

Red vs Blue team

Webshop

Fontys ICT

26-10-2020

## **Chapter 1**

**Management Summary**

No issues were found, this application is completely secured by default due to the choices made in the technologies en functionalities.

**Table of Contents**

[**Chapter 1**](#_p5zugf2e9v6t) **2**

[**Chapter 2**](#_9ebguro5h6st) **4**

[**2.1 Research question**](#_l5zynsppyp6s) **4**

[**2.2 Scope**](#_gm2gnfqavhfj) **4**

[**3.1 Approach**](#_ubioixhhvus6) **5**

[**3.2 Analysis**](#_vf3fa0h49e3n) **5**

[**Chapter 4**](#_l9rj5ydqhqo4) **6**

## **Chapter 2**

**Your request**

The request of the owner of the application is to test the authentication, JWT authorization and (other) well known vulnerabilities.

# **2.1 Research question**

Is the authentication and JWT authorization properly implemented and are there no options for exploiting common vulnerabilities?

# **2.2 Scope**

The entire web application(10.10.1.116) including the backend, hosted on seclab.**Chapter 3**

Our Findings

A description of how every part of the scope is scanned, then a description of the results.

# **3.1 Approach**

The tools we used were mainly nmap and Burp Suite. With these tools(or manual) we tested for malformed input and unauthorized access.

# **3.2 Analysis**

There were no actual problems found, besides a lack of content. We were able to create products with unsafe names, but they didn’t trigger anything, rendering them useless.  
One problem we found was the fact that the application has no roles, anyone logged in can create, edit and remove products. This might be a design choice, but we still mention it.

## **Chapter 4**

**Conclusion and advice**

There were no problems found. It would be wise to implement roles to make sure that not everyone can edit the products.