CS551P Advanced Programming (2024-25) - Web Development Report

Name: YiFan Wang
Deployment URL: CyberSec Events on Render

Project Overview

This project is a database-driven web application developed using Flask. The primary purpose is to demonstrate advanced web development skills by building an interactive application that can filter and display cybersecurity events. The data source is an open dataset containing 6,999 records related to cybersecurity incidents.

Features Implemented

- **Event List with Pagination:** Displays events with 20 records per page.
- **Severity Filtering:** Allows filtering of events based on severity levels (Low, Medium, High, Critical).
- **Event Detail Page:** Displays detailed information about a selected event, including response actions.
- **Custom Error Pages:** Includes 404 and 500 error pages for better user experience.
- **Testing:** Comprehensive test suite using Pytest, covering event list, filtering, detail pages, and error handling.

Deployment Process

1. **Environment:** Render, with Python 3.11 as the runtime environment.
2. **Build Command:**
   pip install -r requirements.txt && flask db stamp head
3. **Start Command:**
   gunicorn run:app
4. **Environment Variables:**
   - FLASK_ENV=production
   - SECRET_KEY=<generated_key>

Testing

- Unit testing using Pytest.
- Tests cover: event list, filtering by severity, detail page response, 404 and 500 pages.
- Test command:
  pytest -q
- All tests passed successfully.
-

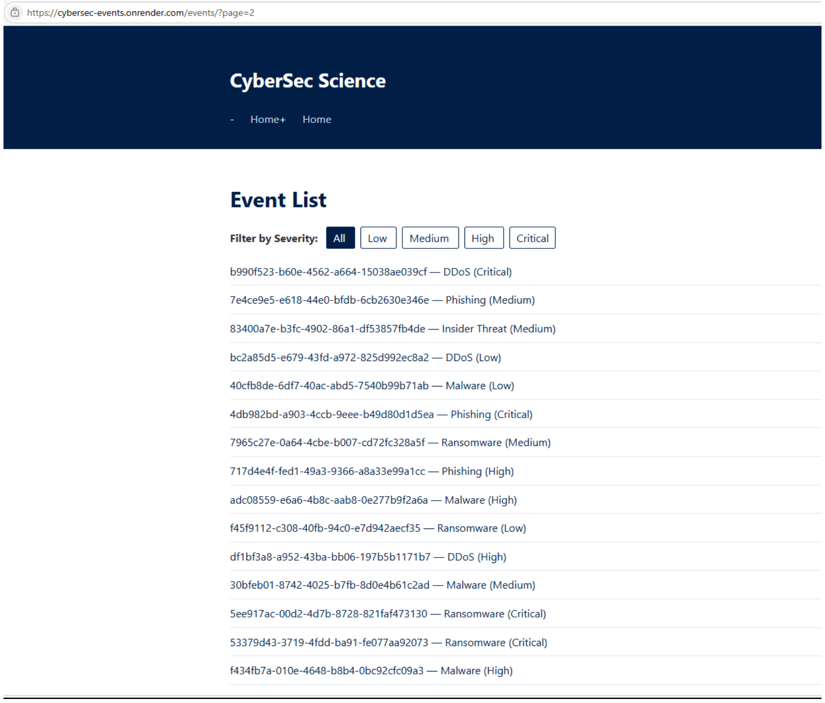
Git and Version Control

- Repository URL: GitHub Repository
- Followed Git best practices with branching and merging.

Final Thoughts

The project demonstrates how to build a reliable, database-driven web application with Flask, implement filtering and pagination, and handle common web errors efficiently. The use of open data sets highlights the practical application of data-driven web apps.

Visual impact



CyberSec Science

Event List

Filter by Severity:

b990f523-b60e-4562-a664-15038ae039cf — DDoS (Critical)

7e4ce9e5-e618-44e0-bfdb-6cb2630e346e — Phishing (Medium)

83400a7e-b3fc-4902-86a1-df53857fb4de — Insider Threat (Medium)

bc2a85d5-e679-43fd-a972-825d992ec8a2 — DDoS (Low)

40cfb8de-6df7-40ac-abd5-7540b99b71ab — Malware (Low)

4db982bd-a903-4ccb-9eee-b49d80d1d5ea — Phishing (Critical)

7965c27e-0a64-4cbe-b007-cd72fc328a5f — Ransomware (Medium)

717d4e4f-fed1-49a3-9366-a8a33e99a1cc — Phishing (High)

adc08559-e6a6-4b8c-aab8-0e277b9f2a6a — Malware (High)

f45f9112-c308-40fb-94c0-e7d942aecf35 — Ransomware (Low)

df1bf3a8-a952-43ba-bb06-197b5b1171b7 — DDoS (High)

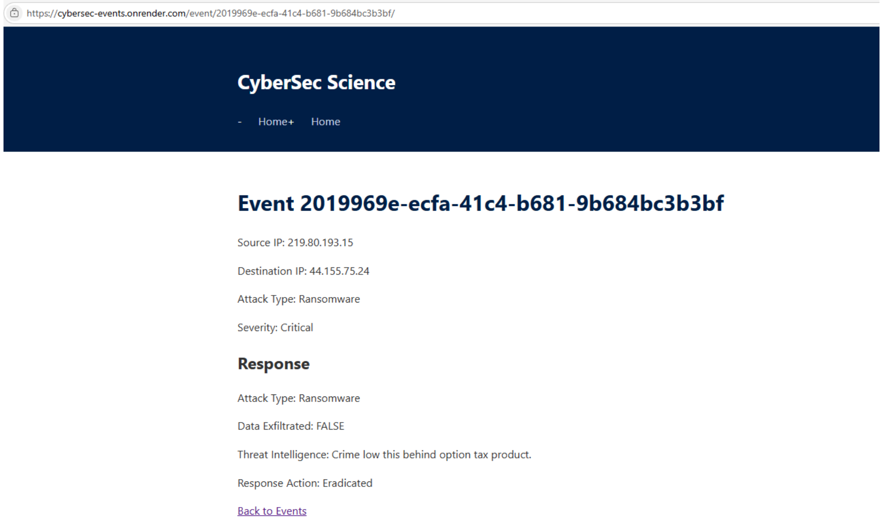
30bfeb01-8742-4025-b7fb-8d0e4b61c2ad — Malware (Medium)

5ee917ac-00d2-4d7b-8728-821faf473130 — Ransomware (Critical)

53379d43-3719-4fdd-ba91-fe077aa92073 — Ransomware (Critical)

f434fb7a-010e-4648-b8b4-0bc92cfc09a3 — Malware (High)

Homepage



https://cybersec-events.onrender.com/event/2019969e-ecfa-41c4-b681-9b684bc3b3bf/

CyberSec Science

Event 2019969e-ecfa-41c4-b681-9b684bc3b3bf

Source IP: 219.80.193.15

Destination IP: 44.155.75.24

Attack Type: Ransomware

Severity: Critical

Response

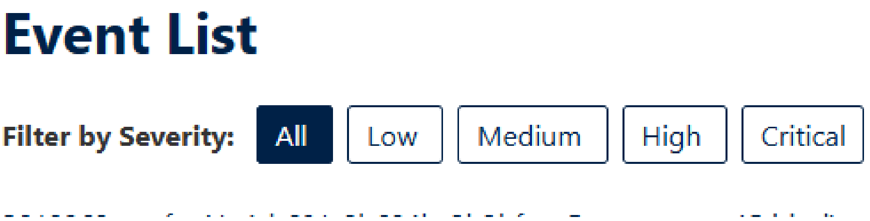
Attack Type: Ransomware

Data Exfiltrated: FALSE

Threat Intelligence: Crime low this behind option tax product.

Response Action: Eradicated

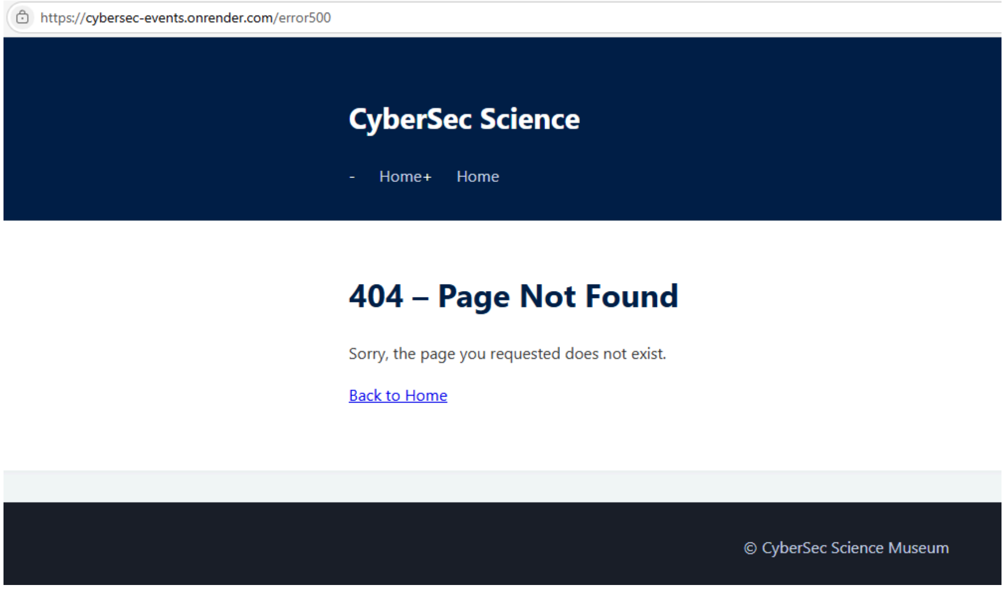
Detailpage



Event List

Filter by Severity:

Filter



https://cybersec-events.onrender.com/error500

CyberSec Science

404 – Page Not Found

Sorry, the page you requested does not exist.

© CyberSec Science Museum

ErrorPage