**Product Management Trainee Assignment**

**1. Overview**

In modern tech systems, developers use container images to package their applications. These images often have many layers and dependencies. Sometimes, they include known security issues called vulnerabilities. The goal of this product is to help users find and fix these problems quickly, especially when they have thousands of images.

**2. User Persona**

Main User: DevOps Engineer or Security Analyst

Needs:

- To know which container images have issues.

- To understand how serious each issue is.

- To take quick action to fix or review them.

**3. Key Features**

A. Dashboard Page

- Shows total images scanned.  
- Number of vulnerable images.  
- Graph of severity levels (Critical, High, Medium, Low).  
- Trends: How many issues fixed vs. found.

B. Image List Table

- Image name and path.  
- Number of issues with severity.  
- Last scanned date.  
- Button to view more details.

C. Detailed View of One Image

- List of layers in the image.  
- Vulnerabilities per layer.  
- For each issue: ID, severity, description, and how to fix it.  
- Option to download report.

D. Filters and Sorting

- Filter by severity, date, and name.  
- Sort by most recent or most risky.

E. Bulk Actions

- Select multiple images to rescan or mark as fixed.

**4. Simple Wireframe Descriptions**

1. Dashboard Example

-----------------------------------------------  
| Total Images | Vulnerable | Critical | Fixed |  
-----------------------------------------------  
| 10,000 | 1,245 | 213 | 8,755 |  
-----------------------------------------------  
Graph: Vulnerabilities Over Time  
Pie Chart: Severity Levels

2. Image Table View

---------------------------------------------------------------  
| Image Name | Path | Critical | High | Last Scanned |  
---------------------------------------------------------------  
| app1:v2 | /repo/app1 | 2 | 4 | 01-Apr-2025 |  
| core:v1.4 | /repo/core | 1 | 1 | 03-Apr-2025 |  
---------------------------------------------------------------  
[Search] [Filters] [Export Button]

3. Image Details View

Image: app1:v2  
-----------------------------------------------------------  
| Layer | Vulnerability | Severity | Fix Suggestion |  
-----------------------------------------------------------  
| 1 | CVE-2023-1234 | Critical | Upgrade to v1.5 |  
| 2 | CVE-2022-4567 | High | Apply latest patch |  
-----------------------------------------------------------  
[Download Report] [Mark as Fixed] [Back Button]

**5. Development Action Items (Optional)**

Frontend Tasks:

- Build dashboard cards and graphs.  
- Design table with filters and sort.  
- Modal to show image details.

Backend Tasks:

- Create APIs to fetch image data and scan results.  
- Connect to CVE databases (like NVD).  
- Store scan history.

DevOps Tasks:

- Link with image registries (like DockerHub).  
- Schedule regular scans.

**6. Conclusion**

This product helps users clearly see which container images have problems and how serious they are. With simple views and useful filters, users can fix issues faster and keep their systems secure. It saves time, improves safety, and works well even with many images.