

Report penetration test

Reading website

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.

**Table of Contents**

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

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

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

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

[**Chapter 3**](#_o48glnspgqg6) **5**

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

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

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

## **Chapter 2**

**Your request**

Authentication, Authorization, input filtering/validation and data encryption

# **2.1 Research question**

Is the Authentication, Authorization, input filtering/validation and data encryption properly implemented, without any way to exploit it?

# **2.2 Scope**

The entire web application(10.10.2.131:80 = front-end, 10.10.2.132:8081 = API, 10.10.2.132:3306 = MySQL database) 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 used were mainly nmap and Burp Suite. We used this to check for malformed input, path traversal and bad authorization.

# **3.2 Analysis**

Apart from the lack of content, there were no problems found on the web application. When unauthorized users accessed the admin-panel they were redirected to the home page.

The administrator could see all the hashes and salts, which is an odd design choice, but not an actual exploit.

## **Chapter 4**

**Conclusion and advice**

There are no security issues found, keep it up