ThriftMedia Application and Services Requirements Document

Functional and Non-Functional Requirements

# 1. Introduction

ThriftMedia is a digital platform designed to connect businesses and consumers through curated media experiences. The solution consists of a public-facing website, a business owner administration website, a mobile application, and a data ingestion backend. This document outlines the functional and non-functional requirements for the ThriftMedia ecosystem, with a special emphasis on secure coding practices and compliance with OWASP Top Ten security recommendations.

# 2. Functional Requirements

## 2.1 Public-Facing Website

* Consumers can browse content, media, and business listings without registration.
* Registered consumers can create, manage, and personalize their profiles.
* Search and filter functionality for finding media and businesses.
* Responsive design for desktop, tablet, and mobile web browsers.
* Support for OAuth 2.0 authentication and authorization for consumer accounts.
* Display business promotions, offers, and featured media.
* To generate revenue, the public-facing website will incorporate advertising through platforms such as Google Ads and/or Microsoft Ads. These ads will be integrated seamlessly within the consumer experience, ensuring that promotional content is relevant and non-intrusive. Advertisements will comply with industry standards for privacy and security, aligning with the platform’s commitment to secure coding and consumer data protection.
* Notably, the website will not provide an ecommerce option; instead, its primary goal is to encourage and increase in-person visits to the local thrift store. All online features are designed to showcase available inventory, share promotions, and highlight special events, motivating consumers to explore offerings firsthand at the physical location.
* There will not be a requirement to register with the website to browse inventory.
* Allow consumers to provide feedback or reviews on the content or businesses.
* Ensure that user-generated content is moderated to prevent inappropriate or harmful content.
* SEO Optimization: Including requirements for search engine optimization to improve the website's visibility.
* The website will use location services to narrow the search of media to the consumer’s location (e.g., stores within a radius of the consumer's location). There will be an option to disable this if the consumer desires.

## 2.2 Business Owner Administration Website

* Secure login for business owners via Oauth 2.0.
* Business profile management: create, edit, and delete business information.
* Media upload and content management (images, videos, promotions).
* Analytics dashboard for tracking engagement, views, and performance metrics.
* Access management for multiple business team members with role-based permissions.
* Data export options (e.g., CSV, PDF) for reports and analytics.
* Notification management for promotions and campaigns.

## 2.3 Mobile Application

* Available on iOS and Android platforms.
* Secure user registration, authentication, and profile management, supporting Oauth 2.0.
* Enables store owners to capture photos of media items (books, audio, video) directly within the store environment and post them to their inventory through the app.
* In-app feedback and support channels for store owners.
* Deep integration with device features such as the camera (for inventory photo capture), maps, and notifications.
* Offline Functionality: Allowing certain features to be accessible even when the user is offline.
* Push Notifications: Enabling push notifications for important updates.

# 2.4 Data Ingestion Backend

* Automated receipt and processing of media data and images uploaded by store owners via the mobile app, posting new items to the store’s inventory database.
* APIs to support real-time data input from partners, businesses, store owners, and third-party content providers.
* Robust data validation, transformation, and normalization processes to ensure inventory accuracy.
* Continuous monitoring and logging of all ingestion activities for reliability and traceability.
* Support for scheduled data updates to the inventory system.
* Secure internal endpoints, protected by authentication and authorization controls.

## 2.4 Data Ingestion Backend

* Automated ingestion of media and business data from verified sources.
* APIs for data input from partners, businesses, and third-party content providers.
* Data validation, transformation, and normalization services.
* Monitoring and logging of data ingestion processes.
* Support for scheduling and real-time data updates.
* Secured internal endpoints with authentication and authorization controls.
* Screen for pornographic content.

## 2.5 General Functional Requirements

* Multi-language support for key user interfaces.
* Accessibility compliance (WCAG 2.1 or higher).
* Comprehensive audit trails for critical actions.
* Logging and monitoring of user activities for security and performance.

# 3. Non-Functional Requirements

## 3.1 Security

* All authentication and authorization must utilize Oauth 2.0 flows with best practices for token security.
* All user data in transit must be encrypted using TLS 1.2 or above.
* Data at rest must be encrypted using industry-standard algorithms.
* Input validation and output encoding must be enforced to prevent injection attacks.
* Session management must use secure, HttpOnly cookies and follow strict timeout policies.
* Implement rate limiting and account lockout to prevent brute-force attacks.
* Comprehensive logging of security events and anomaly detection.

## 3.2 Secure Coding Practices (OWASP Top Ten Emphasis)

* Injection Prevention: Use parameterized queries and ORM frameworks to avoid SQL, NoSQL, and command injection vulnerabilities.
* Authentication & Session Management: Enforce strong password policies, multi-factor authentication, and secure session handling.
* Sensitive Data Exposure: Ensure all sensitive information is encrypted and never logged in plaintext.
* XML External Entities (XXE) Protection: Disable external entity processing and validate XML inputs.
* Access Control: Enforce least privilege and proper authorization checks at every layer.
* Security Misconfiguration: Automate security configuration management and conduct regular vulnerability scans.
* Cross-Site Scripting (XSS): Apply output encoding and sanitize all user inputs.
* Insecure Deserialization: Avoid deserializing objects from untrusted sources.
* Using Components with Known Vulnerabilities: Maintain up-to-date dependencies and regularly patch third-party libraries.
* Insufficient Logging & Monitoring: Ensure real-time logging of security events and establish alerting mechanisms.

## 3.3 Performance

* The system must maintain average response times below 1 second for 95% of user interactions.
* Support at least 10,000 concurrent users across platforms.
* Scalable cloud-based infrastructure with load balancing and auto-scaling capabilities.

## 3.4 Availability & Reliability

* 99.9% uptime, excluding planned maintenance windows.
* Automated backups and disaster recovery plans in place.
* Redundant architecture to prevent single points of failure.

## 3.5 Usability

* Intuitive user interface with clear navigation and responsive feedback.
* Accessibility features for users with disabilities.
* Consistent experience across devices and platforms.

# 4. Compliance and Best Practices

* Adherence to data privacy regulations (e.g., GDPR, CCPA) as applicable.
* Annual security audits and regular penetration testing.
* Continuous staff training on secure coding and privacy practices.

# 5. Appendices

* Definitions and acronyms
* References to OWASP Top Ten: [[URL]/]
* List of supported browsers, devices, and OS versions