Sprint 1 Plan - [USSF] GRC Control Kubernetes

Team Roles

- **Scrum Master (Iteration 1)**: Aditya Gourishetty
- **Product Owner (Iteration 1)**: Shravan Bhat

Customer Meeting Information

Date: 09/24/2024
Time: 18:00
Location: Google Meet
Attendees: Aditya Gourishetty, Drew Hendricks, Maitreya Niranjan, Duy Vu, Prof. Shreyas Kumar, Spencer Yates, Eric D Griffin, Medha Kaushika Podipireddi, Sahil Fayaz, Shravan Bhat, Vasudha Devarakonda

- The group introduced themselves, including the USSF representatives, Prof. Shreyas Kumar, and the developers.
- The project proposal brief provided was discussed to add additional details.
- There were attempts to resolve ambiguities in the definition of terms like object, GRC controls, and environment.
- There was a decision among the participants to create a requirements agreement document with the students' understanding of the requirements that the client can sign off on.
- Developers would meet Prof. Shreyas Kumar to get a better understanding of NIST controls.
- Developers would demonstrate what has been done during the sprint in client meetings.
- The group has to finalize a time for a weekly client meeting.
- USSF would try to provide access to one or more sample images for the developers to run their GRC control scan.

Summary of Main Customer Need

The customer requires an interface for scanning Docker images in accordance with NIST controls, which are guidelines developed by the National Institute of Standards and Technology to help organizations manage cybersecurity risks. These controls offer specific security measures to protect information systems and ensure data integrity. While some NIST controls can be challenging to implement technically or are somewhat vague, the customer prioritizes the implementation of those that are more straightforward.

To address these needs, we propose developing a SaaS application using Ruby on Rails that enables users to upload or pull specific Docker images for scanning. The application will feature a scan button that initiates the process and generates a well-formatted report. Users will have the capability to manage a set of Image objects, along with a history of their scans and reports. Key stakeholders will include users who can log in via Single Sign-On (SSO). Future enhancements may involve adding roles for Application Administrators and view-only guests, as well as features like tagging and versioning of Image objects.

User Stories

Feature: Login to the application

- **As a user** of the application
- **So that** I can log in to the application
- **I want** a login page with a login button through which I can log in via SSO.

Feature: Home Page

- **As a user** of the application
- **So that** I can view all my activities with all my images.
- **I want** a home page with a well-formatted list of all the images.

Feature: New Image Page for GRC

- **As a user** of the application
- **So that** I can add/upload a new image.
- **I want** a form where I can add details of the image.

Feature: Main Image Page

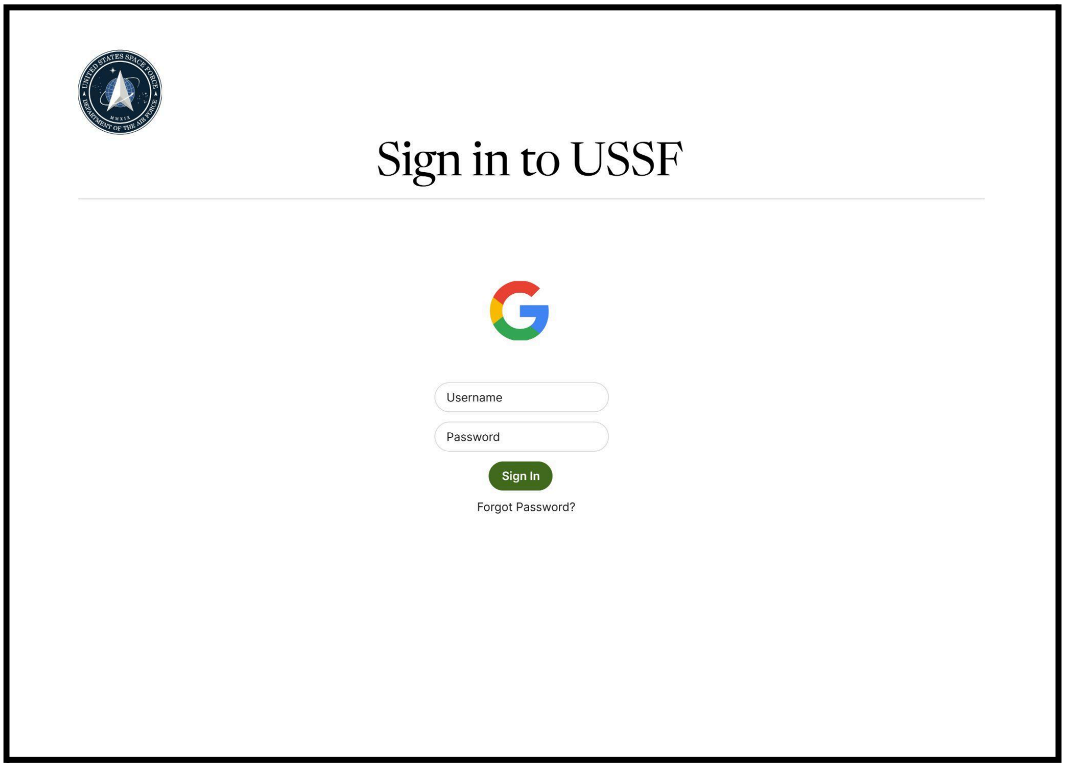
- **As a user** of the application
- **So that** I can view details of a created image
- **I want** a page where I can see the details of the image that I have created

Feature: Report page

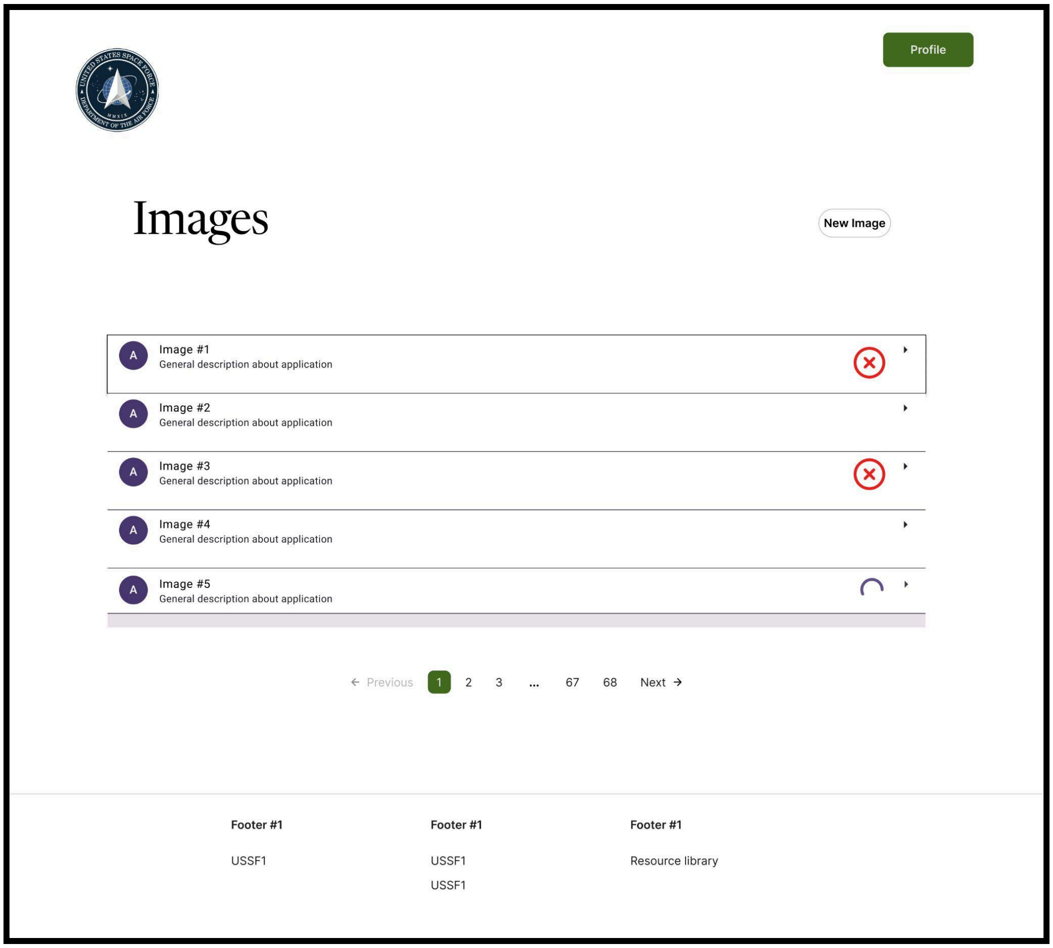
- **As a user** of the application
- **So that** I can view the compliance report of the scan
- **I want** a report page that shows the results of the GRC scan(NIST).

User Interface Mockups and Storyboards

Include photos of lo-fi UI mockups for at least 4 distinct user stories. (You can upload photos directly or paste images here.)
Make sure each mockup addresses a different story or feature.



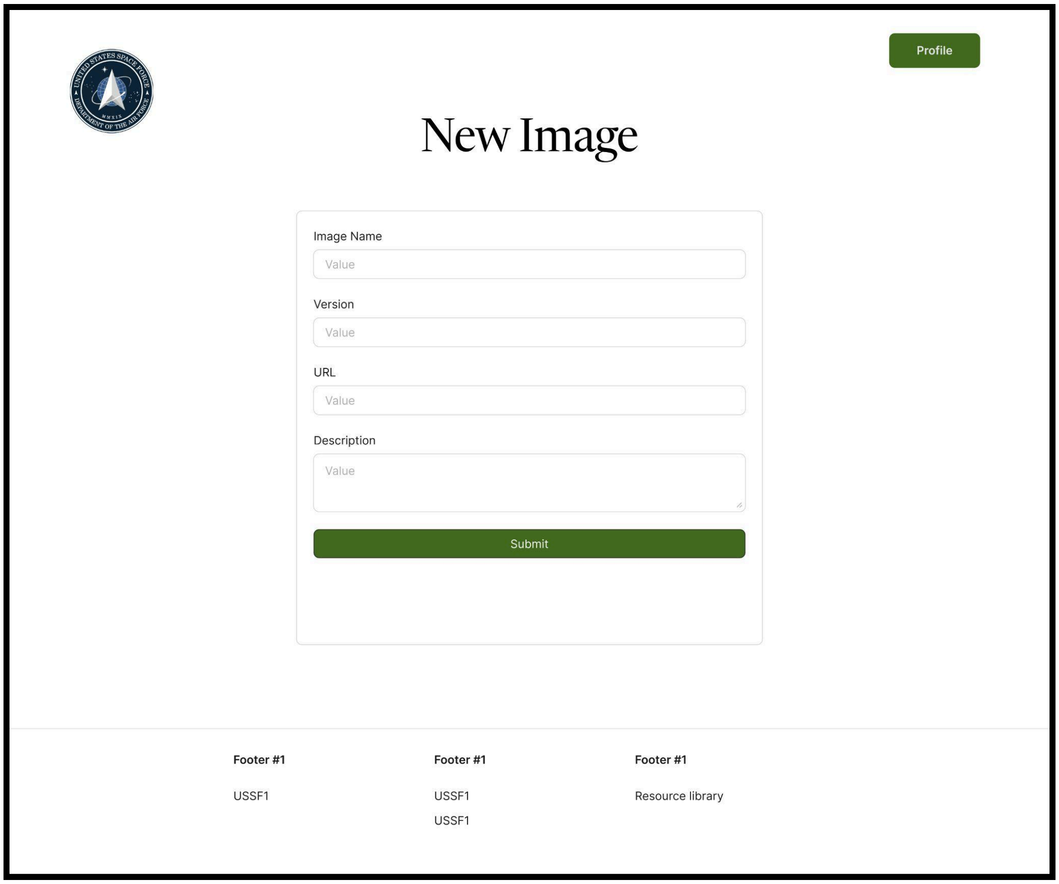
Sign in to USSF



Images

- A Image #1 — General description about application ⊗
- A Image #2 — General description about application
- A Image #3 — General description about application ⊗
- A Image #4 — General description about application
- A Image #5 — General description about application

Footer #1	Footer #1	Footer #1
USSF1	USSF1	Resource library
	USSF1	



New Image

Image Name

Value

Version

Value

URL

Value

Description

Value

Footer #1	Footer #1	Footer #1
USSF1	USSF1	Resource library
	USSF1	

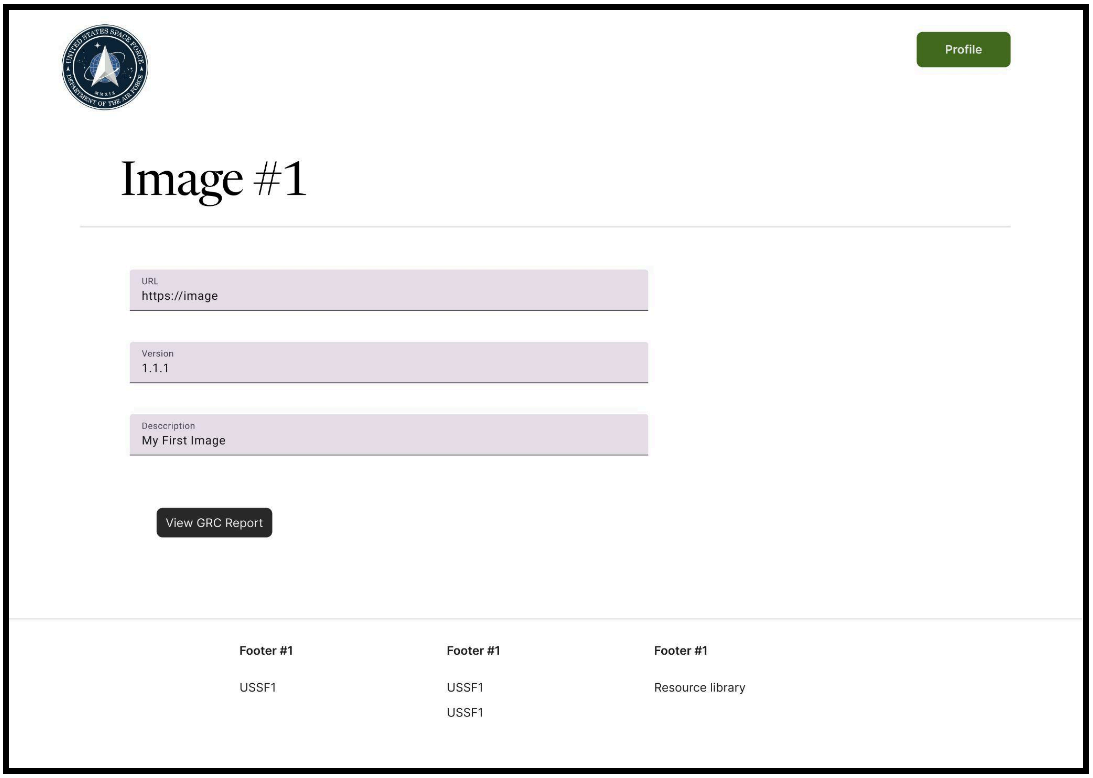


Image #1

URL
https://image

Version
1.1.1

Desccription
My First Image

Footer #1

USSF1

Footer #1

USSF1

USSF1

Footer #1

Resource library

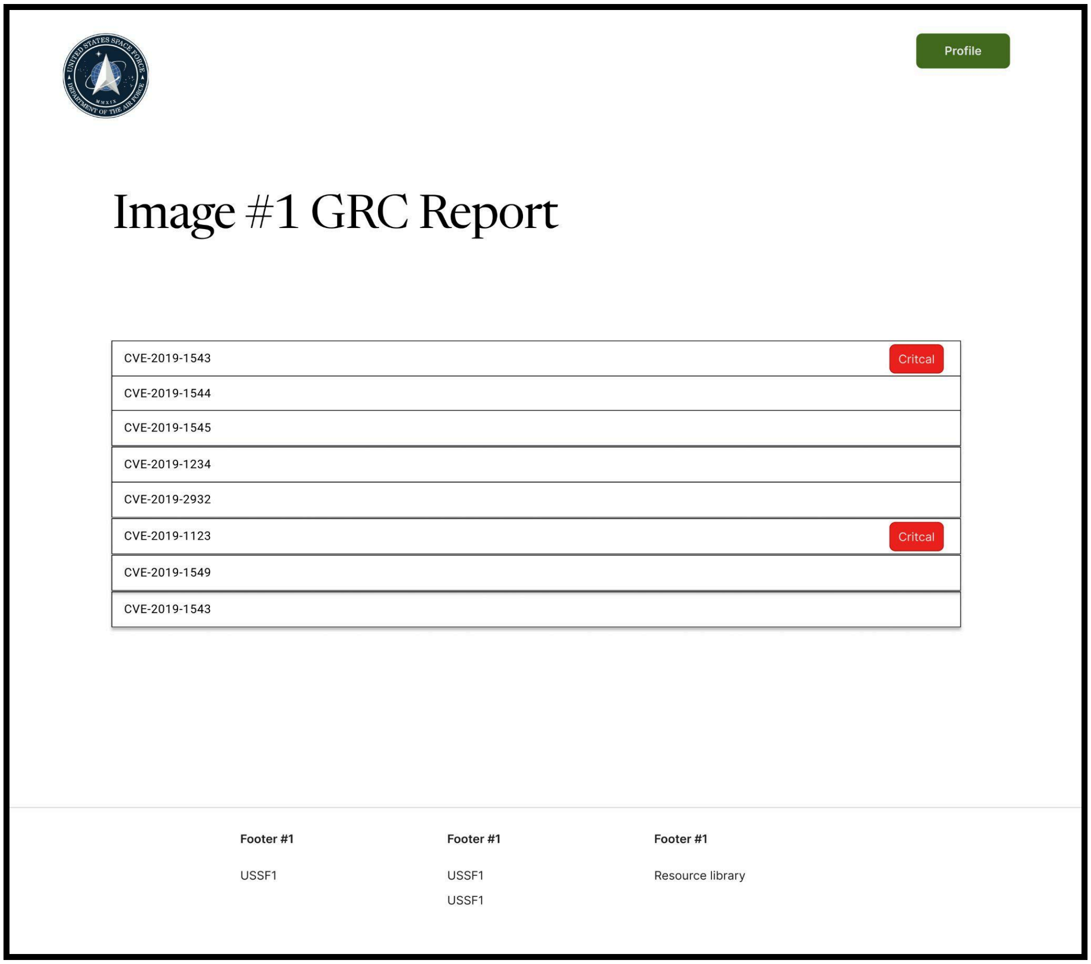


Image #1 GRC Report

CVE-2019-1543	Critcal
CVE-2019-1544	
CVE-2019-1545	
CVE-2019-1234	
CVE-2019-2932	
CVE-2019-1123	Critcal
CVE-2019-1549	
CVE-2019-1543	

Footer #1

USSF1

Footer #1

USSF1

USSF1

Footer #1

Resource library

Sprint Backlog

Sprint Goal

The goal of Sprint 1 is to provide an initial prototype of the SaaS application having static views of multiple pages, to show it to the client so that they can get an understanding of the application that is going to be delivered. The login via SSO feature and finalizing on the tools to be used in the backend to run the scan against the Image objects are also prioritized.

Stories Pulled into Sprint

Story	Story Points	Sub Tasks	Sub Task Points	Assigned To
Login to the application	4	Integrate Google OAuth SSO Provider by creating a new project in Google Developer Console. Implement SSO Login & Session Management	3	Sahil Fayaz
		Test and Validate SSO Functionality	1	Maitreya Niranjan
Home Page	2	Display the images that have already been uploaded by the user along with a button to go to the “Main Image page”. Add a button that takes you to the “New Image page for GRC”.	2	Maitreya Niranjan

New Image Page for GRC	1	Create a form for image upload with necessary fields (e.g., image name, tags). Add a dummy upload button that will finally take you to the “Main Image Page”.	1	Duy Vu
Main Image page	2	Display uploaded image details on the main image page. Add a button (currently a dummy button) that links to the “Report Page”.	2	Duy Vu
Report page	6	Generate the raw output, parse it in a presentable way, and make a demo to pitch to the client and team.	3	Medha Podipireddi
		Figure out all possible solutions compatible with ruby and integrate the best possible one.	3	Vasudha Devarakonda

Links to Key Resources

- **GitHub Repo**: USSF-CSCE606
- **Project Management Page:** USSF-CSCE606-Project-Management
- **Slack Workspace**: Fall 2024 CSCE606: USSF GRC Control Kubernetes
- **Deployed App UR**L: USSF-GRC

Grading Approach (if applicable)

Apart from the SaaS application UI and backend, we would be exploring third party libraries for conducting the GRC scan against a Docker Image.