Security report

Protection against Man-in-the-middle attacks

1. **Password-reset**
   For the password-reset feature, a JSON web token is being used to securely transmit a password reset link to the user. The token is signed to ensure the integrity of the claims contained within it. The chosen algorithm for the token, HMAC512, is constructed from the SHA-512 hash function. Thus, in the event of an unwanted interception, an attacker will not be able to decrypt it. In addition, the token expiration time is set to 3600s, which leaves very little time for the attacker to do harm.

Protection against malicious file uploads

1. **JSON file upload**
   JSON file upload option is a feature only available to admins. Whenever the user navigates to a page where this option is available, their session token is checked to verify the identity of the user and to ensure that the user is an administrator. (note the session token is unique, randomly generated and has an expiration time). After confirming the user's identity, he gets an option to upload the json; code only allows json file extensions and one file at a time.

Protection against Stored XSS

1. **Input sanitization**
   The majority of input fields, including login, registration, where a criminal can enter a malicious code, are being sanitized, only allowing a certain set of characters. For instance, for email feld, a regex is being used defining a whitelist of the allowed characters. Whitelist characters are also used for json upload input fields.