Sri Lanka Institute of Information Technology

Bug Bounty Report 02

WS Assignment

IE2062 – Web Security

IT23159730

W.H.M.S.R.Bandara

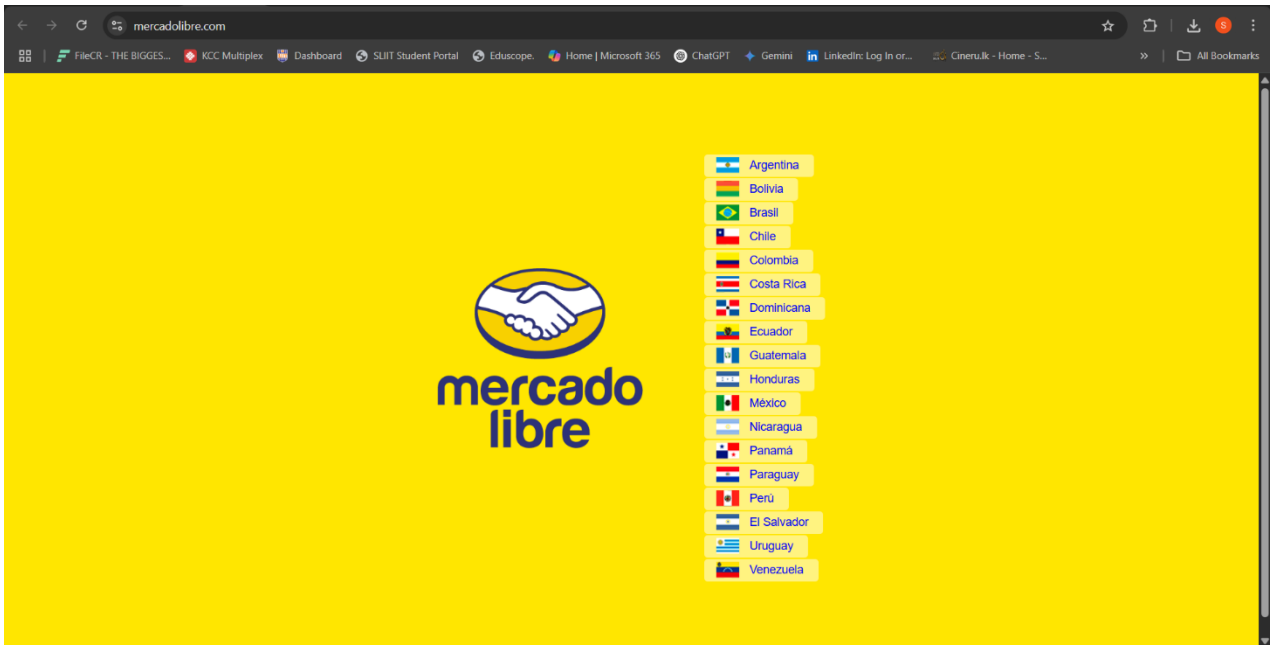
Vulnerability Title

Content Security Policy (CSP) Header Not Set & Cross-Site Scripting possible on https://www.mercadolibre.com/jms/*/lgz/

Vulnerability Description

A Content Security Policy (CSP) is a powerful HTTP header that allows website administrators to control the resources (JavaScript, CSS, images, etc.) that a user agent is allowed to load for a given page. The absence of a CSP header significantly increases the risk of **Cross-Site Scripting (XSS)** and **data injection** attacks, potentially allowing malicious scripts to execute in the browser context.

During a passive scan using OWASP ZAP, it was discovered that the response from https://www.mercadolibre.com/jms/*/lgz does **not include a CSP header**. This misconfiguration leaves the application vulnerable to client-side attacks and reduces its resilience against modern web threats.



Other scans

Firewall Detection.

Before the automated scan with OWASP ZAP (2.16.0), Identify the Firewall by using Wafw00f Tool.

Open Ports Detection

Done the nmap scan for detect open ports.

Scanning for common Issues

These scans done by with Nikto.

Identified vulnerabilities

Missing Security Headers

The target (https://www.mercadolibre.com) lacks critical security headers such as X-Frame-Options, X-Content-Type-Options, and Content-Security-Policy. This could expose the site to clickjacking, MIME-type sniffing, and XSS attacks.

Evidence:

The anti-clickjacking X-Frame-Options header is not present. The X-XSS-Protection header is not defined. The MIME type (text/html) may allow XSS

Affected Components

- **Domain:** www.mercadolibre.com
- **Endpoint:** /jms/*/lgz
- **Risk Level:** Medium
- **Confidence:** High
- **CWE ID:** 693 – Protection Mechanism Failure
- **WASC ID:** 15 – Application Misconfiguration

Impact Assessment

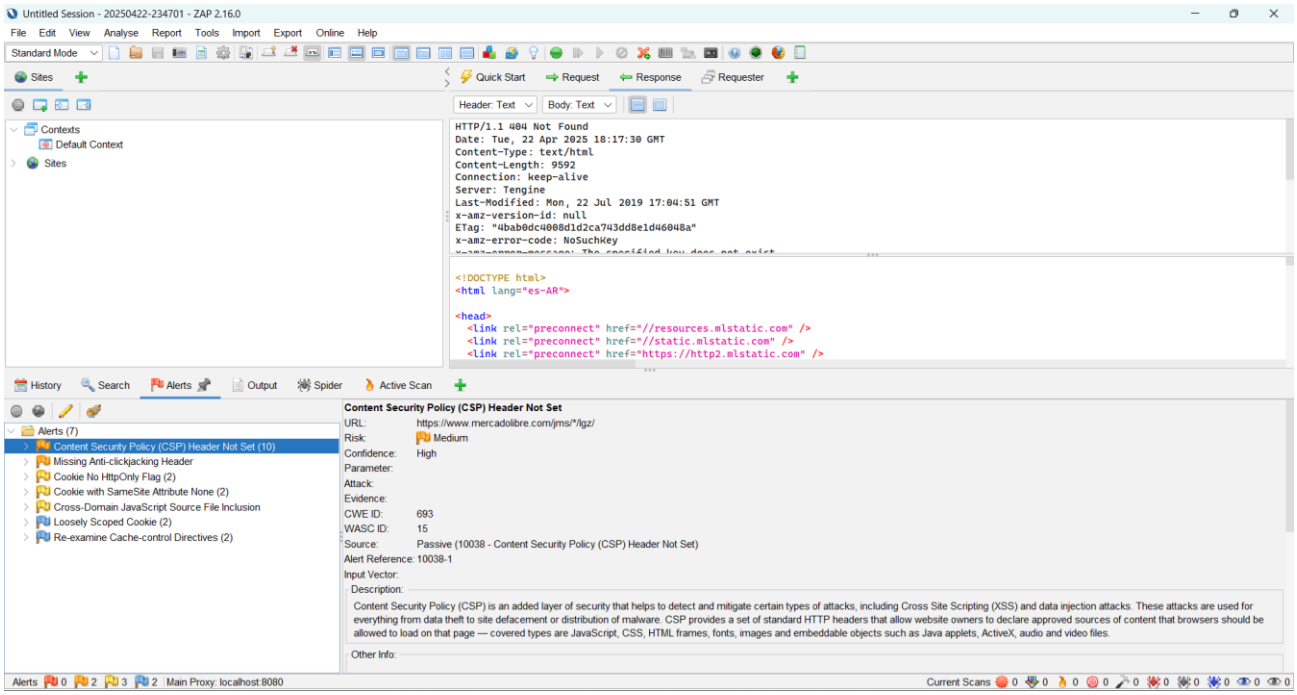
If exploited, this vulnerability may result in:

- **Cross-Site Scripting (XSS):** Attackers can inject scripts that execute in the user's browser, which can steal session cookies or manipulate content.
- **Clickjacking:** Without a strong CSP and other headers like X-Frame-Options, users can be tricked into clicking elements on invisible or disguised frames.
- **Malware Distribution:** The hacker can link malicious scripts or send users to third-party compromised resources.
- **Data Theft**: It stops the scripts from stealing any unauthorized data with CSP.
- **Broken Trust in Browsers:** Modern browsers use headers like CSP to help identify web content that can be trusted, so if they have no such policy it may get a bad reputation in their eyes, with warnings displayed in browsers.

Steps to Reproduce

1. Open OWASP ZAP and perform a passive scan of the domain https://www.mercadolibre.com.
2. Navigate to the endpoint: /jms/*/lgz
3. Navigate to the Alerts tab and look under Content Security Policy (CSP) Header Not Set.
4. Select the affected request and inspect the HTTP response headers.
5. Observe that the Content-Security-Policy header does not exist.

Proof of Concept Screenshot



Proposed Mitigation or Fix

- **Implement a Strict CSP Header:** Add a Content-Security-Policy HTTP header to all responses. A safe starting policy

  Content-Security-Policy: default-src 'self'; script-src 'self'; object-src 'none'; base-uri 'none';

- **Test CSP in Report-Only Mode:** Start with a Content-Security-Policy-Report-Only header to test the effect before enforcement.
- **Use Trusted Sources Only:** Restrict external resources (scripts, styles, frames) to trusted, secure domains only.
- **Avoid Inline Scripts:** CSP blocks XSS by disallowing unsafe-inline scripts. Rewrite JavaScript to avoid inline code blocks.
- **Regular Security Review:** Regularly review headers, test new resources added on the site, and refine policies.

Conclusion.

While the missing CSP header is not technically an exploit, it greatly lowers the site's defensive posture against today's client-side attacks. Having a strong CSP is a solid defense practice and is indeed one of the best practices for securing web applications, especially at MercadoLibre's size and exposure.