TASK 71D

Quality Definition

SWE30010 - Managing IT Projects

Class: Fri 08:00 DT7.2 **- Tutor:** Pham Thi Kim Dung

Name: Trac Duc Anh Luong - **ID**: 103488117

Selection

1. **Sprint backlog item**: Set up user roles, develop user registration and log-in authentication
2. **Characteristic**: Security
3. **Sub-characteristic**: Integrity

Justification

1. **Security**: The selected sprint backlog item interacts directly with sensitive user data, including passwords, personal information, and other potential information specific to our team's application. Ensuring the security of these data is instrumental for multiple reasons:
    a. **Compliance with regulations**: Industry standards like GDPR and HIPAA denote specific security measures to protect user data. With potential legal repercussions from these regulators, it is best to ensure compliance by implementing robust security.
    b. **Protecting user privacy**: Upon the user's agreement to the privacy and security policy when registering for our website, our team is entrusted with the user data and is responsible for handling them well. Strong security measures can enhance the user experience and trust in our system.
    c. **Mitigating security risks**: Unauthorised access and data breaches can lead to enormous revenue losses, reputational damage, and legal repercussions. It is mandatory to follow best practices when developing security measures and minimising future risks.
    d. **Ensuring other functional requirements**: Compromised user data and unauthorised breaches can disrupt critical system functionalities like order placement and payment gateway, impacting overall system integrity.
2. **Integrity**:
    a. **Data accuracy and consistency**: The system's correct operation depends on the integrity of the user data. Modified or inaccurate data might result in errors, malfunctions, and a decline in trust.
    b. **Preventing unauthorised modifications**: Malicious individuals or unforeseen mistakes may alter user data. Maintaining data accuracy and preventing unwanted modifications is achieved through data integrity.
    c. **Supporting audibility and traceability**: Proper recording and logging of user actions and modifications to data is essential for auditing and looking into possible security events.

Metrics and threshold values

Our goals include required fields, password strength, OTP verification, unauthorised access prevention, role-based access rights, and activity logging.

1. Registration:

Metric 1: Percentage of successful registrations with all required fields completed

- Threshold: **99.5%** (accounting for minor edge cases or user errors)
- Justification: Ensures all essential information is captured for user accounts. The validation will be executed on the client's side. Therefore, there can be minor edge cases or client-side exceptions.

Metric 2: Percentage of registrations with strong passwords as defined by your policy

- Threshold: **95%**
- Justification: Protects against weak password attacks and data breaches. Passwords are matched against regex patterns, including length, lowercase, uppercase, numbers, and special characters. However, there can be edge cases where the password matches all regex requirements but is still predictable, for example, "*@Aaaaaa1*".

Metric 3: Percentage of registrations where email OTP verification is successful

- Threshold: **99.9%** (high threshold due to the security importance of email verification)
- Justification: Prevents unauthorised account creation and validates email addresses. Actions that call to the SMTP server for sending email are server-side. Therefore, there are little to no errors exposed by the client side. The only server-side exception can be email timeout due to many concurrent users.

2. Login:

Metric 1: Number of successful unauthorised login attempts

- Threshold: **0 (zero tolerance)**
- Justification: Prevents unauthorised access and potential security breaches. This metric is the most critical metric for login and security measures. Exposing admin privileges to unauthorised users is detrimental. Therefore, this metric has zero tolerance.

Metric 2: Percentage of login attempts with correct user role authorisation

- Threshold: **100%** (high threshold for ensuring appropriate access control)

- Justification: Ensures users only access functions and data authorised for their roles. The application assigns the user role upon systems events - log in and on application ready, which all screens and server actions will later be checked based on the privileges set in each user session.

3. Logging:

Metric 1: Percentage of registration activities successfully logged

- Threshold: **99.9%** (high threshold for complete activity auditing)
- Justification: Enables tracking user actions and identifying potential suspicious activity. The IP address of users who try to perform DDOS or spam the registration action will be blacklisted.

Metric 2: Percentage of login activities successfully logged

- Threshold: **99.9%** (high threshold for complete activity auditing)
- Justification: Provides essential data for security analysis and incident response. IP addresses of users who tried to force break into the system will be blacklisted.

Metric 3: Timeliness of log data availability for analysis

- Threshold: **1 hour** (adjustable based on system criticality and response needs)
- Justification: Ensures quick access to log data for investigation and potential remediation. The threshold can be in a shorter time interval when the number of concurrent users is medium to low, with less logging and faster retrieval time (Excel or CSV export).