**Sri Lanka Institute of Information Technology**

**IE2062 - Web Security**

**Final Assignment**

**Bug Bounty Report 07**

**Name:** Peiris W.S.S.N

**Registration Number:** IT23227286

Contents

[1. Introduction 3](#_Toc196573295)

[2. Reconnaissance 4](#_Toc196573296)

[3. Vulnerability 5](#_Toc196573297)

[4. Vulnerability description 5](#_Toc196573298)

[5. Affected Components 6](#_Toc196573299)

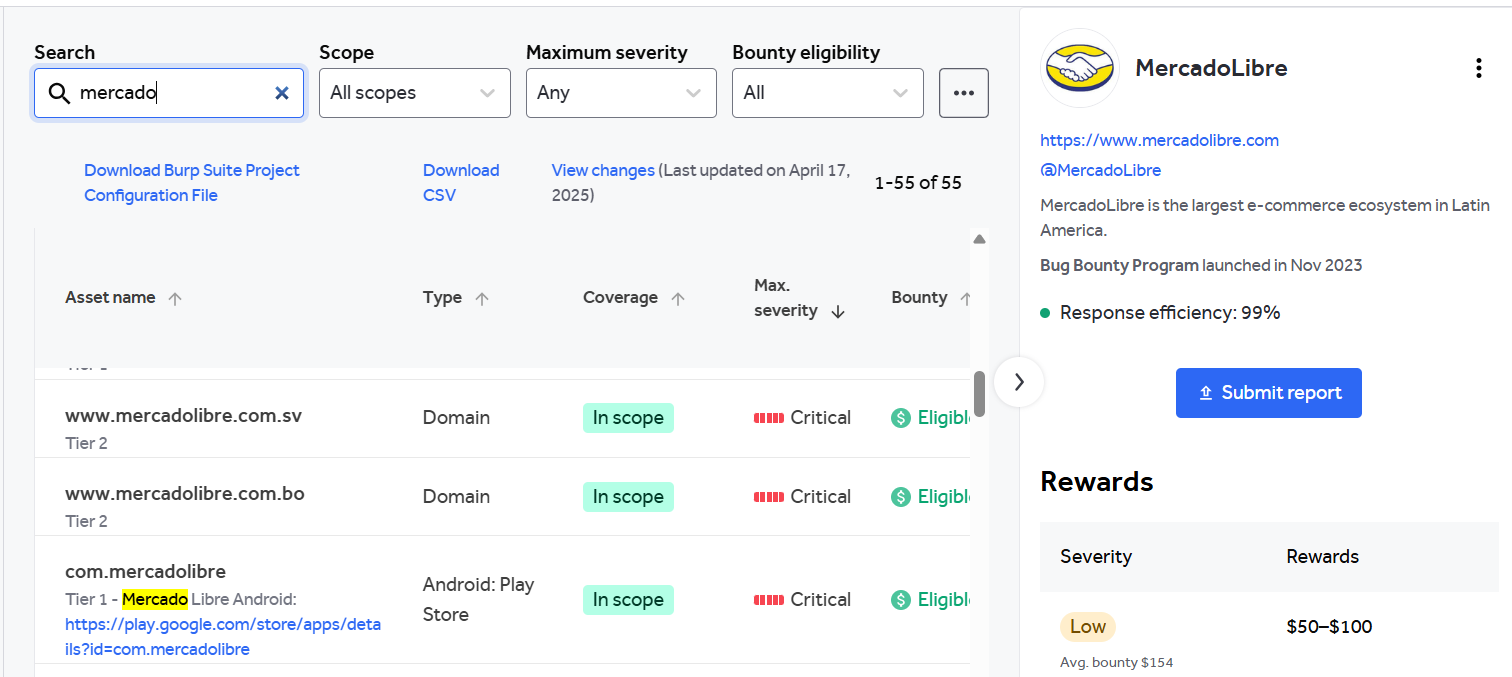
[6. Impact Assessment 6](#_Toc196573300)

[7. Steps to reproduce 7](#_Toc196573301)

[8. Proof of concept 7](#_Toc196573302)

[9. Proposed mitigation or fix 7](#_Toc196573303)

# Introduction

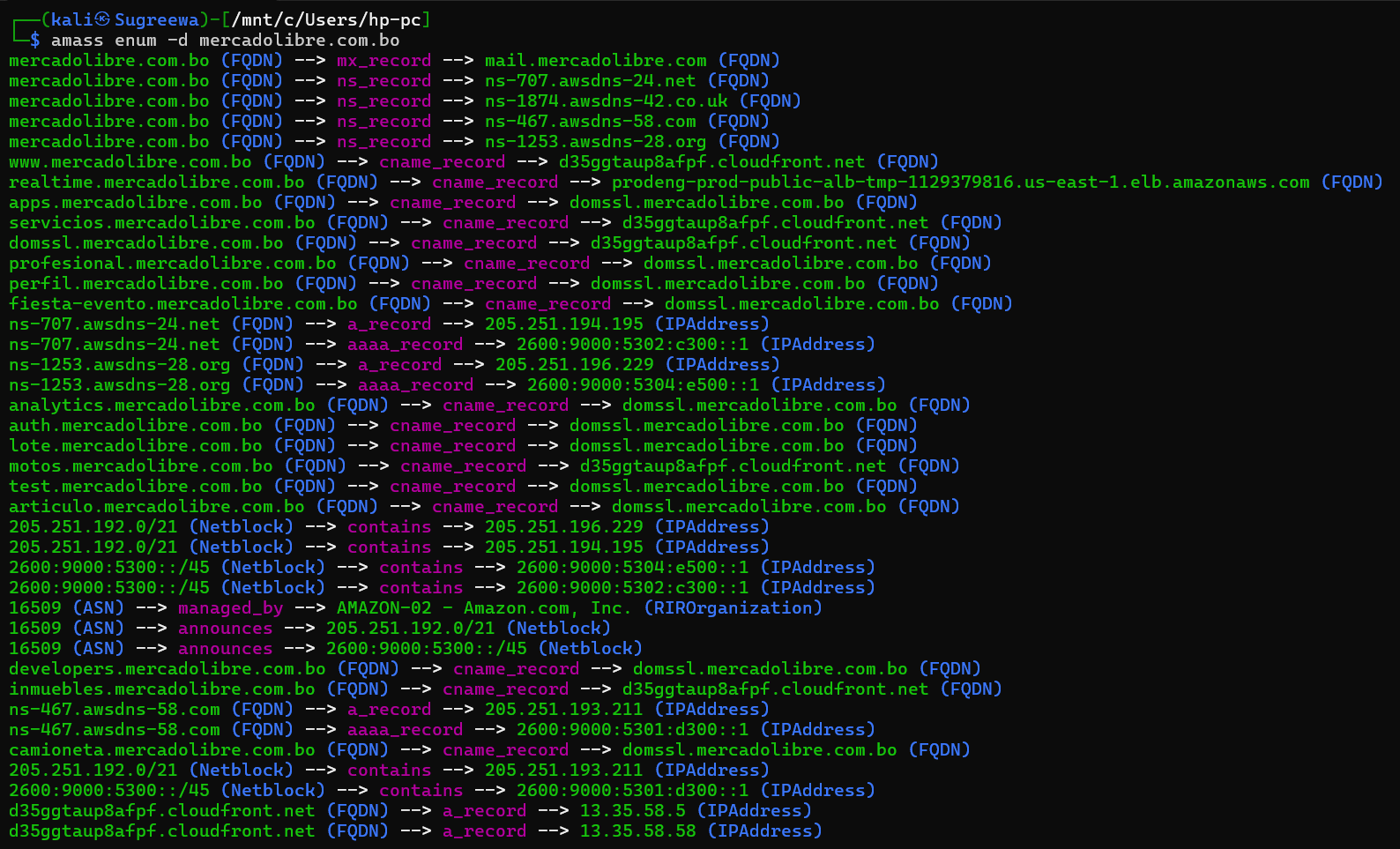


**Website:** <https://www.mercadolibre.com.bo/>

**Listed by:** MercadoLibre

# Reconnaissance

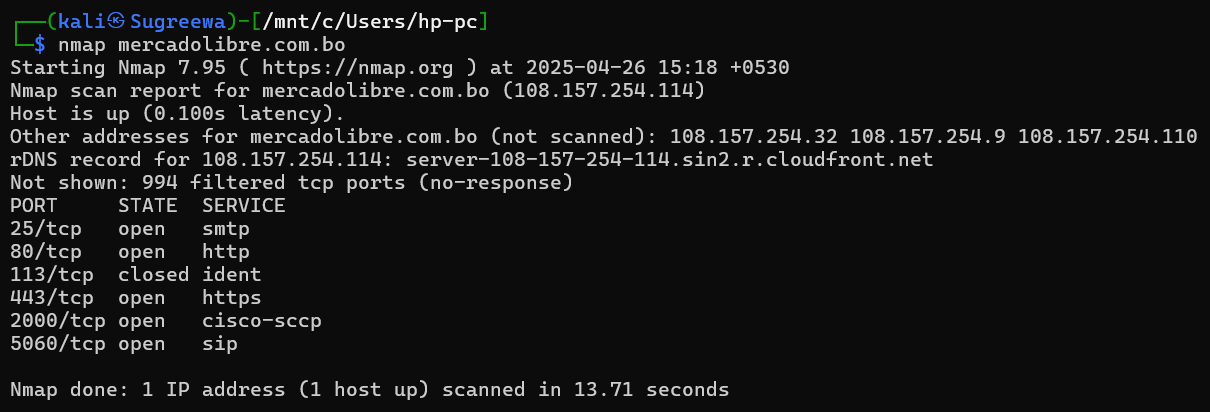
* **Subdomain enumeration using Amass**

****

* **Firewall Detection**

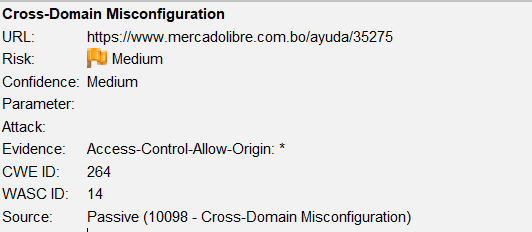
****

* **Nmap Scan**

****

# Vulnerability

* **Cross-Domain Misconfiguration**

****

# Vulnerability description

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

1. Affected Components

* **Component:** HTTP Response Header → Access-Control-Allow-Origin
* **Value Detected:** \*
* **Affected Endpoints:** Any API or web resource returning this header (typically GET requests to public APIs or JSON endpoints)
* **Context:** Applies to unauthenticated resources exposed via cross-origin GET requests

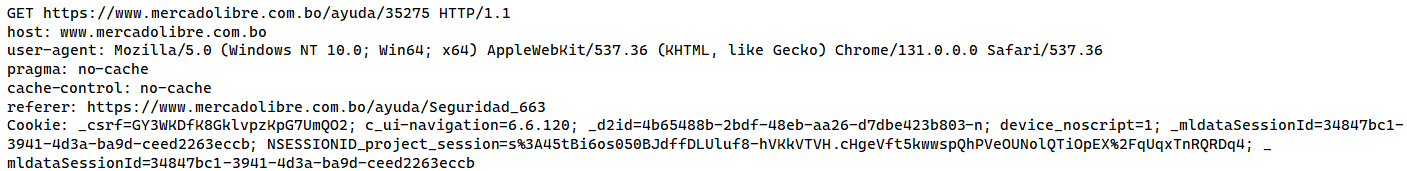
# Impact Assessment

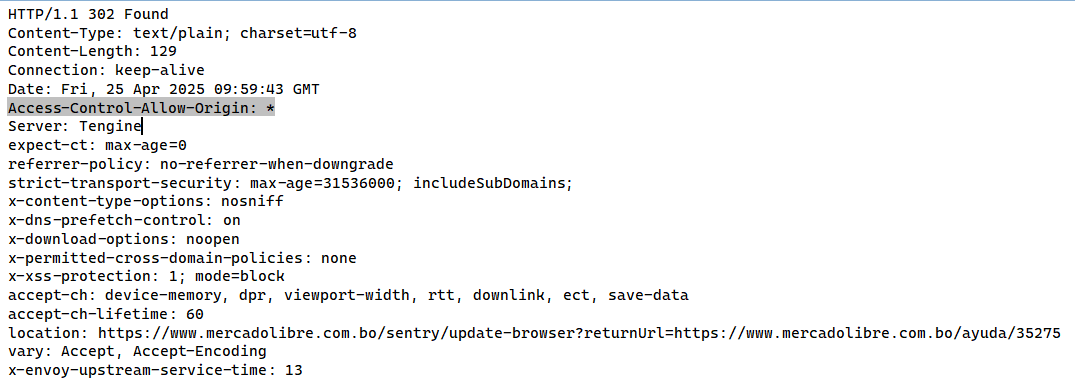
* **Risk Level:** Medium
* **Potential Impacts:**
  + Unauthorized access to publicly available (but sensitive) data
  + Abuse of endpoints intended for internal or IP-restricted use
  + May aid **data harvesting**, **fingerprinting**, or **API abuse**
  + Lower risk for authenticated endpoints (browsers block responses from credentialed cross-origin requests if \* is used)

# Steps to reproduce

* Open your browser’s **DevTools** or use **cURL**, **Burp**, or **Postman**.
* Send a GET request to a known unauthenticated API endpoint.
* Inspect the response headers.
* Confirm the presence of: Access-Control-Allow-Origin: \*

# Proof of concept





# Proposed mitigation or fix

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.