Some of the OWASP Top Ten vulnerabilities in the code and how to address them include:

- A2:2017: Broken Authentication/A7:2021 Identification and Authentication Failures due to the code not implementing proper authentication mechanisms.
    - Implement proper authentication and session management using secure tokens (i.e. JWT) and ensure secure password storage.
- A3:2017 Sensitive Data Exposure/A2:2021 Cryptographic Failures due to passwords being stored in plain text in local storage.:
    - Hash passwords before storing them using a strong hashing algorithm (i.e. bcrypt).
- A5:2017 Cross-Site Request Forgery (CSRF)/A1:2021 Broken Access Control due to forms not including CSRF tokens.
    - Implement CSRF protection by including CSRF tokens in forms and validating them on the server side.
- A6:2017 Security Misconfiguration/A5:2021 Security Misconfiguration due to the application not enforcing HTTPS.
    - Ensure that the application enforces HTTPS to protect data in transit.
- A7:2017 Cross-Site Scripting (XSS)/A3:2021 Injection due to user input being directly inserted into the DOM without sanitization.
    - Sanitize user inputs before inserting them into the DOM using libraries (i.e. DOMPurify to clean HTML inputs).
- A8:2017 Insecure Deserialization/A8:2021 Software and Data Integrity Failures due to data from localStorage being directly parsed and used.
    - Validate and sanitize data retrieved from localStorage before using it.

Notes taken on vulnerabilities while developing features for each module as defined per Sprint:

1. Having the same/similar names for IDs and other variables.
2. Module 4 allowing the user to simply reset password without verifying it is them (anyone could use an email and simply reset the password).
3. Saving data locally is dangerous.
4. Not casting username to either upper or lower case in case the user stores the data in one case and inputs in another (i.e. camel case).
5. Lack of input sanitization on user inputs before using it makes data vulnerable to cross-site scripting (XSS) attacks.
6. When creating a new account requirements only ask for an e-mail address (input type email) however when logging in it ask for a username (input type text) which could cause complications (i.e. creating a new account with an e-mail however having “admin” as a user).