Product Requirement Document

Product : Container Image Vulnerability Scanner
Author : Anikesh S. Gadekar
Version: 1.0
Date : 17 March 2025

1.Introduction:

As more applications use containers, security risks in container images are a big concern. This product helps by scanning container images, finding known vulnerabilities, and giving clear steps to fix them, making it easier for teams to keep their systems secure.

2. Problem Statement:

Users need a way to:

1. Identify vulnerabilities in container images.
2. Prioritize fixes based on severity (Critical, High, Medium, Low).
3. Efficiently scan and manage thousands of container images.
4. Get remediation guidance for fixing vulnerabilities.

3. Target Users:

1. Security Engineers - Monitor and fix security issues in container images.
2. DevOps Engineers - Ensure security compliance before deployment.
3. Developers - Fix vulnerable dependencies in their applications.

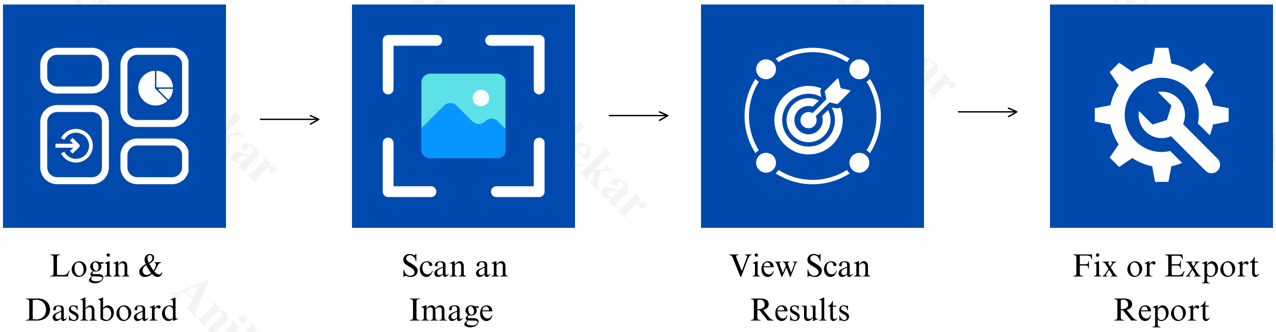
4.Key Features : 4.1 Core Functionalities

Feature	Description
Container Image Scanning	Users can scan individual images or bulk scan multiple images from a repository.
Vulnerability Detection	The system fetches vulnerabilities from databases like CVE, NVD, or Trivy.
Severity Categorization	Vulnerabilities are categorized into Critical, High, Medium, and Low severity.
Filtering & Sorting	Users can filter vulnerabilities by severity, CVE ID, or affected package.
Fix Recommendations	The system provides patch recommendations or alternative mitigation strategies.
Scan History & Reports	Users can scan individual images or bulk scan multiple images from a repository.
Dashboard Overview	Provides an at-a-glance view of recent scans, top vulnerabilities, and trends.
Notifications & Alerts	Users receive alerts for newly detected critical vulnerabilities.

4.2 User Stories

- As a Security Engineer:
  1. Scan container images to identify vulnerabilities.
  2. View the most critical vulnerabilities at the top.
  3. Get remediation suggestions for each vulnerability.
- As a DevOps engineer:
  1. Automate scans for new container images.
  2. Receive alerts for high-risk vulnerabilities.
  3. Generate compliance reports for audits.
- As a developer:
  1. Check if my application dependencies have vulnerabilities.
  2. See the exact package versions that need an upgrade.

5. User Flow :

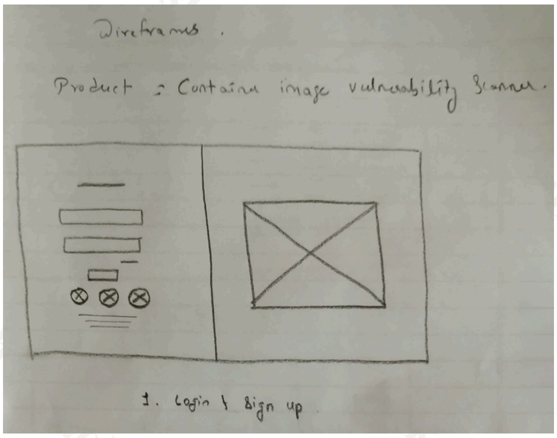


Login & Dashboard → Scan an Image → View Scan Results → Fix or Export Report

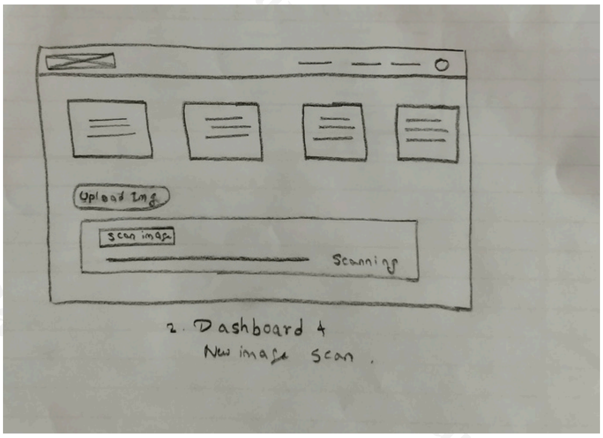
6. Technical Requirements:

Component	Technology
Scanning Engine	Trivy, Clair, or Anchore
Backend API	FastAPI (Python) / Flask (Python) / Go
Database	PostgreSQL / MongoDB
Frontend	React / Vue.js / Simple HTML
Deployment	Docker + Kubernetes
Authentication	OAuth / JWT-based access

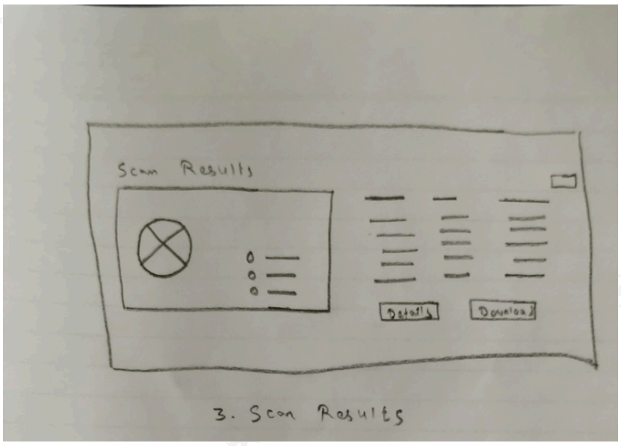
7. Wireframes:



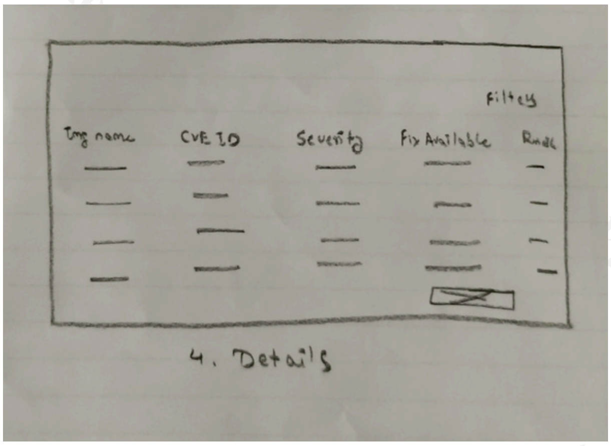
Frame 1 : Login & Sign Up



Frame 2 : Dashboard and Scan Images



Frame 3 : Scan Results : Overview



Frame 4 : Detailed Scan Results

8. Metrics for Success

1. Scan Performance: Must scan an image in under 30 seconds.
2. Accuracy: Should detect 90%+ of known vulnerabilities.
3. User Engagement: At least 70% of users take remediation actions.

9. Conclusion :

The Container Image Vulnerability Scanner simplifies security by detecting and fixing vulnerabilities in container images. With real-time scanning, clear reports, and easy fixes, it helps teams proactively manage risks. A user-friendly design ensures efficient tracking and resolution, making container security simple and effective.