# **Code Analysis Summary**

10/25/2023 Commit: 223

## **Static Application Security Testing (SAST)**

Summary: The analysis has identified 25 code issues in the project, categorized as follows:

- 5 High severity issues
- 3 Medium severity issues
- 17 Low severity issues

## **High Severity Issues:**

**Info**: Unsensitized input from cookies flows into the return value of total\_data, pie\_data, cube\_data, meter\_data, where it is used to render an HTML page returned to the user. This may result in a Cross-Site Scripting attack (XSS)

bokeh.py (line 14, 20, 26, 32, 38)

## **Medium Severity Issues:**

**Info**: Running the application in debug mode (debug flag is set to True in run) is a security risk if the application is accessible by untrusted parties.

server.py (line 40)

**Info**: Unsensitized input from remote resources is utilized to dynamically construct the HTML page on the client side, potentially resulting in DOM Based Cross-Site Scripting (DOMXSS) attacks.

- single-page-index.html (line 1002, 1019)

### **Low Severity Issues:**

**Info**: Sensitive cookies in HTTPS sessions lack the 'Secure' attribute, making them susceptible to man-in-the-middle attacks.

- session.py (line 116)

**Info**: SQL Injection vulnerabilities exist due to unsensitized input from HTTP parameters flowing into SQL queries, potentially leading to SQL Injection attacks.

- app.py (line 132, 162, 193, 197, 133, 163, 194, 198)

**Info**: Cookies are missing the 'HttpOnly' flag, exposing them to malicious client-side code.

- session.py (line 116)

**Info**: Hardcoded credentials are found in the code, which is considered a poor security practice.

- app.py (line 122, 152, 183, 255)

**Info**: Unsensitized input from HTTP parameters flows into functions responsible for rendering HTML pages, potentially resulting in Cross-Site Scripting (XSS) attacks.

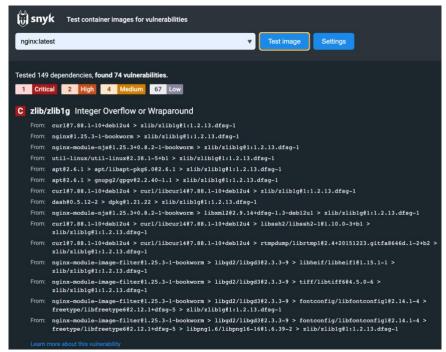
- app.py (line 149, 178, 251)

## **Docker Analysis**

The analysis was an on the following Docker Images using Docker Scout and Snyk: After closer assessment, the vulnerabilities were not relevant and patches are not out.

## nginx:latest and src-web:latest





https://security.snyk.io/vuln/SNYK-DEBIAN12-ZLIB-6008963

#### mariadb:latest



