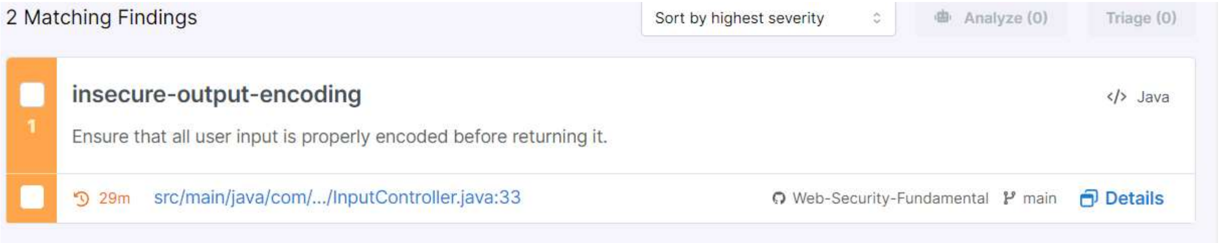
Semgrep report


2 Matching Findings

insecure-output-encoding

Ensure that all user input is properly encoded before returning it.

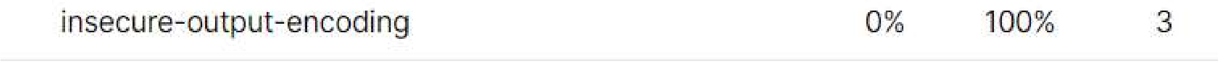
src/main/java/com/.../InputController.java:33

User inputs were not encoded properly before rendering, leading to potential XSS attacks.

Improvements that implemented

- Ensure that all user inputs are encoded before rendering in responses.
- Use Spring Boot’s built-in mechanisms

This is the output after fixing is 100% fixed


| | | | |
|---|---|---|---|
| insecure-output-encoding | 0% | 100% | 3 |

understanding of web security fundamentals

Web security fundamentals focus on protecting web applications from various threats and vulnerabilities. Key concepts include Cross-Site Scripting (XSS), which involves injecting malicious scripts into web pages, and Cross-Site Request Forgery (CSRF), where attackers trick users into making unwanted requests. Effective prevention strategies involve encoding user inputs, using anti-CSRF tokens, and implementing secure communication with HTTPS. Proper authentication and authorization ensure users access only permitted resources, while secure coding practices, such as input validation and using prepared statements, protect against attacks like SQL injection. Regular security scanning, dependency management, and secure error handling are crucial for maintaining application security. Adhering to these practices helps safeguard data, maintain user trust, and enhance overall application security.