Individual Track Project

Web Application - Writeo

OWASP Report

|  |  |
| --- | --- |
|  | **Date : 22/12/2020** |
|  | **Version : 1.0** |
|  | **Author : Kristian Hadzhikolev** |

# A1 Injection

My Application does not give any unauthorized access to data, even if someone tries to load private information of other user of the application. The Application is resistant to SQL Injections. It uses Spring Boot Data and JPA Repositories to connect to the database, which are secure.

# A2 Broken Authentication

My Application uses JJWT(JSON Java Web Token) and Spring Boot Security to ensure that user profiles are safe from numerous attacks. Passwords are hashed and the application uses Bcrypt to decrypt them.

# A3 Sensitive Data Exposure

For now my application uses only hashed passwords, all the other data is not encrypted in the database in any way. However, there is not much sensitive data to be stolen at this moment. In the future, there will be added additional security.

# A4 XML External Entities

This security risk is not applicable for my project.

# A5 Broken Access Control

As mentioned in the first point the application does not allow users to access unauthorized data. There are different types of users with different types of roles: Author(can only access other authors’ public information), Admin(Can access all the information about any user, except the private articles of authors) and Owner(has the same privileges as an admin, but their profile cannot be deleted).

# A6 Security Misconfiguration

All the libraries used in the application are kept up-to-date so there is no vulnerability. The security configuration ensures that specific parts of the application can be only accessed by profile with access.

# A7 Cross-Site Scripting

My application avoids direct data injections.

# A8 Insecure Data Deserialization

This security risk is not applicable for my project.

# A9 Using Components with Known Vulnerabilities

This security risk is not applicable for my project.

# A10 Insufficient Logging and Monitoring

The API logs every action by users.