Progetto di Tecnologie Web

Alberto Marino, matricola 948258 – A.A. 2022/2023

Tema del sito

Il sito sviluppato, chiamato getBook(), è una piattaforma di e-commerce dedicata alla vendita di libri online. Questa piattaforma offre agli utenti la possibilità di simulare ed effettuare l'acquisto di libri, scrivere recensioni e inviare feedback all'azienda.

Le sezioni principali

- Pagina di **registrazione**: utile per la registrazione al sito
- Pagina di **login**: utile per l'accesso al sito
- Sezione "**Home**": presenta la pagina iniziale del sito
- Sezione "**Books**": presenta tutti i libri che sono in vendita sul sito
- Sezione "**Reviews**": presenta le recensioni che gli utenti hanno rilasciato
- Sezione "**About us**": presenta una piccola descrizione dell'azienda fittizia getBook()
- Sezione "**Contact us**": presenta una sezione attraverso la quale è possibile contattare l'azienda fittizia getBook()
- Sezione "**Basket**": presenta il carrello dell'utente
- Sezione "**Logout**": presenta il modulo di disconnessione dal sito

Funzionalità

- **Login/Logout**: è possibile arrivare a questa sezione del sito dalla pagina principale di accesso ("index.php"). Effettuando un click sull'apposito bottone, l'utente verrà rimandato all'apposita pagina ("login.php") contenente un form di accesso che richiede le seguenti informazioni: username e password. Nel caso in cui l'utente che tenta di accedere non abbia già effettuato la registrazione alla piattaforma oppure abbia inserito una password errata, viene riportato un messaggio di errore. Il comportamento della pagina di accesso è interamente gestito dall'apposita porzione di codice presente all'interno del file JavaScript denominato "functions.js". La pagina "login.php" effettua un controllo dei campi lato server e verifica la presenza dell'utente tramite la funzione "user_login" richiamata dal file "functions.php" e implementata nel file "functions_implementation.php". Se l'accesso va a buon fine, si viene rimandati alla pagina principale del sito, ovvero "home.php". Per quanto riguarda il logout, nella navbar presente nella home del sito, è presente un bottone che effettua la disconnessione dalla piattaforma eliminando le variabili di sessione e distruggendo completamente la sessione corrente.
- **Registrazione**: è possibile arrivare a questa sezione del sito dalla pagina principale di accesso ("index.php"). Effettuando un click sull'apposito bottone, l'utente verrà rimandato all'apposita pagina ("subscribe.php") contenente un form di registrazione che richiede le seguenti informazioni: nome, cognome, username, email e password. Nel caso in cui sia già presente sulla piattaforma un utente con l'username inserito viene riportato un messaggio di errore. Il comportamento della pagina di registrazione è interamente gestito dall'apposita porzione di codice presente all'interno del file JavaScript denominato "functions.js". La pagina "subscribe.php" effettua un controllo dei campi lato server ed effettua la query di inserimento tramite la funzione "user_subscribe" richiamata dal file "functions.php" e implementata nel

file "functions_implementation.php". Se la registrazione va a buon fine, si viene rimandati alla pagina principale del sito, ovvero "home.php".

- **Ruoli e gestione del contenuto generato dall'utente**: i ruoli considerati sono due, ovvero:
  - **admin**: vi è solo un utente con questo ruolo. Egli ha accesso a tutte le funzionalità del sito, comprese quelle alle quali "l'utente semplice" non può accedere, ovvero:
    - aggiunta di un prodotto alla piattaforma tramite un apposito form presente nella pagina "insert_book". Ogni campo del form è controllato da appositi pattern e viene richiesto l'inserimento di: titolo del libro, autore, prezzo, editore e trama. Al fondo della pagina sono presenti un bottone e un avviso che compare per notificare la buona o cattiva riuscita dell'azione di inserimento;
    - rimozione di un prodotto dalla piattaforma tramite un apposito form presente nella pagina "remove_book" sottoforma di menù a tendina. Anche qui, al fondo della pagina sono presenti un bottone e un avviso che compare per notificare la buona o cattiva riuscita dell'azione di rimozione;
    - rimozione di una recensione dalla piattaforma anch'esso tramite un apposito form presente nella pagina "remove_review" sottoforma di menù a tendina. Anche qui, al fondo della pagina sono presenti un bottone e un avviso che compare per notificare la buona o cattiva riuscita dell'azione di rimozione.
  - **user**: tutti i nuovi utenti nascono con tale ruolo. In fase di registrazione, un utente può iscriversi solo come user. Le restanti azioni che l'utente normale (e quindi anche l'utente admin) può effettuare sono:
    - visualizzazione dell' intera descrizione dei prodotti in vendita, ovvero titolo del libro, autore/i, prezzo, editore e trama. Queste informazioni sono accessibili dalla pagina "view_book" tramite un click su un apposito bottone presente nella sezione "Books" della piattaforma. Nel caso in cui non ci siano prodotti in vendita, viene visualizzato un apposito messaggio;
    - aggiungere uno o più prodotti al carrello tramite un click sul bottone "Add to basket" presente nella card di ogni prodotto. Al carrello è possibile accedere tramite un click sul bottone "Basket" presente nella navbar. In questa sezione l'utente può visualizzare i prodotti presenti nel carrello, aumentarne la quantità, visualizzare il prezzo totale dell'ordine e completare l'ordine (semplice simulazione di un vero check-out in cui il carrello dell'utente loggato viene svuotato e appare un'animazione di completamento dell'ordine). Nel caso in cui non ci siano prodotti nel carrello, viene visualizzato un apposito messaggio;
    - rimuovere uno o più prodotti dal carrello tramite un click sul bottone "Remove books from your cart" all'inizio dell'apposita pagina. La rimozione è gestita dalla pagina "remove_book" ed è effettuabile selezionando un titolo in un menù a tendina e confermando tramite il click di un bottone "Remove book". Nel caso in cui il/i prodotto/i sia/siano stato/i rimosso/i correttamente o meno, viene visualizzato un apposito messaggio;
    - aggiungere una recensione su un determinato prodotto tramite un click sul bottone "Add a new review" presente nella sezione "Reviews" della piattaforma. È possibile aggiungere una recensione completando un apposito form presente nella pagina "insert_review". Ogni campo del form è controllato da appositi pattern. Viene inoltre richiesta la scelta del titolo del libro che si

vuole recensire tramite un menù a tendina e l'inserimento del testo della recensione in una textbox. Al fondo della pagina sono presenti un bottone e un avviso che verifica la buona o meno riuscita dell'azione di inserimento;
- simulare l'invio di un messaggio di feedback riempiendo un apposito form presente nella pagina "contact_us". È possibile simulare l'invio di un messaggio completando un apposito form che viene svuotato al click del bottone "Send message".

La gestione di tale suddivisione di ruoli all'interno del database è stata definita tramite una colonna nella tabella "user" chiamata "role".

Caratteristiche

- **Usabilità**: questa caratteristica è stata rispettata prestando attenzione ai particolari punti:
  - In tutti i form in cui è richiesto l'inserimento del testo (es. nome, cognome, ecc. in fase di registrazione), finché l'input non rispetta il preciso pattern (visualizzabile all'utente passando sul campo con il mouse), il campo viene colorato di colore rosso. Nel momento in cui il pattern viene rispettato, invece, il campo viene colorato di verde;
  - Quando un utente accede o si registra alla piattaforma, viene stampato un saluto nella barra di navigazione con il seguente formato: "Hi, *username*!" (es. Hi, Mario!);
  - Tutti i messaggi, eccetto quelli presenti nella pagina di registrazione e di login (es. avviso del corretto caricamento di un prodotto nel database da parte dell'admin) scompaiono gradualmente dopo 1.5 secondi;
  - La piattaforma presenta un font semplice e chiaro (Poppins) e un buon contrasto di colori in modo da rendere semplice ed efficace la leggibilità della pagina. I colori utilizzati sono stati principalmente: #001489 (blu scuro) e #B4D7E7 (azzurro). Inoltre, al passaggio del mouse su ogni bottone e su ogni elemento della navbar, vengono modificati alcuni colori degli elementi stessi.
- **Interazione/animazione**: le animazioni sviluppate sono le seguenti:
  - **Animazione per l'aggiunta di un prodotto al carrello**: la funzione "add_to_basket" utilizza l'animazione per fornire un feedback visivo all'utente durante l'aggiunta di un prodotto al carrello. L'animazione è gestita tramite la funzione "animate()". Quando l'utente aggiunge un prodotto, viene eseguita una richiesta Ajax per inviare i dati al server. In base alla risposta del server, viene mostrato un messaggio appropriato. Se l'aggiunta del prodotto ha successo, l'elemento ".add_to_basket" viene animato con una dissolvenza graduale e viene cambiato il suo contenuto. Se l'aggiunta non ha successo, viene utilizzato un messaggio diverso. In entrambi i casi, l'animazione indica all'utente che il prodotto è stato aggiunto o era già presente nel carrello;
  - **Animazione per il completamento dell'ordine**: anche qui l'animazione utilizza la funzione "animate()". Al click del bottone "Click here to complete your order", gli vengono aggiunte la classe CSS "animate_button" e viene avviata l'animazione. Durante l'animazione, l'opacità del bottone diminuisce gradualmente a 0 tramite "animate({opacity: 0}, 500)". Una volta completata questa dissolvenza, il contenuto del bottone viene cambiato. Infine, viene eseguita un'animazione per far riapparire gradualmente il bottone, aumentando l'opacità a 1 con "animate({opacity: 1}, 500)";
  - **Animazione per il feedback utente**: anche qui l'animazione utilizza la funzione "animate()". Al click del bottone "Send message", viene aggiunta una classe CSS "animate_button" e il suo contenuto viene modificato per mostrare un messaggio di ringraziamento. Dopo un breve ritardo, i campi del modulo vengono resettati e il

pulsante viene nascosto gradualmente tramite un'animazione di dissolvenza. Successivamente, il testo del pulsante viene ripristinato e viene eseguita un'animazione per farlo riapparire gradualmente. Dopo un altro ritardo, la classe "animate_button" viene rimossa per terminare l'animazione.

- **Sessioni**: le sessioni vengono create ed inizializzate in fase di registrazione/login dell'utente. Al momento del logout vengono rimosse tutte le variabili di sessione e viene interamente distrutta la sessione. In fase di registrazione e login è stata inoltre utilizzata $_SESSION["advise"] per mostrare i messaggi che indicano il motivo della fallimento della registrazione o dell'accesso alla piattaforma.
- **Interrogazione del database**: le interrogazioni del database sono presenti all'interno delle funzioni richiamate nel file "functions.php" (che contiene inoltre la funzione per la connessione al database) e implementate in "functions_implementation.php".
- **Validazione dati input**: i dati vengono sempre validati sia lato client, attraverso l'utilizzo di espressioni regolari, input type e tramite la clausola "required", e sia lato server con i controlli di sanitizzazione, funzione di hash "md5()" per crittografare la password e "quote()" per l'inserimento dei dati nel database.
- **Sicurezza**: tutte le richieste al server vengono gestite utilizzando il metodo "POST" per garantire la sicurezza delle informazioni trasmesse. Per prevenire attacchi di XSS e SQL Injection, vengono adottate le funzioni "quote()" e "filter_input()".
- **Presentazione**: la piattaforma è progettata come una singola pagina che offre accesso alle diverse sezioni attraverso una navbar che rimane costantemente visibile in cima alla pagina. Il design del sito è basato su un layout flessibile che si adatta in modo responsive alla presentazione su diversi dispositivi. Inoltre, ogni sezione è dotata di un footer che contiene una serie di link posizionati nella parte inferiore della pagina.

Front-end

- **Separazione presentazione/contenuto/comportamento**:
  - **Presentazione**: è unobstrusive. Lo stile è stato gestito attraverso 3 file css: "index.css" per lo stile della pagina iniziale, "access.css" per lo stile delle pagine di registrazione e login, "styles.css" per lo stile del resto della pagine.
  - **Contenuto**: è presente in tutti i files HTML ("about_us.html", "contact_us.html", "footer.html", "home.html", "insert_book.html", "insert_review.html", "top.html") e in alcuni files PHP ("basket.php", "books.php", "home.php", "index.php", "insert_book.php", "insert_review.php", "login.php", "navbar.php", "remove_book", "remove_book_from_basket.php", "remove_review.php", "reviews.php", "subscribe.php", "view_book.php") per agevolare la gestione delle sessioni.
  - **Comportamento**: è gestito da un unico file JavaScript "functions.js".
- **Soluzioni cross-platform**: la maggior parte delle misure definite nei fogli di stile sono in percentuale in modo da garantire, come accennato in precedenza, un layout flessibile che si adatta in modo responsive alla presentazione su diversi dispositivi. Nei fogli di stile sono inoltre state utilizzate le regole @media, che consentono di applicare stili specifici a diverse dimensioni dello schermo o a diversi dispositivi.
- **Organizzazione file e cartelle di progetto**: la cartella di progetto è così composta:
  - **Cartella "css"**: contiene tutti i fogli di stile CSS;
  - **Cartella "database"**: contiene il database utilizzato;
  - **Cartella "html"**: contiene i file HTML;
  - **Cartella "img"**: contiene alcune immagini utilizzate per abbellire il sito (es. logo);

  - **Cartella "imgBooks"**: contiene le immagini delle copertine dei libri che si intende vendere;
  - **Cartella "javascript"**: contiene i file JavaScript;
  - **Cartella "php"**: contiene i file PHP.
- **Soluzioni HTML/CSS/JavaScript degne di nota**: cambio di colore di tutti i bottoni al passaggio del mouse; creazione di una checkbox che permette di mostrare/nascondere la password in fase di registrazione/login; apparsa e scomparsa graduale di alcuni messaggi come gli avvisi del corretto caricamento del prodotto e della recensione nel database, della corretta rimozione di un prodotto o di una recensione dal database.

Back-end e comunicazione front/back-end

- **Architettura generale classi/funzioni PHP**: l'architettura generale prevede sempre una verifica per determinare se la sessione è presente o meno. Le pagine PHP che includono codice HTML contengono sempre top e footer, oltre a sviluppare il codice per una specifica sezione HTML. Spesso, queste pagine includono anche altri file HTML necessari per il completo caricamento della sezione desiderata. Quando è necessario accedere a variabili di sessione specifiche e/o limitare l'accesso solo agli utenti con privilegi di amministratore, vengono effettuati controlli appositi. Per quanto riguarda il file PHP che implementa le funzioni (chiamato "functions_implementation.php"), l'architettura generale verifica se sono state definite alcune variabili di sessione specifiche, stabilisce una connessione al database, effettua controlli sui dati per garantire la sicurezza ed esegue le query necessarie.
- **Schema del database**:
  cart (<u>title, username</u>)
  - PRIMARY KEY: (title, username)
  - FOREIGN KEY: username fa riferimento alla tabella "users" (username)

  products (<u>title</u>, author, price, publisher, plot, image)
  - PRIMARY KEY: (title)

  review (<u>username, title</u>, text)
  - PRIMARY KEY: (username, title)
  - FOREIGN KEY: username fa riferimento alla tabella "users" (username)
  - FOREIGN KEY: title fa riferimento alla tabella "products" (title)

  username (<u>username</u>, name, surname, email, password, role)
  - PRIMARY KEY: (username)
- **Descrizione delle funzioni remote**: la comunicazione tra il client e il server si basa sull'utilizzo delle chiamate AJAX di JavaScript, che impiegano esclusivamente il metodo POST. Ogni richiesta viene inoltrata al server per essere elaborata e ottenere una risposta. Nel caso si verifichino errori, verrà eseguita la funzione "ajaxFailed()", la quale mostrerà nella console la risposta e lo stato restituiti dal server. Le funzioni implementate sono, come detto in precedenza, richiamate nel file "functions.php" ed implementate nel file "functions_implementation.php". Esse sono:
  - **user_subscribe()**: funzione che permette ad un utente di registrarsi alla piattaforma verificando che siano presenti le variabili di sessione di nome, cognome, username, email e password. Se l'inserimento va a buon fine viene stampato il valore "1" e si viene reindirizzati alla home, altrimenti stampa il valore "0" e si viene reindirizzati nuovamente alla pagina di registrazione;
  - **user_login()**: funzione che permette ad un utente di accedere alla piattaforma verificando che siano presenti le variabili di sessione di nome, cognome, username, email e password. Se l'inserimento va a buon fine viene stampato il valore "1" e si

viene reindirizzati alla home, altrimenti stampa il valore "0" e si viene reindirizzati nuovamente alla pagina di login;

- **show_uploaded_book()**: funzione che mostra i prodotti in vendita sulla piattaforma verificando che sia presente la variabile di sessione dell'username;
- **upload_book()**: funzione che inserisce un nuovo prodotto in vendita sulla piattaforma verificando che siano presenti le variabili di sessione di username, ruolo (che deve corrispondere ad "admin"), titolo, autore, prezzo, editore e trama. Se l'inserimento va a buon fine viene stampato il valore "1", altrimenti il valore "0";
- **show_select_titles()**: funzione che seleziona i titoli dei prodotti in vendita che sono disponibili per la rimozione da parte dell'admin e i titoli dei prodotti che possono essere recensiti dagli utenti. Viene effettuata inoltre una verifica sull'esistenza della variabile di sessione dell'username;
- **remove_book()**: funzione che rimuove un prodotto dalla piattaforma verificando che siano presenti le variabili di sessione di username e ruolo (che deve corrispondere ad "admin"). Se la rimozione va a buon fine viene stampato il valore "1", altrimenti il valore "0";
- **show_description_book()**: funzione che mostra la descrizione dei prodotti presenti sulla piattaforma verificando che sia presente la variabile di sessione dell'username;
- **show_basket()**: funzione che mostra i prodotti presenti nel carrello verificando che sia presente la variabile di sessione dell'username;
- **upload_to_basket()**: funzione che inserisce un nuovo prodotto nel carrello verificando che sia presente la variabile di sessione dell'username. Se l'inserimento va a buon fine viene stampato il valore "1", altrimenti il valore "0";
- **show_removed_book_from_basket()**: funzione che seleziona i titoli dei prodotti nel carrello che sono disponibili per la rimozione verificando che sia presente la variabile di sessione dell'username;
- **remove_book_from_basket()**: funzione che rimuove un prodotto dal carrello verificando che sia presente la variabile di sessione dell'username. Se la rimozione va a buon fine viene stampato il valore "1", altrimenti il valore "0";
- **complete_order()**: funzione che completa l'ordine al momento del check-out svuotando il carrello di un determinato utente e verificando che sia presente la variabile di sessione dell'username. Se la rimozione va a buon fine viene stampato il valore "1", altrimenti il valore "0";
- **show_reviews()**: funzione che mostra le recensioni effettuate dagli utenti verificando che sia presente la variabile di sessione dell'username;
- **upload_review()**: funzione che inserisce una nuova recensione verificando che siano presenti le variabili di sessione dell'username, del titolo presente nel menù a tendina e del testo della recensione. Se l'inserimento va a buon fine viene stampato il valore "1", altrimenti il valore "0" (N.B.: per come è stata gestita questa parte, un utente recensisce una sola volta un determinato libro);
- **remove_review()**: funzione che rimuove una recensione dalla piattaforma verificando che siano presenti le variabili di sessione di username e ruolo (che deve corrispondere ad "admin"). Se la rimozione va a buon fine viene stampato il valore "1", altrimenti il valore "0";
- **show_removed_reviews()**: funzione che seleziona le recensioni disponibili per la rimozione verificando che siano presenti le variabili di sessione di username e ruolo (che deve corrispondere ad "admin").