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.

## Stage 1 - Basic Security:

**Password Hashing:**

Issue: Password stored in plain text

Solution:

|  |
| --- |
|  |

**Input Validation:**

Issue: User input not validated.

Solution:

|  |
| --- |
|  |

**Input Sanitisation:**

Issue: API is vulnerable to XSS attacks.

Solution:

|  |
| --- |
|  |

Stage 2 - Intermediate Security:

**Session Management:**

Issue:

Solution:

|  |
| --- |
|  |

**CSRF Protection:**

Issue:

Solution:

|  |
| --- |
|  |

**Race Conditions:**

Issue:

Solution:

|  |
| --- |
|  |

## Stage 3 - Advanced Security:

**Invalid Forwarding:**

Issue:

Solution:

|  |
| --- |
|  |

**Token Validation:**

Issue:

Solution:

|  |
| --- |
|  |

## Dynamic Application Security Test (DAST)

An extensive and accurate evaluation of the effectiveness of your software engineering solution including security vulnerabilities and how they were fixed.

Vulnerabilities Detected:

E.g. XSS vulnerability in user input forms or Insecure API endpoints exposed to unauthorised access.  
  
**Evaluation:**

|  |
| --- |
|  |