EE6052/ED5022/CE4208/EE4023 Group Project

1.Overview

This is a group project with groups of 3-5 students (groups with less than 3 students will not be accepted). 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 develop an web application (outlined below) and deploy it on a virtual machine. Feel free to use any Java EE container and database you like. However, your sources must be submitted as a NetBeans project. All features should be implemented using EJB, entity classes and JSF/HTML **only**. **Do not use any other frameworks** such as Hibernate or Spring. If you really "need" to use any other framework/library, you must first confirm with me that it is ok to use these.

2. Description

Your task is to write an online shop application using HTML, JSF, EJB and entity classes (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. Access to your shop is limited – you must provide an authentication scheme. Access rights are role based, where your system provides two roles: customer and administrator.

- Provide two accounts: Customer 'joe' with password "1D10T?" (second last is zero) and administrator 'toor' with password "4uIdo0!" (third is capital i - not one, second last is zero) - 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.
  - Remove items from their shopping cart.
  - Edit their profile - must contain at least name, Customer ID and a message to other users. Name and ID are taken from Customer table, message can be any text – allow at least for 500 characters.
  - View profiles from other users – provide search by name and search by ID.
  - Check out or cancel current order.
- Administrators can perform:
  - Add new products to the database.
  - Remove products from the database.
  - Increase/decrease the available amount (quantity_on_hand) 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 in the database cannot drop below 0 – if an order would cause this, display an error message to the user's screen. On successful order, you need to add a purchase order (PO) entry.
- When customers cancel their order, the database should remain unchanged.
- A logging facility (Message driven bean(s) must be used for the logging facility):
  - Every time a customer confirms an order or cancels an order a corresponding entry is added to the log (either a log-file or database table).
  - Every time an administrator adds/removes a product an entry is added to the log.
- Your application must avoid the following OWASP Top 10 vulnerabilities:
  - A1: Injection
  - A3: Cross-Site Scripting (XSS)

  - A7: Missing Function Level Access Control
  - A8: Cross Site Request Forgery (CSRF)
- Deploy your application to a Java EE server of your choice. **Do not use an IDE-based** deployment – you must describe how you deployed your application in your report (see below).

3. Deadline and Deliverables

Deadline for submission of your solution is Friday of week 12 (Friday, 22.04.2016). 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 (only submit your NetBeans project and your Report via SULIS). Only one group member should submit the solution (if multiple students submit, I will mark the first submission that I find)

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 individual source code files!)
- Report (MS Word or PDF) that contains:
  - A description of techniques you used to ensure that your application it not vulnerable to the required OWASP Top 10 vulnerabilities. Please detail what you are using and how this technique ensures your application is not vulnerable. Please ensure your report is accurate – I will not search your code to look for security features (if something is not mentioned in your report, I assume it is not present in the code)
  - Details on how you tested your application to ensure your chosen defence is working correctly (I recommend to use screenshots in addition to your explanation).
  - Description of the steps undertaken to deploy your application
- In addition to these SULIS submissions, you need to prepare a virtual machine that runs your application and database. This virtual machine should be deployed to ECE's VMware server. You can either create a virtual machine on your own PC/Laptop and import it to the our server or you can use a blank virtual machine on the server and deploy your application directly on it. Please contact Eoin O'Connell (eoin.oconnell@ul.ie, room B2005a) to obtain or import your virtual machine. **Note:** As we are currently experiencing some issues with our server (which I hope will be resolved soon), if deployment on our VMware is not possible, you need to demonstrate your working virtual machine to me.

5. Marking

The project is worth 40% 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)	15
Report on used techniques to secure application	8
Report on testing your applications security	7
Successful deployment	10
Total	**40**

6. Miscellaneous & Hints

- Don't waste time on creating fancy web pages - functionality is all that is required.
- For any queries, please refer to the question and answer section on the module's SULIS page.