User Manual
Information Security Project

Daniel Planötscher, 19615 `dplanoetscher@unibz.it`
Leo Kerschbaumer, 19072, `lekerschbaumer@unibz.it`
Roland Bernard, 19598 `rolbernard@unibz.it`

I. GETTING STARTED

A. Requirements

- Maven[1]
- Java 17 JDK[2]

The application is written in Java using features introduced with Java version 17. For compiling the project, it is therefore required to install the Java JDK version 17 or later. The Maven software is used for dependency management and must be installed on the system for the recommended install procedure.

B. Installation

To quickly download the source for this application, compile it, and start the secure version of the project execute the following commands.

```
git clone https://github.com/rolandbernard/is-project
cd ./is-project/secure/
mvn compile spring-boot:run
```

Installation and compilation from source is handled thought Maven. After cloning the git repository of this project, you will three different projects located within it. The insecure version of the application can be found in the directory `insecure/`, while the secure version is located in `secure`. The third project inside the repository at `rainbow/` contains an implementation of rainbow tables and tools for generating and using them.

C. Starting

To compile one of the projects, navigate into the proper directory (e.g., `cd ./is-project/secure/`) and execute the Maven command `mvn compile`. Maven will automatically download all required dependencies and compile the classes in the project. Then, to start the server of either the secure or insecure web application execute the Maven command `mvn spring-boot:run`. The project is using the Spring Boot[3] framework for handing web interaction. Additionally, we use a Maven plugin that allows starting the web server using this simple command.

After starting the web server, the application will be available on port 8080. You can navigate to `http://localhost:8080` in your browser to access it. Note that the secure version of the application will redirect you to the HTTPS version of the site at `https://localhost:8443`. Since the default certificate contained in the repository is self-signed, most browsers will give you a warning saying that the site is not secure. In order to use the applicaion with the distributed certificate, you should tell the browser to accept the risk and continue to `https://localhost:8443`. This option is often hidden behind the "Advanced" button.
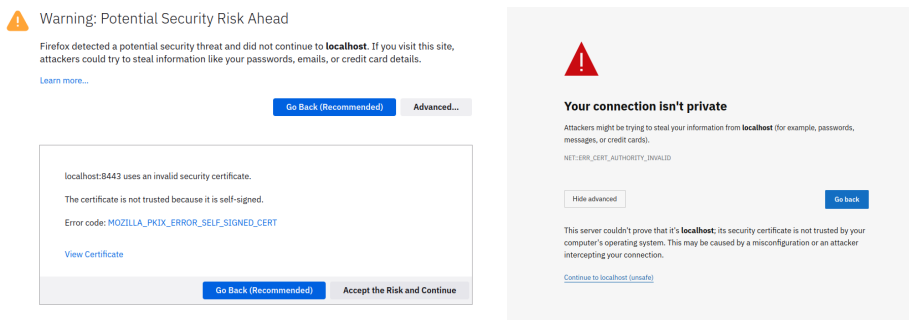

Fig. 1: Warning as presented by different browsers (Firefox on the left; Microsoft Edge on the right).

---

[1]https://maven.apache.org/
[2]https://www.oracle.com/java/technologies/downloads/#java17
[3]https://spring.io/projects/spring-boot

II. USAGE

A. General

(a) The first screen presented to users.

(b) Example of the registration form.

Fig. 2: Example of the registration procedure.

1) Registration: To register, the user must supply a username containing at least 3 characters. In the secure version, aside from underscores and dots, only alphanumerical ASCII characters are permitted in usernames. The user is also asked to enter a password twice. The two repetitions of the password must match and, in the secure version, there are additional constraints on the password. Passwords in the secure version must be at least 8 characters long, contain lowercase and uppercase letters, numbers, and special characters. Usernames are unique, so if another user has already taken the desired username, registration will fail.

The user is further asked to declare whether they are a vendor or a customer. Vendors should check the checkbox at the bottom of the form labelled "Vendor". Customers and vendors have access to different functionality and the choice made during registration can not be changed later.

Fig. 3: Example of the login form.

2) Login: If the user already has an account, they can select the "Already have an account?" button, or use the "Login" button in the header of the website. To log into the web application the user must provide username and password. If these do not match any known user, the user will not be allowed to access any other part of the application.
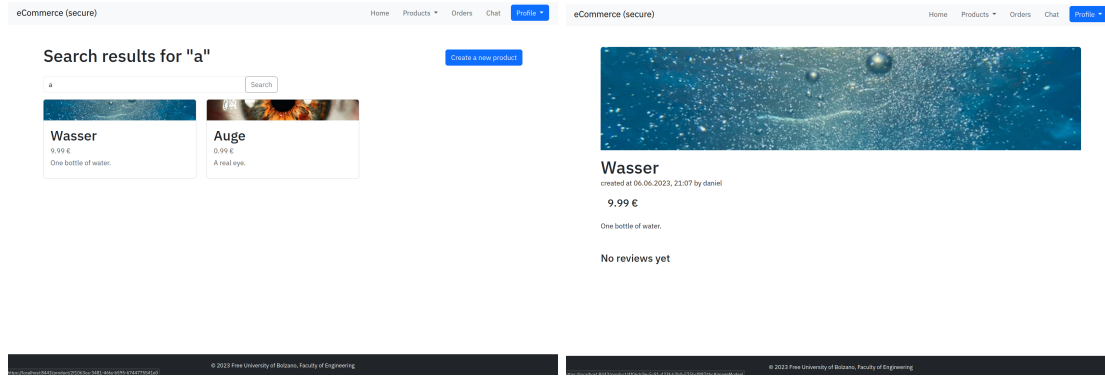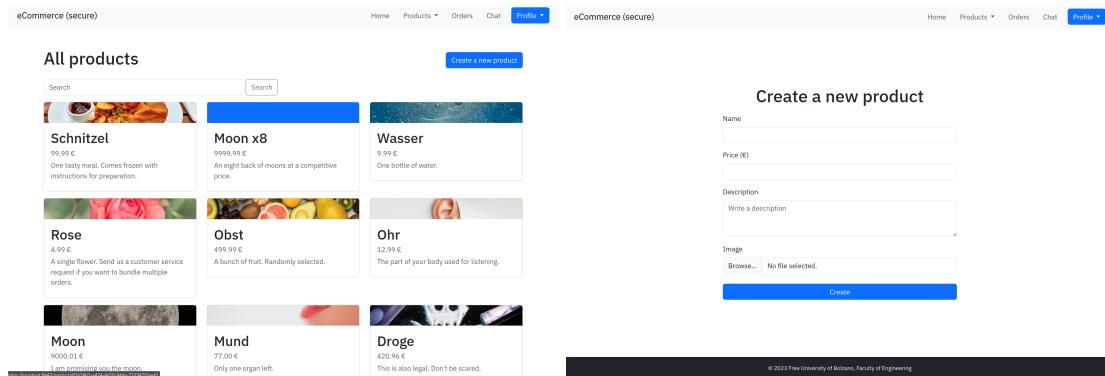
(a) The listing of all products contained in the search.   (b) Detailed view of one product.

Fig. 4: Shows the process of searching and reading product cards.

3) Search and read products: To search for a product, use the search field at the beginning of the product list. The product list is accessible by using the "Products" menu in the header of the webpage. Vendors have a special version of the product list that shows only product cards posted by them under the menu item "My products". To see further details on a single product, select it in the list of products by clicking on the product card. This is also the section in which reviews for products and relies to those reviews are made visible.

B. Vendors

(a) The listing of all products currently posted.   (b) Example of the form for creating new product posts.

Fig. 5: Example of the steps for creating a new product.

1) Post product: New products can be posted by vendors by navigating to one of the product lists through the "Products" menu in the header of the webpage and then selecting "Create a new product". The user will be presented with a form that requests a product name, price, description, and image. Both the product name and the price are mandatory, while the description and image may optionally be left blank.

3

Fig. 6: Example showing the list of orders for a vendors products.

2) Check orders: A vendor can check the incoming orders from his customers by navigating to the orders view using the "Orders" button of the top navigation bar. For each order an order identifier, the product purchased, the customer that performed the purchase, and the data of purchase are displayed. Additionally, the secure version of the application also features support for digital signatures of the order documents. If the order has a valid signature in the database, a check mark will be displayed. If no signature is present, or it is somehow invalid, a red x-mark will be shown for that order.

Fig. 7: Example showing the way vendors can reply to reviews.

3) Reply to reviews: If a customer has posted a review for a product of a vendor, that vendor can reply to the review. This is possible by navigating to the product information page and writing the response in the text field underneath the review. To post the reply press the "Submit" button underneath the text area.

(a) List of all user the vendor has communicated with.　　　(b) An example chat with a client.

Fig. 8: Example showing how vendors can chat with customers.

4) Chat with customers: The application offers the customers the ability to message vendors over a private chat. The vendor can see all users which whom they have exchanged chat messages by navigating to the chat list using the "Chats" button in

the menu at the top of the page. By selecting one of the chats, the user is able to type a message into the text area at the bottom of the page and click "Send" to send me message. Messages are stored encrypted using the DES algorithm and are not accessible to anyone but the users participating in the communication.

C. Customers
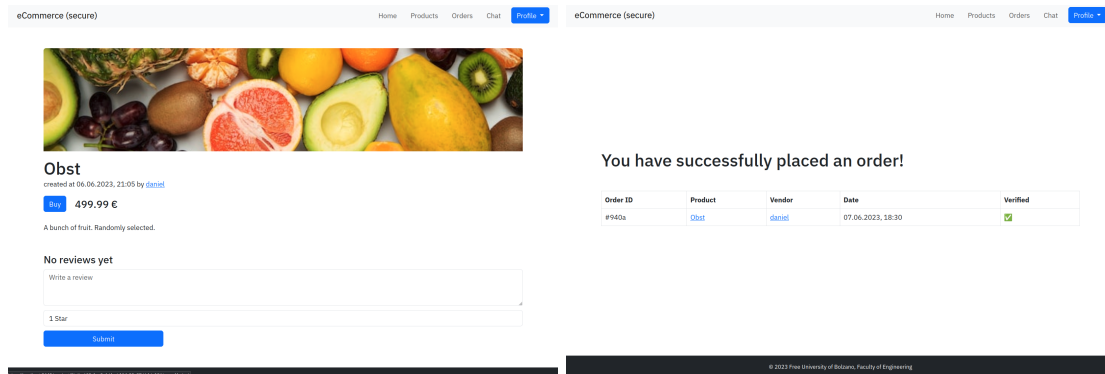
(a) The product details page for a customer.

(b) Example of the page displayed after placing an order.

Fig. 9: Example of how a customer can place an order.

1) Buy products: To place an order for a product, a customer can navigate to the products details page. From there, a customer is able to by a product using the "Buy" button above the description of the product. After placing an order, a confirmation page will be displayed, showing also the information for the ordering document and, for the secure version, whether it was successfully signed with a digital signature.
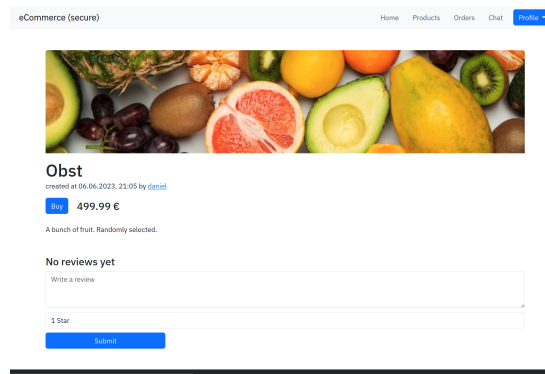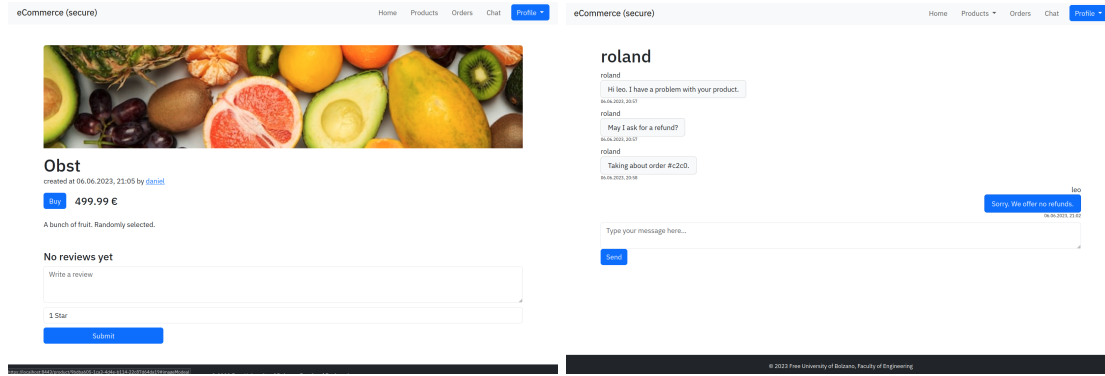

Fig. 10: Example of a product page where users can post reviews.

2) Post reviews: After a user has bought a product, the product details page will show the option to post a review. Using the text area at the beginning of the reviews list, selecting a 1-5 start rating, and clicking the "Submit" button, a review can be posted.

(a) The product details page for a customer.   (b) An example chat between vendor and customer.

Fig. 11: Example showing how customers can chat with vendors.

3) Chat with vendors: The application offers the customers the ability to message vendors over a private chat. The customers can click on the name of the vendor beneath the product name on the product information page. This will bring them to the direct chat page for the selected vendor. All chats the customer has started are also available in the chats list by navigating using the "Chats" button in the header of the webpage. By selecting one of the chats, the user is able to type a message into the text area at the bottom of the page and click "Send" to send me message. Messages are stored encrypted using the DES algorithm and are not accessible to anyone but the users participating in the communication.