1. Which elements of your Web application require protection against threats? Which ones do not require protection? Why?

- Data -- Only a few admins should be able to access administration section of the book shop, to see orders and manage the book shop inventory
- UI -- Data entered by users shouldn't cause XSS or SQL-injection and be protected from hijacking.
- Payments should be secure with HTTPS/SSL.
- Users should only be granted write access to making an order. Everything else should only be editable by admins.

2. Describe the techniques that can be used to protect the elements of your Web application that require protection.

- HTTPS: Secure HTTP that ensure encryption between web server and user. It makes data manipulation very for a third party.
- SQL permission per account. This grants access only the most necessary information.
- Password protected CMS.
- Putting the quotes around values which are inserted to database to prevent SQL-injection
- Replace all HTML markup signs in the values from database (i.e. replace '`<`' with '`<`') to prevent rendering of malicious HTML
- Usage of trusted payment gate

3. Describe the drawbacks of ensuring the highest possible security for all the elements of your Web application.

- It can be time consuming
- Performance might be a little slower
- Not all browsers may be supported.

4. Describe one attack on the network, one attack on the user's session and one attack on the browser request that your Web application or its clients could be victim of. In case any of the attack types is not possible for your Web application, explain why.

- Eavesdropping/MitM -- the data about user's credit card could be stolen by using one of these attacks
- UI Redressing. The user can be compelled to use an attacker's fake login page to enter his/hers authentication credentials.
- Authenticating using stolen credentials by phishing.

5. From the plan given as answer to the question 3 of the assignment 5, which activities have you already performed? how has the Web application been improved after performing these activities?

- None of them.

6. Continue the development of your Web Application. Report its status.

- We have struggled using Maven/Spring and changed development language from Java to PHP.
- The skeleton for the Model is complete. Next Thursday will be spent on writing the skeleton for the control and/or some views.
- The database has been developed and setup SQL file has been made. No test data yet though.

Christian Friis Lyngbo Andersen (can11@student.aau.dk)

Eva Šmijáková (esmija17@student.aau.dk)