|  |  |
| --- | --- |
| **Practical No:** | **5** |
| **Title:** | **Software Requirement Specification** |
| **Date of Performance:** | 31/08/2023 |
| **Roll No:** | 9593 |
| **Team Members:** |  |

Rubrics for Evaluation:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No** | **Performance Indicator** | **Excellent** | **Good** | **Below Average** | **Total Score** |
| 1 | On time Completion & Submission (01) | 01 (On  Time ) | NA | 00 (Not on Time) |  |
| 2 | Theory Understanding(02) | 02(Correct  ) | NA | 01 (Tried) |  |
| 3 | Content Quality (03) | 03(All used) | 02 (Partial) | 01 (rarely followed) |  |
| 4 | Post Lab Questions (04) | 04(done well) | 3 (Partially Correct) | 2(submitted) |  |

Eden Evelyn Charles

9593

Eden Evelyn Charles

9593

TE COMPS B

SE EXP: 5 DATA FLOW DIAGRAM

For Women Safety and Period Management App

**Explanation**

Process

**Home Page:** The user logs in and is directed to the home page.

**Emergency Page:** The user enters the emergency page and initiates the shake feature.

**Call e.contact:** An call is initiated to the e.contact which is stored in user acc. info.

**Symptoms:** The users answer the questions based on how they feel.

**Suggestions:** The users are given suggestions on how to help with their symptoms.

**Prediction:** Displays all the information to the user.

Data Stores

**User acc. Info.:** Contains personal information of the user.

**Questions:** Contains all the questions the user needs to answer.

External Entities

**User:** Initiates the Home Page and Symptoms Page

Data Flows

**Log in:** Flows from User to Home Page.

**Retrieve user info.:** Flows from User acc. info.  to the Emergency Page.

**User uses the shake feature:** Flows from Emergency Page to Call e.contact .

**User answers the questions:** Flows from Symptoms Page to Suggestions Page.

**Displays all the info.:** Flows from Suggestions Page to Prediction Page.

**POSTLAB:**

a) Evaluate the benefits of using Data Flow Diagrams (DFD) to analyse and visualise the data movement in a complex software system.

1. **Clarity and Simplification:**
   * Simplifies complex systems for better understanding.
2. **Effective Communication:**
   * Serves as a universal language for technical and non-technical stakeholders.
3. **Identification of Processes and Data Stores:**
   * Clearly identifies system processes and data storage.
4. **Boundary Definition:**
   * Distinguishes between internal processes and external entities.
5. **Data Transformation and Processing:**
   * Shows how data is processed and transformed within the system.
6. **Change Management:**
   * Facilitates managing system changes and updates.
7. **Error Detection and Prevention:**
   * Helps identify potential errors and bottlenecks.
8. **Scalability and Optimization:**
   * Aids in identifying areas for performance and scalability improvements.
9. **Documentation and Training:**
   * Useful for documentation and onboarding new team members.
10. **Requirements Analysis:**
    * Supports early-stage requirements gathering and system behavior definition.

b) Apply data flow analysis techniques to a given project and identify potential data bottlenecks and security vulnerabilities.

1. **Data Flow Definition:**
   * Identify key data flows within the app, including user data, location data, and emergency contact details.
2. **Create a Data Flow Diagram (DFD):**
   * Develop a DFD to visualize data flow, including processes, data stores, data flows, and external entities.
3. **Data Flow Tracing:**
   * Trace sensitive data to understand how it moves through the app.
4. **Identify Data Bottlenecks:**
   * Look for areas where data processing or transfer may cause delays or bottlenecks.
5. **Data Validation and Sanitization:**
   * Assess how the app validates and sanitizes user inputs to prevent security vulnerabilities.
6. **Data Encryption:**
   * Examine encryption standards for sensitive data in transit and at rest.
7. **Data Access Controls:**
   * Review user access controls and permissions to prevent unauthorized data access.
8. **Authentication and Authorization:**
   * Ensure secure user authentication and authorized access to sensitive features or data.
9. **Data Leakage and Privacy:**
   * Identify potential data leakage points, especially regarding period tracking and location data.
10. **External Data Sources:**
    * Assess security during interactions with external data sources or APIs.
11. **Data Backup and Recovery:**
    * Review data backup and recovery processes for data integrity and availability.
12. **Logging and Monitoring:**
    * Implement robust logging and real-time monitoring for security events.
13. **Security Audits and Testing:**
    * Conduct periodic security audits and penetration tests.
14. **Incident Response Plan:**
    * Develop an incident response plan for prompt security incident handling.
15. **Data Retention and Purge Policies:**
    * Implement data retention and purging policies to minimize data exposure.
16. **Compliance and Documentation:**
    * Ensure compliance with privacy regulations and maintain documentation of security processes.

c) Propose improvements to the data flow architecture to enhance the system's efficiency and reduce potential risks.

1. **Data Validation and Sanitization:**
   * Strengthen validation and sanitization processes.
   * Implement standardized input validation libraries.
2. **Data Encryption:**
   * Upgrade encryption protocols for data at rest and in transit.
   * Maintain robust key management practices.
3. **Access Controls:**
   * Refine access controls and follow the principle of least privilege.
   * Consider role-based or attribute-based access control.
4. **Multi-Factor Authentication (MFA):**
   * Introduce MFA for enhanced user authentication security.
5. **Secure External Data Sources:**
   * Enhance security for external data sources with validation and rate limiting.
   * Use API security tokens.
6. **Data Leakage Prevention:**
   * Implement DLP solutions and outbound data encryption.
7. **Backup and Recovery:**
   * Strengthen backup and recovery strategies.
   * Regularly test and validate backups.
8. **Logging and Monitoring:**
   * Implement comprehensive logging and real-time monitoring.
9. **Security Audits and Penetration Testing:**
   * Conduct routine security audits and penetration testing.
   * Promptly address identified vulnerabilities.
10. **User Education and Training:**
    * Educate users and staff on security best practices.
    * Provide security awareness training.
11. **Incident Response Plan:**
    * Develop a robust incident response plan with clear roles and procedures.
12. **Data Retention and Purge Policies:**
    * Implement data retention policies and regular data purging.
13. **External Dependency Assessment:**
    * Continuously assess external dependency security.
    * Keep dependencies updated and patched.
14. **Documentation and Compliance:**
    * Maintain detailed security process documentation.
    * Ensure compliance with security standards and regulations.
15. **Regular Security Reviews:**
    * Conduct periodic security reviews and risk assessments to adapt to evolving threats.