Books Testing Review

Part I. Summary

Overall, we are extremely impressed with the first version of the books marketplace. Despite the time limitations and the complexity of the project, the books team has developed a robust and user-friendly online book marketplace system. The initial implementation appears to have met almost all of the specified requirements, save password security and email notification. While the website user interface is simple and intuitive, a more stylish GUI could present search results and user profiles more gracefully, and perhaps allow the user to sort items by price, author, time since added to database, etc. Perhaps a restructuring of the website could make for more efficient and elegant book buying/selling. In addition, a simple 'About' page, maybe located under the Home tab, should explain the overall purpose and functionality of the project, so that the user is aware of how to transfer money and complete book delivery. Although we were able to discover some minor flaws, we conclude that the project is generally fail-safe and easy to use! Good job!

Part II. Findings

Our findings are grouped by books system functionality, with each section containing a list of bugs and unimplemented features. By unimplemented features, we mean functionality that was not developed in this version but was mentioned in the requirements documentation and/or would make the use of the product a lot easier. And by bugs we mean... well, bugs!!

General

Bugs:

1) Malicious users can send code to database that can cause scripting attacks!
   Severity: Severe!
   Suggestion: Filter all user input for cross-site scripting attacks (ie filter out all < and > with < and >).

Transactions

Bugs:

1) Availability: Books still appear available even after being purchased.
   Severity: Moderate
   Suggestion: On a purchase, update the book’s database entry to reflect it’s purchase.
2) Adding a book for sale: A user can only add a book after having searched for it. This is unnecessarily frustrating for a user. First, a user must search for a book. Then, if the book isn’t in the database, the user must add the book to the database. After that, the user must search again for the book and only after that is the user offered the chance to add the book for sale.
Severity: Moderate (ly annoying)
Suggestion: Instead of having the “Add New Book” page, I would have a “Sell A Book” page. There, the user could enter his offer for a book. The server could query the database for the book and if it exists, update the entry. If the book is not in the database, the server could add the book to the database.

3) Editing a book offer: User is unable to edit his book offer.
Severity: Moderate

4) Search results/Empty user input: The server doesn’t check for empty user input on the search page. If an empty search is submitted, the server returns all books in the database. This is an issue because if the database were to grow large, as is implied by the requirements, every empty search would be extremely demanding on the server and useless for the user. While this might be helpful for debugging and testing the server, it should not be in the final release.
Severity: Severe
Suggestion: On a user search submission, the server should check that the user submitted at least one search variable.

Unimplemented Features:
1) Email notification: Email notification on book availability unimplemented. Email notification of book sale unimplemented. User has no idea when a sale has been made.
Severity: Severe

Add New Book

Bugs:
1) Users are not required to be logged in before adding a book. This allows anybody to add a book without being able to trace the item to any seller. As a result, the database may become clobbered with junk entries and spam.
Severity: Moderate
Suggestion: Require users to log in before adding sale items.

2) the show/hide debug option does not work if javascript is disabled.
Severity: Minor

3) In the title bar "Search Books" is spelled incorrectly.
Severity: Severe

4) There is no error checking on the ISBN field (I can type complete garbage and it accepts it).
Severity: Moderate
Suggestion: Parse the input to ensure it consist only of digits and is the appropriate length.

5) Not properly working since the user can add a book and still not find same book in a new search.
Severity: Severe - the whole purpose of the project is to find books
Suggestion: Modify insertion or search queries.

6) User can submit blank or incomplete forms.
Severity: Moderate
Suggestion: Add some sort of indicator of which are the necessary fields (asterisks, red text, etc) Add javascript code to notify user of which fields were not filled out. Do not permit user to continue until preconditions are met.

Unimplemented Features:
1) Users should have to type ISBN or title/author. Not all three. ISBN could be used to look up all the information for example.
Severity: Moderate

3) Fields like quantity, condition and price should be added.
Severity: Minor

3) After books are added, there is no message that confirms the inventory addition.
Severity: Minor
Suggestion: Display a simple message that says 'book [book name] added'.

Create New Account

Bugs:
1) User can create account without filling all necessary fields.
Severity: Severe
Suggestion: Add some sort of indicator of which are the necessary fields (asterisks, red text, etc). Add javascript code to notify user of which fields were not filled out. Do not permit user to continue until preconditions are met.

2) There is no validation for creating a username that may already exist.
Severity: Severe
Suggestion: Implement a search for current usernames and make sure new username doesn't match any of these.

Login

Bugs:
1) Disallows login with any password but the empty string
Severity: Severe
Suggestion: Enable password feature
2) “Edit Profile” feature does not display new information after user updates his account  
*Severity:* Moderate  
*Suggestion:* The database should be properly updated when user edits data.

3) “Edit profile” feature allows user to edit username  
*Severity:* Minor  
*Suggestion:* This is not a feature that seems to be common practice – most comparable services allow the user to edit contact information but one piece of data (i.e. username) usually stays intact. Simply remove this field from the Edit Profile feature.

4) No logout/timeout feature: Questionable security  
*Severity:* Moderate  
*Suggestion:* Add logout button that causes the session info to be discarded and forces user to log-in anew

Unimplemented Features:  
1) Security: Password protection on login unimplemented.  
*Severity:* Severe

---

**Home**

Unimplemented Features:  
1) No description of Books Marketplace functionality or instructions about how to use the system.  
*Severity:* Minor  
*Suggestion:* Include a few paragraphs that explain your product, mentioning how to complete money transfers. It is clear to us (your classmates) that you are not responsible for payment processing, however, anyone who stumbles upon your website may be confused as to why there are no 'make payment' buttons.

2) There should be a link to log in directly on the main page.  
*Severity:* Minor

---

**My Home**

**Bugs:**  
1) If a price of a book was entered with a $ in the front, inventory shows that the price is $0.00  
*Severity:* Severe  
*Suggestion:* Update the price of the books when it's listed, even if it starts with $

2) When user clicks on Edit Inventory, he is taken to a blank page- ie it is impossible to actually edit the inventory.  
*Severity:* Moderate

Unimplemented Features  
1) There is no feedback features
Severity: Moderate (this was part of the requirements doc)

2) It is impossible to view my own profile or another user's profile and transaction history
Severity: Moderate

3) There are no sorting features, so it is impossible to view transactions sorted by date, author, price, etc.
Severity: Minor