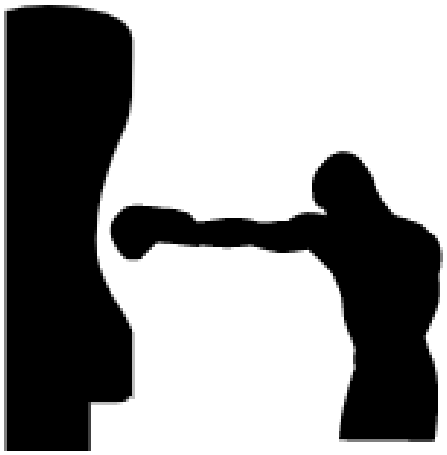
OWASP Top 10 security risks analysis



BOXVENT

Vlad Dumitru – 3367231

Student at Fontys University of Applied Sciences – S3CB04

Sprint 5

Document version 1.0

Contents

Analysing against the OWAP top 10 security risks

	Likelihood	Impact	Risk	Actions possible	Planned
A1: broken access control	Low	High	Low	Proper authentication and authorization. Role-based access control. Input validation and sanitization	Yes
A2: Cryptographic Failures	Low	High	Medium	Up-to Date encryption algorithms.	Yes
A3: Injection	Low	Medium	Low	Use prepared queries. Use input validation and sanitization. Use good injection resistant libraries.	Yes
A4: Insecure Design	Medium	High	High	Follow secure coding practices. Use secure libraries and frameworks. Regularly review and test the design of the application.	Yes
A5: Security Misconfiguration	Low	High	High	Force usage of strong passwords	Yes
A6: Vulnerable and Outdated Components	Low	High	Low	Use secure and regularly updated components	Yes
A7: Identification and Authentication Failures	Low	High	Low	Use strong, unique passwords. Implement strong authentication methods.	Yes

A8: Software and Data Integrity Failures	Low	High	Medium	Regularly review and test the integrity of the software and data in the application	Yes
A9: Secuity Logging and Monitoring Failures	Low	Low	Low	Implement logging and monitoring mechanisms. Regularly review and analyze logs.	No
A10: Server-Side Request Forgery	Low	High	Medium	Use input validation and sanitization. Implement measures to detect and prevent SSRF attacks. Use tools to monitor the application for SSRF attacks and other vulnerabilities.	Yes

Reasoning

Risk A1: Broken access control

refers to the failure of a system to properly restrict access to resources based on the defined access control rules. This can allow unauthorized users to access sensitive data or perform actions they should not have access to, leading to a high impact on the application. The likelihood of this risk occurring is low, as proper authentication and authorization measures such as role-based access control and input validation and sanitization have been planned to be implemented.

Risk A2: Cryptographic failures

refer to issues with the implementation or use of cryptographic algorithms, such as using weak or outdated library, or failing to properly secure the keys used for encryption. This can lead to sensitive data being compromised, resulting in a high impact on the application. The likelihood of this risk occurring is low, as up-to-date encryption algorithms are planned to be used.

Risk A3: Injection

refers to the injection of malicious code into a system through user input, such as through SQL injection. This can allow an attacker to access or manipulate sensitive data, and can have a medium impact on the application. The likelihood of this risk occurring is low, as measures such as prepared queries and input validation and sanitization are planned to be implemented.

Risk A4: Insecure design

refers to issues with the overall design of the application that can lead to vulnerabilities. This can have a high impact on the application, as a poorly designed application may have multiple vulnerabilities that can be exploited. The likelihood of this risk occurring is medium, as secure coding practices and the use of secure libraries and frameworks are planned to be followed, and the application will include multiple types of unit tests.

Risk A5: Security misconfiguration

refers to issues with the configuration of the system or application that can lead to vulnerabilities. This can have a high impact on the application, as a misconfigured system can be more easily exploited by attackers. The likelihood of this risk occurring is low, as measures such as enforcing the use of strong passwords are planned to be implemented.

Risk A6: Vulnerable and outdated components

refer to the use of components or libraries that have known vulnerabilities or are outdated, which can make the application more vulnerable to attacks. This can have a high impact on the application. The likelihood of this risk occurring is low, as secure and regularly updated components are used.

Risk A7: Identification and authentication failures

refer to issues with the identification and authentication of users, such as using weak or easily guessable passwords, or failing to properly implement strong authentication methods. This can allow unauthorized users to gain access to the application, and can have a low impact on the application. The likelihood of this risk occurring is low, as measures such as the use of strong passwords.

Risk A8: Software and data integrity failures

refer to issues with the integrity of the software or data being used by the application, such as tampering or corruption. This can have a medium impact on the application, as it can lead to incorrect or unreliable data being used or displayed. The likelihood of this risk occurring is medium, as the integrity of the software and data will be regularly reviewed and tested.

Risk A9: Security logging and monitoring failures

refer to issues with the implementation or use of logging and monitoring mechanisms, such as a lack of logging or the failure to regularly review and analyze logs. This can have a low impact on the application, as it can make it more difficult to detect and respond to security incidents. The likelihood of this risk occurring is low.

Risk A10: Server-side request forgery (SSRF)

refers to the exploitation of a vulnerability in a server that allows an attacker to send illegitimate requests to other servers on behalf of the vulnerable server. This can allow an attacker to access sensitive data or perform actions they should not have access to, and can have a high impact on the application. The likelihood of this risk occurring is medium, as measures such as input validation and sanitization, measures to detect and prevent SSRF attacks.

Conclusion

In conclusion, the security risks identified in this report all have the potential to have a significant impact on the application if not properly addressed. However, a variety of measures have been planned to mitigate these risks, such as the use of strong passwords, input validation and sanitization, and the implementation of secure coding practices. Based on these measures, it is believed that the application will be sufficiently secure. However, it is important to continuously review and test the security of the application to ensure that it remains secure against potential future threats.

References

OWASP Top 10:2021. (n.d.).

https://owasp.org/Top10/

Veracode. (n.d.). *OWASP Top 10 Vulnerabilities*.

https://www.veracode.com/security/owasp-top-10