Descrizione del Sistema
BiblioTech è un'applicazione web per la gestione digitale dei prestiti bibliotecari di un istituto scolastico. L'obiettivo principale dell'applicazione web è garantire un controllo accurato, sicuro e sempre aggiornato sui libri.
Deve consentire la gestione di un catalogo bibliotecario composto da titoli per i quali la scuola possiede più copie fisiche. Per ogni libro vengono mantenute informazioni dettagliate (titolo, autore, ISBN) e, soprattutto, lo stato delle giacenze, distinguendo tra numero totale di copie possedute e numero di copie attualmente disponibili per il prestito.
Deve essere implementato un sistema di autenticazione obbligatoria e differenzia le funzionalità in base al ruolo dell'utente, garantendo che ogni attore del sistema possa accedere esclusivamente alle operazioni di propria competenza.
Gli attori del sistema possono essere lo studente o il bibliotecario.
Per prevenire accessi non autorizzati alle funzionalità amministrative, nel caso in cui venga selezionato il ruolo di bibliotecario il sistema richiede un controllo aggiuntivo. Dopo la verifica delle credenziali principali, l'utente viene reindirizzato a una pagina dedicata nella quale deve inserire un codice bibliotecario fisso, stabilito dall'amministrazione del sistema. Solo in caso di inserimento corretto di tale codice l'utente può accedere alle funzionalità riservate ai bibliotecari. In caso contrario, l'accesso viene negato.
Gli studenti, una volta autenticati, possono consultare il catalogo dei libri disponibili, visualizzare in tempo reale la disponibilità delle copie ed effettuare autonomamente il prestito di un libro, solo se sono presenti copie disponibili. Il sistema registra automaticamente il prestito, associandolo allo studente e salvando la data di inizio. Inoltre, ogni studente può visualizzare l'elenco dei libri attualmente in suo possesso, ottenendo una visione chiara e aggiornata dei propri prestiti attivi.
I bibliotecari devono disporre invece di una visione globale del sistema. Possono consultare l'elenco completo dei prestiti attivi, identificando per ciascun libro lo studente che lo detiene e la data di inizio del prestito. Essi sono inoltre responsabili della registrazione delle restituzioni, con cui si chiude il prestito, si aggiorna la data di restituzione e si ripristina correttamente il numero di copie disponibili del libro.
Le sessioni di ogni utente vengono registrate nel database includendo informazioni quali orario di inizio, scadenza, codice OTP, scadenza OTP e data di logout, garantendo tracciabilità e maggiore controllo degli accessi.
Dal punto di vista tecnico, BiblioTech è sviluppato come applicazione web basata su PHP lato server e MySQL come sistema di gestione del database.
La sicurezza è un aspetto centrale del progetto perché le credenziali degli utenti devono essere memorizzate in forma cifrata tramite hashing delle password.
L'intero sistema è distribuito tramite container Docker per assicurare riproducibilità, portabilità e facilità di avvio dell'ambiente di sviluppo.

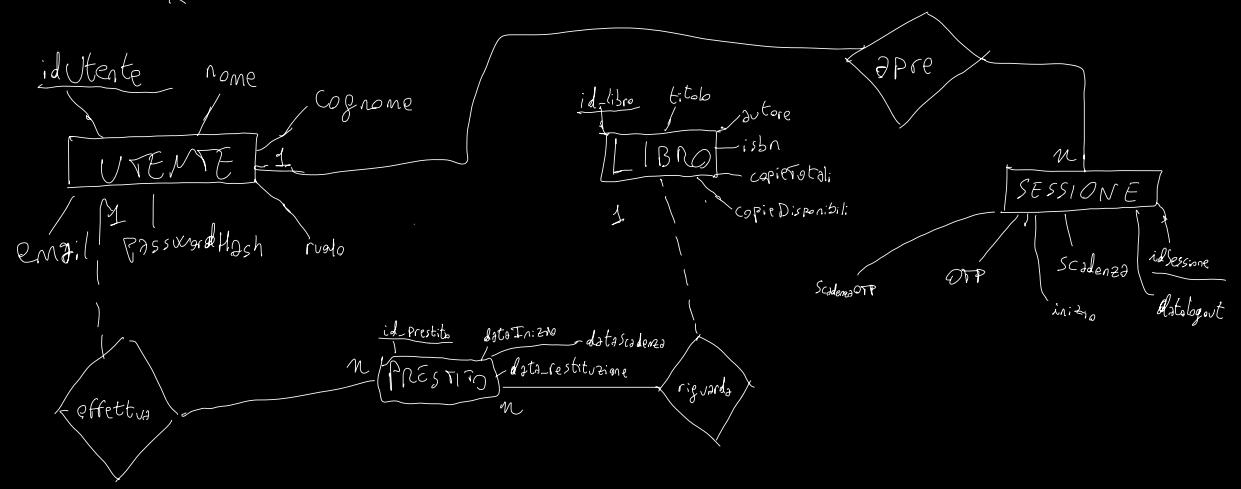
Customizzazioni
Sono state introdotte due customizzazioni principali, l'implementazione dell'autenticazione a due fattori (2FA) e l'introduzione di un limite massimo di prestiti attivi per ciascuno studente.

La prima customizzazione riguarda il rafforzamento del processo di autenticazione. Oltre alla verifica di email e password, il sistema implementa un meccanismo di autenticazione a due fattori basato sull'invio di un codice OTP (One Time Password) temporaneo tramite email. Dopo l'inserimento corretto delle credenziali, e nel caso dei bibliotecari anche dopo la verifica del codice fisso richiesto per l'accesso amministrativo, il sistema genera automaticamente un codice numerico casuale a validità limitata nel tempo. Tale codice viene salvato nel database all'interno della sessione attiva, insieme alla relativa scadenza, e inviato all'utente tramite email utilizzando il servizio SMTP configurato nel container Mailpit. L'utente deve quindi inserire correttamente l'OTP entro il tempo

stabilito per completare l'accesso. In questo modo si riduce il rischio di accessi non autorizzati anche in caso di compromissione delle credenziali principali.

La seconda customizzazione riguarda l'introduzione di una regola che limita il numero massimo di prestiti attivi per ciascuno studente. Il sistema verifica, prima di consentire un nuovo prestito, il numero di libri attualmente non restituiti dall'utente. Se il limite massimo configurato è stato raggiunto, l'operazione viene bloccata e il sistema informa lo studente dell'impossibilità di effettuare ulteriori prestiti fino alla restituzione di almeno un libro. Questa regola garantisce una distribuzione più equa del patrimonio librario per evitare che un singolo utente possa monopolizzare un numero eccessivo di copie.

SCHEMA ER



REGOLE DI LETTURA

UN UTENTE PUÒ EFFETTUARE n PRESTITI, UN PRESTITO DEVE ESSERE EFFETTUATO DA UN SOLO UTENTE.

UN PRESTITO DEVE RIGUARDARE UN SOLO LIBRO, UN LIBRO PUÒ ESSERE OGGETTO DI n PRESTITI

UN UTENTE DEVE APRIRE n SESSIONI NEL TEMPO, UNA SESSIONE APPARTIENE AD UN SOLO UTENTE.

SCHEMA RELAZIONALE

UTENTI (idUtente, nome, cognome, email, passwordHash, ruolo)

LIBRI (idLibro, titolo, autore, isbn, copieTotali, copieDisponibili)

PRESTITI (idPrestito, dataInizio, dataScadenza, dataRestituzione, idUtente, idLibro)

SESSIONI (idSessione, inizio, scadenza, dataLogout, OTP, scadenzaOTP, idUtente)

DIAGRAMMI DELLE CLASSI (UML)

SPECIFICHE DI SESSIONE E SICUREZZA

Tabella con dati salvati in $_SESSION al login

Variabile di sessione	tipo	Descrizione
$_SESSION['idUtente']	int	Identificativo dell'utente nel database
$_SESSION['nome']	String	Nome dell'utente
$_SESSION['cognome']	String	Cognome dell'utente
$_SESSION['email']	String	Email utilizzata per il login
$_SESSION['ruolo']	String	Ruolo dell'utente (studente o bibliotecario)
$_SESSION['login_time']	datetime	Timestamp del momento di login
$_SESSION['2fa_verificato']	boolean	Indica se l'autenticazione a due fattori è stata completata

Il sistema di gestione della biblioteca implementa un meccanismo di sicurezza progettato per garantire la separazione dei ruoli tra studenti e bibliotecari e per proteggere le funzionalità amministrative da accessi non autorizzati.
Il processo di autenticazione avviene in più fasi, l'utente inserisce email e password, che vengono verificate confrontando l'hash salvato nel database. Se le credenziali risultano corrette, si passa allo

step successivo; il sistema controlla il ruolo associato all'utente.
Nel caso in cui il ruolo sia "studente", il sistema procede direttamente alla fase di autenticazione a due fattori. Nel caso in cui il ruolo sia "bibliotecario", l'utente viene reindirizzato ad una pagina dedicata dove deve inserire un codice bibliotecario fisso. Questo codice è configurato nel sistema ed è obbligatorio per poter accedere alle funzionalità amministrative. Se il codice inserito non è corretto, l'autenticazione viene interrotta e l'accesso negato.

Dopo la verifica corretta del codice bibliotecario (quando richiesto), il sistema genera un codice OTP (One Time Password), lo salva nella tabella Sessione con una data di scadenza e lo invia via email tramite il servizio Mailpit configurato come container nel docker-compose. L'utente deve inserire l'OTP ricevuto per completare il processo di autenticazione.

Una volta verificato l'OTP, viene creata la sessione applicativa. Nella variabile globale $_SESSION vengono salvati i dati citati nella tabella sovrastante. Questi dati permettono al sistema di gestire autorizzazione e controllo accessi durante la navigazione.

Ogni pagina riservata ai bibliotecari (come ad esempio la dashboard amministrativa) effettua controlli obbligatori prima di essere caricata. Il sistema verifica che esista una sessione attiva, che l'autenticazione a due fattori sia stata completata, cheil ruolo dell'utente sia "bibliotecario" e che il codice bibliotecario sia stato correttamente validato.

Se una di queste condizioni non è soddisfatta, l'utente viene automaticamente reindirizzato alla pagina di login o alla dashboard studente. In questo modo uno studente autenticato non può in alcun modo accedere alle funzionalità amministrative, e nemmeno un bibliotecario può accedervi senza aver inserito il codice aggiuntivo.