Date: 24-06-2022

Group: S3-CB01

Student: Oleksandr Gurianov

Version: 1.0

Security Report

Table of content

OWASP Top 10

	Likelihood	***Impact***	***Risk***	***Actions possible***	***Planned***
A01: Broken Access Control	Low	Medium	Low	N/A	N/A
A02: Cryptographic Failures	Medium	High	High	• Encrypt all sensitive data at REST • Keys should be stored in memory as byte arrays	No, risk accepted
A03: Injection	Low	High	Medium	• Use LIMIT and other SQL controls within queries	No, risk accepted
A04: Insecure Design	Low	High	Medium	• Write unit and integration tests	No, risk accepted
A05: Security Misconfiguration	Low	High	Medium	• Remove unused features and frameworks	No, risk accepted
A06: Vulnerable and Outdated Components	Medium	Medium	Medium	• Remove unused dependencies, unnecessary features, components, files, and documentation	No, risk accepted
A07: Identification and Authentication Failures	Medium	High	High	• Do not deploy with any default credentials • Implement weak password checks • Limit or increasingly delay failed login attempts	No, risk accepted
A08: Software and Data Integrity Failures	Medium	High	High	• Ensure libraries and dependencies are consuming	No, risk accepted

				trusted repositories	
A09: Security Logging and Monitoring Failures	Low	Medium	Low	N/A	N/A
A10: Server-Side Request Forgery	Low	High	Medium	- Do not send raw responses to clients	No, risk accepted

Reasoning

- ***A01:*** The Low Security Risk means that the Broken Access Control vulnerability does not possess any danger to the current version of the application and its likelihood is little. However, a possible impact of this vulnerability on the application can lead to unlawful data alteration, deletion, or disclosure, as well as carrying out a business task that is beyond the user's authority.
- ***A02:*** The High Security Risk means that the Cryptographic Failures vulnerability possesses severe danger to the current version of the application, but its likelihood is moderate. This vulnerability impacts the application in a way that can lead to revealing private information such as passwords, credit card numbers, health information, personal information, trade secrets, etc.
- ***A03:*** The Medium Security Risk means that the Injection vulnerability possesses moderate danger to the current version of the application, but its likelihood is little. This vulnerability can impact the application in a way that leads to system compromise, service denial, data loss, loss of data integrity, and data theft.
- ***A04:*** The Medium Security Risk means that the Insecure Design vulnerability possesses moderate danger to the current version of the application, but its likelihood is little. This vulnerability can impact the application in a way that leads to web application compromise or leaking of sensitive information.
- **A05:** The Medium Security Risk means that the Security Configuration vulnerability possesses moderate danger to the current version of the application, but its likelihood is little. This vulnerability can impact the application in a way that leads to a significant data breach and has financial ramifications, including a temporary loss of business, lost clients owing to a lack of trust (and hence, lost revenue), penalties through litigation, and perhaps regulatory fines.
- ***A06:*** The Medium Security Risk means that the Vulnerable and Outdated Components vulnerability possesses moderate danger to the current version of the application and its likelihood is moderate as well. This vulnerability can impact the application in a way that leads to, for example, enabling the installation of malicious software on the application server by attackers.
- ***A07:*** The High Security Risk means that the Identification and Authentication Failures vulnerability possesses severe danger to the current version of the application, but its likelihood is moderate. This vulnerability impacts the

application in a way that can lead to allowing automated attacks, default/weak/well-known passwords, session identifier exposure in the URL, or reuse of session identification after successful login.

- ***A08:*** The High Security Risk means that the Security Logging and Monitoring Failures vulnerability possess severe danger to the current version of the application, but its likelihood is moderate. This vulnerability impacts the application in a way that can lead to increasing the possibility of unauthorized access, malicious code, or system breach, enabling attackers to distribute and use their updates of plugins, libraries, modules, repositories, and CDNs.
- ***A09:*** The Low Security Risk means that the Security Logging and Monitoring Failures vulnerability does not possess any danger to the current version of the application and its likelihood is little. However, a possible impact of this vulnerability on the application can lead to the undetectability of the breaches making the application vulnerable to information leakage by making logging and alerting events visible to a user or an attacker.
- ***A10:*** The Medium Security Risk means that the Server-Side Request Forgery (SSRF) vulnerability possesses moderate danger to the current version of the application, but its likelihood is little. This vulnerability can impact the application in a way that leads to enabling the attacker to trick the program into sending a forged request to an unanticipated recipient, even when it is shielded by a firewall, VPN, or another kind of network access control list (ACL).

Conclusion

In conclusion, the majority of the time, all of the aforementioned vulnerabilities result in either data loss or a security breach that gives attackers access to the web application's exposed data in a variety of different ways.

However, the OWASP Top 10 analysis of the current version of my project reveals that all of these vulnerabilities have a low to medium risk of being exploited, making the application reasonably secure and protected against various types of breaches. However, as indicated before in the analysis, the application security still has to be improved.