EE6052/ED5022/CE4208/EE4023 Programming Project 3

1. Description

This is a group project with groups of up to 4 students. Please add the names and ID numbers of your group members to the wiki page on the module's SULIS page. You can also leave messages there if you are looking for additional group members of for a group to join.

Your task is to write an online shop application using EJB, entity classes and servlets/JSP/HTML (think amazon or something similar). Customers browse through your offerings, add or remove them from their shopping cart and eventually either check out their order or cancel it. Your store can sell whatever you like: books, movies, computers, cars, etc. However, you have to provide the following features:

- Access to your shop is limited – you must provide an authentication scheme (simple authentication providing username/password or session token in cookies is sufficient) . Access rights are role based, where your system provides two roles: customer and administrator.
- Provide (at least) two accounts: Customer joe with password "1tbh?5g" and administrator toor with password "4u!ido@" (feel free to add other accounts, but these must exist).
- Customers can perform the following:
  - Browse through all your items.
  - Search products by ID number and browse through the search results.
  - Search products by name and browse through the search results.
  - Add displayed items to their shopping cart.
  - Add comments to any product.
  - View comments that have been added to a product.
- Administrators can perform:
  - Add new products to the sale database.
  - Remove products from the sale database.
  - Increase/decrease the available amount of any product.
- When customers check out, the quantity for your items in the database is adjusted correspondingly - make sure the quantity of a product cannot drop below 0. Your program should check for availability of products before the check-out process is started.
- When customers cancel their order, the database should remain unchanged.
- A logging facility:
  - Every time a customer confirms an order or cancels an order a corresponding entry is added to the log (use either a log-file or a table in the database).
  - Every time an administrator adds or removes a product a corresponding entry is added to the log.
- Your application must avoid the following OWASP Top 10 vulnerabilities:
  - Injection
  - Cross-Site Scripting
  - Insecure Direct Object References
  - Failure to Restrict URL Access
- You must include a document in your submission that discusses:
  - What techniques you used to ensure that your application it not vulnerable to the required OWASP Top 10 vulnerabilities.
  - How you tested your application to ensure your chosen defence is working correctly.

2. Instructions

In addition to these features, you must follow these instructions:

- All features should be implemented using servlets, JSP pages and EJBs only.
- A stateful session bean is used for the shopping cart.
- Message driven bean(s) are used for a logging facility.
- Development must be done in NetBeans using Java EE 6 on a MS Windows machine (otherwise I cannot easily copy the employed database).
- Use the ID numbers of all group members as name for the NetBeans project.
- Use one of your student IDs as name for your database (to guarantee a unique database name when running your applications on my computer).

3. Deadline and Deliverables

Deadline for submission of your solution is Friday of week 12 (Friday, 25.04.2014). Please submit your solution as a **single** zip or rar archive (please do not use any other format and do not remove the extension (.rar/.zip) from the archive) via the module's SULIS page.

A complete solution includes the following items:

- Well documented and formatted source code as a NetBeans project (submit the entire project folder, not only the source code!)
- Database files (these are usually located at: C:\Documents and Settings\Name\.netbeans-derby\DBName, where "Name" is your Windows user name).
- Report (preferably MS Word or RTF, but PDF is also acceptable) that analyses your application against the requested OWASP Top Ten vulnerabilities.

4. Marking

The project is worth 20% of the module. In general, all students of a group will receive the same mark. However, if any group members are not contributing sufficiently, please let me know and marks will be adjusted correspondingly (no contribution means 0 marks).

Application (implementation of all features, coding style, quality of comments)	10
Security (quality of security features and resistance against OWASP Top 10)	5
Report (presentation, completeness, quality of used testing techniques)	5
Total	**20**

5. Miscellaneous & Hints

- Don't waste time on creating fancy web pages - functionality is all that is required.
- If any queries are coming up, please refer to the question and answer section on the module's SULIS page.
- Make sure all files (including source files etc.) contain the names & IDs of all group members.