Documentation Scaffold

## Data Dictionary

This section tracks all variables and data structures used throughout the API to ensure proper management and security.

## Static Application Security Test (SAST)/ Vulnerability assessment

In this section, document the vulnerabilities found through SAST and how they were resolved at each development stage. Provide an analysis of all vulnerabilities identified in the API throughout development, and explain the applied solutions. Provide code samples of before and after with evidence.

### SAST Documentation

- Stage 1 - Basic Security:  
 - Password Hashing:  
 - Issue: Password stored in plain text.  
 - Fix: Implemented crypt for secure password hashing.  
 - Input Validation:  
 - Issue: User input not validated.  
 - Fix: Added strict validation rules to ensure valid input types.  
 - Input Sanitisation:  
 - Issue: API is vulnerable to XSS attacks.  
 - Fix: Input sanitisation implemented for all user inputs.  
  
- Stage 2 - Intermediate Security:  
 - Session Management:  
 - Issue:   
 - Fix:   
 - CSRF Protection:  
 - Issue:   
 - Fix:   
 - Race Conditions:  
 - Issue:   
 - Fix:   
  
- Stage 3 - Advanced Security:  
 - Invalid Forwarding:  
 - Issue:   
 - Fix:   
 - Issue:   
 - Fix:

## Dynamic Application Security Test (DAST)

Document the vulnerabilities found during DAST and how runtime attacks were mitigated.

### DAST Documentation

- Vulnerabilities Detected:  
 - XSS vulnerability in user input forms.  
 - Insecure API endpoints exposed to unauthorised access.  
  
- Fixes:  
 - Applied input sanitisation for all forms.  
 - Implemented authentication checks for all API requests.

## Penetration Test

After applying security fixes, simulate attacks to test the robustness of your API.

### Penetration Test Documentation

- Test Details:  
 - Simulated SQL injection on login and user data endpoints.  
 - Tried brute-force attacks on login page.  
  
- Outcomes:  
 - SQL injection attempts failed due to parameterised queries.  
 - Brute-force protection in place via rate-limiting and account lockout.