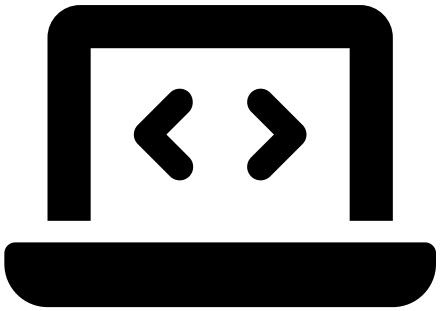

Documentație tehnică InfoToday

Cuprins

I. Introducere

Ambiția proiectului InfoToday este de a îmbunătății experiența meditațiilor online la informatică. InfoToday oferă sesiuni în timp real între elev și profesor, în care elevul, poate rezolva probleme și poate fi îndrumat mult mai ușor de către profesor.Plata unei sesiuni se face direct din platformă la acceptarea unei sesiuni de studiu, de către elev.

II. Tehnologii folosite

Aplicația InfoToday este alcătuită din 2 mari părți: front-end-ul (clientul aplicației) și back-end-ul (serverul aplicației).

Front-end-ul este bazat librăria React. Această librărie oferă avantajul de a avea componente reutilizabile și oferă o documentație amplă.

https://reactjs.org/docs/getting-started.html

Un framework important folosit pentru front-end este Tailwind CSS. Acesta este folosit pentru

stilizarea clientului și pentru adaptarea layout-urilor în funcție de rezoluția de vizionare.

https://tailwindcss.com/docs/installation

Pentru „syntax highlighting-ul” text editorului, am folosit CodeMirror. https://codemirror.net

Partea de back-end este alcătuită dintr-un REST API folosind Node.js împreună cu framework-ul Express și un WebSocket server folosind framework-ul Socket.IO.

https://nodejs.org/en/docs/

https://expressjs.com/en/starter/installing.html

Poziția mouse-ului, scrierea codului, sublinierea codului și compilarea acestuia sunt transmise în sesiuni folosind Socket IO.

https://socket.io/docs/v4/

Baza de date folosită este MongoDB, o bază de date NoSQL. MongoDB stochează datele sub formă de documente JSON cu scheme dinamice. Drept abstraction layer pentru MongoDB am folosit Mongoose.

https://mongoosejs.com/docs/api.html

Autorizarea plăților se face cu ajutorul platformei Stripe.

https://stripe.com/docs

III. Validarea datelor, autentificare, securitate

Autentificarea este bazată pe strategia JWT (JSON Web Token). La autentificarea unui utilizator, server-ul generează un token de acces, salvat in cookie-urile utilizatorului. Acest token este utilizat pentru a accesa aplicatia. La fiecare apel al API-ului, acest token este verificat, doar după ce este validat, utilizatorul primeste acces la rutele și funcțiile aplicației.

http://www.passportjs.org/packages/passport-jwt/

Parolele sunt criptate, iar mai apoi salvate în baza de date. Criparea este realizată folosind algoritmul one-way Bcrypt.

https://www.npmjs.com/package/bcrypt

Pentru securitatea aplicației am folosit middleware-ul Helmet, ce protejează aplicația împotriva atacurilor XSS, XFS, MITM.

https://helmetjs.github.io

IV. Implementări viitoare

Următorul lucru ce urmează să fie implementat

este o funcție de retragere a banilor pentru profesori. O altă funcționalilate ce urmează să fie implementată este apelul audio, eventual și video în sesiuni pentru a nu fi nevoie de folosirea unui soft third-party. Atribuirea unor teme este un alt feature ce va fi implementat.

Multumesc pentru atenție.