This project relates to a vulnerable fictitious website/electronic store (e-Store). Access the e-Store through the URL: http://localhost:8080/estore/

Notes:

1. Because Tomcat uses port 8080, you may want to set the port for Burp to some other value, for example 8082. Consequently, to use Burp alongside your browser, your browser's proxy should be set to use 127.0.0.1 with port 8082.
2. You do **not** need to start the Apache and MySQL services in this coursework.
3. You can work on this project using your own laptop (provided you have xampp installed). Simply download the estore.zip file and unzip it under **c:\xampp\tomcat\webapps**

Task(s)

Task 1: Offensive Security

The aim of this task is to exploit certain vulnerabilities on the website.

The website has a score board that contains a list of 12 challenges. The score board can be accessed by browsing to the "**About Us**" page then clicking on the "**Scoring Page**" link or by directly accessing: http://localhost:8080/estore/score.jsp

Challenges will be shown as green once solved as shown below:

Notes:

1. When you stop the Tomcat service and access the e-Store again, the score board will be reset and will show red against all challenges. This is normal and is nothing to worry about as you do not need to provide a screenshot of the score board with all the challenges solved in one go.
2. You do not need to attempt the challenges in the order specified in the score board.
3. **You do not need to solve challenge 2** (login as user1) **nor challenge 3** (login as admin) because they are similar to challenge 1.
4. I will provide you with the solution to **challenge 5** (Find diagnostic data) because it will help you with other challenges. The e-Store uses a parameter called *debug* to display error messages. For example, visiting the following page will solve challenge 5: http://localhost:8080/estore/login.jsp?debug=true
5. To complete the ***9 remaining challenges***, you mainly need a browser, the browser's web development tools, and Burp Suite. But feel free to use any other tool you deem appropriate (including those in the Kali VM).

6. Remember that, in this task, you are taking the perspective of an attacker. Therefore, you shouldn't attempt to edit and modify the website's source code (on the server side) to complete the challenges. Here are some hints to help you complete the challenges:

Challenge	**Hint**
Challenge 1: Login as test…	SQL-injection. Your injected code needs to terminate the closing bracket shown in the error code. Remember to add the ?debug=true to the URL.
Challenge 4: Find hidden content	
Challenge 6: Level 1 XSS	Reflective XSS.
Challenge 7: Level 2 XSS	Stored XSS.
Challenge 8: Access someone…	
Challenge 9: Get the store…	Time for a bit of shopping and some simple arithmetic.
Challenge 10: Change your password…	From POST to GET.
Challenge 11: Conquer AES encryption, and display a popup	Inject script in the "Type" input box of "Advance Search". The form has a JavaScript function that calls another function which replaces special characters with their URL encoding. Try to bypass it.
Challenge 12: Conquer AES encryption and append a list of the table names	Combine the bypassing of validation from the previous challenge with SQL injection. Remember to use *?debug=true* to get the website to display errors.

Task 2: Defensive Security

The e-Store website is available under the folder **c:\xampp\tomcat\webapps\estore**
Propose **Five (5)** security measures that can be implemented to mitigate against some of the e-Store vulnerabilities (identified in task 1) including:

- **Three (3)** security measures related to the configuration of Tomcat; and
- **Two (2)** security measures to address vulnerabilities in the source code (jsp files) of the website:
  - one to mitigate against SQL injection and
  - one to mitigate against XSS.

Note:

1. In this task, you should not only describe the proposed security measure but also implement them and show that they work as intended. You should provide details of any new code and/or configuration to be added, and the location (file) where it is added, and testing of the new code and/or configuration. Remember to cite any source used in your answers.
2. If using your own laptop, ensure you use the same version of xampp as the one in the Virtual Machine.

Task 3: Legal, Ethical, Social and Professional (LESP) Issues

Assume that e-Store is now deployed in a real environment for paying customers. Based on your research into examples of similar web applications (companies/organizations), discuss what it means for this website to adhere to legal requirements, act ethically, be socially responsible, and follow professional standards.