OWASP Report

NBA portal

Date	**:**	**15/06/2022**
Version	**:**	**0.1**
State	**:**	
Author	**:**	**Nikola Stankov**

Version history

Version	Date	Author(s)	Changes	State
0.1	15/06/2022	All members	Initial version	Finish

Distribution

Version	Date	Receivers

Table of contents

1. Introduction

This document's purpose is to show how the application NBA portal fits into the security risks determined by the OWASP top 10. We will go through each of the OWASP top 10 and analyze the project against these security risks as well as give explanation and reasoning about the state of the application security.

2. Analysis

OWASP	Likelihood	Impact	Risk	Actions possible	Planned
A1: Broken Access Control	Unlikely	Moderate	Low	N/A	No, risk accepted
A2: Cryptographic Failures	Unlikely	Severe	Low	N/A	No, risk accepted
A3: Injection	Very unlikely	Severe	Very low	Incorrect user input that has not been handled	N/A
A4: Insecure Design	Moderate	Moderate	Moderate	N/A	N/A
A5: Security Misconfiguration	Low	Low	Moderate	N/A	N/A
A6: Vulnerable and Outdated Components	Moderate	Moderate	Moderate	Something may break as there are too many dependencies some of which have unknown versions.	No, risk accepted
A7: Identification and Authentications Failures	Moderate	Moderate	Moderate	Breaches may be possible as the authentication is pretty simple as per the requirements for this project	No, risk accepted
A8: Software and Data Integrity Failures	Low	Low	Moderate	N/A	N/A

A9: Security Logging and Monitoring Failures	Moderate	Moderate	Low	N/A	N/A
A10: Server-Side Request Forgery	Moderate	Low	Low	N/A	N/A

3. Meaning

Despite the fact that I cannot say the application has a top standard security, I think it is secure enough based on the requirements of the educational program I am partaking in. While testing, I haven't come upon any severe risk failures. By no means does that mean the security aspect of the application cannot be improved, however, taking into account the requirements, deadlines and stored data and user actions in the application, I think the application is secure enough.

4. Conclusion

All in all, although not perfect the application is, in my opinion, secure enough. No sensitive data is being stored that can be exposed and the actual functionalities of the application do not suggest that a breach, even if it happens, will be of a high risk for any stakeholders or users, except for me, the creator of the app.