

Cybersecurity Internship

Intern Name: *Mahnoor Khurram*

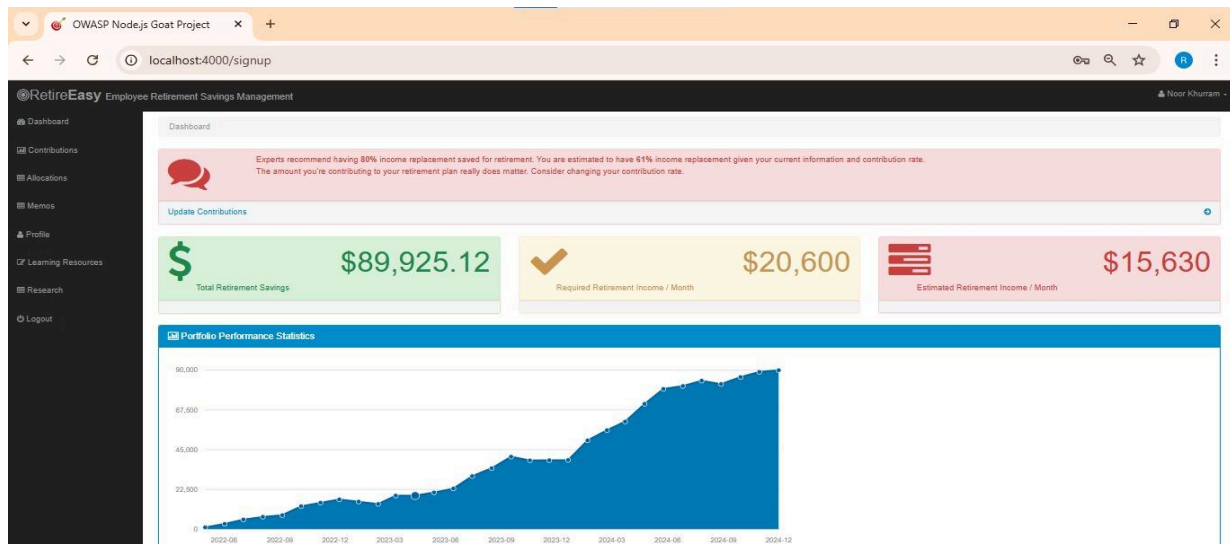
Security Progress Report – Week 2

1. Project Overview

In Week 2, I focused on fixing two major security risks from the OWASP Top 10 list: **Broken Authentication (A2)** and **Input Validation**.

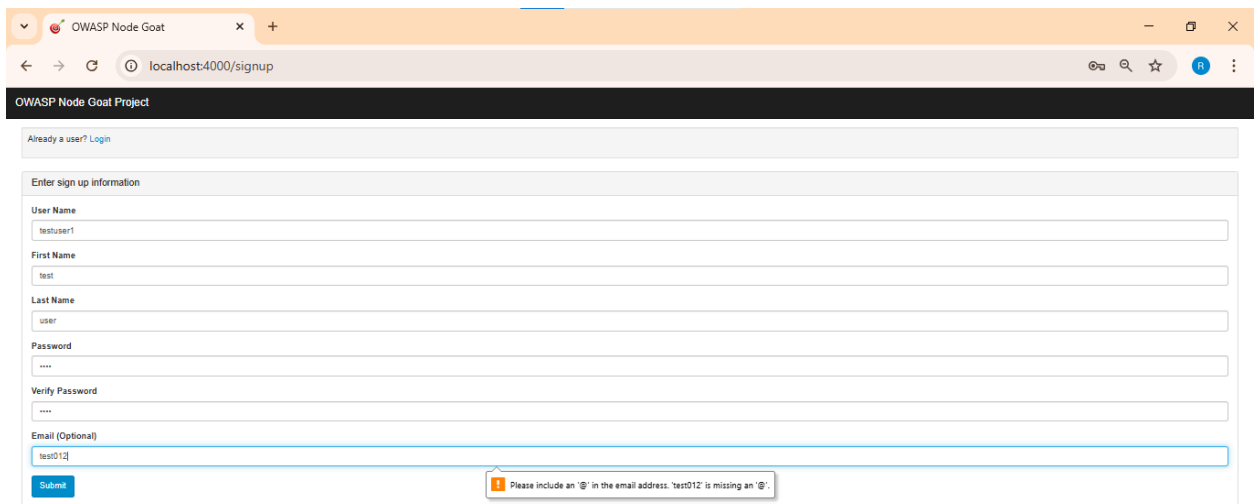
2. Task 1: Fixing Broken Authentication (A2)

- **Problem:** User passwords were saved in "Plain Text" in the database, making them easy to steal if the database was breached.
- **Solution:** I implemented **BCrypt hashing** using the `bcrypt-nodejs` library to encrypt passwords before saving them.
- **Evidence:** * **Terminal Error:** My screenshot shows the error "**Not a valid BCrypt hash**" when trying to log in with an old, unhashed password.
 - **Successful Login:** After creating a new user with a hashed password, I successfully accessed the **Dashboard**.



3. Task 2: Input Validation (User Signup)

- **Problem:** The signup form accepted any text in the email field, allowing users to enter invalid or malicious data.
- **Solution:** I installed the `validator` package and added a check to ensure only valid email formats (e.g., name@email.com) are accepted.
- **Implementation:** I added `const validator = require("validator")` at the top of `user-dao.js` and included an email validation check in the `addUser` function.
- **Evidence:** * **Browser Error:** When I tested a fake email (without "@"), the browser blocked the signup and displayed an error message.



The screenshot shows a web browser window with the title "OWASP Node Goat Project" and the URL "localhost:4000/signup". The page displays a signup form with the following fields: "User Name" (filled with "testuser1"), "First Name" (filled with "test"), "Last Name" (filled with "user"), "Password" (filled with "****"), "Verify Password" (filled with "****"), and "Email (Optional)" (filled with "test012"). A blue "Submit" button is at the bottom left. A red error message box at the bottom right states: "Please include an '@' in the email address. 'test012' is missing an '@'." Above the form, there is a link that says "Already a user? Login".

4. Final Outcome

The application is now significantly more secure. Passwords are protected by hashing, and the signup process is guarded against invalid data.