

Name: Amira Afolabi

ID: 2583034

Github link: <https://github.com/amiraa-code/RateFlixWeb>

Security Vulnerability Explanation

After first scan I had one high risk vulnerability and 35 others, I fixed it and added more security headers like: X-Content-Type-Options: nosniff which Stops MIME sniffing; browsers won't guess file types, reducing drive-by script execution risks and X-Frame-Options: DENY which Blocks the site from being embedded in iframes; prevents clickjacking.

The screenshot shows a web-based security audit tool. At the top, there are tabs for History, Search, Alerts (which is selected), Output, Spider, and AJAX Spider. Below the tabs, there are icons for Home, Logout, Refresh, and Help.

The main area displays a list of vulnerabilities under the 'Alerts' tab:

- Vulnerable JS Library (1)
- Absence of Anti-CSRF Tokens (3185)
- Application Error Disclosure (256)
- CSP: Failure to Define Directive with No Fallback (2152)
- CSP: script-src unsafe-eval (2151)
- CSP: script-src unsafe-inline (2151)
- CSP: style-src unsafe-inline (2151)
- Content Security Policy (CSP) Header Not Set (488)
- Cross-Domain Misconfiguration (7)
- Directory Browsing (244)
- Missing Anti-clickjacking Header (336)
- Vulnerable JS Library (2)
- Application Error Disclosure (1)
- Big Redirect Detected (Potential Sensitive Information Leak) (163)
- Cookie No HttpOnly Flag (11)
- Cookie without SameSite Attribute (11)

To the right, a detailed view of the 'Vulnerable JS Library' alert is shown:

Vulnerable JS Library

URL: http://localhost/phpmyadmin/doc/html/_static/underscore.js
Risk: High
Confidence: Medium
Parameter:
Attack:
Evidence: // Underscore.js 1.9.1
CWE ID: 1395
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
The identified library appears to be vulnerable.
Other Info:
The identified library underscore.js, version 1.9.1 is vulnerable.
CVE-2021-23358
<https://nvd.nist.gov/vuln/detail/CVE-2021-23358>
Solution:

At the bottom, there are summary statistics: Alerts 1, Critical 11, High 11, Medium 13, and Main Proxy: localhost:8080.

I had these afterwards and I couldn't solve them because it was complaining mostly about my outdated xampp version, font awesome and tailwind headers: