Progetto Tecnologie Web

Lorenzo Quellerba, MAT. 899537

Tema del sito:

Il sito si chiama BookLoversItalia, è il sito di una community fittizia di amanti del libro.
L'obiettivo del sito è permettere ai propri utenti di condividere le loro nuove letture e dare un'idea agli altri utenti su cosa aspettarsi dalla letture del libro in questione.
Oltre al meccanismo di recensione di un libro, c'è una parte di esplorazione del contenuto attraverso il bottone "un libro a caso".

Sezioni:

Home

L'utente che arriva nella homepage del sito si trova davanti una serie di "card" riassuntive dei libri letti di recente dagli utenti della piattaforma.
Cliccando su una di esse si apre in dettaglio la pagina del libro selezionato dove vengono mostrate anche le recensioni.

Pagina del libro

È la pagina che si apre in seguito al click di una card nella homepage.
Contiene la scheda del libro più tutte le recensioni fatte dagli utenti.
Per ogni recensione è possibile segnalarla oppure aggiungere un upvote o un downvote a seconda che l'utente concordi o meno con l'opinione espressa.

Ricerca

Cliccando sulla casella di ricerca l'utente può cercare o parte di un nome di un autore o parte di un titolo di un libro e i risultati presenti all'interno del sito verranno mostrati a schermo per permettere la consultazione dei contenuti.

Aggiungi un libro

Partendo dalla home, cliccando sul bottone "Aggiungi un libro" nella navbar si apre a schermo un form che permette all'utente di aggiungere tutti i dettagli del libro che ha letto insieme (obbligatoriamente) alla sua recensione.
Non possono essere presenti all'interno del sito libri senza avere associata anche una recensione.

Aggiungi una recensione

Quando l'utente partendo dall'interno della pagina di un libro, cliccando il bottone "Aggiungi una recensione" presente nella navbar, si trova davanti un form dove può inserire la sua recensione.

Profilo utente

Cliccando sul bottone "Profilo utente" della navbar, l'utente si trova davanti una pagina dove vengono mostrate due card, una cliccabile che mostra tutti i libri recensiti dall'utente e l'altra che mostra semplicemente il numero totale di upvote che l'utente ha ricevuto con le sue recensioni.
Oltre a queste statistiche sono presenti due bottoni, uno per la modifica della password e uno per l'eliminazione del profilo.

Pagina dell'admin

Se l'utente che si autentica è l'amministratore del sito, la pagina a cui arriva è una collezione di statistiche sul sito.

Oltre ai dati di utilizzo, si trova davanti due card cliccabili, una che mostra le schede riassuntive dei libri che sono state segnalate e una che mostra le recensioni degli utenti che sono state segnalate.
Per ogni recensione segnalata l'amministratore può scegliere se "approvarla" o se eliminarla.
Per ogni libro invece all'amministratore è offerta la possibilità di modificare i dati ritenuti non appropriati o errati.

Dettagli tecnici

Organizzazione
Il codice è diviso in cartelle, una per ogni parte del sito (backend con la cartella php, pagine html con la cartella html, file javascript con la cartella js eccetera).
Tutto il codice segue lo stile unobtrusive.

Comunicazione frontend-backend
La comunicazione tra frontend e backend avviene attraverso i metodi GET e POST di HTTP.
Il backend è sviluppato secondo l'approccio "web-service" e risponde con dei messaggi che usano il formato

```
{
      "codiceRispostaHTTP": numero,
      "message": messaggio
}
```

Sicurezza
Tutto l'input dell'utente viene validato sia lato client che lato server.
In tutte le pagine viene controllato che l'utente abbia effettivamente accesso.
Il sito si protegge dagli attacchi XSS facendo ricorso alla funzione `htmlspecialchars()` di PHP e dall'attacco di SQL Injection attraverso la funzione `prepare()` che viene chiamata su tutte le query in cui vengono inserite variabili provenienti dall'utente.

Nel seguito, i dettagli tecnici di ogni pagina

Registrazione
Per registrarsi è necessario compilare un form con 3 campi, nome utente, password e conferma della password. Il form dopo essere stato validato lato client, viene mandato al server con metodo `POST` a `/php/user/register.php`.
Dopo una parte di validazione, viene calcolato l'hash della password e inserito nel database. A questo punto il client viene ridiretto verso la pagina `/html/home.php`.

Login
Per fare login l'utente deve inserire nome utente e password.
I dati vengono mandati al serve attraverso il metodo `POST` a `/php/user/login.php`.
Dopo aver controllato che l'utente sia presente all'interno del database, avviene un redirect verso la pagina `/html/home.php`.
Le informazioni quali username e il fatto che l'utente sia amministratore o meno vengono salvati nell'array `$_SESSION` in corrispondenza delle chiavi `"USERNAME"` e `"ADMIN"`.
L'accesso viene mantenuto attraverso un cookie che contiene il session_id generato al momento del login o della registrazione.

Home
Tutti i dati presenti nella home vengono caricati attraverso una richiesta `GET` a `/php/feed/get.php`, successivamente il DOM viene aggiornato con JQuery mostrando i dati ricevuti dal server.
Tutte le card dei libri hanno associate un evento “click" tale per cui, appena vengono cliccate, parte una richiesta `GET` a `/php/book-page/get.php` che avrà come parametro l’isbn del libro richiesto.

Ricerca
In alto alla pagina è presente una casella di ricerca (la casella di ricerca cambia aspetto in base alla dimensione dello schermo, se il sito è in modalità “mobile”, la casella viene nascosta dietro la pressione di un bottone di ricerca).
Appena l’utente preme il bottone “Cerca”, avviene una richiesta `GET` a `/php/search/get.php`. I risultati della ricerca vengono mostrati a schermo aggiornando il DOM con JQuery.

Nuovo libro
Quando l’utente clicca il bottone per aggiungere un nuovo libro, il contenuto della pagina viene rimosso dal DOM usando JQuery e compare un form con una serie di campi che l’utente deve compilare.
Appena l’utente preme il tasto conferma, avviene una richiesta con metodo `POST` a `/php/feed/insert.php`.

Nuova recensione
Similmente a “Nuovo libro”, se l’utente clicca sul bottone “nuova recensione”, le recensioni presenti nella pagina vengono rimosse usando JQuery e al loro posto compare un form. Alla compilazione del form avviene una richiesta `POST` a `/php/feed/insert.php`.

Pagina del libro
Per arrivare alla pagina di un libro con le relative recensioni è necessario fare una richiesta `GET` alla pagina `/php/book-page/get.php` specificando come parametro l’ISBN del libro richiesto.
All'arrivo dei dati, tutta la pagina viene aggiornata modificando il DOM come fatto per tutte le altre pagine.
Ogni recensione ha due bottoni, rispettivamente il bottone di upvote e il bottone di downvote. Alla pressione di uno dei due bottoni avviene una richiesta `POST` a `/php/utils/add_upvote.php` o `/php/utils/add_downvote.php` a seconda che si tratti di uno o dell’altro.
Prima che avvenga l’inserimento si controlla che l’utente non abbia già effettuato la valutazione.

Un libro a caso
La pagina “un libro a caso” in realtà non è una vera a propria pagina. Alla pressione del bottone avviene una richiesta `GET` a `/php/book-page/rand_isbn.php`. La richiesta restituisce un ISBN a caso tra quelli presenti nella tabella Book del database. A quel punto, avendo un isbn, avviene una richiesta `GET` come specificato nella sezione “Pagina del libro”.
Come per tutte le altre pagine, il contenuto viene aggiornato modificando il DOM con JQuery.

Profilo utente
Quando si arriva alla pagina del profilo utente, il contenuto dinamico (le statistiche) vengono caricate e mostrate all'arrivo dei dati dalla richiesta `GET` fatta a `/php/user/user_data.php`.
In modo analogo a quanto fatto per tutto il resto del sito, alla click della card dei libri recensiti, il contenuto della pagina viene aggiornato mostrando il risultato della richiesta `GET` a `/php/user/get_all_reviews.php`.

Segnalazione
Sia le schede libro che le recensioni hanno un tasto per la segnalazione (le schede libro hanno un link cliccabile subito sotto la scheda, le recensioni invece un bottone).
Il click del bottone comporta l'invio di una richiesta `POST` a `/php/book-page/book_summary_report.php`.

Logout
Appena l'utente preme il bottone di logout avviene una richiesta `POST` a `/php/user/logout.php` che comporta la distruzione della sessione e l'eliminazione del cookie.

Admin page
Alla pagina dell'admin si accede inserendo le credenziali admin - admin (nome utente e password) nel form di login.
A login effettuato avviene un redirect verso la pagina `/html/admin-home.php`.
Le statistiche della pagina vengono popolate attraverso una richiesta `GET` a `/php/admin/get-stats.php`.
Quando l'amministratore clicca sulle card che mostrano i libri e le recensioni segnalate avvengono delle richieste `GET` rispettivamente a `/php/admin/get_rep_books.php` e `/php/admin/get_rep_reviews.php`.

API Routes

`GET /php/admin/get_rep_book_card.php?isbn=isbn`	`response:`
	`{“statuscode”:200,`
	` “message”: {`
	`title: titolo,`
	`isbn: isbn,`
	`author: autore,`
	`genre: genere,`
	`descritpion: descrizione,`
	`year: anno}`
	`}`

`GET /php/admin/get_rep_books.php`	`response:`
	`{“statuscode”:200,`
	` “message”: {`
	`title: titolo,`
	`isbn: isbn,`
	`}`
	`}`

`GET /php/admin/get_rep_review_content.php?isbn=isbn&author=author`	`response:`
	`{“statuscode”:200,`
	` “message”: {`
	`content: content,`
	`}`
	`}`

GET /php/admin/
get_rep_review_content.php
	response:
	{“statuscode”:200,
	“message”: {
	title: content,
	author: author,
	isbn: isbn,
	}
	}

GET /php/admin/get-stats.php	response:
	{“statuscode”:200,
	“message”: {
	booksNumber: number,
	reviewNumber: number,
	upvoteTotal: number,
	userTotal: number,
	reportedBookTotal: number,
	reportedReviewTotal: number,
	username: username,
	}
	}

POST /php/admin/review-report-del.php	response: {“statuscode”:200, “message”: “Success" }
POST /php/admin/review-report-save.php	response: {“statuscode”:200, “message”: “Recensione approvata” }
POST /php/admin/update_book_card.php	response: {“statuscode”:200, “message”: “Form salvato con successo” }
POST /php/book-page/ book_summary_report.php	response: {“statuscode”:200, “message”: “Segnalazione ricevuta con successo. Grazie!” }

GET /php/book-page/get.php?isbn=isbn	response:
	{“statuscode”:200,
	“message”: {
	“bookdata”: data,
	“reviewdata": data}
	}

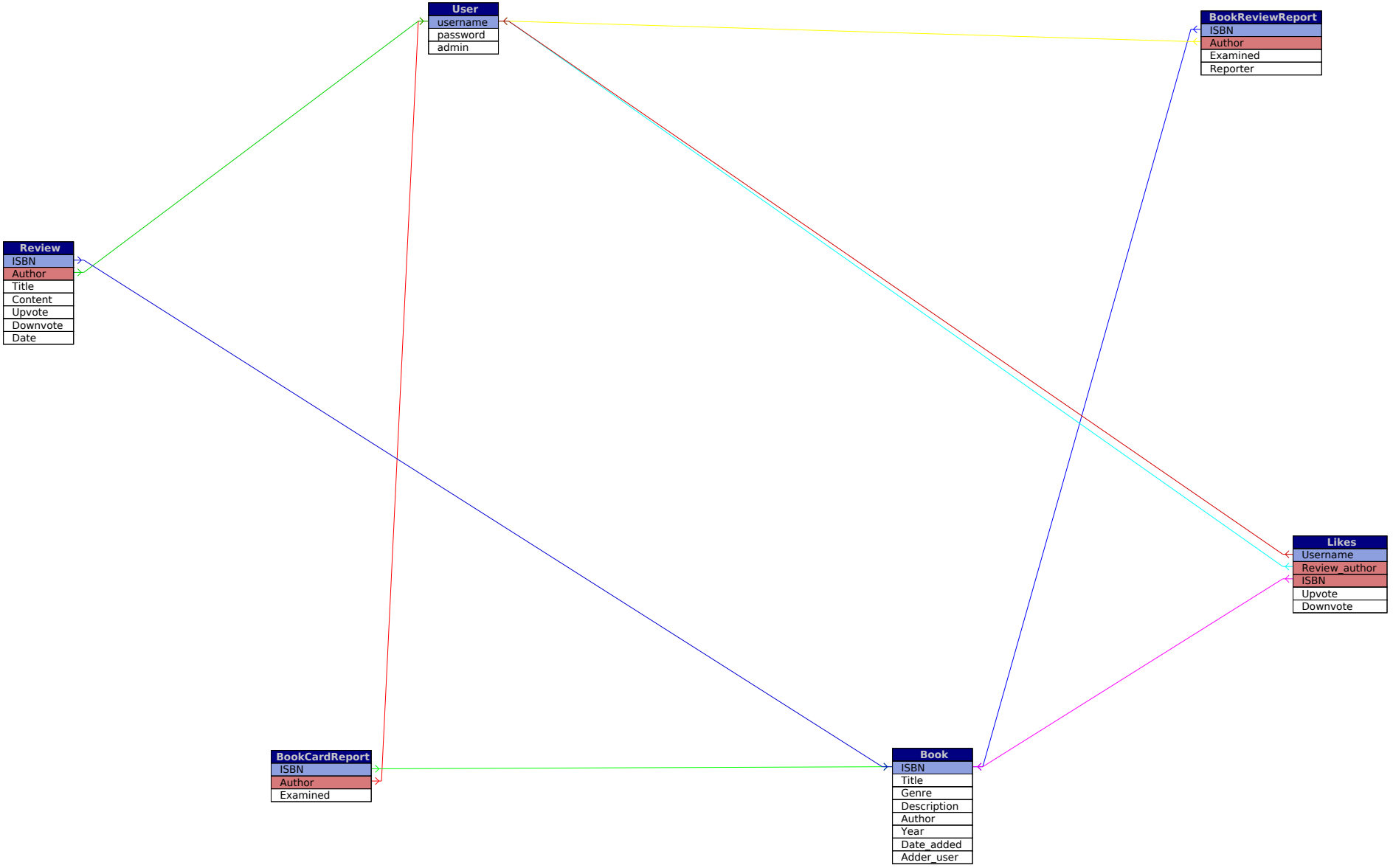
GET /php/book-page/rand_isbn.php	response:
	{“statuscode”:200,
	“message”: {
	isbn: "isbn"}
	}

GET /php/feed/get.php	response:
	{“statuscode”:200,
	“message”: {
	ISBN: number,
	Author: string,
	Title: string,
	Genre: string,
	Date: number,
	. . .},
	{
	ISBN: number,
	Author: string,
	Title: string,
	Genre: string,
	Date: number,
	. . .}
	}

GET /php/search/get.php?
keyword=keyword
	response:
	{“statuscode”:200,
	“message”: {
	ISBN: number,
	Author: string,
	Title: string,
	Genre: string,
	Date: number,
	. . .
	}
	}

GET /php/user/user_data.php	response:
	{“statuscode”:200,
	“message”: {
	username: value,
	numbooks: value,
	upvotes: value
	}
	}

POST /php/user/login.php	response: {“statuscode”:200, “message”: “home.php”}


User
username
password
admin
BookReviewReport
ISBN
Author
Examined
Reporter
Review
ISBN
Author
Title
Content
Upvote
Downvote
Date
Likes
Username
Review_author
ISBN
Upvote
Downvote
BookCardReport
ISBN
Author
Examined
Book
ISBN
Title
Genre
Description
Author
Year
Date_added
Adder_user