Republic of Yemen
Ministry of Higher Education & Scientific Research
AL-Rasheed Private University
Computer Science & Information Technology

Secure Software Engineering

Lab04: Requirements Identification

Mohammed Alqmase

12/18/2024

SUBSYSTEM NAME: *Judicial Management System*

GROUP NAMES:

1. *Mohammed Qasabah*
2. *Mazen Al-ammari*
3. *Mohanned Shaaf*
4. *Mohammed Al-howshabi*

Secure Software Engineering

Lab04: Requirements Identification

Mohammed Alqmase

12/18/2024

Table of Contents

1 Software Requirements Specification

Use the following templates to write the Requirements of the system

Templates:

1. The <system name> shall <system response>.
2. WHILE <precondition> the <system name> shall <system response>.
3. WHEN <trigger> the <system name> shall <system response>.
4. WHERE <feature is included> the <system name> shall <system response>.
5. IF <trigger> THEN the <system name> shall <system response>.
6. WHILE <precondition> WHEN <trigger> the <system name> shall <system response>.

1.1 Functional Requirements

In this section, the functional requirements are collected and formulated.

ID	Requirements Description
1	WHILE a new user is registered, the administrative tools subsystem shall send a confirmation email to the user.
2	The administrative tools shall take the technical issues.
3	IF a user attempts to access restricted features, THEN the administrative tools subsystem shall deny access and log the attempt.
4	WHILE a user is logged in WHEN the session times out, the administrative tools subsystem shall automatically log the user out.

1.2 Non-Functional Requirements

In this section, the non-functional requirements are identified and formulated.

ID	Requirements Description
1	The administrative tools subsystem shall respond to user requests within 2 seconds under normal operating conditions.
2	The system shall support at least 500 concurrent users without degradation in performance.
3	The administrative tools subsystem shall be able to scale horizontally to accommodate increased user load and data volume.

1.3 Security Requirements

In this section, the non-functional requirements are identified and formulated.

1.1.1 Confidentiality Requirements

The confidentiality requirements must be identified in this section.

ID	Requirements Description
1	The scheduling system shall ensure that only authorized users can **view** schedules.
2	WHILE sensitive data is stored, the administrative tools subsystem shall ensure that it is encrypted using AES-256 encryption
3	WHEN data is transmitted over the network, the administrative tools subsystem shall use TLS to secure the connection.

1.1.2 Integrity Requirements

The Integrity requirements must be identified in this section.

ID	Requirements Description
1	The scheduling system shall ensure that only authorized users can **modify** schedules.
2	WHILE a user attempts to modify sensitive information, the administrative tools subsystem shall check their permissions before allowing the action.
3	WHERE data validation features are included, the administrative tools subsystem shall provide feedback to users about any errors or required corrections.

1.1.3 Availability Requirements

The Integrity requirements must be identified in this section.

ID	Requirements Description
1	WHILE the system is in use, the administrative tools subsystem shall provide alerts for any planned maintenance or downtime.
2	WHEN unexpected downtime occurs, the administrative tools subsystem shall notify users promptly via email or system alerts.
3	The administrative tools subsystem shall implement a disaster recovery plan to restore functionality within 1 hour of a critical failure.
4	WHEN data backups are performed, the administrative tools subsystem shall ensure that backups are completed successfully and stored securely.
5	The administrative tools subsystem shall be capable of handling a minimum of 500 concurrent users without degradation in performance.

1.1.4 Authentication Requirements

The authentication requirements must be identified in this section.

ID	Requirements Description
1	WHEN a user logs in, the administrative tools subsystem shall validate their credentials and grant access based on their role.
2	IF a user exceeds the maximum number of login attempts, THEN the administrative tools subsystem shall temporarily lock the account and notify the user via email.
3	WHILE the user is logged in WHEN they change their account settings, the administrative tools subsystem shall require re-authentication to ensure security.

1.1.5 Authorization Requirements

The authorization requirements must be identified in this section.

ID	Requirements Description
1	The administrative tools subsystem shall implement role-based access control to manage user permissions based on their roles.
2	WHILE a user is assigned a specific role, the administrative tools subsystem shall grant access only to features and data appropriate for that role.
3	WHILE a user's role is active WHEN they request access to sensitive information, the administrative tools subsystem shall verify their permissions before granting access.

1.1.6 Non-repudiation Requirements

The non- repudiation requirements must be identified in this section.

ID	Requirements Description
1	The administrative tools subsystem shall implement digital signatures for all critical transactions and documents.
2	The administrative tools subsystem shall maintain comprehensive audit trails for all user actions within the system.
3	IF a digital signature is invalid, THEN the administrative tools subsystem shall reject the transaction and notify the user of the error.

1.1.7 Accountability Requirements

The accountability requirements must be identified in this section.

ID	Requirements Description
1	The administrative tools subsystem shall require unique identification for each user to ensure accountability for their actions.
2	WHILE a user performs any action, the administrative tools subsystem shall log the action type, affected records, and timestamp.

3	WHEN a user performs sensitive actions, the administrative tools subsystem shall require confirmation to ensure accountability.