Security Test Plan

The purpose of this test plan is to outline the strategies of the security testing for the Open Customer Data API in a high-level.

Scope:

The following areas will be focused on this test plan:

* Authorization mechanism
* Data Validation

Objectives:

The objective is to ensure:

* Only authorized users can access the API.
* Users input is properly validated.
* Protect sensitive data.

Test Environment:

Server: ‘localhost:8080/test-api’

Tools: Postman.

**Test Cases**

Authorization

1. Test Case: Verify the API endpoints require valid Authorization headers.
   1. Description: Send requests with and without valid Authorization headers.
   2. Expected Result: Requests without valid Authorization headers should be denied and return a 403 Forbidden response which means the server refuses to authorize the request.

Data Validation

1. Test Case : Validate sensitive data is not exposed in response or logs.
   1. Description: Inspect API response for sensitive information (tokens, passwords, etc).
   2. Expected Result: Sensitive data should be masked or not included in the responses.

Vulnerabilities discovered and Recommendations:

Vulnerability: Financial and token data exposure in responses and logs

* Mitigation Strategy: Mask or encrypt sensitive data in responses or logs, using TLS/SSL protocols.