**Security Report**

***DaClothes***

*Fontys*

|  |
| --- |
| **Date : 22.12.2023** |
| **Version : 1.0** |
| **State : Finished** |
| **Author : Rodrigo Bedoya** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk Name | Likelihood | Impact | Risk Level | Actions Possible | Planned |
| A1: Broken Access Control | Likely | Severe | High | |  |  |  | | --- | --- | --- | |  | Access controls at the server-side via roles and disabling certain UI elements based on the user's role |  | | Yes |
| A2: Cryptographic  Failure | Very unlikely | Severe | Low | Use strong cryptographic algorithms and ensure proper key management | Yes |
| A3: Injection | Unlikely | Severe | High | Use parameterized queries | Implement input validations to prevent client-side injection attacks. |
| A4: Insecure Design | Unlikely | Medium | Medium | Review application architecture and design every sprint for design flaws | Yes |
| A5: Security Misconfiguration | Unlikely | Severe | High | Follow secure coding practices and principles, and ensure that client-side configuration do not expose sensitive information | Yes |
| A6: Vulnerable and Outdated Components | Unlikely | Low | Low | Follow best practices, monitors security advisories via SonarQube and consult with teachers. | Yes |
| A7: Identification and Authentication failures | Unlikely | Severe | Low | Use authentication mechanisms like JWT and strong password encryption like BCrypt, and use session management | Yes |
| A8: Software and Data Integrity failures | Likely | Severe | Medium | Implement data integrity tests and secure software practices | Yes |
| A9: Security logging and monitoring failures | Unlikely | Low | Medium | Implementing alerting with exceptions and proper error handling and logging on the client side | Yes |
| A10: Server-side request forgery | Very Unlikely | Severe | Medium | Implement input validation and restrict access with CORS configurations | Yes |