Sri Lanka Institute of Information Technology

IE2062 - Web Security

Final Assignment

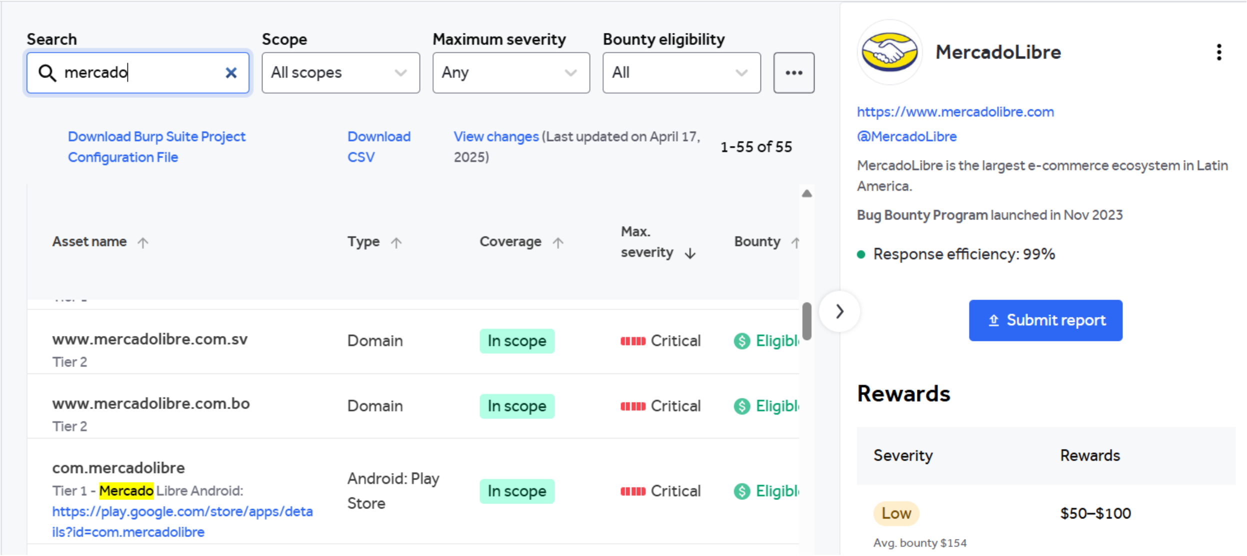
Bug Bounty Report 07

Name: Peiris W.S.S.N

Registration Number: IT23227286

Contents

1. Introduction



Search: mercado

Scope: All scopes

Maximum severity: Any

Bounty eligibility: All

Download Burp Suite Project Configuration File

Download CSV

View changes (Last updated on April 17, 2025)

1-55 of 55

Asset name	Type	Coverage	Max. severity	Bounty
www.mercadolibre.com.sv Tier 2	Domain	In scope	Critical	Eligibl
www.mercadolibre.com.bo Tier 2	Domain	In scope	Critical	Eligibl
com.mercadolibre Tier 1 - Mercado Libre Android: https://play.google.com/store/apps/details?id=com.mercadolibre	Android: Play Store	In scope	Critical	Eligibl

MercadoLibre

https://www.mercadolibre.com

@MercadoLibre

MercadoLibre is the largest e-commerce ecosystem in Latin America.

Bug Bounty Program launched in Nov 2023

● Response efficiency: 99%

Submit report

Rewards

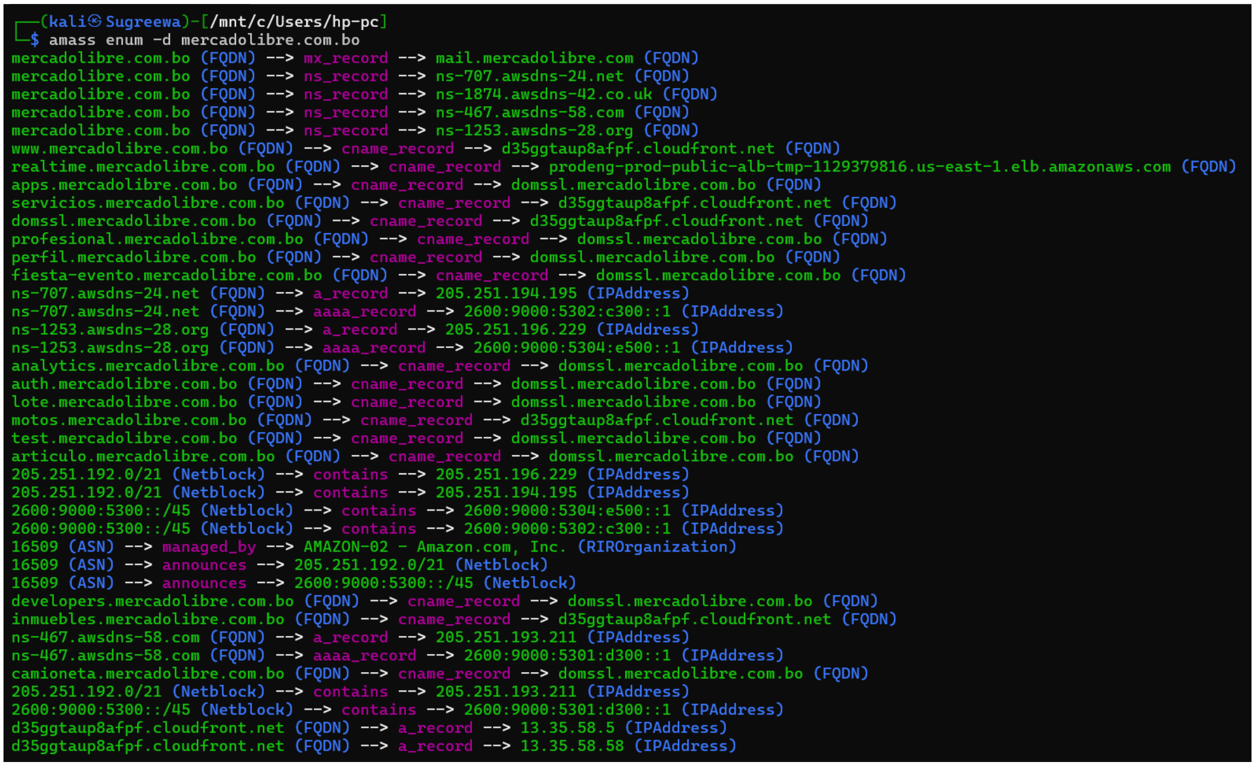
Severity	Rewards
Low Avg. bounty $154	$50–$100

Website: https://www.mercadolibre.com.bo/

Listed by: MercadoLibre

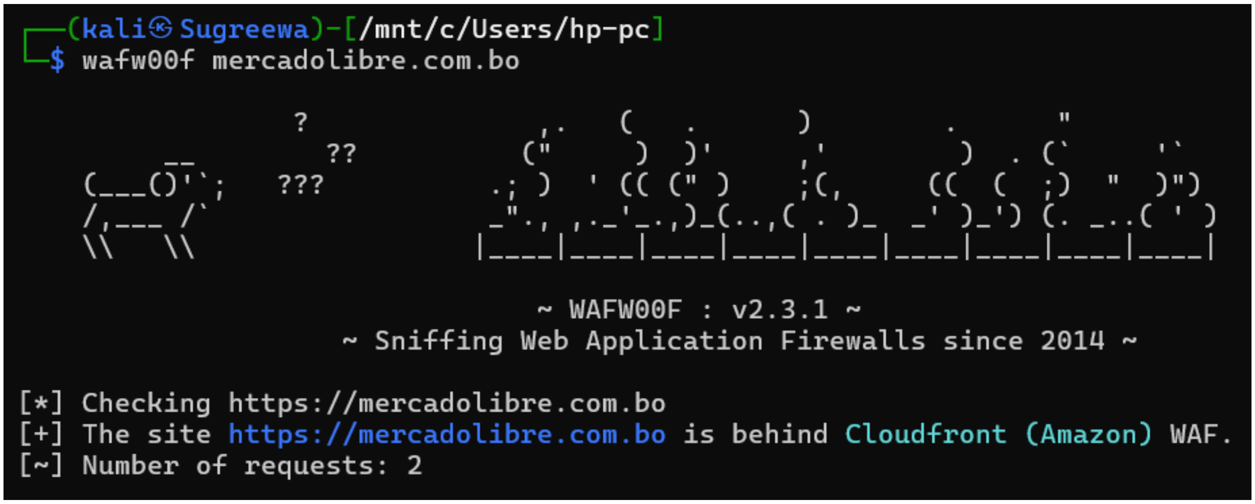
2. Reconnaissance

- **Subdomain enumeration using Amass**



```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ amass enum -d mercadolibre.com.bo
mercadolibre.com.bo (FQDN) --> mx_record --> mail.mercadolibre.com (FQDN)
mercadolibre.com.bo (FQDN) --> ns_record --> ns-707.awsdns-24.net (FQDN)
mercadolibre.com.bo (FQDN) --> ns_record --> ns-1874.awsdns-42.co.uk (FQDN)
mercadolibre.com.bo (FQDN) --> ns_record --> ns-467.awsdns-58.com (FQDN)
mercadolibre.com.bo (FQDN) --> ns_record --> ns-1253.awsdns-28.org (FQDN)
www.mercadolibre.com.bo (FQDN) --> cname_record --> d35ggtaup8afpf.cloudfront.net (FQDN)
realtime.mercadolibre.com.bo (FQDN) --> cname_record --> prodeng-prod-public-alb-tmp-1129379816.us-east-1.elb.amazonaws.com (FQDN)
apps.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
servicios.mercadolibre.com.bo (FQDN) --> cname_record --> d35ggtaup8afpf.cloudfront.net (FQDN)
domssl.mercadolibre.com.bo (FQDN) --> cname_record --> d35ggtaup8afpf.cloudfront.net (FQDN)
profesional.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
perfil.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
fiesta-evento.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
ns-707.awsdns-24.net (FQDN) --> a_record --> 205.251.194.195 (IPAddress)
ns-707.awsdns-24.net (FQDN) --> aaaa_record --> 2600:9000:5302:c300::1 (IPAddress)
ns-1253.awsdns-28.org (FQDN) --> a_record --> 205.251.196.229 (IPAddress)
ns-1253.awsdns-28.org (FQDN) --> aaaa_record --> 2600:9000:5304:e500::1 (IPAddress)
analytics.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
auth.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
lote.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
motos.mercadolibre.com.bo (FQDN) --> cname_record --> d35ggtaup8afpf.cloudfront.net (FQDN)
test.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
articulo.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
205.251.192.0/21 (Netblock) --> contains --> 205.251.196.229 (IPAddress)
205.251.192.0/21 (Netblock) --> contains --> 205.251.194.195 (IPAddress)
2600:9000:5300::/45 (Netblock) --> contains --> 2600:9000:5304:e500::1 (IPAddress)
2600:9000:5300::/45 (Netblock) --> contains --> 2600:9000:5302:c300::1 (IPAddress)
16509 (ASN) --> managed_by --> AMAZON-02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) --> announces --> 205.251.192.0/21 (Netblock)
16509 (ASN) --> announces --> 2600:9000:5300::/45 (Netblock)
developers.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
inmuebles.mercadolibre.com.bo (FQDN) --> cname_record --> d35ggtaup8afpf.cloudfront.net (FQDN)
ns-467.awsdns-58.com (FQDN) --> a_record --> 205.251.193.211 (IPAddress)
ns-467.awsdns-58.com (FQDN) --> aaaa_record --> 2600:9000:5301:d300::1 (IPAddress)
camioneta.mercadolibre.com.bo (FQDN) --> cname_record --> domssl.mercadolibre.com.bo (FQDN)
205.251.192.0/21 (Netblock) --> contains --> 205.251.193.211 (IPAddress)
2600:9000:5300::/45 (Netblock) --> contains --> 2600:9000:5301:d300::1 (IPAddress)
d35ggtaup8afpf.cloudfront.net (FQDN) --> a_record --> 13.35.58.5 (IPAddress)
d35ggtaup8afpf.cloudfront.net (FQDN) --> a_record --> 13.35.58.58 (IPAddress)
```

- **Firewall Detection**



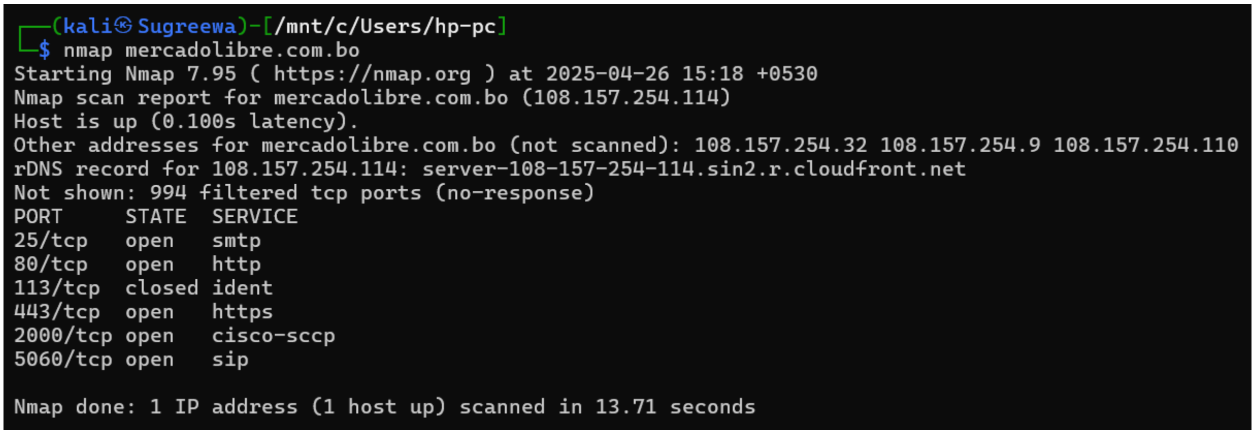
```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ wafw00f mercadolibre.com.bo

                ?              ,.   (   .      )        .      "
        __     ??          ("     )  )'     ,'        )  . (`     '`
    (___()'`;   ???          .; )  ' (( (" )    ;(,     ((  (  ;)  "  )")
    /,___ /`                 _"., ,._'_.,)_(..,( . )_  _' )_') (. _..( ' )
    \\   \\                 |____|____|____|____|____|____|____|____|____|

                                ~ WAFW00F : v2.3.1 ~
                    ~ Sniffing Web Application Firewalls since 2014 ~

[*] Checking https://mercadolibre.com.bo
[+] The site https://mercadolibre.com.bo is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

- **Nmap Scan**

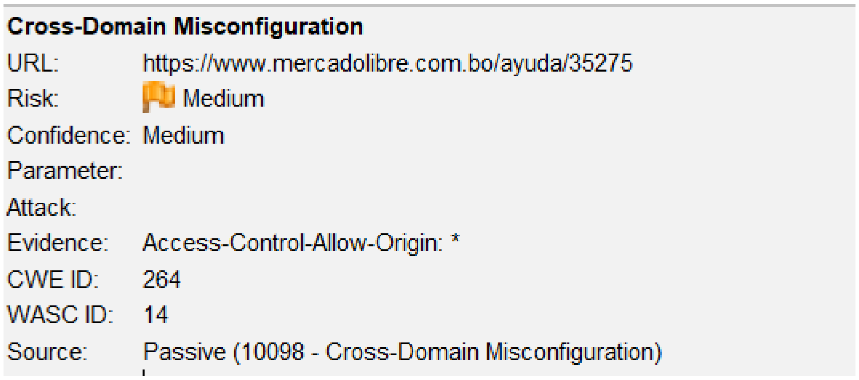


```
┌──(kali㉿Sugreewa)-[/mnt/c/Users/hp-pc]
└─$ nmap mercadolibre.com.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 15:18 +0530
Nmap scan report for mercadolibre.com.bo (108.157.254.114)
Host is up (0.100s latency).
Other addresses for mercadolibre.com.bo (not scanned): 108.157.254.32 108.157.254.9 108.157.254.110
rDNS record for 108.157.254.114: server-108-157-254-114.sin2.r.cloudfront.net
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE  SERVICE
25/tcp   open   smtp
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
2000/tcp open   cisco-sccp
5060/tcp open   sip

Nmap done: 1 IP address (1 host up) scanned in 13.71 seconds
```

3. Vulnerability

- **Cross-Domain Misconfiguration**



Cross-Domain Misconfiguration

URL:	https://www.mercadolibre.com.bo/ayuda/35275
Risk:	Medium
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	Access-Control-Allow-Origin: *
CWE ID:	264
WASC ID:	14
Source:	Passive (10098 - Cross-Domain Misconfiguration)

4. Vulnerability description

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

5. 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

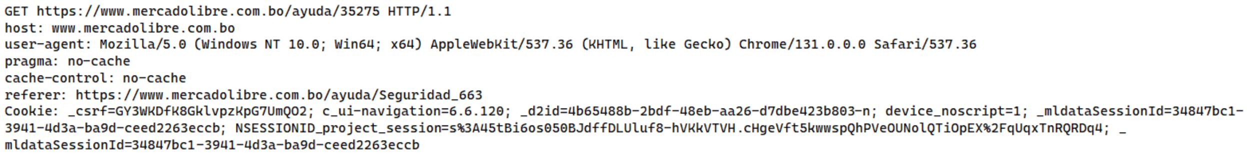
6. Impact Assessment

- **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)

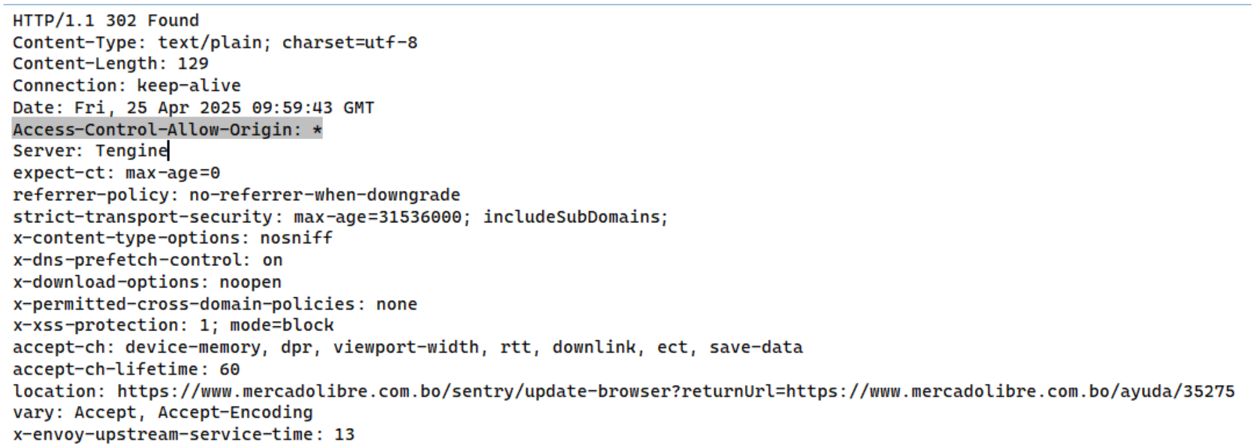
7. Steps to reproduce

- 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: *

8. Proof of concept



```
GET https://www.mercadolibre.com.bo/ayuda/35275 HTTP/1.1
host: www.mercadolibre.com.bo
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://www.mercadolibre.com.bo/ayuda/Seguridad_663
Cookie: _csrf=GY3WKDfK8GklvpzKpG7UmQO2; c_ui-navigation=6.6.120; _d2id=4b65488b-2bdf-48eb-aa26-d7dbe423b803-n; device_noscript=1; _mldataSessionId=34847bc1-
3941-4d3a-ba9d-ceed2263eccb; NSESSIONID_project_session=s%3A45tBi6os050BJdffDLUluf8-hVKkVTVH.cHgeVft5kwwspQhPVeOUNolQTiOpEX%2FqUqxTnRQRDq4; _
mldataSessionId=34847bc1-3941-4d3a-ba9d-ceed2263eccb
```



```
HTTP/1.1 302 Found
Content-Type: text/plain; charset=utf-8
Content-Length: 129
Connection: keep-alive
Date: Fri, 25 Apr 2025 09:59:43 GMT
Access-Control-Allow-Origin: *
Server: Tengine
expect-ct: max-age=0
referrer-policy: no-referrer-when-downgrade
strict-transport-security: max-age=31536000; includeSubDomains;
x-content-type-options: nosniff
x-dns-prefetch-control: on
x-download-options: noopen
x-permitted-cross-domain-policies: none
x-xss-protection: 1; mode=block
accept-ch: device-memory, dpr, viewport-width, rtt, downlink, ect, save-data
accept-ch-lifetime: 60
location: https://www.mercadolibre.com.bo/sentry/update-browser?returnUrl=https://www.mercadolibre.com.bo/ayuda/35275
vary: Accept, Accept-Encoding
x-envoy-upstream-service-time: 13
```

9. 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.