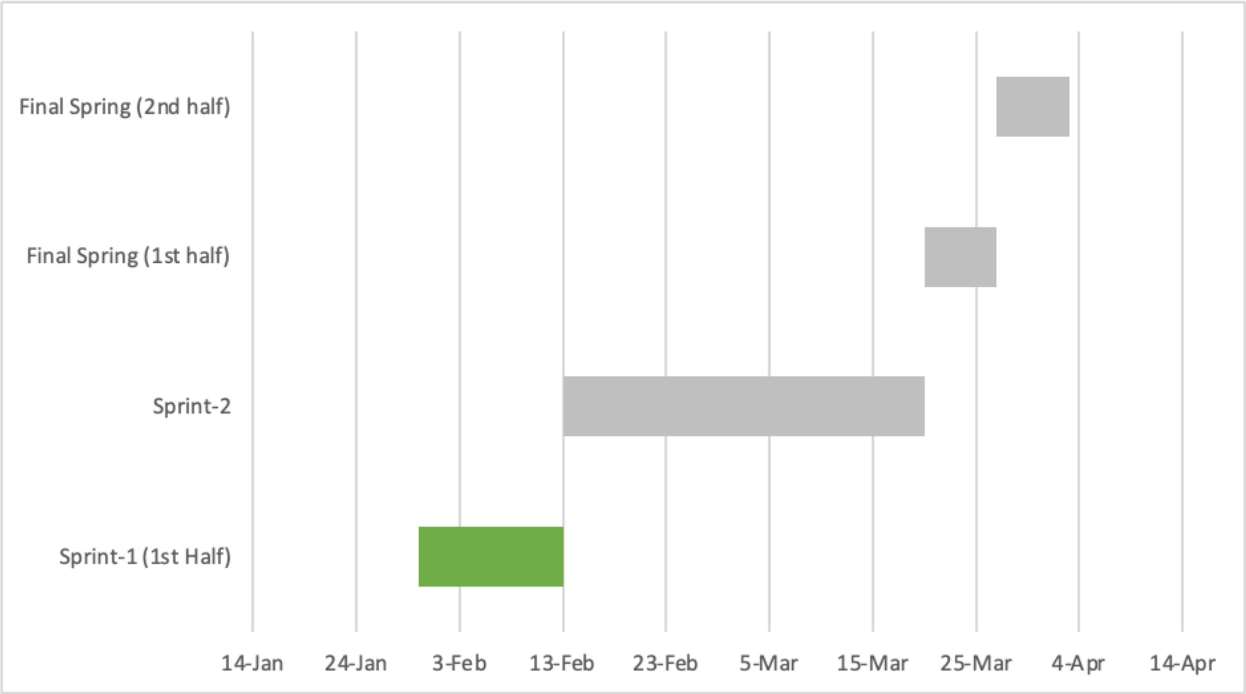
CAPSTONE TEAM 1 - SPRINT-1: RETROSPECT

TABLE OF CONTENTS

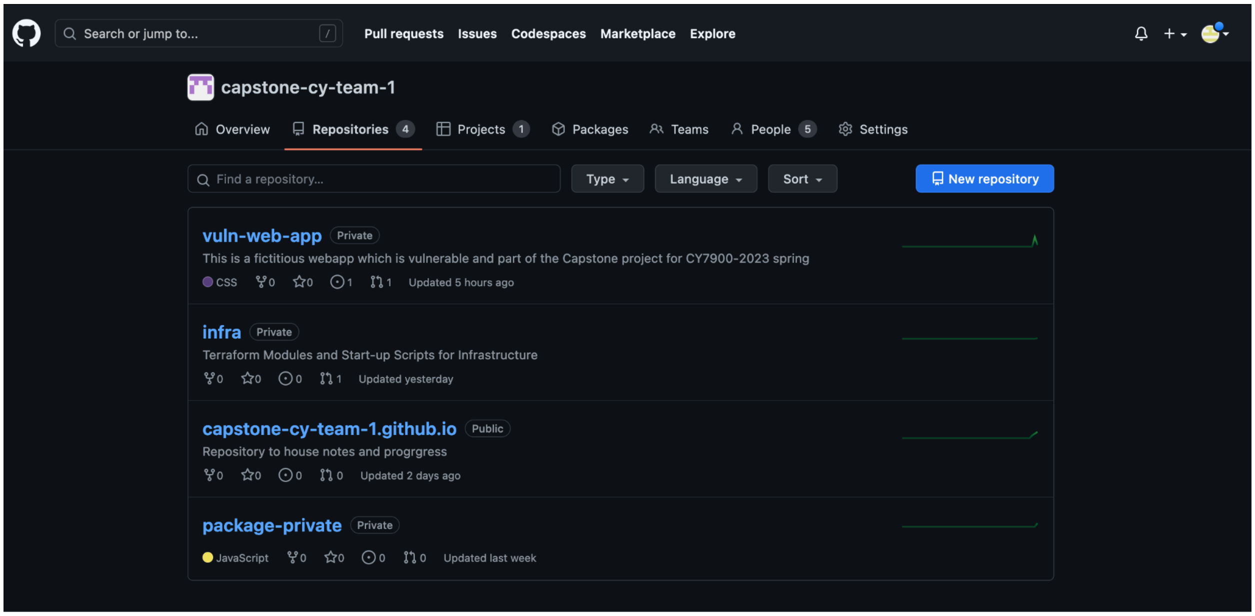
Overview

This document outlines the progress made by Team 1 of CY Capstone in the Sprint 1.



GitHub Organization

We have created a dedicated organization for the Capstone project named Capstone-cy-team-1. The progress of the whole project can also be tracked via a dedicated website hosted on GitHub pages: https://capstone-cy-team-1.github.io/



capstone-cy-team-1

vuln-web-app Private
This is a fictitious webapp which is vulnerable and part of the Capstone project for CY7900-2023 spring
CSS 0 0 1 1 Updated 5 hours ago

infra Private
Terraform Modules and Start-up Scripts for Infrastructure
0 0 0 1 Updated yesterday

capstone-cy-team-1.github.io Public
Repository to house notes and progrgress
0 0 0 0 Updated 2 days ago

package-private Private
JavaScript 0 0 0 0 Updated last week

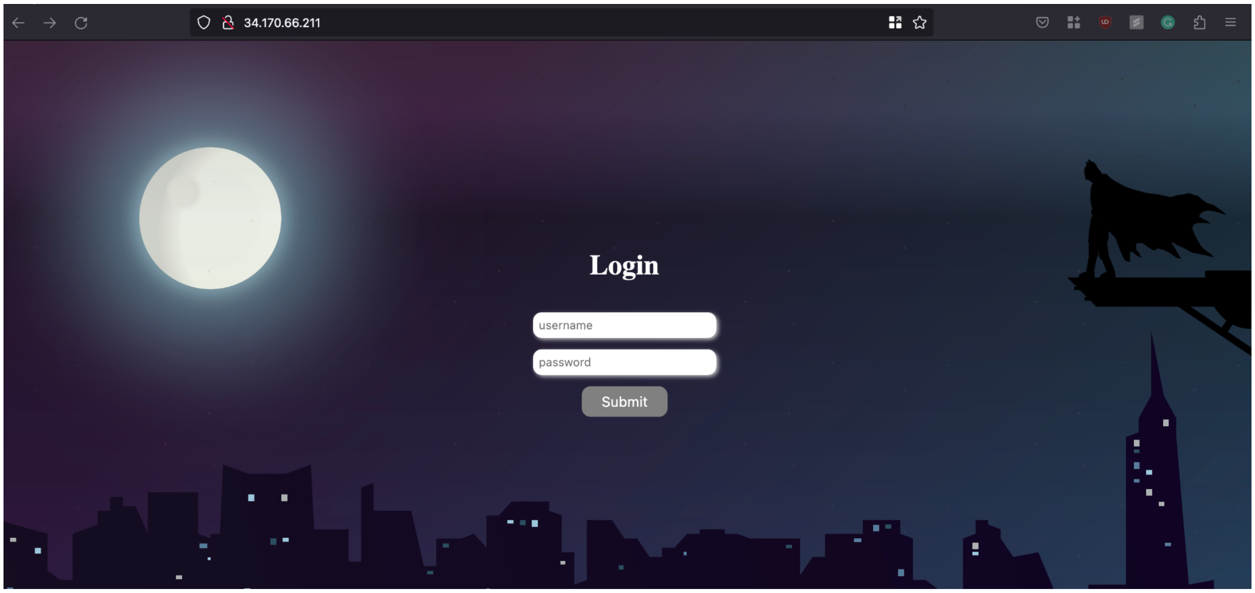
Repositories

1. **Vuln web:**

   We have created dedicated repositories to organize the code better and to enable easy tracking and deployment of code from individual repositories.

   The repository can be found here: https://github.com/capstone-cy-team-1/vuln-web-app.

   The app is hosted here: http://34.170.66.211/



2. **Infrastructure:**

   This repository houses Terraform Modules and Start-up Scripts for Infrastructure.

   The repository can be found here: https://github.com/capstone-cy-team-1/infra

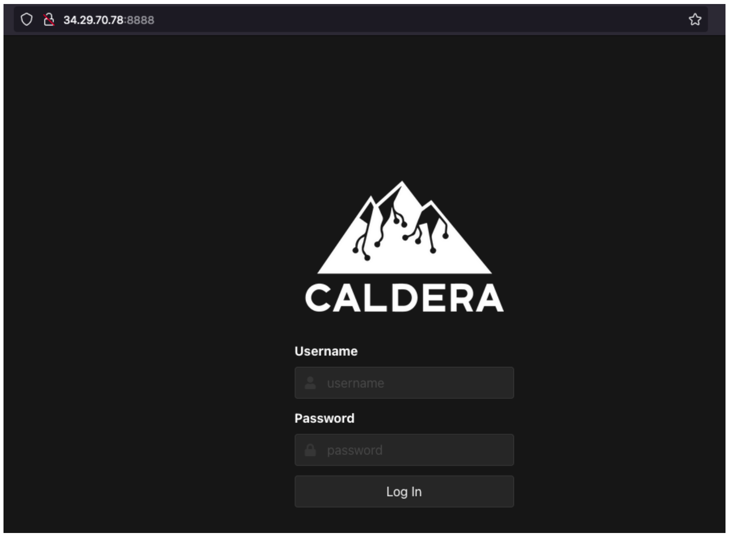
3. **Private Package Template:**

   This package is private to the vuln-web app and can be downloaded only from their own privately hosted repository (which sits somewhere in their cloud).

   The repository can be found here: https://github.com/capstone-cy-team-1/package-private

Caldera

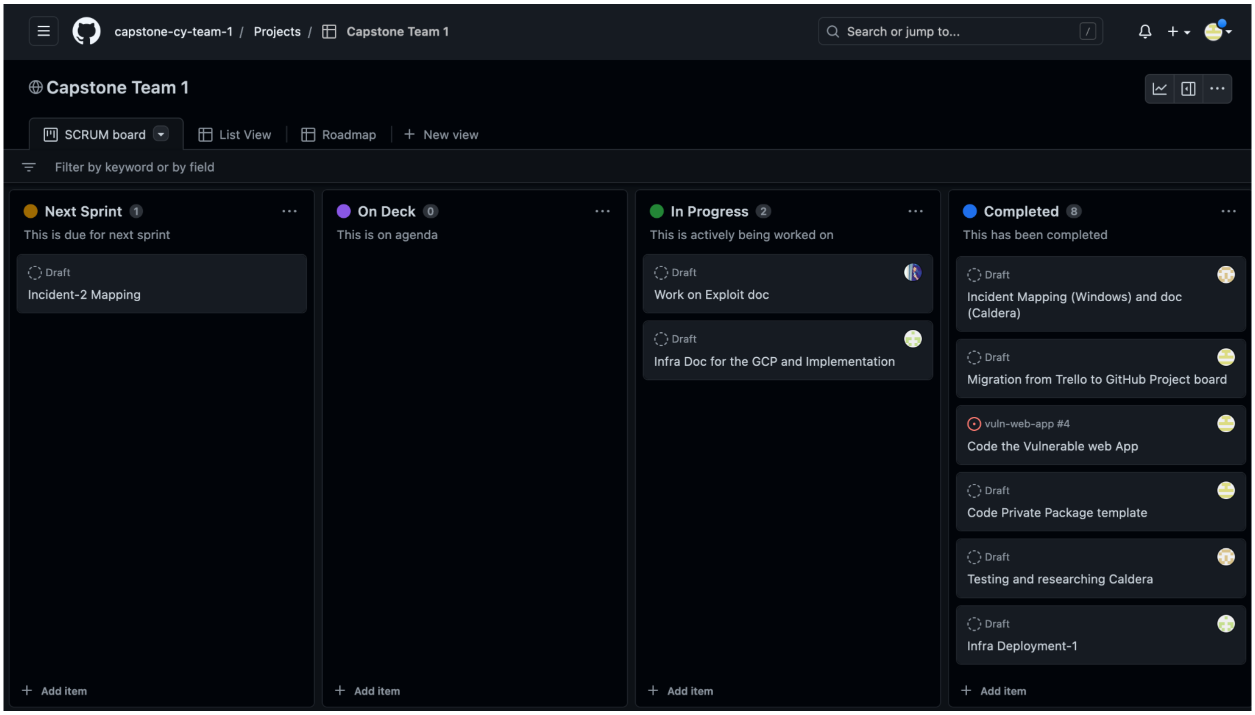
- Mitre Tool used for conducting automated risk assessments
- Team will be creating Caldera server that will be attacking the victim server
- Tool allows for not only attacking but as well as incident response
- The tool gives access to two users red and blue
  - Each user gives access to separate tools and operations that can be used to teams advantage
- Attacks such as collecting information from victim machine can be conducting giving access to host information, and possible files and directories that have been used on the machine
- The Caldera application is hosted on http://34.29.70.78:8888 as shown below.



Scrum Board

4. **Scrum Board here:** Team-1 Scrum Board

   All the Sprint items, Backlogs, and to-do items can be found on this scrum board.



Next Sprint 1
This is due for next sprint
- Draft — Incident-2 Mapping

On Deck 0
This is on agenda

In Progress 2
This is actively being worked on
- Draft — Work on Exploit doc
- Draft — Infra Doc for the GCP and Implementation

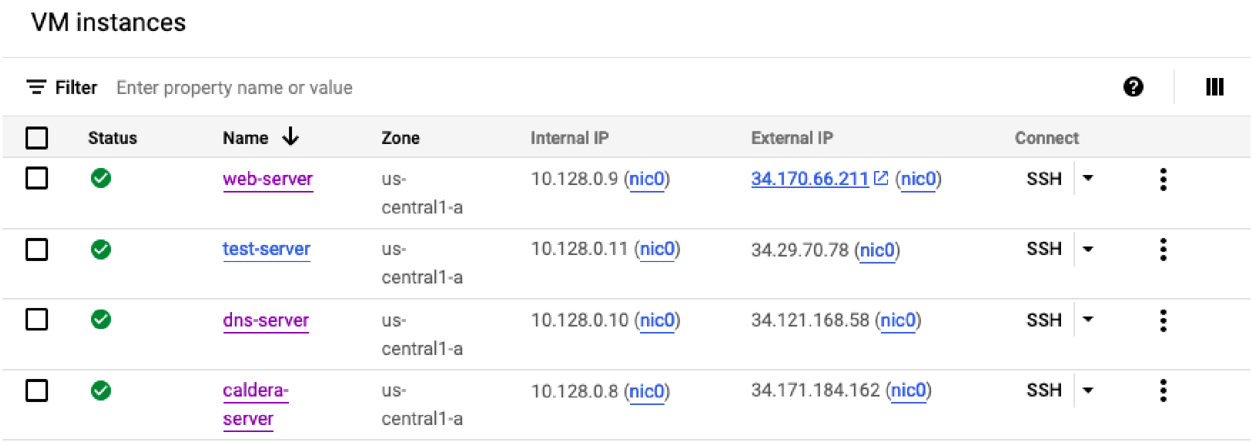
Completed 8
This has been completed
- Draft — Incident Mapping (Windows) and doc (Caldera)
- Draft — Migration from Trello to GitHub Project board
- vuln-web-app #4 — Code the Vulnerable web App
- Draft — Code Private Package template
- Draft — Testing and researching Caldera
- Draft — Infra Deployment-1

Team Communication:

- The team uses Microsoft Teams as the primary mode of communication
- Update and brainstorming session twice a week on Wednesdays and Saturdays for a duration of 1 to 2 hours
- Most of the documentation is created and collaborated on Google Docs
- Google Slides and Canva were used to create presentations that were submitted and presented during sessions with the Scrum Master (Prof. Jose)
- Tasks and Issues are created and tracked on the GitHub Scrum board. This was earlier done using Trello.

Infrastructure:

- The project is implemented on GCP as suggested by the Scrum Master.
- All infrastructure implementations using Terraform to maintain Infrastructure as a Code.
- Currently, a Virtual Private Network, Subnetworks, four compute servers (Web-Server, Caldera-Server, DNS-Server, and a Test-Server), and necessary firewall rules have been implemented.
- The team is discussing whether to implement a Load Balancer and the necessary target groups to receive a persistent domain URL for the web server since it would be closer to an industry-level infrastructure. Based on the decision, other components, such as the Application Load balancer, target groups, firewalls, DNS records, and SSL certificates, may be implemented and configured.
- For exploitation, we bought a domain “0xparthhackerone.me” for DNS Server.



□	Status	Name ↓	Zone	Internal IP	External IP	Connect	
□	✓	web-server	us-central1-a	10.128.0.9 (nic0)	34.170.66.211 (nic0)	SSH ▾	⋮
□	✓	test-server	us-central1-a	10.128.0.11 (nic0)	34.29.70.78 (nic0)	SSH ▾	⋮
□	✓	dns-server	us-central1-a	10.128.0.10 (nic0)	34.121.168.58 (nic0)	SSH ▾	⋮
□	✓	caldera-server	us-central1-a	10.128.0.8 (nic0)	34.171.184.162 (nic0)	SSH ▾	⋮