OWASP Security Report

Dimitar Prisadnikov

Contents

Version table 3
Intro 4
OWASP top security concerns (2021) 5
Conclusion 6

Version table

Version	Date	Action
1.0	15.12.22	Added OWASP table
1.1	16.12.22	Added intro and conclusion

Intro

Nowadays, there is a considerable number of different online attacks that should be prevented at any cost in order to ensure that data is protected and there is no misuse of recourses. The application I am developing is a household management tool using Java Spring Boot, React.js and MySQL database. In addition, I decided to implement identity access management with Auth0 which ensure secure authentication and authorization. Below is a table showing how the application deals, does not deal or is planning to deal with the top 10 security concerns for 2022.

OWASP top security concerns (2021)

	Likelihood	Impact	Risk	Possible actions	Status
Broken Access Control	Medium	Medium	**High**	Use roles for API authorization	Planned
Cryptographic Failures	High	High	**High**	Removing any sensitive data that is no longer needed; Hashing passwords using a strong hashing algorithm; Store JWT tokens in browser's memory	Finished
Injection	Low	High	**High**	Server-side input validation.	Won't do
Insecure Design	Medium	Medium	**Medium**	Use software to analyse the code and find security vulnerabilities (for example, Sonarqube)	Finished
Security Misconfiguration	Medium	High	**High**	Proper Spring Security config; Try to use a more standard Spring Sec config; remove test account from production	Finished
Vulnerable and Outdated Components	Low	Medium	**Medium**	Make sure all components and dependencies used are up to date. Remove unnecessary components.	Finished
Identification and Authentication Failures	Medium	Medium	**High**	Validate for weak or well-known passwords using a common password list; Hash the user's password using a strong hashing algorithm; Use vague login failure messages when your users enter an incorrect username or password	Finished
Software and Data Integrity Failures	Low	High	**Medium**	Use only verified images for the GitLab CI/CD pipeline; Store sensitive data in environment variable.	Finished (partially)
Security Logging and Monitoring Failures	Medium	High	**Medium**	Implement login for authentication and permission activities.	Finished (partially)
Server-Side Request Forgery (SSRF)	High	Medium	**High**	Sanitize and validate Inputs; Enforce URL schemas.	Wont'do

Conclusion

The application deals with most of the OWASP top 10 security concerns for 2021 on a basic to medium level with a few more changes coming in the future. Since the project is a web-based management tool, the focus is on providing proper authentication and authorization and keeping all the user data safely in the database. In addition, keeping passwords encrypted in the database is crucial. Since Auth0 is used for IAM, there is login activity monitoring, encrypted passwords that are separately stored from the rest of the data and minimal changes to the default Spring Boot configuration which prevent mistakes.