# OWASP Security Report

| Security risks | Likelihood | Impact | Risk | Actions possible | Planned |
|---|---|---|---|---|---|
| **A01:2021 – Broken Access Control** | High | Severe | High | None, fixed | Yes |
| **A02:2021 – Cryptographic Failures** | Likely | Severe | Moderate | None, cannot use HTTPS | No |
| **A03:2021 – Injection** | Likely | Severe | High | None, prevented | Yes |
| **A04:2021 – Insecure Design** | Likely | High | Moderate | None, actions taken already | Yes |
| **A05:2021 – Security Misconfiguration** | Not Likely | Moderate | Moderate | Remove console logging of errors | Yes |
| **A06:2021 – Vulnerable and Outdated Components** | Not Likely | Low | Low | None | No |
| **A07:2021 – Identification and Authentication Failures** | High | High | Moderate | Do not accept weak passwords | No, risk accepted |
| **A08:2021 – Software and Data Integrity Failures** | Likely | High | Moderate | None | No, risk accepted |
| **A09:2021 – Security Logging and Monitoring Failures** | Likely | Moderate | Low | Log events like authentication, failed authentication, etc. | No, risk accepted |
| **A10:2021 – Server-Side Request Forgery (SSRF)** | Not Likely | Severe | Low | None, no user-supplied URL’s are being used | No |

A01: Broken Access Control - Endpoints take into account whether a user is an admin or the owner of the specific resource.

A02: Cryptographic Failures - Sensitive data is being transported in plain text due to the use of HTTP. Currently it is not possible for me to use HTTPS or and cryptographic algorithms to encode sensitive data when sending it between the front and backend.

A03: Injection - SQL and JS injection is being automatically prevented by the technologies I use, more specifically JPA repository and React.

A04: Insecure Design - I believe that my application is securely designed, as I have followed the recommended design from the resources presented to us for the project and the recommendations I have found online.

A05: Security Misconfiguration - Currently there are a lot of places in my application where if something goes wrong, I am logging information that would be too sensitive for regular users to see.

A06: Vulnerable and Outdated Components - I do not use the most recent versions of a lot of my technologies, because they would be unstable, incompatible, or too difficult to implement.

A07: Identification and Authentication Failures - Currently, my application accepts weak passwords, and would also be vulnerable to attacks such as credential stuffing, but I am not capable of fixing the vulnerability to attacks, and I do not plan to change the password handling, as I find it is not that important to dedicate the time I would need to, realistically speaking.

A08: Software and Data Integrity Failures - SonarQube and NPM both protect my project against vulnerable libraries and modules.

A09: Security Logging and Monitoring Failures - I could start logging events like authentication requests and the other important events in my application, but I feel like that is not very necessary to do right now, seeing as there is very little time left to finish the projects.

A10: Server-Side Request Forgery - My application does not use user-supplied URL’s, therefore it is not at risk.