Security and Testing Report

Project Title

Donation Management Mobile Application (Flutter-Based)

Prepared By

Esmael Shikur – Security & Testing

Betselot Ertumo – Security & Testing

1. Introduction

This report documents the security and testing activities carried out for the Donation Management Mobile Application. The application aims to connect donors, hotels, and NGOs through a unified platform to reduce food and item wastage. The purpose of this report is to demonstrate that the system was tested for functionality, reliability, and security before final submission.

Testing and security validation were conducted to ensure that the application meets its functional requirements and protects user data through proper authentication and authorization mechanisms.

2. Testing Objectives

The main objectives of testing were:

- To verify that all core features work as expected

- To ensure secure user authentication and authorization

- To validate role-based access control (RBAC)

- To detect and report functional and security-related bugs

- To ensure data integrity throughout the donation workflow

3. Testing Strategy and Methodology

Due to time constraints, **manual testing** was primarily used. Testing was performed continuously during development and before final submission.

3.1 Types of Testing Performed

- Functional Testing
- Integration Testing
- Security Testing
- API Testing
- User Acceptance Testing (UAT)

3.2 Tools Used

- Postman (API testing)
- Flutter application (manual UI testing)
- Browser Developer Tools
- GitHub (bug reporting and coordination)

4. Functional Testing

4.1 User Authentication Testing

Authentication was tested to ensure only registered users can access the system.

Test Case	Expected Result	Status
Valid login credentials	Successful login	Passed
Invalid password	Error message displayed	Passed
Empty input fields	Validation error	Passed
Expired JWT token	Redirect to login	Passed

4.2 Role-Based Access Control Testing

Each role was tested to confirm access restrictions.

Role	Allowed Actions	Result
Donor / Hotel	Post donations	Passed
NGO	Browse and accept donations	Passed
Admin	Verify NGOs and monitor activities	Passed
NGO posting donation	Access denied	Passed
Donor verifying NGO	Access denied	Passed

4.3 Donation Workflow Testing

The complete donation lifecycle was tested:

Posted → Accepted → Completed

Workflow Step	**Result**
Donation posted by Donor/Hotel	Passed
Donation visible to NGO	Passed
Donation accepted by NGO	Passed
Status update reflected correctly	Passed
Donation marked as completed	Passed

5. API Testing

Backend APIs developed using Express.js were tested using Postman.

5.1 Tested API Endpoints

- POST /login
- POST /register
- GET /donations
- POST /donations
- PUT /donations/:id

5.2 API Security Validation

- JWT token required for protected routes
- Unauthorized requests returned HTTP 401
- Role-based restrictions enforced at API level

All tested APIs responded correctly and securely.

6. Security Testing

6.1 Authentication Security

- JWT-based authentication implemented
- Tokens validated on each protected request
- Expired or invalid tokens rejected

6.2 Authorization Testing

- Unauthorized role access was tested
- Admin-only routes protected
- Donor and NGO privileges restricted appropriately

6.3 Input Validation

- Empty and invalid inputs tested
- Email format validation confirmed
- Long text and special characters handled correctly

6.4 Common Vulnerabilities Checked

Threat	Mitigation
Unauthorized access	JWT authentication
SQL Injection	Parameterized PostgreSQL queries
Data exposure	Role-based access control
Token misuse	Token expiration handling

7. Bug Tracking and Issue Management

Any bugs identified during testing were reported to the development team through GitHub issues or direct communication. Most issues were resolved before final submission, while minor UI improvements were documented for future enhancement.

8. Limitations

- Automated testing was not implemented due to time constraints
- Performance and load testing were not conducted

These can be added in future versions of the system.

9. Conclusion

The Donation Management Mobile Application was tested for functionality and security using manual testing methods. Core features, authentication, authorization, and donation workflows function correctly. Security mechanisms such as JWT authentication and role-based access control successfully prevent unauthorized actions. The system is stable and suitable for initial deployment.

10. Future Recommendations

- Implement automated testing using Jest or Flutter testing framework
- Add performance and load testing
- Enhance security with token refresh mechanisms
- Add detailed audit logs for admin monitoring