Sawyer Kent

Cybersecurity Assessment

The cybersecurity assessment identified several key areas where improvements were recommended to enhance the overall security, privacy, and reliability of the application. One of the primary recommendations was to ensure that all sensitive information, such as API keys and service credentials, is stored securely using environment variables rather than being hardcoded into the source code. To address this, all sensitive keys were moved into environment configuration files, and these files were excluded from version control using a `.gitignore` policy. Additionally, only public-facing keys are exposed on the client side, while more sensitive service role keys are kept securely on the server. This recommendation has been fully implemented.

Another major area of concern involved protecting the application from injection attacks, particularly within the database layer. The recommendation was to ensure that all database interactions are handled securely and that proper access controls are enforced. In response, the application uses Supabase client libraries, which inherently support parameterized queries and reduce the risk of SQL injection. Furthermore, Row Level Security (RLS) has been enabled across all database tables, with carefully defined policies that restrict users to accessing and modifying only their own data. The use of raw SQL queries has also been minimized. These measures have been fully implemented.

The assessment also highlighted the importance of ensuring that any external links shared within the application are safe for users to access. To mitigate potential risks, basic URL validation has been implemented to check links before they are opened. Where possible, links are restricted to trusted domains, and external content is opened using system-level protections provided by the device's default browser. While these protections provide a solid baseline, more advanced filtering and verification mechanisms may be introduced in the future. As a result, this recommendation has been partially implemented.

In terms of authentication and session management, the recommendation was to ensure that user accounts and sessions are handled securely. The application uses Supabase's authentication system to manage user login and session handling. Email verification has been implemented for new accounts, and session management practices have been reviewed to ensure expired sessions are handled appropriately. This area has been fully implemented.

The protection of user data and privacy was another important focus of the assessment. It was recommended that the application minimize the amount of sensitive data stored and enforce strict access controls. In response, only necessary user information is stored, and access to profile data is controlled based on user permissions. Additional privacy features, such as blocking and more granular user controls, are currently being developed. Therefore, this area is still in progress.

Input validation and error handling were also identified as areas for improvement. The recommendation was to validate all user inputs and ensure that errors do not expose sensitive system information. Basic validation has been implemented for user inputs such as profile fields and user-generated content, and error handling has been improved to reduce the likelihood of crashes or unintended information disclosure. However, further refinement is planned, making this recommendation partially implemented.

The security of file uploads, particularly user profile images, was also addressed. The recommendation was to ensure that only safe file types are accepted and that uploads are handled securely. The application now restricts uploads to specific image formats and compresses files before uploading to reduce size and improve efficiency. Files are stored using Supabase Storage with appropriate access controls in place. This recommendation has been fully implemented.