Kalila Lin Cen

# Cyber Security Analysis Report

FitStudio Web Management

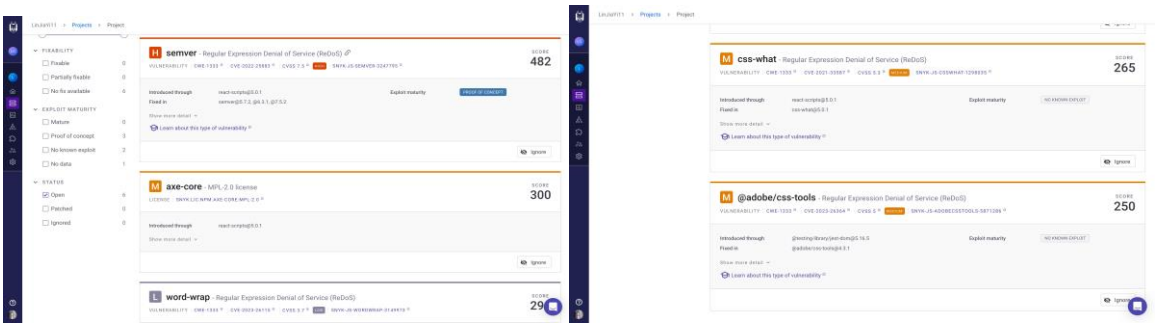
FitStudio is a web application developed for the gym manager, personal trainers, and their trainees, with the primary purpose of streamlining operations and improving efficiency within the fitness training business. The project focuses on creating a user-friendly platform that facilitates various tasks with the following key Features: The website will include a visually appealing homepage that effectively showcases personal training services to attract potential clients. Trainees will have access to their profiles, enabling them to manage personal information, view course details, and provide feedback and ratings for training sessions. Trainers, on the other hand, will have a portal where they can easily access their profiles and trainee lists. A significant feature for trainers is the automation of program card generation, reducing the manual effort required. Administrators will have secure access to all trainer and trainee profiles, course information, and the ability to create trainer accounts. They can also review trainer feedback and scores, simplifying bonus calculations. Lastly, the website will be optimized for mobile devices to accommodate trainers who need on-the-go access to essential features and information while working in the gym.

**Static Code Scanning with Snyk**

| Vulnerabilities | Severity | Vulnerabilities Exploitation | Solution |
|---|---|---|---|
| nth-check Regular Expression Denial of Service (ReDoS)<br><br>(Low frequency) | Because the affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) while parsing contrived erroneous CSS nth checks, the severity is high. | It can be used to generate excessive backtracking inside the regular expression engine by manipulating particular regular expressions. | To prevent ReDoS, redesign the regular expressions and employ techniques such as input validation, rate limitation, and so on, as well as web application firewalls and security tools. |
| Semver Regular Expression Denial of Service (ReDoS)<br><br>(Low frequency) | Because the affected versions of this package are vulnerable to ReDoS via the function new Range, the severity is high. | It can be abused by tampering with a regular expression pattern used to parse Semantic Version (Semver) strings. | Instead of regular expressions that allow backtracking, use an approach like non-backtracking regex. |
| css-what Regular Expression Denial of Service (ReDoS)<br><br>(Low frequency) | Because the affected versions of this package are vulnerable to ReDoS via attribute parsing, the severity is medium. | It can be utilised when a regular expression used to parse and process CSS selectors is prone to backtracking. | Optimise the regular expression and apply the strategies listed above. |

Kalila Lin Cen

## Screenshots Evidence




## Static Code Scanning with OX Security

| Vulnerabilities | Severity | Vulnerabilities Exploitation | Solution |
|---|---|---|---|
| Open-source security: @testing- library/jest-dom@5.16.5 is a JavaScript direct dependency having 1 indirect vulnerability and no direct vulnerabilities. Top risk: CVE-2023-26364 is the most severe vulnerability.<br><br>(Medium frequency) | Because development dependencies are usually not critical to fix right away, the severity is low. | It can lead to denial-of-service attacks in which an attacker enters malicious regular expressions that cause excessive CPU utilisation and slow down the affected system. | Consider using a se a library with less security issues. |
| Open-source security: react-scripts@5.0.1 is a JavaScript direct dependency having 3 indirect vulnerabilities and no direct vulnerabilities. The dependency is not imported into the code.<br><br>(Medium frequency) | The severity is high because this vulnerability has the potential to trigger ReDoS. | This is due to a bug in the nth-check Node.js module. When specific checks are run, this vulnerability may use a substantial amount of system resources.<br>Attackers could take advantage of this flaw to perform denial-of-service attacks or cause resource depletion in affected systems. | Consider using a se a library with less security issues. |

| | | | |
|---|---|---|---|
| Open-source security: react-scripts@5.0.1 is a JavaScript direct dependency having 3 indirect vulnerabilities and no direct vulnerabilities. The dependency is not imported into the code.<br><br>(Medium frequency) | The severity is medium since the packages that are triggering these vulnerabilities are no longer in use and may be deleted or upgraded. | A bug in the Node.js word-wrap module has been discovered, making it vulnerable to a denial of service triggered by a ReDoS issue in the result variable. A remote attacker can create a denial of service by providing carefully crafted regex input. | Consider removing these dependencies because they are not in used anyway. |

## Screenshots Evidenc