Cybersecurity Internship Report: Week 1

Intern Name: Mahnoor Khurram

Project: Security Assessment of NodeGoat Application

Date: December 30, 2025

---

1. Introduction

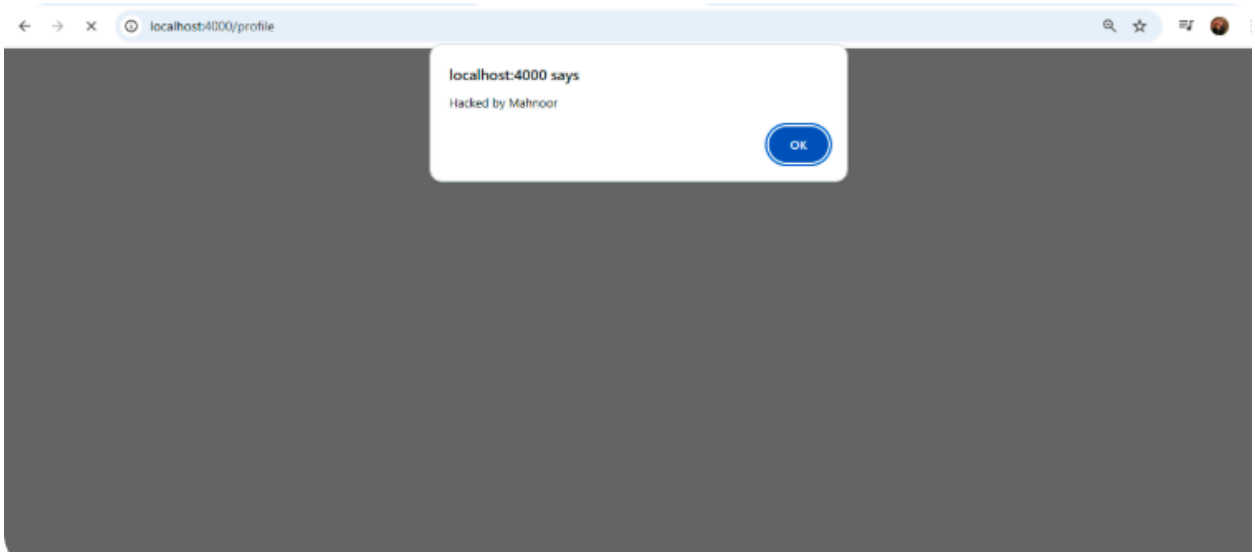
The goal of this week's task was to perform a manual security assessment on a local web application (NodeGoat). I focused on identifying common vulnerabilities such as **Cross-Site Scripting (XSS)** and **SQL Injection (SQLi)** using manual techniques and Browser Developer Tools.

---

2. Security Findings

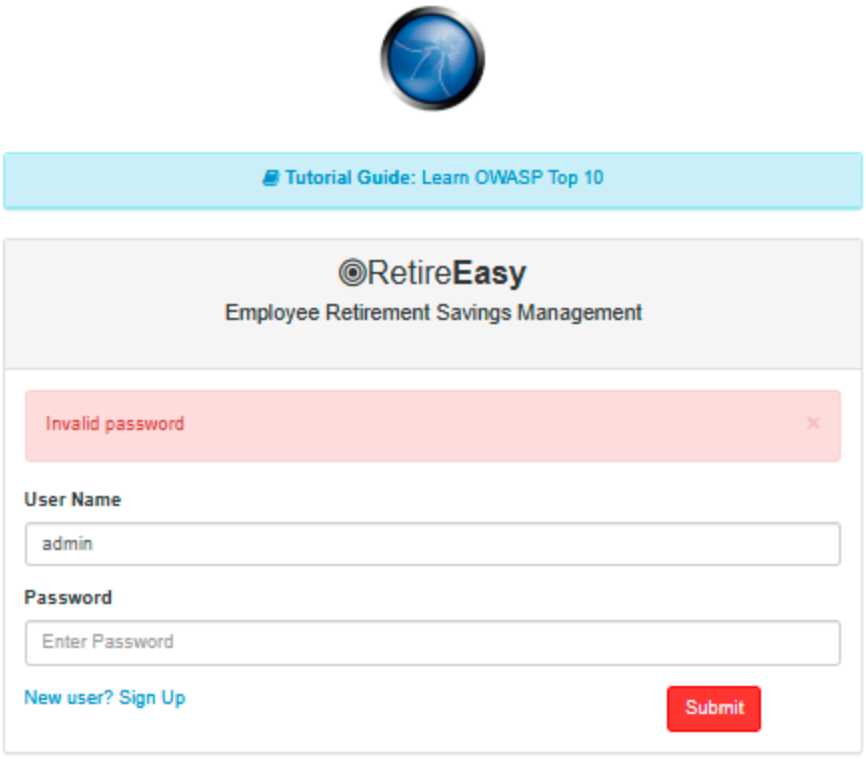
A. Stored Cross-Site Scripting (XSS)

- **Method:** I entered a malicious JavaScript payload `<script>alert('Hacked by Mahnoor')</script>` into the "First Name" field on the Profile page.
- **Result:** The application failed to sanitize the input, and the script executed automatically, displaying an alert box.
- **Impact:** This is a **High** severity issue because an attacker could use this to steal user cookies or session data.



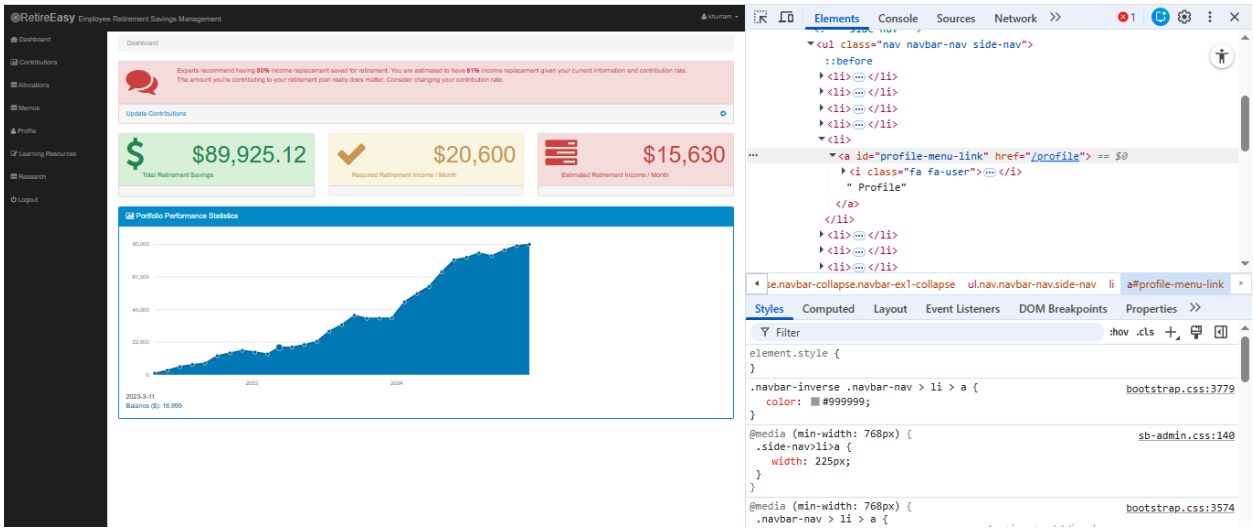
B. SQL Injection (SQLi) Attempt

- **Method:** I attempted to bypass the login screen by entering a common SQL payload: `admin' OR '1'='1` in the username and password fields.
- **Result:** The application returned an "Invalid username" error message.
- **Conclusion:** This indicates that the login form has basic input validation or protection against simple SQL injection attacks.



C. Browser Developer Tools Analysis

- **Method:** I used the browser's "Inspect Element" feature to analyze the website's frontend code and DOM structure.
- **Result:** I was able to see how the application handles data and identify specific input fields for testing.



3. Recommendations

- **Fix XSS:** Implement strict input validation and output encoding to prevent scripts from running in the browser.
- **Improve Security:** Ensure the application uses HTTPS to encrypt data between the user and the server.