**Problem Statement 1:**

**Product Requirement and Low-Fidelity Wireframes**

**Background**: Although container images are essential to developing modern applications, there is a possibility that they include security flaws. A method is required for users to scan these images, find vulnerabilities, and rank the severity of the remedies.

**Lower-Resolution Wireframes**:

1. Dashboard Wireframe No. 1 Overview:  
   Header: Images, Reports, Settings, Home, and Navigation Menu  
   Primary Section:  
   - In brief Stats: Total Images, Images which are Vulnerable, Images that are Critical, Vulnerability Graph Distribution of Severity (pie chart)  
   - List of most recent scans and updates from the recent activity log.
2. Image Vulnerability List in Wireframe 2:  
   Columns in Table: Image Name, Vulnerability Count, Level of Severity, Last Scanned, vulnerability proof and Fix

Status: Image search bar is at the top of the table.  
Filter Options: Severity and status filter dropdown menus.

1. Vulnerability Details in Wireframe 3 View:

Header: Image overview with relevant details  
List of Vulnerabilities: Column-based table Vulnerability ID, Severity, Description, exclusion button, Vulnerability proof, Fix

Action: Export Report, Mark as Fixed

**Action Items for Development:**

* Discuss about the best technology stack for the frontend, backends, Testing.
* Create APIs regarding this.
* Establish the database structure for storing vulnerability information and container images.
* Plan for Integrations for scanning regularly on Images for vulnerability updating.

**Problem Statement 2:**

**Kubernetes Security Scan**