

CS3101-P2-Databases

150008859

01/12/2017

1 Introduction

This practical involved writing a front end in html, css and php for an audiobook streaming website.

1.1 Features

1.1.1 Basic

1. View all audiobooks
2. View all audiobooks by author
3. View all reviews for audiobooks
4. Search for popular audiobooks
5. Purchase audiobook

1.1.2 Extensions

1. Register/Login system
2. View all purchased books
3. Leave review on purchased audiobooks

Screenshots are present at the end of this document (and in the report's image directory).

2 Design

2.1 Usage

You may access the live version at:

<https://saaz.host.cs.st-andrews.ac.uk/cs3301/>

You may register an account using the register page and then login using a (made up) **email** and a **password**. (An already existing account is **test1@mail.com:12345**).

In the navigation bar, click Browse to view all books. Click Popular to view the most popular books. Click on My Books to view your purchase history.

Clicking a book's title take's you to that book's page.

Clicking the name of an author take's you to a list of books by that author.

A book's page contains an option to purchase a book, view all the reviews and the option to leave a review.

2.2 Layout

All classes can be found in the includes directory. I used the autoload technique to automatically include the class on instantiation [1].

All files that the user may interact are found in the top most parent directory.

I have used a style of PHP where in general each php file displays a feature or provides a service through some form of a request.

Some classes are able to fetch their own information from the database, for example the Book class.

2.3 Usage of SQL

I used the MySQL Improved interface in the OOP style [2]. This style involves using an object as opposed to passing handles to functions.

I used prepared statements. By reading the documentation, I found that prepared statements provide many advantages. In particular, the greatest advantage is the prevention of sql injection. Input is sent seperately after the query has been parsed, so the input does not interfere with the query.

2.4 Usage of HTML/CSS

This is my first project in which I have used html/css. Hence, I adapted examples on w3schools. In particular, I adapted the examples for tables [3] and the navigation bar [4].

The tables are used for displaying the results of SQL queries in a neat way. The navigation bar allows user friendly navigation.

2.5 Login and Registration System

First, I added a new column to the person table for storing passwords.

Passwords are hashed using the bcrypt algorithm.

If an attacker had read access to the database, they wouldn't be able to obtain the cleartext version of the users password easily.

I used bcrypt in particular because it automatically includes a salt, this means an attacker wouldn't be able to glean users with the same password or use precomputed rainbow tables.

In addition, bcrypt is easily configurable to increase the time taken to hash an input exponentially. This is better than using an algorithm like md5 which is computable very quickly. An attacker would have to expend significant computing power to calculate a hash.

During the login process, the password is verified using the recommended procedure in the documentation which involves using the password_verify method.

Finally, the session variable is updated to store the user's id. The session variable is used to refer when purchasing, or leaving a review.

Logging out involves unsetting the user id stored in the session variable.

2.6 Purchasing

A "Buy Now!" link is displayed to the user when clicking on a book's title. This performs a request to purchase.php.

The purchase.php acts as a service. Given an isbn as a GET request, it will perform the purchase operation for a logged in user. The user can't accidentally purchase it twice as a book can't be purchased if it has already been purchased.

After a book is purchased, the user is informed that they may listen to a book (although such a feature exists).

2.7 Review

A review is similar to a purchase. A form is submitted which performs a POST request on review.php.

Some extra care was taken to sanitize user input.

A malicious user may attempt to store code in a review so that it will be executed when a review is fetched in an attack known as cross site scripting [6].

Hence, the `strip_tags` function is used to sanitize user input before it is stored into the database.

3 Conclusion

In conclusion, I found it enjoyable to create this audiobook streaming website.

In particular, it was interesting to research some of the security precautions taken into consideration when dealing with user input. A malicious user may try to inject SQL queries, or attempt to execute malicious JavaScript in a client-sided cross site scripting attack. In addition, storing passwords must be done very carefully just in case a malicious reader gets read access to the database to limit the impact on users.

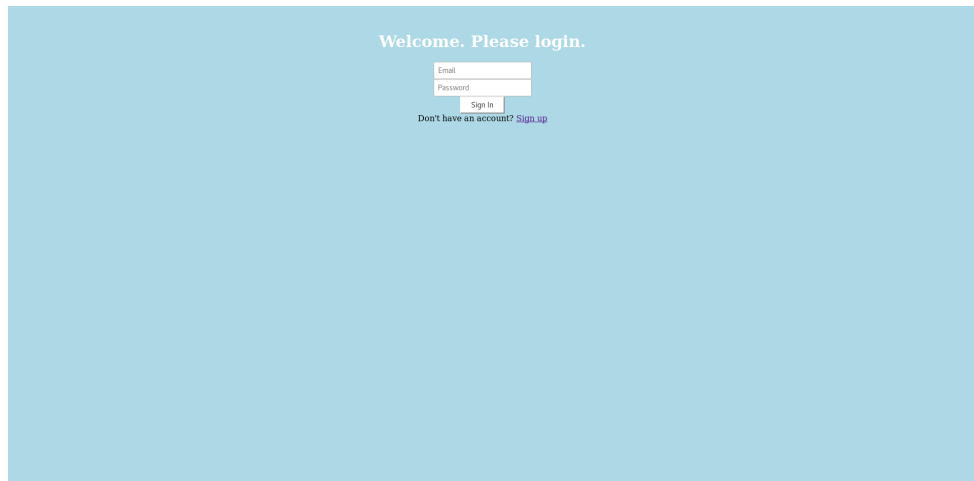
The word count is 836.

References

- [1] PHP autoload
<http://php.net/manual/en/language.oop5.autoload.php>
- [2] PHP MySQL Improved
<http://php.net/manual/en/book.mysql.php>
- [3] w3schools HTML tables
https://www.w3schools.com/html/html_tables.asp
- [4] w3schools navigation bar
https://www.w3schools.com/css/css_navbar.asp
- [5] PHP hashing passwords
<http://php.net/manual/en/faq.passwords.php>
- [6] OWASP XSS attack
[https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

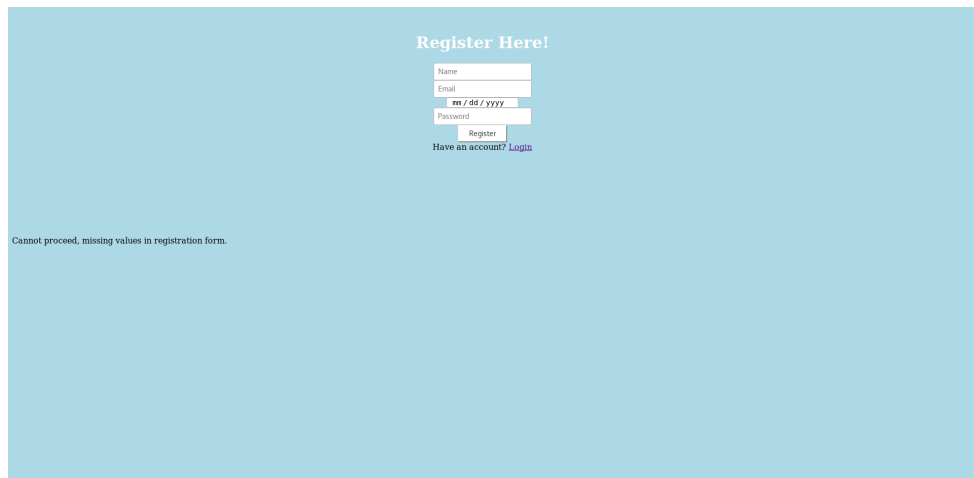
4 Screenshots

Figure 1: Login Page



A screenshot of a login page with a light blue background. The text "Welcome. Please login." is centered at the top. Below it are two input fields: "Email" and "Password". A "Sign In" button is positioned below the "Password" field. At the bottom, the text "Don't have an account? [Sign up](#)" is displayed, with "Sign up" as a purple link.

Figure 2: Sign Up Page



A screenshot of a sign-up page with a light blue background. The text "Register Here!" is centered at the top. Below it are four input fields: "Name", "Email", "Password", and "Confirm Password". A "Register" button is positioned below the "Confirm Password" field. At the bottom, the text "Have an account? [Login](#)" is displayed, with "Login" as a purple link. In the bottom left corner, there is a message: "Cannot proceed, missing values in registration form."

Figure 3: Show all books

Home	Browse	Popular Books	My Books	Logout		
Book Title		Author	Duration	Age Rating	Price	
The Lorax		Dr. Suess	00:33:20	3+	£1.50	
The Hobbit		J. R. R. Tolkien	02:00:00	12+	£1.95	
Artemis Fowl		Eoin Colfer	00:30:00	8+	£1.00	
Alice's Adventures in Wonderland		Lewis Carroll	00:56:40	12+	£1.25	
The Cat in the Hat		Dr. Suess	00:35:00	3+	£1.50	
Lord of the Rings		J. R. R. Tolkien	10:00:00	12+	£4.00	
A Dance with Dragons		George R. R. Martin	04:10:00	18+	£3.00	
A Game of Thrones		George R. R. Martin	05:33:20	18+	£3.00	
Misery		Stephen King	00:48:20	18+	£2.00	
Harry Potter and the Prisoner of Azkaban		J. K. Rowling	01:23:20	12+	£2.00	
Harry Potter and the Philosopher's Stone		J. K. Rowling	01:40:00	12+	£2.00	
Half Moon Investigations		Eoin Colfer	00:50:00	8+	£1.00	

01

Figure 4: Popular Books

Home	Browse	Popular Books	My Books	Logout		
Book Title	Author	Duration	Age Rating	Price		
Lord of the Rings	J. R. R. Tolkien	10:00:00	12+	£4.00		
The Lorax	Dr. Suess	00:33:20	3+	£1.50		
The Cat in the Hat	Dr. Suess	00:35:00	3+	£1.50		
A Game of Thrones	George R. R. Martin	05:33:20	18+	£3.00		
Artemis Fowl	Eoin Colfer	00:30:00	8+	£1.00		
Harry Potter and the Prisoner of Azkaban	J. K. Rowling	01:23:20	12+	£2.00		
Half Moon Investigations	Eoin Colfer	00:50:00	8+	£1.00		
The Hobbit	J. R. R. Tolkien	02:00:00	12+	£1.95		
A Dance with Dragons	George R. R. Martin	04:10:00	18+	£3.00		
Harry Potter and the Philosopher's Stone	J. K. Rowling	01:40:00	12+	£2.00		
0						

Figure 5: Book's by Dr Suess

Home Browse Popular Books My Books Logout					
Book Title	Duration	Author	Age Rating	Price	
The Lorax		Dr. Suess	00:33:20	3+	£1.50
The Cat in the Hat		Dr. Suess	00:35:00	3+	£1.50

0

Figure 6: The book page for The Lorax

<div>HomeBrowsePopular BooksMy BooksLogout</div>				
Book Title	Author	Duration	Age Rating	Price
The Lorax	Dr. Seuss	00:33:20	3+	£1.50
You can listen to this book!				
Reviews				
Review				Rating
A quirky story.				4
I thoroughly enjoyed reading this book!				4
<div><div>4</div><div></div><div>Review</div></div>				

Figure 7: An unpurchased book

HomeBrowsePopular BooksMy BooksLogout				
Book Title	Author	Duration	Age Rating	Price
A Game of Thrones	George R. R. Martin	05:33:20	18+	£3.00
Buy Now!				
Reviews				
Review	Rating			
A thrilling story.	5			
An inspiring tale.	5			