**ASVS Analysis**

1. **– Error Handling and Logging**

**Level 1 standards:**

7.1.1 (valid): Original application did not log credentials or payment details.

7.1.2 (valid): Original application did not log session tokens.

7.4.1 (not valid): There was no failsafe for unexpected errors, which had to be added to the registration page.

A black background with white text

Description automatically generated

**Level 2 standards** **considered:**

7.1.3 (not valid): No logs were done in the application. Partially fixed by logging authentication events.

7.1.4 (not valid): Same as previous standard. Fixed by adding timestamps to all new logs.

A computer code on a black background

Description automatically generated

1. **– Business Logic**

**Level 1 standards:**

11.1.1 (not valid): User was not required to be logged in to complete a purchase. Fixed by adding the following php code to the checkout page:

A screen shot of a computer program

Description automatically generated

11.1.2 (not valid): It was possible for a user to spam a payment request, which should not be done consecutively. Fixed by adding a 60 second timer between requests from the same user through the code in the file “checkout.php”:

A computer screen shot of code

Description automatically generated

11.1.3: Considered to not be applicable to the application since it is missing a lot of functionalities. To give an example of a realistic scenario, every product should have a limited amount in stock and, therefore, a user should not be able to surpass it with requests. Since there is currently no stock tracking, it is not possible to enforce such a limit.

11.1.4 (not valid): It was considered that with the current version of the application, data exfiltration and file uploads should not be possible. Also, excessive business logic requests and denial of service were limited by the change implemented for the standard 11.1.2.

11.1.5: Because of the previously mentioned lack of functionalities in the application, it is hard to identify any business risks or threats, and thus this was considered not applicable.