

Name: Amirat 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 displays the Burp Suite application window. The top toolbar includes icons for History, Search, Alerts, Output, Spider, and AJAX Spider. The left sidebar shows a list of alerts under the 'Alerts (36)' section. The 'Vulnerable JS Library' alert is selected, showing details for the URL `http://localhost/phpmyadmin/doc/html/_static/underscore.js`. The alert is categorized as 'High' risk with 'Medium' confidence. The description states: 'The identified library appears to be vulnerable.' The 'Other Info' section provides additional context: 'The identified library underscore.js, version 1.9.1 is vulnerable. CVE-2021-23358 https://nvd.nist.gov/vuln/detail/CVE-2021-23358'. The bottom status bar indicates 'Main Proxy: localhost:8080'.

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:

I had these afterwards and I couldn't solve them because it was complaining mostly about my outdated xampp version, font awesome and tailwind headers:

The screenshot displays the Burp Suite application interface. On the left, a sidebar lists 20 alerts, with 'CSP: script-src unsafe-inline (86)' selected. The main panel on the right provides details for this specific alert:

- URL:** `http://localhost/RATEFLIXWEB/user/frontend/login.php?return_to=%2FRATEFLIXWEB%2Fuser%2Ffrontend%2Findex.php`
- Risk:** Medium
- Confidence:** High
- Parameter:** Content-Security-Policy
- Attack:** Content-Security-Policy
- Evidence:** `default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net; img-src 'self' data; font-src 'self' https://fonts.gstatic.com; connect-src 'self';`
- CWE ID:** 693
- WASC ID:** 15
- Source:** Passive (10055 - CSP)
- Alert Reference:** 10055-5
- Input Vector:**
- Description:** Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable
- Other info:** script-src includes unsafe-inline.
- Solution:** Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
- Reference:** <https://www.w3.org/TR/CSP/>, <https://caniuse.com/#search=content+security+policy>

The bottom status bar shows 'Alerts: 0 7 5 8' and 'Main Proxy: localhost:8080'. A Windows watermark 'Activate Windows. Go to Settings to activate Windows.' is visible in the bottom right corner.

Test report is included in the zip files.