

Security report adventurehub

By Arenco Meevissen



16 december 2022

**Revision Table**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | change(s) |
| 1.0 | 25/11/2022 | Arenco Meevissen | Initial document |
|  |  |  |  |
|  |  |  |  |

Contents

[Analysing security risks in my project 3](#_Toc122088458)

[Conclusion 4](#_Toc122088459)

[What I did 4](#_Toc122088460)

[What needs to happen? 4](#_Toc122088461)

[Why I didn’t do it ? 4](#_Toc122088462)

# Analysing security risks in my project

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Likelihood | | | | |
| Very unlikely | Unlikely | Likely | Moderate | High |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Impact | | | | |
| Very low | Low | Moderate | High | Severe |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk | | | | |
| Very low | Low | Moderate | high | Severe |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| OWAP risks | Likelihood | impact | Risk | Actions | Planned |
| A01:2021-Broken Access Control | Unlikely | Severe | Moderate | Limit access to sensitive pages, fixed | yes |
| A02:2021-Cryptographic Failures | Very unlikely | Severe | Low | Don’t send back sensitive information that shouldn’t be given e.g. passwords, fixed | yes |
| A03:2021-Injection | Unlikely | High/ Severe | Very Low/ Low | Validate input from the frontend first, then another time in the backend | Yes |
| A04:2021-Insecure Design | Unlikely | Moderate | Moderate | Limit resource consumption by user or service | No, risk accepted |
| A05:2021-Security Misconfiguration | Unlikely | High | Moderate | Check access where user can go and reach, fixed | Yes |
| A06:2021-Vulnerable and Outdated Components | Likely | Moderate | Moderate | Remove unused dependencies, features, components and files | Yes |
| A07:2021-Identification and Authentication Failures | Unlikely | High/severe | High | Implement password checks, limit login attempts | Yes, till a certain extend no checks for account attacks and brute force attacks |
| A08:2021-Software and Data Integrity Failures | Moderate | Moderate/ High | Low | Limit libraries that need to be used, not using libraries not getting security updates | Yes, but can’t check every library used |
| A09:2021-Security Logging and Monitoring Failures | Unlikely | High | Moderate | Log the login and logout, | No, risk accepted |
| A10:2021-Server-Side Request Forgery | Moderate | Moderate | Moderate | Enforce “deny by default” firewall policies | Between, although in configuration I deny any request that doesn’t exist in the config there could be a chance it still can happen and I accept it |

# How it was determined

I determined for each case the likelihood with the following method:

I determined for each case the Impact with the following methods

I determined for each case the Risk in the way of:

# Conclusion

Everything where is did say yes on from the table above is being implemented and watched on. Where as the no’s are not necessarily looked into and can just be passed. At number 10 there is a between now this is exactly how it’s being treated just the basic premise is being looked into but not the bigger things

What needs to happen is the actions explained in the table above and some other minor things that are not added to this column that could easily be added.

I didn’t do some of these risk because I don’t have necessarily have the time to do some of the prevention measures that could be done and some are not possible because of the hardware that is available to me such as the security logging.