**OWASP Report**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Likelihood | Impact | Risk | Action Possible | Planned |
| A01: Broken Access Control | Unlikely | Unauthorized access, data breaches, information disclosure | High risk if not properly managed, unauthorized users gaining access to sensitive info | Implement proper access controls, role-based access management | N/A |
| A02: Cryptographic Failures | Might Happen | Data exposure, compromised confidentiality, and integrity of sensitive information | High risk, especially if the cryptographic algorithms and implementations are weak or outdated | Use strong encryption algorithms, keep cryptographic libraries updated | N/A |
| A03: Injection | Unlikely | Data manipulation, unauthorized access, and potential data loss | High risk, as injection attacks can lead to the execution of malicious code on the system. | Input validation, parameterized queries, and using prepared statements to prevent injection attacks | N/A |
| A04: Insecure Design | Might Happen | System vulnerabilities, potential exploits, and unauthorized access | High risk, as insecure design can create a foundation for various security issues | Conduct secure design reviews, follow secure coding practices | N/A |
| A05: Security Misconfiguration | Unlikely | Unauthorized access, data exposure, and system vulnerabilities | Moderate to high risk, as misconfigurations can lead to security gaps | Regularly audit configurations, follow security best practices for server and application settings | N/A |
| A06: Vulnerable and Outdated Components | Unlikely | Exploitation of known vulnerabilities, potential security breaches | High risk, especially if software components are not regularly update | Use up-to-date libraries and frameworks, and regularly scan for vulnerabilities | N/A |
| A07: Identification and Authentication Failures | Might Happen | Unauthorized access, identity theft, and compromised user accounts | High risk, as weak or compromised authentication can lead to unauthorized access | Implement strong authentication mechanisms and multi-factor authentication | N/A |
| A08: Software and Data Integrity Failures | Unlikely | Data manipulation, corruption, and loss of trust in the system | High risk, as integrity failures can lead to unreliable data | Implement integrity checks, use digital signatures, and ensure secure data transmission | N/A |
| A09: Security Logging and Monitoring Failures with Known Vulnerabilities | Unlikely | Inability to detect and respond to security incidents, potential data breaches | High risk, as monitoring and logging are essential for identifying and responding to security events | Regularly review and update logging and monitoring tools and ensure proper configuration | N/A |
| A10: Server-Side Request Forgery | Unlikely | Unauthorized access to internal resources, data exposure | High risk, as it allows attackers to make requests on behalf of the server | Validate and sanitize user input, use whitelists for allowed resources, and implement proper server-side controls | N/A |

**Explanation:**After using Swagger UI, the cases that I marked as “Unlikely”, means that they are safe, and in the cases that I marked as “Might Happened”, means that there is a possibility that unauthorized user break them. If anything goes wrong, I noted the Impacts and Risks related to OWASP security violations, along with possible actions to take.