**OWASP Report**

For Individual track project S3

Logo

Description automatically generated with medium confidence

Student name: Kristian Kolev

Student number: 4154738

Class: S3-CB04

Contents

[1. Analyze 3](#_Toc90672599)

[2. Reasoning 4](#_Toc90672600)

# Analyze

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Likelihood | Impact | Risk | Actions possible | Planned |
| A1: Broken access control | High | High | Critical | Implement role-based authentication mechanism | Yes |
| A2: Cryptographic Failures | Medium | High | High | Encrypt all the sensitive information | Yes |
| A3: Injection | Low | Medium | Low |  | Yes |
| A4: Insecure design | Low | Low | Low | Make unit test for both the happy and bad scenarios | Yes |
| A5: Security Misconfiguration | Medium | Medium | Medium | Do not return error messages to the user because they can expose vulnerabilities | Yes |
| A6: Vulnerable and Outdated Components | Low | Low | Low | Remove all the unused files, features, dependencies, etc. | Yes |
| A7: Identification and Authentication Failures | Low | Medium | Low | Implement checks for weak credentials, limit the failed login attempts and log them | No |
| A8: Software and Data Integrity Failures | Medium | Medium | Medium | Make CI/CD deploy properly to ensure the integrity of the code | Yes |
| A9: Security Logging and Monitoring Failures | Low | Low | Note |  | No |
| A10: Server-Side Request Forgery | Low | Medium | Low |  | No |

# Reasoning

While measuring the security risk, it is important to consider the possibility of a malicious user finding and exploiting vulnerabilities and how impactful that would be. The risk is determined closely by the amount of data that is being impacted during the attack. Even if my application starts being used by real restaurants, most of the risks will still remain the same.