Security Report

VENDOR Online MARKETPLACE

Robert Enuta

2021

Contents

[Project Assignment 2](#_Toc84619813)

[1. Context 2](#_Toc84619814)

[2. Goal of the project 2](#_Toc84619815)

[3. Scope and preconditions 2](#_Toc84619816)

[Software Architecture 3](#_Toc84619817)

# Context

Vendor is an online marketplace where users can sell and buy items. The main purpose of the app is making buying and selling as easy and as safe as possible. This is achieved by allowing the user to rate the experiences they had with others and making it obvious when something shady is happening. Users will be dissuaded to interact with malicious sellers and if an account keeps getting reported it will be banned from buying or selling anymore.

After selecting an item to buy, the user will enter a conversation with the seller and discuss the details. And after settling on a price and the delivery, the seller is supposed to take care of the rest themselves.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Likelihood | Impact | Risk | Actions possible | Planned |
| A1: Broken Access Control | High | Moderate | Moderate | Implementing OAuth2 and JWT Tokens | Yes |
| A2: Cryptographic Failures | Low | Low | Low | Changing the way headers work and adding a random element to them | Yes |
| A3: Injection | Moderate | High | High | Server-side input validation | No |
| A4: Insecure Design | Moderate | High | Moderate | Tests and peer reviews, adding plausibility checks | Yes |
| A5: Security Misconfiguration | Low | Moderate | Moderate | Updating and removing unneeded components, changing or removing default accounts | Yes |
| A6: Vulnerable and Outdated Components | Low | Low | Low | Removing unnecessary dependencies and files | Yes |
| A7: Identification and Authentication Failures | Medium | High | Moderate | Implementing multi-factor authentication | No |
| A8: Software and Data Integrity Failures | Low | Medium | Low | CI/CD pipeline is properly configured, encrypt serialized data | Yes |
| A9: Security Logging and Monitoring Failures | Low | Low | Low | Log and encrypt logs | No |
| A10: Server-Side Request Forgery | High | Medium | High | Disable HTTP redirects, sanitize and validate client input | No |