# Security Report

Viktor Skachkov

**11-06-2022**

Tutors: Tim Kurvers and Paixão Márcio

# Table of contents

## Contents

# OWAP Top 10

| | Likelihood | Impact | Risk | Actions possible | Planned |
|---|---|---|---|---|---|
| A1: Broken Access Control | Very unlikely | Low | Low | | Yes. There is authentication and authorization in place which validates the roles of the users. |
| A2: Cryptographic Failures | Likely | Medium | Medium | Encrypting the passwords for the user accounts | No, because cryptographic encryption causes the app to crash for some reason. |
| A3: Injection | Very unlikely | Low | Low | | Yes. The system validates the input of a user. |
| A4: Insecure Design | Very unlikely | Low | Low | | Yes. The system checks if the user is an employee or a client and gives authority according to the role. |
| A5: Security Misconfiguration | Low | Low | Low | | Yes. |
| A6: Vulnerable and Outdated Components | Unlikely | Low | Low | | Yes. All the components used are up-to-date. |
| A7: Identification and | Moderate | Moderate | Moderate | Making sure that the password are | No. The encryption of password |

| | | | | | |
|---|---|---|---|---|---|
| Authentication Failures | | | | hashed and encrypted. | causes the application to break. |
| A8: Software and Data Integrity Failures | Moderate | Moderate | Moderate | Making sure that SonarQube is properly integrated in the CI/CD pipeline. | Yes. I tried to integrate it inside GitLab but it still doesn’t work. However, the other parts of the CI work and I use SonarQube to check the app. However, the app consumes trusted repositories and data is not sent to unauthorized people. |
| A9: Security Logging and Monitoring | Moderate | Moderate | Moderate | The logs should be stored in a database. | The logging feature works properly, and it sends warning when the user tries to log with non-existent credentials but the logs are stored locally. |
| A10: Server-Side Request Forgery | Likely | Moderate | Moderate | Improve framework implementation | No, risk accepted. |

# Reasoning

A security risk means something which endangers the overall flow of the application and its processes.
In my opinion, there is not a big chance of that happening and the impact wouldn’t be too severe.

# Conclusion

I think my application is sufficiently secure for the level we are currently at. Some things that could be improved are implementing encryption for the password and making sure that a session is not deleted upon loading the page. However, the implementation of encryption for the passwords causes my application to break and I couldn't find how to improve the sessions.

Also, according to Google Lighthous, the application is performing relatively well (you can view the Google Lighthous screenshots that are attached).