CST336 Final Project

Dakota Hyman

Sam Numan

Alexandra Miller

12 August 2025

Project Report

1. Project Title: “Secure My Node: Node JS Vulnerability Database”
2. Description:
    - The project is implemented as an interactive website dedicated to a collection of Node JS vulnerabilities, rated with the industry standard CVSS (Common Vulnerability Scoring System score) method. Such collections are useful for conducting application security assessments for Node JS-based Web applications.
    - The website has a functionality allowing users to add new vulnerabilities to the database, update existing vulnerability records and review existing vulnerabilities.
    - The website provides users with an opportunity to score a rank in the Contributors Board page, making it a fun and engaging experience to add new vulnerabilities.
    - The website has a page dedicated to the team members, where their background and skills are introduced, allowing the audience to learn more about the team.
    - The Contact page of the website allows users to provide feedback on the site, where a user can send a message, comment or suggestion to the project team.
    - The below table provides a more detailed description of how the tasks were distributed among the team members.

Task Distribution	Implementation
Database modeling: table design, SQL file implementation, key designation.	Alex designed the database scheme and implemented the initial SQL file for building tables, Dakota prepared the data for tables and Sam made important improvements to the SQL file to ensure stability of data processing and correct data formatting.

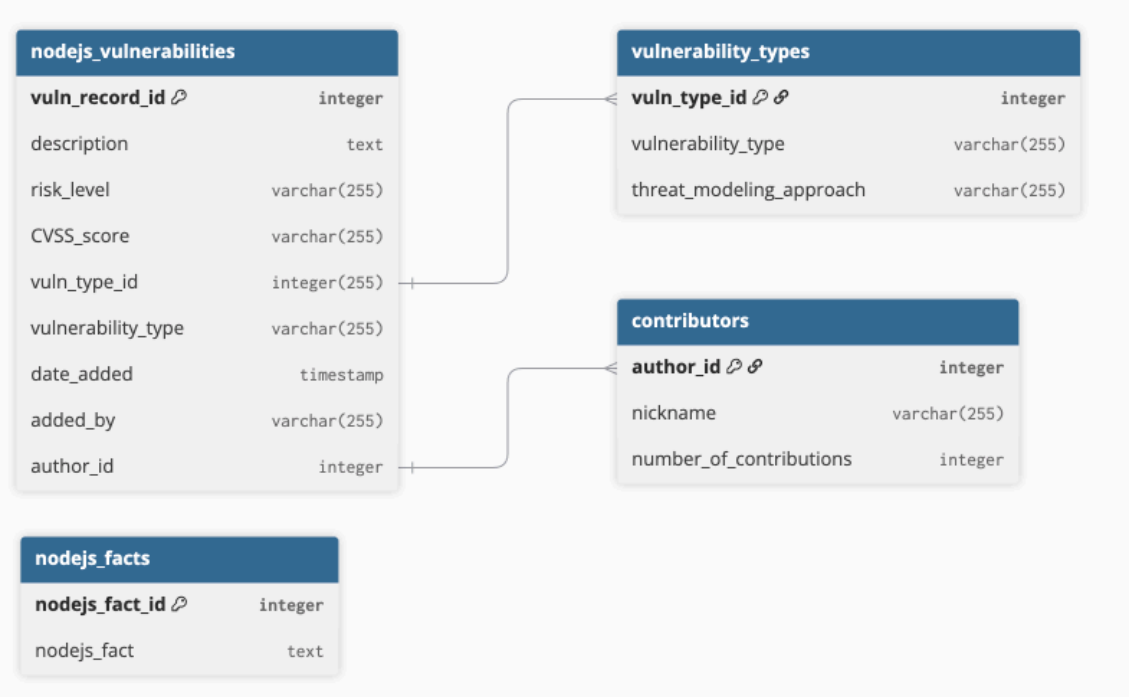
Adding Vulnerability Records	Sam has implemented the functionality for adding new vulnerability records based on the Team's agreed-upon design that meets the requirements for having different types of interactive elements. There are multiple interactive elements in the form, which include a drop down menu, a checkbox, a text input box and a colorful picker.
Internal API for Vulnerability of the Day (shows Random Node JS Vulnerability on the Home page)	Alex, Dakota and Sam all contributed to the APIs development, with Sam designing the original display space and fetching, Alex configuring the index.mjs file with SQL queries to display a random vulnerability and a fun fact about Node JS on the home page, while Dakota contributed valuable input for JSON formatting of the output.
Internal API for the Node JS Fun Fact	
View and Edit Vulnerability Records	Sam has implemented the viewing and editing functionality based on the Team's agreed upon ideas and formatting which ensures clean and user-friendly view for editing an existing vulnerability record, while meeting the requirement that the user is able to edit at least three fields and the fields show as pre-populated with record data.
Contributor Board Page	Dakota has implemented the Contributor Board page, which provides an interactive and fun way for users to participate in the community by scoring a rank on the Contributor's page in return for adding new vulnerabilities to the site.
Team SeaQuence Page	Alex has implemented the Team SeaQuence Page, with Sam and Dakota contributing their Bios. This is a fun way for the users to meet the team and learn about their background.
Contact Page	Alex has implemented the Contact page, where she utilized Java Script client-side code for user input data validation to ensure that user provides a valid email when submitting feedback to the site team.

CSS, Visual Design, Site Logo	Sam led the implementation, while Alex and Dakota contributed to Visual Design and User Experience with emphasis on clear-cut, modern tech style, with top navigation that is user-friendly, slick and intuitive for the users. Alex created the Site Logo.
Deployment of Project to Fast Comet	Alex deployed the project to Fast Comet, established the database with phpMyAdmin, SQL and database connection configuration.

Implementation Details:

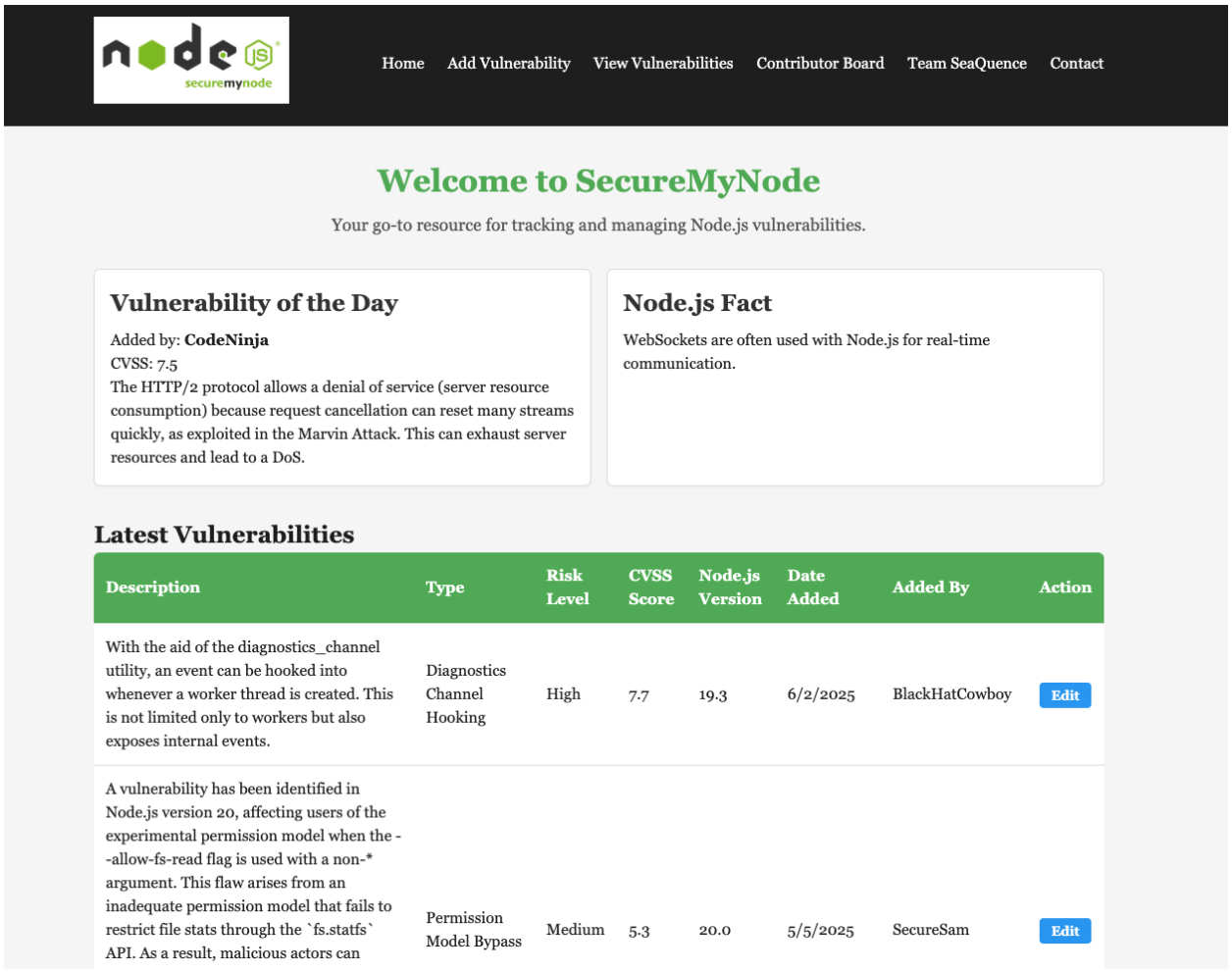
Where are the Fetch Calls Located:	The fetch calls are located in the scripts.js file, which is placed in the /public/js folder.
How AI was utilized for the Project:	The AI was utilized to explore various options for server-side implementation, including assessment of resource requirements for the app. It was also utilized to scout for visual aids and some debugging.

Database Schema:



Project Screenshots:

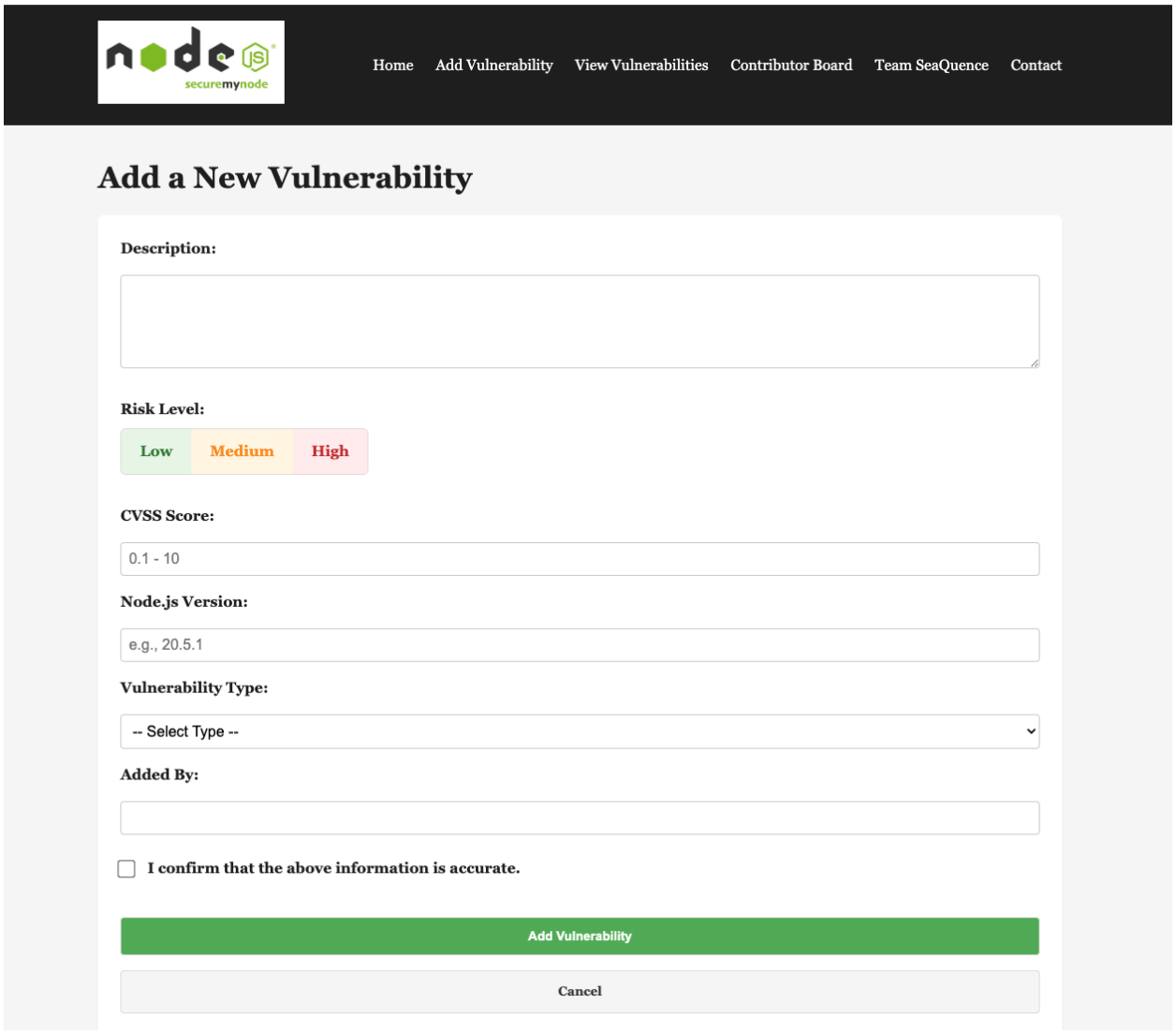
Home Page: www.mysecurenode.com



Note: The Vulnerability of the Day and the Node JS Fact APIs are displayed in the top section.

Project Screenshots:

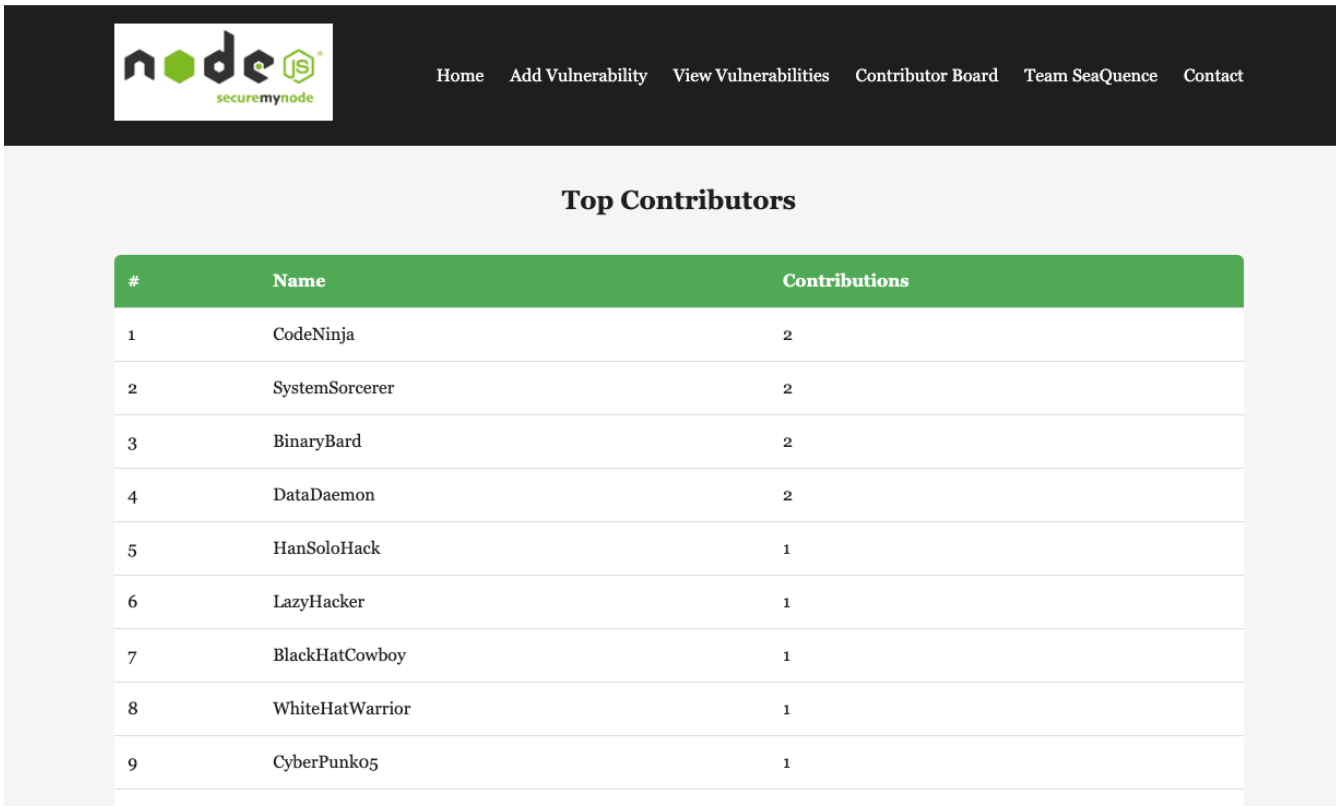
Add New Vulnerability Page: www.mysecurenode.com/addVulnerability



Note: Interactive elements on the form include drop down menu, check box, color picker and input text box.

Project Screenshots:

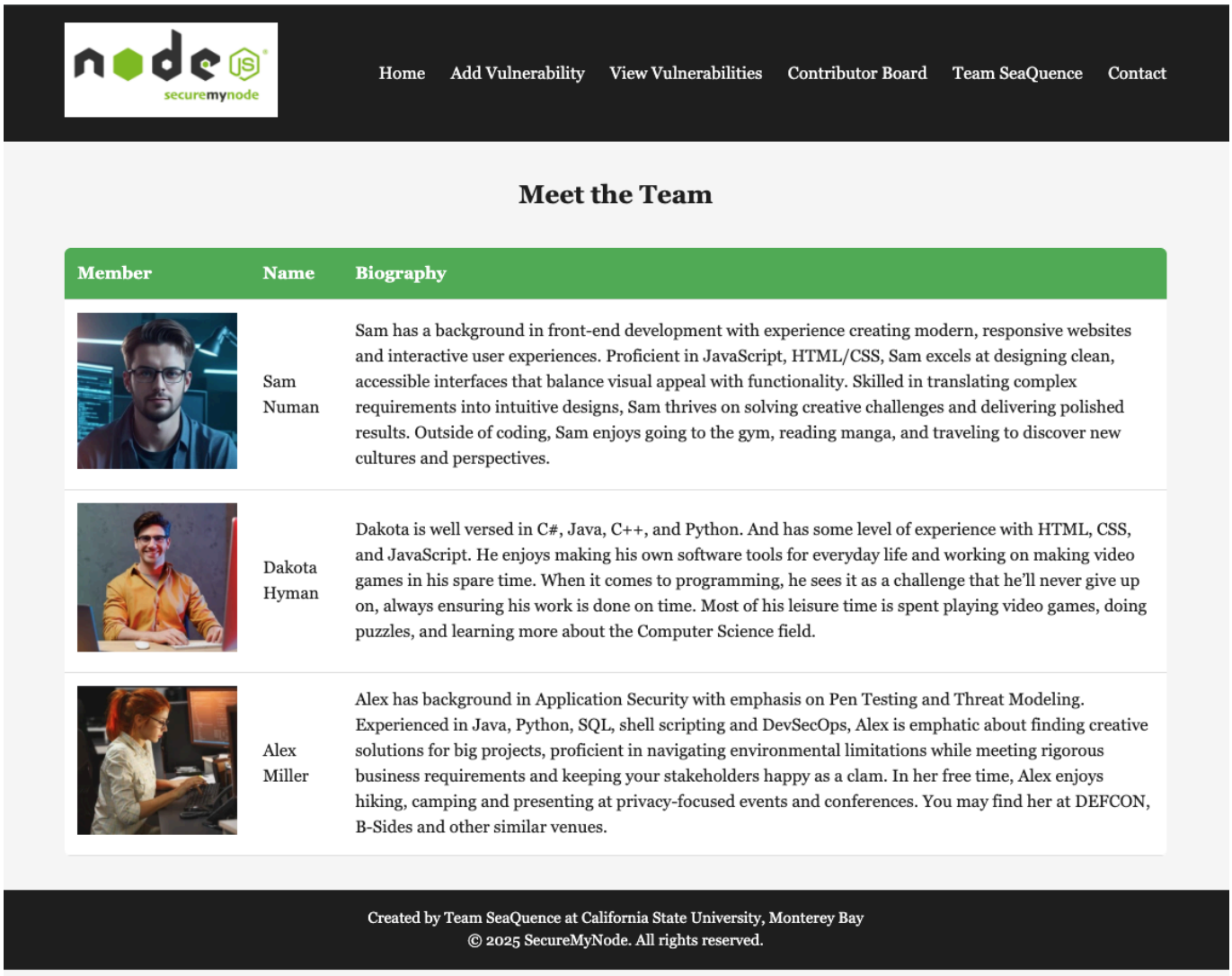
Contributor Page: www.mysecurenode.com/contributors



Note: The Contributor Board displays the top users who contributed vulnerabilities to the site.

Project Screenshots:

Contributor Page: www.mysecurenode.com/team

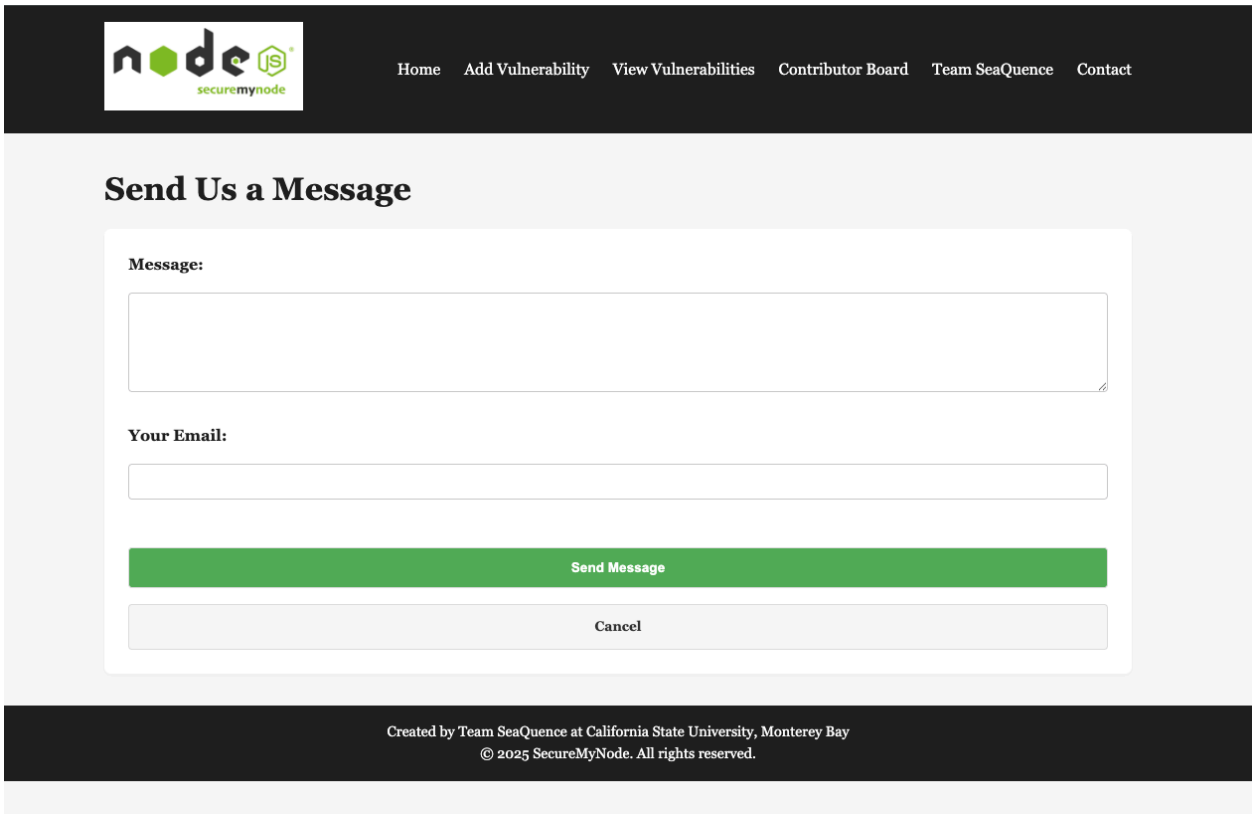


Note: The team page contains introductions and background information for each team member.

Disclaimer: team images are close replications of team members, adjusted for privacy purposes.

Project Screenshots:

Contact Page: www.mysecurenode.com/contact



Note: The Contact page allows users to submit feedback to the site.