorizzato: creata la cartella “\_\_test\_\_” allo stesso livello della cartella “components”.

Il button con variazione ‘link’ non sembra essere recuperabile tramite getByRole (per recuperare il button <https://stackoverflow.com/questions/58408178/query-a-button-with-specific-text> ). Allora ho impiegato getByText <https://stackoverflow.com/questions/57827126/how-to-test-anchors-href-with-react-testing-library> .

16.11.2022

Validazione dei form in react con react-hook-form: <https://www.npmjs.com/package/react-hook-form> , <https://react-hook-form.com/> . Si tratta di una libreria da quasi 2.7 mio. di download settimanali.

Nota: in react per le proprietà si procede come segue, passando un oggetto <https://www.w3schools.com/react/react_css.asp> .

Palette di colori html <https://www.w3schools.com/colors/colors_names.asp> .

Inoltre sembra intelligente impiegare uno schema sfruttando Yup così da evitare di inserire nel form le varie validazioni. npm install @hookform/resolvers yup

Refactoring nello schema yup.

Specificare dei messaggi di errore <https://stackoverflow.com/questions/60356911/how-to-change-default-error-text-in-yup-formik> .

Aggiunti altri campi al form di registrazione: nome, cognome, descrizione di sé stessi, data di nascita (con datepicker (<https://www.npmjs.com/package/react-datepicker>) e possibilmente un’immagine ().

Validazione dei campi presenti.

Devo capire come validare la data e come impostare il datepicker affinché sia più immediato tornare indietro nel tempo (ora andrebbe di mese in mese, ma già per me è lunga tornare indietro rapidamente e sono nato nel ’93…).

18.11.2022

Angelo sembra apprezzare i nostri sforzi!

Installare Sequelize, bcrypt, jsonwebtoken e per lavorare con il file .env.

19.11.2022

Inserito “proxy”: <http://localhost:3000> nel package json del frontend in modo da collegarlo al backend.

Ora, si potrebbe impiegare uno useEffect per seguire la fetch verso l’api del backend, ma sembra leggermente più laborioso rispetto all’impiego di axios (37mio di download settimanali) <https://www.npmjs.com/package/axios> .

Tuttavia si segnala su cve un problema risalente al 2021 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3749> in cui si parla di “axios is vulnerable to Inefficient Regular Expression Complexity”. Ossia “The product uses a regular expression with an inefficient, possibly exponential worst-case computational complexity that consumes excessive CPU cycles.” Da <https://cwe.mitre.org/data/definitions/1333.html> .

Problema del collegamento, forse dovuto alle politiche CORS, scarico cors <https://www.npmjs.com/package/cors> .

Dopo diversi inconvenienti, problemi, Axios funziona: frontend sembra collegato con il backend.

// Destruct necessary in order to manage the inputs/forms validation

const { register, handleSubmit, formState: { errors } } = useForm({ resolver: yupResolver(schema)});

// onSubmit function call on the nodejs backend

const onSubmit = data => {

axios.get("/login").then(response => {

console.log(response.data);

})

};

Le righe di codice di Axios sono state inserite nella funzione onSubmit presa grazie a yup.

Installati bcrypt, Sequelize, nodemon, jsonwebtoken, dotenv (per lavorare con il file .env) <https://www.npmjs.com/package/dotenv> .

Creato il database: due tabelle, verifications per la verifica della mail e user per gli utenti. <https://www.tutsmake.com/node-js-express-mysql-email-verification-tutorial/>

22.11.2022

Scritti i modelli in Sequelize di User e Verification.

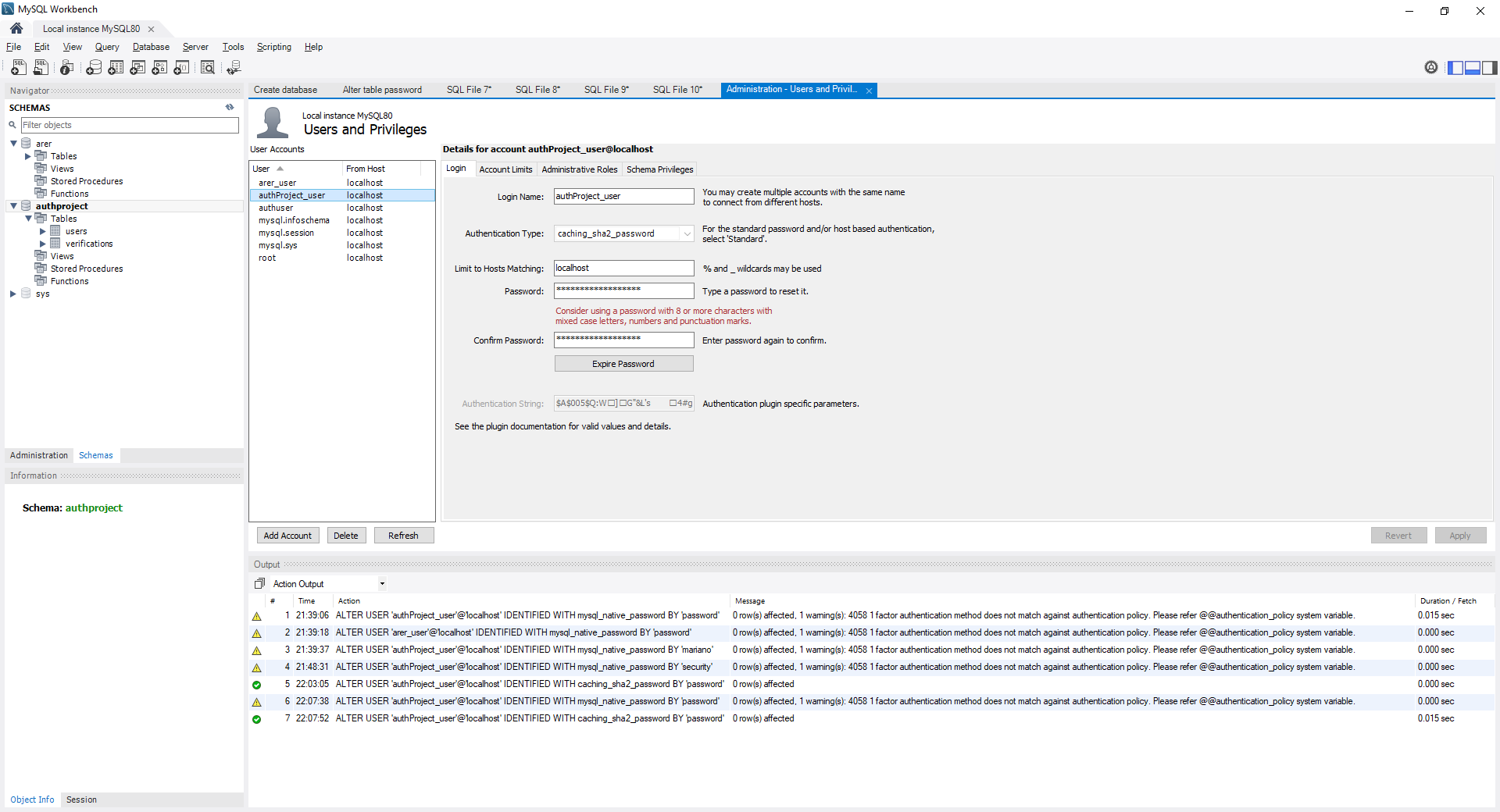
Filtrate nel Datepicker le date future rispetto a oggi (new Date()). Bisogna velocizzare il passaggio alle date passate per ora limitato al salto di mese in mese. E aggiungere il recaptcha.

Sistemo il backend.

Non riesco a collegare sequelize al database…

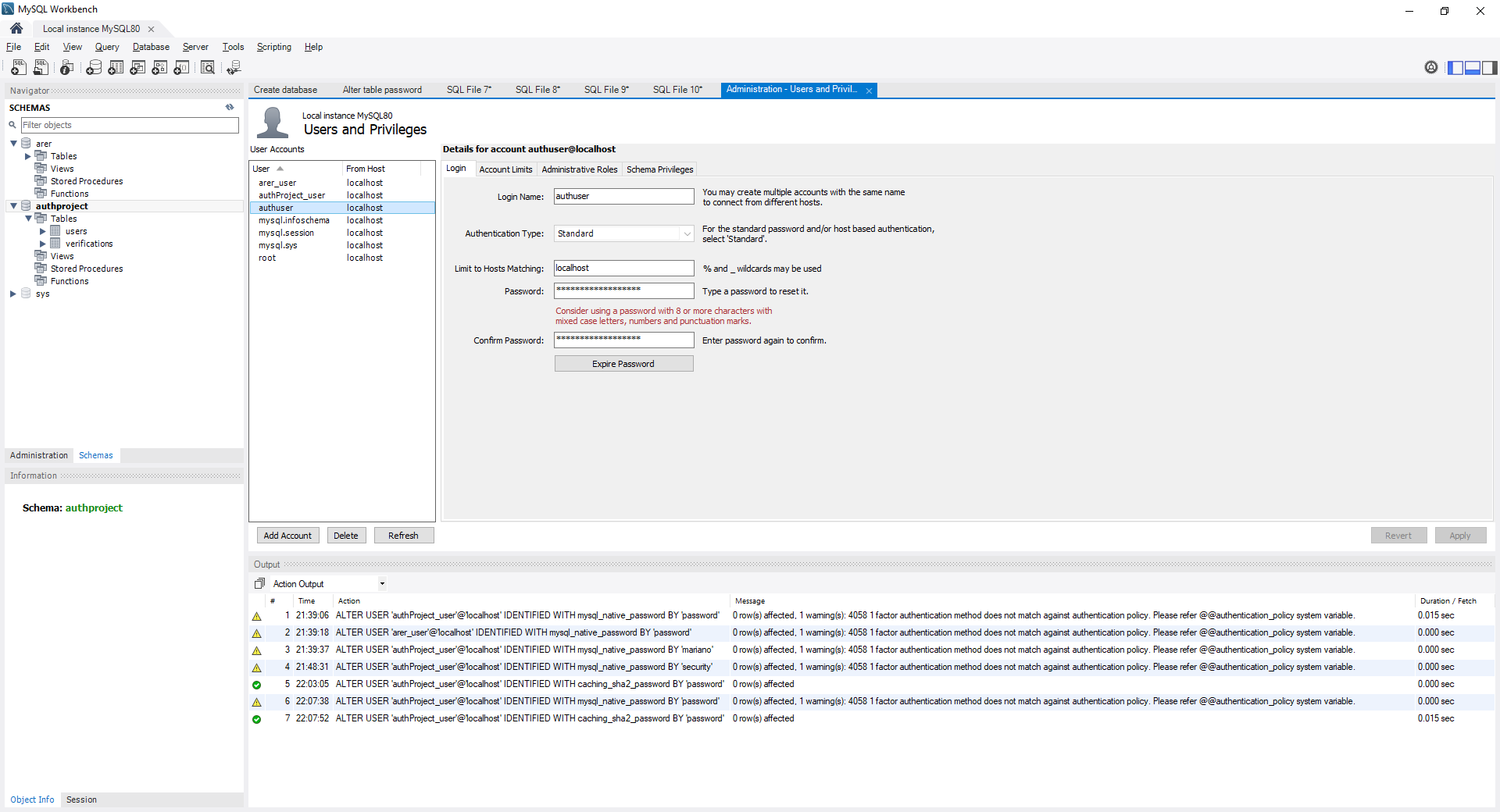


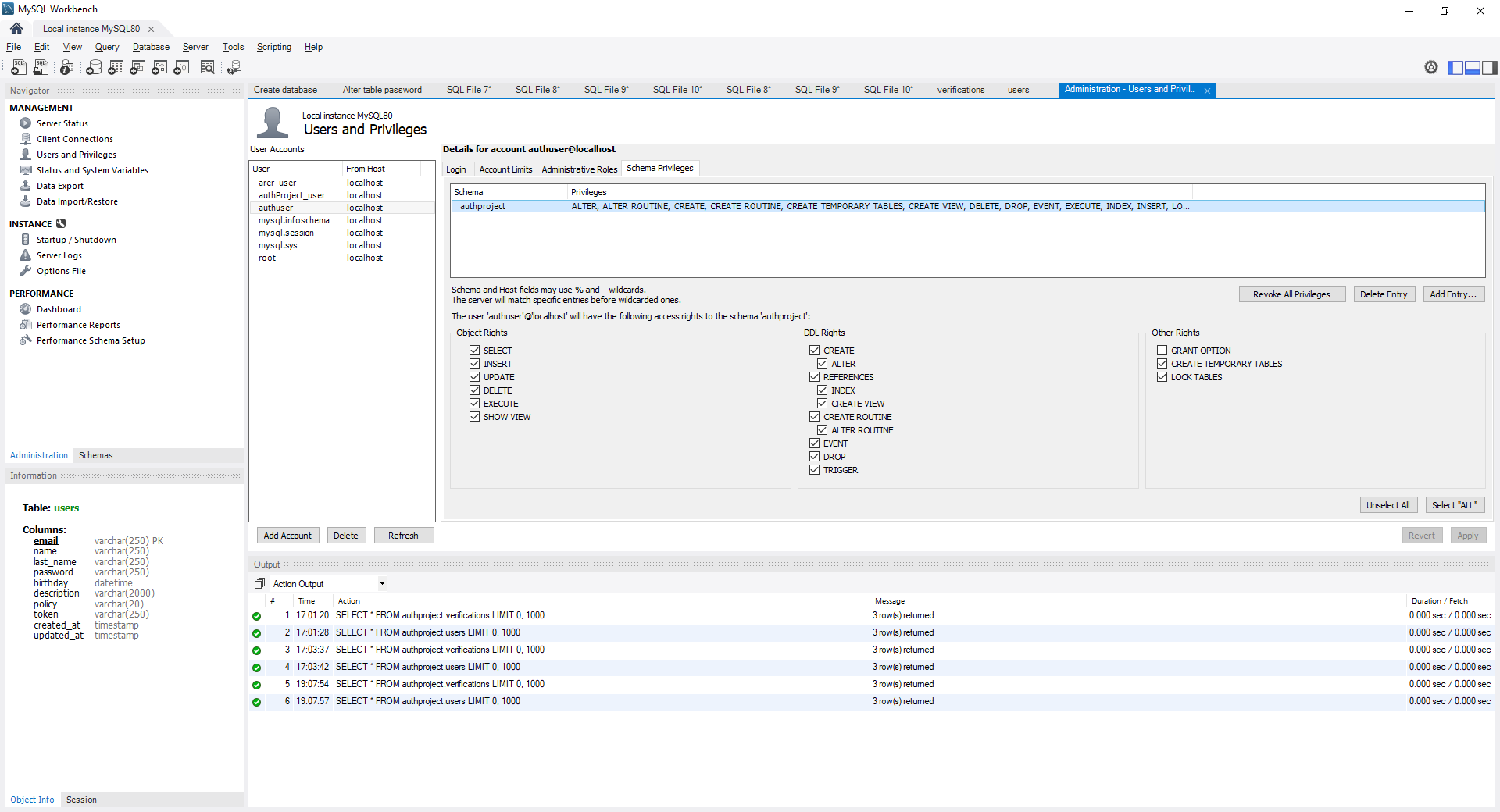
Il problema è stato risolto. Inserendo l’utente root e la rispettiva password il collegamento avveniva. Rispetto all’utente arer del progetto di diploma, l’utente che si cercava di autenticare



Aveva un tipo di autenticazione differente da quella standard.

Conseguentemente ho creato un utente ulteriore impiegando il tipo di autenticazione standard. Facendo partire il server non si sono verificati errori: Sequelize si connette con MySQL.





Privilegi dell’utente.

23.11.2022

Inserire la visualizzazione dell’utente loggato (card). Kitchen sink da <https://react-bootstrap.github.io/components/cards/> .

Creata la card utente, ma è da testare.

Passare al routing anche lato client <https://www.npmjs.com/package/react-router-dom> . Si cambia dalla single page application al routing.

Docs <https://v5.reactrouter.com/web/guides/quick-start> .

<https://www.geeksforgeeks.org/reactjs-router/#:~:text=React%20Router%20is%20a%20standard,how%20the%20React%20Router%20works>. Indica che Switch non è più un export della libreria ma è Routes.

Effettuato il routing

* “/” 🡪 login
* “/register” 🡪 form di registrazione
* “/user” 🡪 la scheda utente

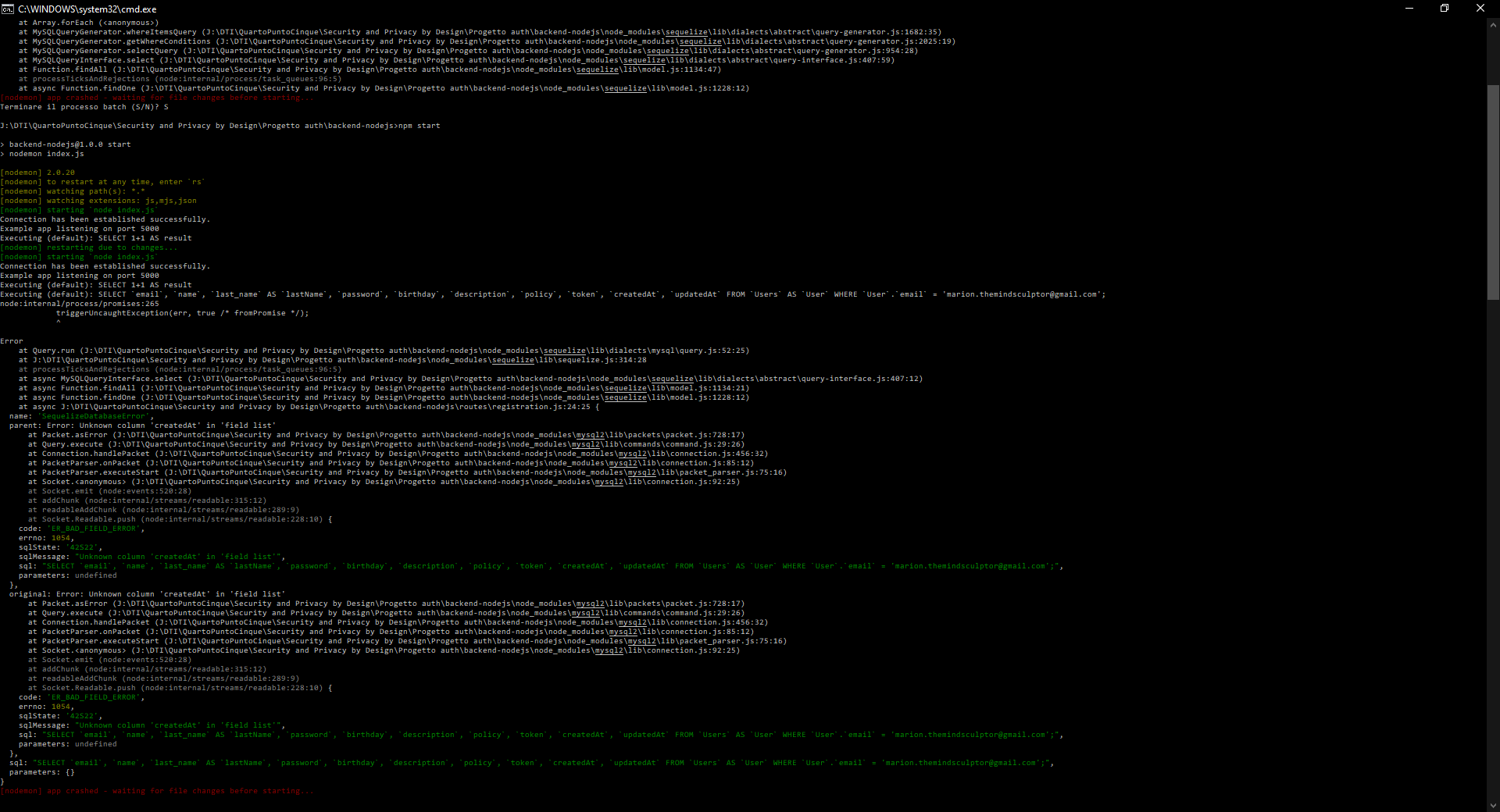
24.11.2022

Sistemo la registrazione. Probabilmente, per praticità, il tutto verrà poi gestito da una route unica; magari user.

Inserito il controllo per il match della password <https://www.positronx.io/add-confirm-password-validation-in-react-with-hook-form/> .

Ora scrivo la re-direzione dopo la corretta registrazione. <https://stackoverflow.com/questions/53900739/redirection-using-axios-and-react> . Installato react-router per importare Redirect.

Ho sistemato il post, in parte, l’errore generato è ora differente a livello di server



Sembra che sia dovuto al createdAt e updatedAt. Devo capire come risolvere, ossia come inserire automaticamente le date.

Ho creato le colonne nella tabella users in mysql workbench.

Nonostante l’inserimento delle colonne nel db l’errore persiste.



Provo anche a creare una verification. Continua a esserci il problema, allora ho disattivato il timestamps per l’intero database <https://stackoverflow.com/questions/20386402/sequelize-unknown-column-createdat-in-field-list> .

Così sembra funzionare, inoltre birthday nel db è stata cambiata in datetime da timestamp, per il modello con sequelize (<https://sequelize.org/docs/v6/core-concepts/model-basics/#data-types> ). New Date() crea l’istanza anche dell’orario, ma con toDateString() dovrei ottenere unicamente la data selezionata (<https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Date/toDateString> ), questo sembrerebbe funzionare meglio, testato in un interprete online (<https://stackoverflow.com/questions/2013255/how-to-get-year-month-day-from-a-date-object> ).

Redirect ora funziona <https://www.geeksforgeeks.org/how-to-redirect-to-a-relative-url-in-javascript/> .

25.11.2022

Gestito il login a livello di codice, da testare. In ordine: si controlla l’esistenza dell’utente, si controlla che l’account sia verificato, si controlla che la password sia corretta. Se tutti questi check sono corretti si crea e si invia il token.

Mi dedico al frontend per gestire il componente di login e i componenti di risposta. Devo aggiungere l’oggetto da assegnare al post.

Al json di risposta dal backend in caso di errori al momento del login ho aggiunto un campo legato al problema (se è legato alla password o alla verifica) poiché entrambi ritornerebbero lo stesso codice di errore 🡪 risolto: non eseguivo il send sulla risposta della route…

26.11.2022

Dopo il login, provo a inserire una semplice ridirezione a seconda della condizione. Nel componente App inserisco le route che mi servono per la ridirezione con i relativi componenti e i props necessari.

Hooks ed eventuali funzioni:

isUserLog (true/false), un hook per il messaggio e la relativa funzione per settarlo, un hook per il problema e la relativa funzione per settarlo.

Gli hook non funzionano, quindi ho creato delle pagine ad hoc.

Inoltre ho risolto il perché non si vedeva console.log() nella console del browser web. Axios divide quella che è la risposta da quello che è l’errore.

.then(response => {…} ) 🡪 per la risposta

.catch(error => {…} ) 🡪 per gli errori (es. 401, 404, ecc…)

Ora cerco di gestire l’invio della email.

Mischio un pochino <https://www.tutsmake.com/node-js-express-mysql-email-verification-tutorial/> , <https://www.youtube.com/watch?v=76tKpVbjhu8> e il relativo codice su github <https://github.com/benawad/graphql-express-template/tree/25_confirmation_email> .

Installo il nodemailer <https://www.npmjs.com/package/nodemailer> con oltre 2 mio di download settimanali.

Creata la route verifymail che gestisce il link di verifica che si invia via mail:

router.get('/verifymail/:token', async (req, res) => {

try {

const { user: { email } } = jwt.verify(req.params.token, process.env.MAIL\_TOKEN\_SECRET);

const verification = await Verification.findOne({where: {token: req.params.token}});

// Update verify flag

verification.verify = '1';

// Save updated verification element

verification.save();

} catch (e) {

res.send('error');

}

return res.redirect('http://localhost:3000/');

});

Creato un account mail volante su ethermail. La configurazione su nodejs è:

const transporter = nodemailer.createTransport({

host: 'smtp.ethereal.email',

port: 587,

auth: {

user: 'mitchel.schiller69@ethereal.email',

pass: 'YXk5E5MZJB74qdnHdt'

}

});

Qualora si andasse in produzione potrebbe essere corretto usare questa configurazione per distinguere test e produzione

var mailConfig;

if (process.env.NODE\_ENV === 'production' ){

// all emails are delivered to destination

mailConfig = {

host: 'smtp.sendgrid.net',

port: 587,

auth: {

user: 'real.user',

pass: 'verysecret'

}

};

} else {

// all emails are catched by ethereal.email

mailConfig = {

host: 'smtp.ethereal.email',

port: 587,

auth: {

user: 'ethereal.user@ethereal.email',

pass: 'verysecret'

}

};

}

let transporter = nodemailer.createTransport(mailConfig);

Provo la verifica della mail.

Salta fuori un errore: “error: self signed certificate in certificate chain”.

<https://stackoverflow.com/questions/45088006/nodejs-error-self-signed-certificate-in-certificate-chain> segnalano una soluzione, ma la soluzione viene smentita qui <https://github.com/nodemailer/nodemailer/issues/406> .

Sempre all’interno dell’ultimo link si suggerisce la seguente soluzione da aggiungere ai parametri del transporter.

tls: {

rejectUnauthorized: false

}

Effettivamente l’errore è sparito. Verificherò che l’email sia arrivata, inviata alle 22.46.

28.11.2022

L’email non arrivava. Dopo infinite prove, sono riuscito a mandare l’email: <https://stackoverflow.com/questions/45478293/username-and-password-not-accepted-when-using-nodemailer> inoltre ho disattivato l’antivirus. Il problema principale era che da maggio 2022 gmail non consentiva più il less secure app.

Tuttavia



29.11.2022

Implementazione del recaptcha. Oltre alle informazioni già acquisite da Giuseppe si impiegano anche altre fonti.

<https://www.youtube.com/watch?v=e_vMoPCBfqU>

Download del recaptcha <https://www.npmjs.com/package/react-google-recaptcha> (ritengo normale che non sia aggiornato da un paio di anni).

Non sembra andare…. Bad request a ogni tentativoooooooo…

30.11.2022

Commentato il controllo del recaptcha fintanto che non va, così come il controllo della verifica della mail, poiché ci sono a volte dei problemi durante l’invio della mail.

Iniziato a scrivere la route dello user, nella quale ho ricopiato il codice del controllo del token e l’estrazione della mail dal token stesso.

1.12.2022

Per la pagina di visualizzazione dei dati dell’utente devo scrivere la richiesta al backend in un useEffect poiché la chiamata avviene durante l’inizializzazione del componente e non in seguito ad altre cause. Un esempio <https://designcode.io/react-hooks-handbook-fetch-data-from-an-api> .

Ci sono degli errori, poiché effettivamente non salvo il token lato client.

Ma grazie a <https://stackoverflow.com/questions/42873693/save-api-token-to-local-storage-reactjs> è possibile salvare alcuni dettagli nel local storage.

I dati memorizzati si recuperano con un get <https://www.freecodecamp.org/news/how-to-use-localstorage-with-react-hooks-to-set-and-get-items/> . Dopodiché si inseriscono come header nella richiesta di axios <https://stackoverflow.com/questions/44245588/how-to-send-authorization-header-with-axios> .

Il token ora viene riconosciuto, bisognerebbe gestire il logout e l’accesso alle route di react.

Prima quindi il logout. Logout creato e testato.

Provo a proteggere l’accesso alle route di frontend impiegando lo useEffect. Sostanzialmente vorrei verificare se sono state salvate localmente sul browser le credenziali dell’utente corrente.

Funziona! Lo useEffect controlla il login, poiché non si desidera che un utente si possa ri-loggare nel caso le sue credenziali siano già memorizzate nel browser e si viene indirizzati sulla pagina di benvenuto, e controlla il messaggio di benvenuto, poiché solo chi possiede delle credenziali memorizzate può accedervi, in caso contrario si viene indirizzati al login.

Grazie a <https://stackoverflow.com/questions/72090838/how-to-do-non-existent-routes-redirect-to-homepage-in-react-router-dom> invece si gestiscono le route inesistenti indirizzandole alla root, ossia il login.

Ora mi metto a scrivere parte della documentazione. La validazione lato server e ciò che al momento ha dato problemi (mail di verifica dell’account e recatpcha) sarà sistemato successivamente.

3.12.2022

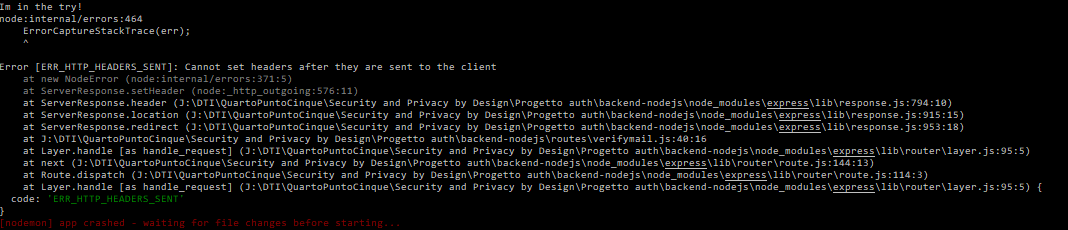
QUEL FIGLIO DI UN maledetto di axios non funzionava… Siamo impazziti a causa del captcha quando in realtà la causa era la chiamata axios. Usando fetch di ‘node-fetch’ (<https://www.npmjs.com/package/node-fetch> ) abbiamo ottenuto il risultato auspicato. Inoltre già inserendo l’indirizzo del captcha di google nella barra degli indirizzi di Chrome si riceveva la chiamata GET con il json; la chiamata reale è un POST.

Attenzione: la versione di node-fetch installata dal package manager potrebbe portare a un errore lato server sul suo import: const fetch = require(‘node-fetch’).

Per risolvere il problema abbiamo installato una versione meno recente, la 2, per far fronte alla problematica. La versione 2 ha funzionato 😊. <https://stackoverflow.com/questions/69087292/requirenode-fetch-gives-err-require-esm>

7.12.2022

Il link di verifica causa un errore lato server



La route viene quantomeno raggiunta, ma restituisce l’errore. Ho tolto la destruct e ho assegnato il ritorno a una variabile. Funziona perfettamente.

Tuttavia se inserisco un token sbagliato, il server crasha…ma non è quello che deve accadere. Piuttosto mi deve indirizzare su un’altra pagina o simile. In questo istante è sufficiente creare un account, copiare il link, modificarne il token e inviare quella richiesta. Comparirà sì un messaggio di errore, ma nel frattempo il server ha un crash.

<https://stackoverflow.com/questions/69683067/app-crashes-after-the-verification-of-jwt-token> questa potrebbe essere una soluzione.

8.12.2022

Alla fine anche con diverse versioni di soluzione il server andava in crash. Quindi è stato effettuato un indirizzamento al login anche in caso di errore della funzione verify. L’utente non avrà l’account verificato.

Una soluzione migliore per questa procedura di registrazione sarebbe quella di renderla temporanea e in caso di verifica non effettuata cancellare la registrazione.

Inserisco la validazione anche lato server tramite express validator (<https://www.npmjs.com/package/express-validator> ).

<https://www.youtube.com/watch?v=7i7xmwowwCY> video di spunto.

Creato la validazione, riprendendo parti di codice da precedenti lavori per velocizzare (è la seconda volta che inserisco il validator 😊). Vedremo con i test se la soluzione è efficace.

Ora devo far tornare qualcos’altro per differenziare user e admin.

L’admin ha la lista degli utenti che non sono admin.

L’ideale sarebbe far sì che il database venga creato se non esiste e che le tabelle vengano create qualora non esistessero. Per le tabelle si usa il sync.