TRACCIA: BIBLIOTECH

ANALISI DEL SISTEMA

Il progetto prevede la realizzazione di un'applicazione web denominata **BiblioTech**, destinata alla gestione digitale dei prestiti librari di una biblioteca scolastica.
Il sistema sostituisce il registro cartaceo introducendo un archivio centralizzato capace di mantenere aggiornato in tempo reale lo stato della biblioteca. L'applicazione deve conoscere in ogni momento quali libri sono presenti, quante copie risultano disponibili e quale utente possiede una determinata copia.
Ogni operazione modifica lo stato del sistema e deve quindi preservare la consistenza dei dati.

Accesso e autenticazione

L'utilizzo del sistema è consentito solo previa autenticazione.
Un utente può utilizzare un account già esistente oppure registrarsi creando un nuovo account studente. Dopo l'inserimento di username e password il sistema non concede immediatamente l'accesso ma richiede una verifica aggiuntiva tramite codice temporaneo OTP. Il codice viene generato dal server, associato all'utente e inviato all'indirizzo email registrato. Solo dopo l'inserimento corretto del codice viene creata la sessione definitiva. Fino alla conferma del codice l'utente è considerato in stato di autenticazione parziale e non può accedere alle pagine protette.
Il codice ha durata limitata e viene invalidato dopo l'utilizzo o allo scadere del tempo. Questo meccanismo richiede contemporaneamente la conoscenza delle credenziali e la disponibilità dell'email associata all'account.

Gestione della sessione

Poiché il protocollo HTTP è privo di mmoria, il sistema utilizza le sessioni per mantenere lo stato dell'utente tra le richieste. Dopo la verifica OTP vengono salvate nella sessione le informazioni necessarie al riconoscimento dell'utente, tra cui identificativo, nome utente e ruolo. Ogni pagina controlla tali dati prima di eseguire qualsiasi operazione. In assenza di sessione valida l'utente viene reindirizzato alla pagina di login.
Alla disconnessione tutte le informazioni vengono eliminate e l'utente torna non autenticato.

Ruoli e permessi

Il comportamento dell'applicazione varia in base al ruolo associato all'utente autenticato. Sono previsti due ruoli: studente e bibliotecario. Lo studente può consultare il catalogo e richiedere un prestito se è disponibile almeno una copia del libro.
Il bibliotecario può visualizzare tutti i prestiti attivi e registrare la restituzione dei libri. La separazione dei permessi è gestita lato server tramite controllo del ruolo memorizzato nella sessione. Un utente non autorizzato non può accedere alle funzionalità amministrative anche conoscendo manualmente l'indirizzo della pagina.

Gestione dei prestiti

Il prestito rappresenta un collegamento temporale tra un utente e un libro.

Quando uno studente richiede un libro il sistema verifica la disponibilità delle copie.
Se esiste almeno una copia disponibile viene creato un nuovo prestito e il numero di copie disponibili diminuisce. In caso contrario l'operazione viene bloccata. La restituzione viene registrata dal bibliotecario inserendo la data di fine del prestito e incrementando il numero di copie disponibili. Un prestito privo di data di fine rappresenta un libro ancora fuori biblioteca.

Coerenza dei dati

Il sistema deve impedire situazioni incoerenti come copie disponibili negative, restituzioni duplicate o accessi non autorizzati. Le operazioni di prestito e restituzione modificano contemporaneamente lo stato del libro e lo storico dei movimenti. Le due modifiche vengono trattate come un'unica operazione logica per garantire la sincronizzazione dei dati.

Dati gestiti dal sistema

Il funzionamento dell'applicazione si basa su quattro gruppi di informazioni: utenti registrati, libri disponibili, prestiti effettuati e codici temporanei di autenticazione.
I prestiti collegano utenti e libri nel tempo, mentre i codici OTP permettono la creazione sicura della sessione.

Obiettivo dell’analisi

Questa fase definisce il comportamento logico del sistema prima della progettazione del database. Vengono individuate le operazioni possibili, i vincoli che devono rimanere sempre validi e le informazioni necessarie al corretto funzionamento dell’applicazione.

SPECIFICHE DI SESSIONE E SICUREZZA

Dati salvati nella sessione

Durante il processo di autenticazione il sistema utilizza la variabile globale `$_SESSION` per mantenere lo stato dell’utente tra le diverse richieste HTTP. In una prima fase, dopo l’inserimento corretto di username e password ma prima della verifica OTP, viene salvato solo l’identificativo temporaneo dell’utente che sta completando l’accesso.
L’utente non è ancora considerato autenticato e non può accedere alle pagine protette.

Dopo l’inserimento corretto del codice OTP viene creata la sessione definitiva e vengono memorizzati i dati necessari al funzionamento dell’applicazione.

Protezione delle pagine amministrative

Le pagine riservate al bibliotecario eseguono un ulteriore controllo sul ruolo memorizzato nella sessione. Il server verifica che il valore di `ruolo` sia uguale a *bibliotecario*.
Se la condizione non è soddisfatta l’accesso viene negato e l’utente viene riportato alla pagina principale. Questo controllo avviene lato server e impedisce ad uno studente di accedere manualmente alle pagine amministrative digitando direttamente l’indirizzo nel browser. In questo modo i permessi non dipendono dall’interfaccia grafica ma esclusivamente dai dati di sessione verificati dal server.