

# **INFORME DE RECONOCIMIENTO**

## **Web Analizada:**



Informe de Reconocimiento  
Scope (\*.mercadolibre.com)

Recopilación de Información / Seguridad de la Información

Jordan Andres Diaz Sanchez

# TABLA DE CONTENIDO

## 1. INTRODUCCIÓN

- 1.1. Objetivo de la revisión

## 2. TECNICAS DE FROOTPRINTING

- 2.1. DNS Brute Force – Shufflendns
- 2.2. Google Analytics – Analyticrelationships
- 2.3. TLS Probing – Cero
- 2.4. Web Scraping – Katana
- 2.5. Certificate Transparency Logs – Ctfr
- 2.6. Archivos Web / Cache - Gau

## 3. TECNICAS DE FINGERPRINTING

- 3.1. Identificación de Subdominios – httpx
- 3.2. Escaneo de puertos y detección de servicios – Masscan / Nmap
- 3.3. Identificación tecnologías Web – Gowitness / Wappalyzer
- 3.4. Identificaciones posibles WAF – Wafw00f
- 3.5. Descubrimiento de contenido / Fuzzing - Ffuf

## 4. ANÁLISIS DE VULNERABILIDADES

- 4.1. Análisis estándar – Greenbone y Nuclei
- 4.2. Análisis web – wpscan
- 4.3. Análisis SSL/TLS
- 4.4. Análisis de servidores correo (DMARC/DKIM/SPF)
- 4.5. Detección de subdominios takeover (subzy)

## 5. TECNICAS OSINT

- 5.1. OSINT – Redes Sociales

## 6. CONCLUSIÓN

## 7. REFERENCIAS Y BIBLIOGRAFÍA

## 1. INTRODUCCIÓN

Este informe tiene como finalidad evaluar el entorno del dominio (\*.mercadolibre.com) mediante un proceso de recolección y análisis de información pública, se emplearán diversas técnicas específicas para identificar la estructura, servicios y posibles vulnerabilidades del sistema, lo que permitirá detectar configuraciones erróneas y puntos de riesgo potenciales.

### ❖ **Floorprinting Vertical:**

Se mapeará la estructura interna y las relaciones entre subdominios y servicios asociados, identificando el alcance y la jerarquía de la infraestructura.

### ❖ **Fingerprinting:**

Se recopilará información detallada sobre las tecnologías, sistemas operativos y versiones utilizadas en los servicios expuestos, lo cual servirá para identificar configuraciones obsoletas o inseguras.

### ❖ **Análisis de vulnerabilidades:**

Se evaluarán los servicios y configuraciones identificadas para detectar posibles vulnerabilidades, utilizando herramientas automatizadas como revisión manual de puntos críticos.

### ❖ **OSINT (Open Source Intelligence):**

Se complementará la información técnica con los datos obtenidos de fuentes públicas, lo que permitirá enriquecer el análisis y obtener una visión más completa del entorno.

### 1.1. Objetivos de la Revisión

Los objetivos principales de este análisis son, detectar y documentar la información expuesta en el Scope (\*.mercadolibre.com), identificar posibles vulnerabilidades y configuraciones por defecto, proveer una base de información solida que sirva como punto de partida para futuras evaluaciones y acciones correctivas en materia de seguridad.

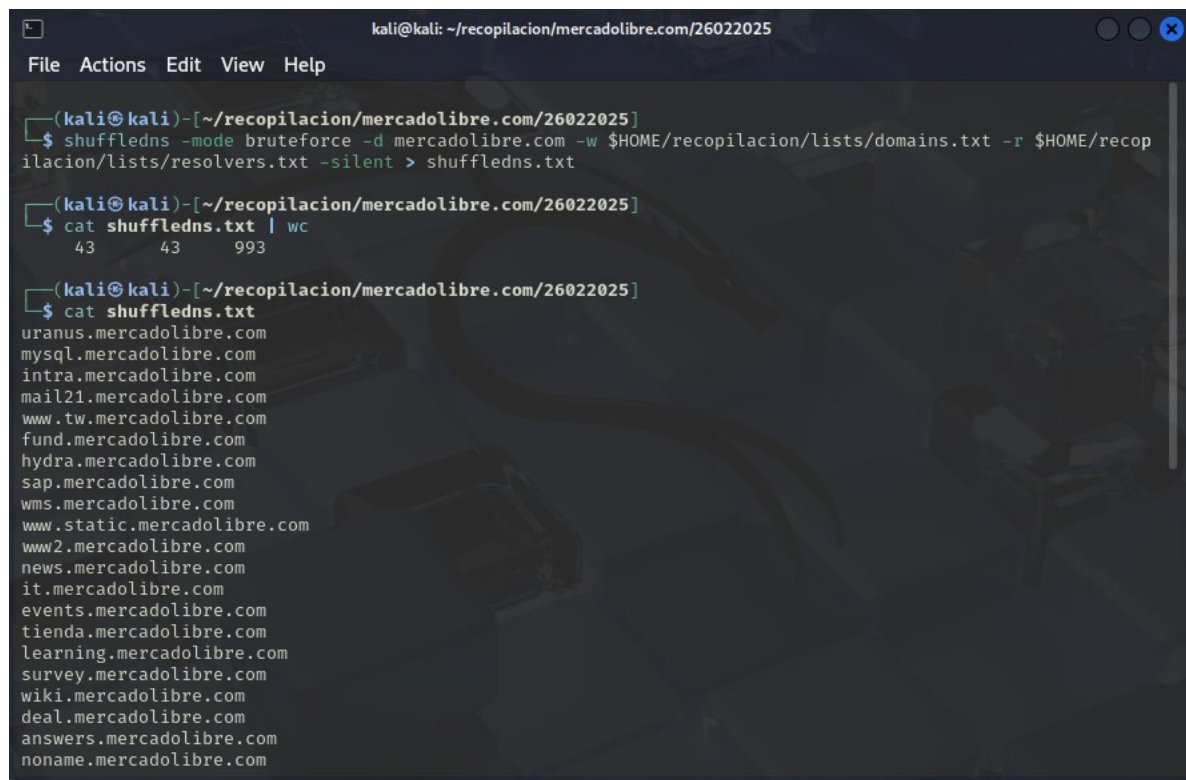
## 2. TECNICAS DE FROOTPRINTING VERTICAL

El Froorprinting vertical es una fase esencial en el reconocimiento dentro de una auditoría de seguridad, enfocándose en recopilar información detallada sobre los servicios y tecnologías utilizadas en un objetivo específico.

Para ello, se emplean herramientas especializadas como Shuffledns, Subfinder, Nmap y WhatWeb, entre otras, que permiten mapear la infraestructura digital del objetivo, detectando posibles vectores de ataque. El objetivo final es obtener una visión detallada del entorno tecnológico y evaluar posibles vulnerabilidades que puedan ser explotadas en fases posteriores del pentesting.

### 2.1. DNS Brute Force – Shufflendns

Shuffledns es una herramienta de enumeración de subdominios que combina listas de palabras con resoluciones DNS activas para descubrir subdominios válidos de un dominio objetivo.



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ shuffledns -mode bruteforce -d mercadolibre.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > shuffledns.txt

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ cat shuffledns.txt | wc
43      43    993

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ cat shuffledns.txt
uranus.mercadolibre.com
mysql.mercadolibre.com
intra.mercadolibre.com
mail21.mercadolibre.com
www.tw.mercadolibre.com
fund.mercadolibre.com
hydra.mercadolibre.com
sap.mercadolibre.com
wms.mercadolibre.com
www.static.mercadolibre.com
www2.mercadolibre.com
news.mercadolibre.com
it.mercadolibre.com
events.mercadolibre.com
tienda.mercadolibre.com
learning.mercadolibre.com
survey.mercadolibre.com
wiki.mercadolibre.com
deal.mercadolibre.com
answers.mercadolibre.com
noname.mercadolibre.com
```

Ilustración 1 Shufflendns

#### Subdominios relevantes encontrados

- mysql.mercadolibre.com – Podría indicar una base de datos accesible o una configuración mal protegida.
- intra.mercadolibre.com – Posiblemente un portal interno, lo que podría representar una superficie de ataque interesante.
- sap.mercadolibre.com – SAP suele usarse en gestión empresarial, lo que podría revelar sistemas internos críticos.
- auth.mercadolibre.com – Un endpoint de autenticación que podría ser un objetivo en pruebas de seguridad.
- billing.mercadolibre.com – Relacionado con facturación, lo que podría ser sensible si no está bien protegido.

#### Conclusión

El escaneo ha identificado múltiples subdominios potencialmente sensibles, incluyendo bases de datos, autenticación, facturación y sistemas internos. Si estos servicios no están adecuadamente configurados, podrían representar vectores de ataque en una evaluación de seguridad.

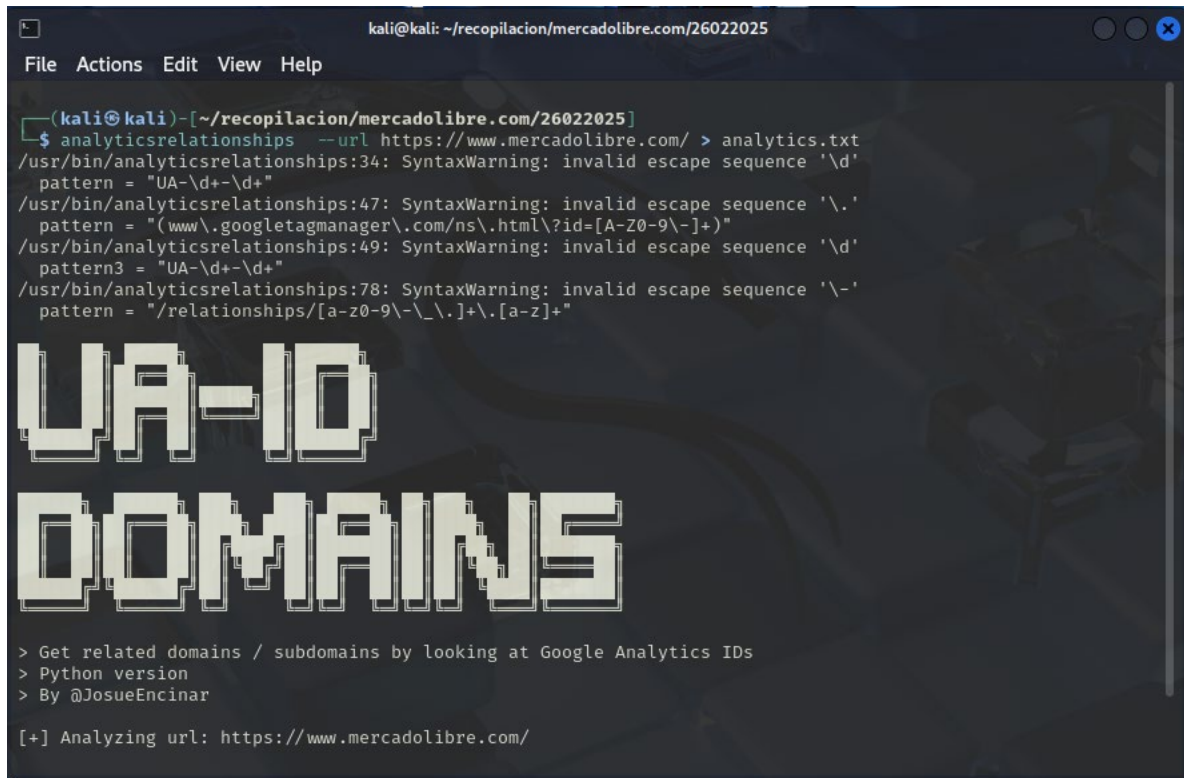
---

#### 2.2. Google Analytics – Analyticrelationships

Google Analytics es una herramienta de reconocimiento basada en identificadores de Google Analytics. Asignó un código único de seguimiento (UA-80810547), lo que nos permite identificar otros dominios que podrían pertenecer a la misma organización o estar vinculados a la infraestructura del objetivo.

#### Conclusión

Nos muestra un error al obtener resultados, lo que indica que la consulta no devolvió información útil o que la herramienta no pudo resolver el identificador. Esto puede deberse a restricciones en la API de Analytics o configuraciones de privacidad del sitio objetivo.



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)~/recopilacion/mercadolibre.com/26022025
$ analyticsrelationships --url https://www.mercadolibre.com/ > analytics.txt
/usr/bin/analyticsrelationships:34: SyntaxWarning: invalid escape sequence '\d'
pattern = "UA-\d+-\d+"
/usr/bin/analyticsrelationships:47: SyntaxWarning: invalid escape sequence '\.'
pattern = "(www\.googletagmanager\.com/ns\.html\?id=[A-Z0-9-]+)"
/usr/bin/analyticsrelationships:49: SyntaxWarning: invalid escape sequence '\d'
pattern3 = "UA-\d+-\d+"
/usr/bin/analyticsrelationships:78: SyntaxWarning: invalid escape sequence '\-'
pattern = "/relationships/[a-z0-9-_\.\.]+\.[a-z]+"

UA-ID
DOMAINS

> Get related domains / subdomains by looking at Google Analytics IDs
> Python version
> By @JosueEncinar

[+] Analyzing url: https://www.mercadolibre.com/
```

Ilustración 2 analytics relation

---

### 2.3. TLS Probing – Cero

cero es una herramienta utilizada en reconocimiento pasivo y activo para analizar la implementación de TLS/SSL en un dominio objetivo. Su propósito es identificar configuraciones de seguridad, certificados SSL y posibles vulnerabilidades en la comunicación cifrada de un servidor web.

#### Conclusión

No se han encontrado subdominios en este análisis, posiblemente el dominio principal no tenga dominios accesibles con esta técnica utilizada.



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cero -d mercadolibre.com > cero.txt

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat cero.txt
mercadolibre.com

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat cero.txt | wc
 1    1   17

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$
```

Ilustración 3 Cero

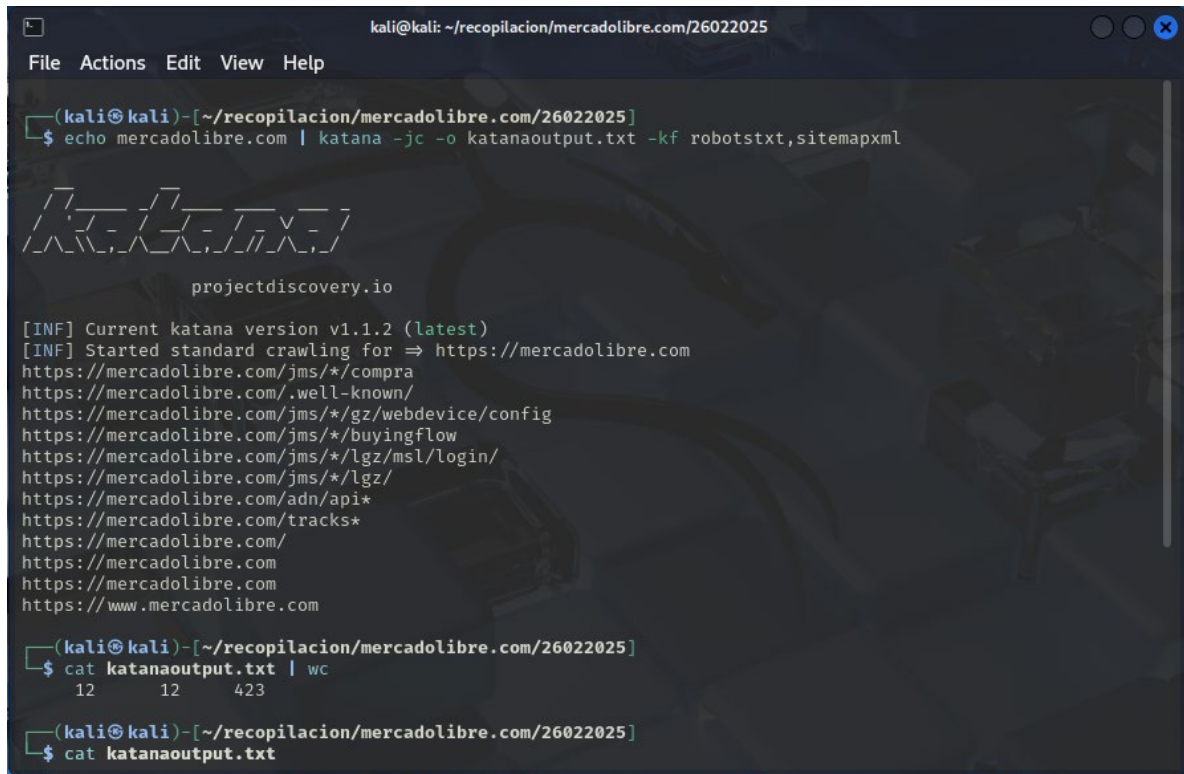
---

## 2.4. Web Scraping – Katana

Katana es un crawler de contenido web. Su función principal es rastrear y mapear URLs dentro de un dominio objetivo para identificar rutas accesibles, subdominios y posibles puntos de entrada a sistemas internos.

### Conclusión

El archivo solo muestra mercadolibre.com y www.mercadolibre.com, lo que indica que Katana no descubrió nuevas rutas o subdominios interesantes en este análisis.



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ echo mercadolibre.com | katana -jc -o katanaoutput.txt -kf robotstxt,sitemapxml

projectdiscovery.io

[INF] Current katana version v1.1.2 (latest)
[INF] Started standard crawling for => https://mercadolibre.com
https://mercadolibre.com/jms/*/compra
https://mercadolibre.com/.well-known/
https://mercadolibre.com/jms/*/gz/webdevice/config
https://mercadolibre.com/jms/*/buyingflow
https://mercadolibre.com/jms/*/lgz/msl/login/
https://mercadolibre.com/jms/*/lgz/
https://mercadolibre.com/adn/api*
https://mercadolibre.com/tracks*
https://mercadolibre.com/
https://mercadolibre.com
https://www.mercadolibre.com

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat katanaoutput.txt | wc
 12      12    423

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat katanaoutput.txt
```

Ilustración 4 Katana

## 2.5. Certificate Transparency Logs – Ctfr

CTFR es una herramienta que aprovecha transparencia de certificados SSL/TLS para descubrir subdominios de un dominio objetivo. Consulta registros públicos de certificados en servicios como crt.sh, revelando subdominios utilizados en certificados digitales emitidos para el dominio en cuestión.

### Subdominios relevantes encontrados

El análisis muestra múltiples subdominios interesantes, incluyendo:

- Infraestructura y desarrollo:
- ✓ nginx.m-int-dev.mercadolibre.com
- ✓ nginx.s1-int-dev.mercadolibre.com
- ✓ prodeng-playground-internal.mercadolibre.com
- ✓ test.mercadolibre.com



Posible entorno de desarrollo, pruebas o staging, que podría estar menos protegido que la infraestructura en producción.

- Autenticación y seguridad:
- ✓ auth-identity.mercadolibre.com.ec
- ✓ auth.mercadolibre.com.ec
- ✓ seguridad.mercadolibre.com.ec

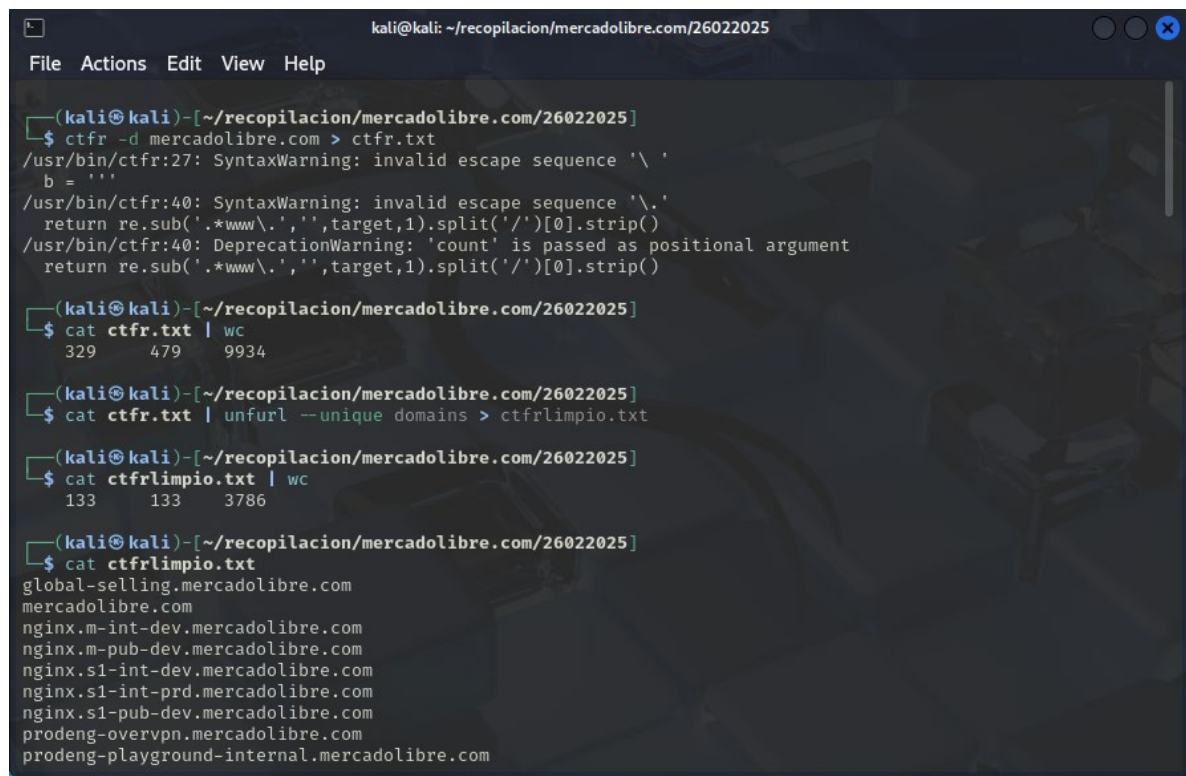
Endpoints críticos que podrían estar involucrados en procesos de autenticación y acceso.

- Subdominios relacionados con datos y análisis:
- ✓ analytics.mercadolibre.com.ec
- ✓ www.data.mercadolibre.com

Podrían exponer información analítica sensible o endpoints de recopilación de datos.

- Plataformas internas y soporte:
- ✓ www.servicedesk.mercadolibre.com
- ✓ www.universidad.mercadolibre.com
- ✓ www.vendedores.mercadolibre.com

Sistemas internos que podrían estar restringidos pero accesibles desde internet.



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ ctfR -d mercadolibre.com > ctfr.txt
/usr/bin/ctfr:27: SyntaxWarning: invalid escape sequence '\ '
b = ''
/usr/bin/ctfr:40: SyntaxWarning: invalid escape sequence '\.'
return re.sub('.*www\.', '', target, 1).split('/')[0].strip()
/usr/bin/ctfr:40: DeprecationWarning: 'count' is passed as positional argument
return re.sub('.*www\.', '', target, 1).split('/')[0].strip()

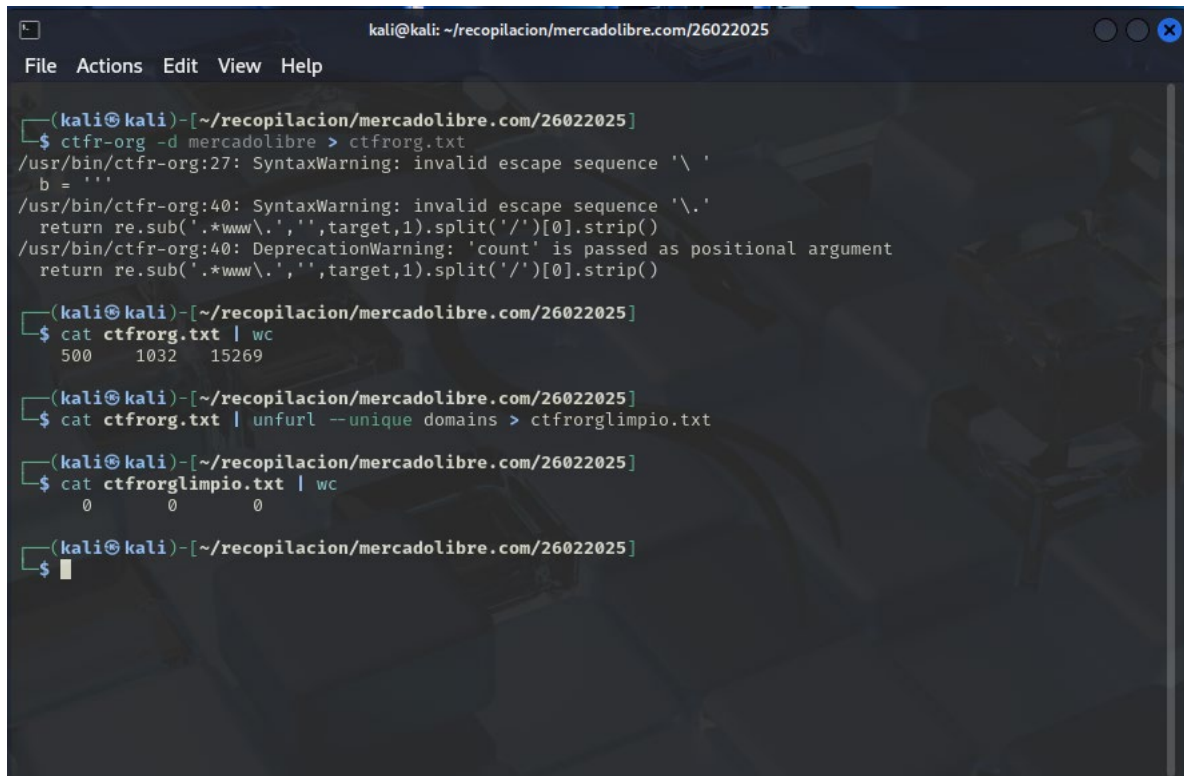
(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ cat ctfr.txt | wc
 329   479  9934

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ cat ctfr.txt | unfurl --unique domains > ctfrlimpio.txt

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ cat ctfrlimpio.txt | wc
 133   133  3786

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ cat ctfrlimpio.txt
global-selling.mercadolibre.com
mercadolibre.com
nginx.m-int-dev.mercadolibre.com
nginx.m-pub-dev.mercadolibre.com
nginx.s1-int-dev.mercadolibre.com
nginx.s1-int-prd.mercadolibre.com
nginx.s1-pub-dev.mercadolibre.com
prodeng-overvpn.mercadolibre.com
prodeng-playground-internal.mercadolibre.com
```

Ilustración 5 CtfR



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ ctfr-org -d mercadolibre > ctfrorg.txt
/usr/bin/ctfr-org:27: SyntaxWarning: invalid escape sequence '\ '
  b = ''
/usr/bin/ctfr-org:40: SyntaxWarning: invalid escape sequence '\.'
  return re.sub('.*www\.', '', target, 1).split('/')[0].strip()
/usr/bin/ctfr-org:40: DeprecationWarning: 'count' is passed as positional argument
  return re.sub('.*www\.', '', target, 1).split('/')[0].strip()

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat ctfrorg.txt | wc
500    1032   15269

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat ctfrorg.txt | unfurl --unique domains > ctfrorglimpio.txt

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat ctfrorglimpio.txt | wc
0      0      0

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$
```

Ilustración 6 Ctfr-org

---

## 2.6. Archivos Web / Cache - Gau

Gau es una herramienta que recopila todas las URLs indexadas de un dominio objetivo desde múltiples fuentes públicas su principal uso es extraer rutas y subdominios históricos que podrían seguir accesibles.

### Subdominios relevantes encontrados

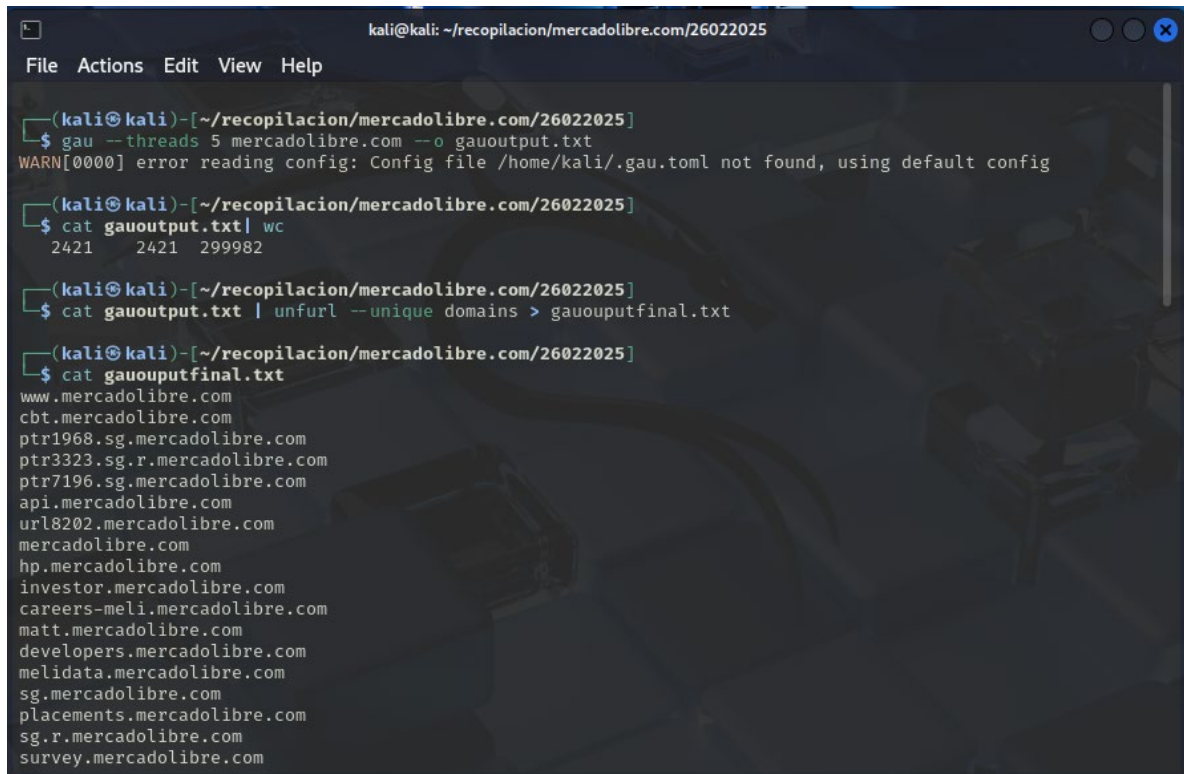
Este escaneo ha identificado varios subdominios potencialmente interesantes:

- Servicios internos y API:
- ✓ internal-api.mercadolibre.com → Posible API privada o endpoint interno.
- ✓ sandbox-cbt.mercadolibre.com → Ambiente de pruebas (sandbox), que podría estar menos protegido.

- Autenticación y seguridad:
  - ✓ [auth.mercadolibre.com](https://auth.mercadolibre.com) → Endpoint de autenticación, podría ser clave en la gestión de sesiones.
  - ✓ [myaccount.mercadolibre.com](https://myaccount.mercadolibre.com) → Sistema de cuentas de usuario.
  
- Marketing y análisis de datos:
  - ✓ [analytics.mercadolibre.com](https://analytics.mercadolibre.com) → Podría exponer datos sobre el tráfico o usuarios del sitio.
  - ✓ [publicidad.mercadolibre.com](https://publicidad.mercadolibre.com) → Posiblemente relacionado con anuncios o estrategias comerciales.
  
- Plataformas y foros internos:
  - ✓ [developers.mercadolibre.com](https://developers.mercadolibre.com) → Portal para desarrolladores, podría tener documentación sobre APIS internas.
  - ✓ [developers-forum.mercadolibre.com](https://developers-forum.mercadolibre.com) → Foro donde podrían filtrarse información técnica sensible.
  
- Sistemas de notificaciones y errores:
  - ✓ [notifications-11.mercadolibre.com](https://notifications-11.mercadolibre.com), [notifications-13.mercadolibre.com](https://notifications-13.mercadolibre.com) → Sistemas de notificaciones, podrían exponer logs o configuraciones.
  - ✓ [error.mercadolibre.com](https://error.mercadolibre.com) → Podría revelar mensajes de error detallados útiles para un atacante.

## Conclusión

El uso de Gau ha revelado subdominios con posibles implicaciones de seguridad, incluyendo APIS internas, entornos de prueba, autenticación y sistemas de análisis. Estos hallazgos pueden ser valiosos para continuar con una fase de explotación o búsqueda de vulnerabilidades específicas.



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ gau --threads 5 mercadolibre.com --o gauoutput.txt
WARN[0000] error reading config: Config file /home/kali/.gau.toml not found, using default config

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat gauoutput.txt | wc
 2421    2421  299982

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat gauoutput.txt | unfurl --unique domains > gauoutputfinal.txt

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat gauoutputfinal.txt
www.mercadolibre.com
cbt.mercadolibre.com
ptr1968.sg.mercadolibre.com
ptr3323.sg.r.mercadolibre.com
ptr7196.sg.mercadolibre.com
api.mercadolibre.com
url8202.mercadolibre.com
mercadolibre.com
hp.mercadolibre.com
investor.mercadolibre.com
careers-meli.mercadolibre.com
matt.mercadolibre.com
developers.mercadolibre.com
melidata.mercadolibre.com
sg.mercadolibre.com
placements.mercadolibre.com
sg.r.mercadolibre.com
survey.mercadolibre.com
```

Ilustración 7 Gau

# PERMUTACIONES

Alterx es una herramienta utilizada para generar permutaciones, alteraciones y variaciones de subdominios de un dominio objetivo. Su función principal es detectar posibles subdominios no documentados mediante la mutación de nombres existentes.

The screenshot shows a Kali Linux terminal window with the title bar "kali@kali: ~/recopilacion/mercadolibre.com/26022025". The menu bar includes "File", "Actions", "Edit", "View", and "Help".

```
(kali㉿kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat subdominios.txt | alterx | dnsx -o alterx01.txt
```

The output displays two ASCII art logos for "projectdiscovery.io". Each logo consists of a stylized graphic made of backslashes and forward slashes, followed by the text "projectdiscovery.io".

```
[INF] Current alterx version v0.0.4 (outdated)
[INF] Generated 132356 permutations in 0.3364s
acc.prodeng.mercadolibre.com
acc.nginx.s1-int-prd.mercadolibre.com
acc.prodeng-playground.mercadolibre.com
acc.nginx.s1-pub-dev.mercadolibre.com
acc.prodeng-playground-internal.mercadolibre.com
acc.nginx.m-int-dev.mercadolibre.com
acc.nginx.m-pub-dev.mercadolibre.com
acc.nginx.s1-int-dev.mercadolibre.com
acc.ucs.orion-dev.mercadolibre.com
access.prodeng-playground-internal.mercadolibre.com
access.ucs.orion-dev.mercadolibre.com
```

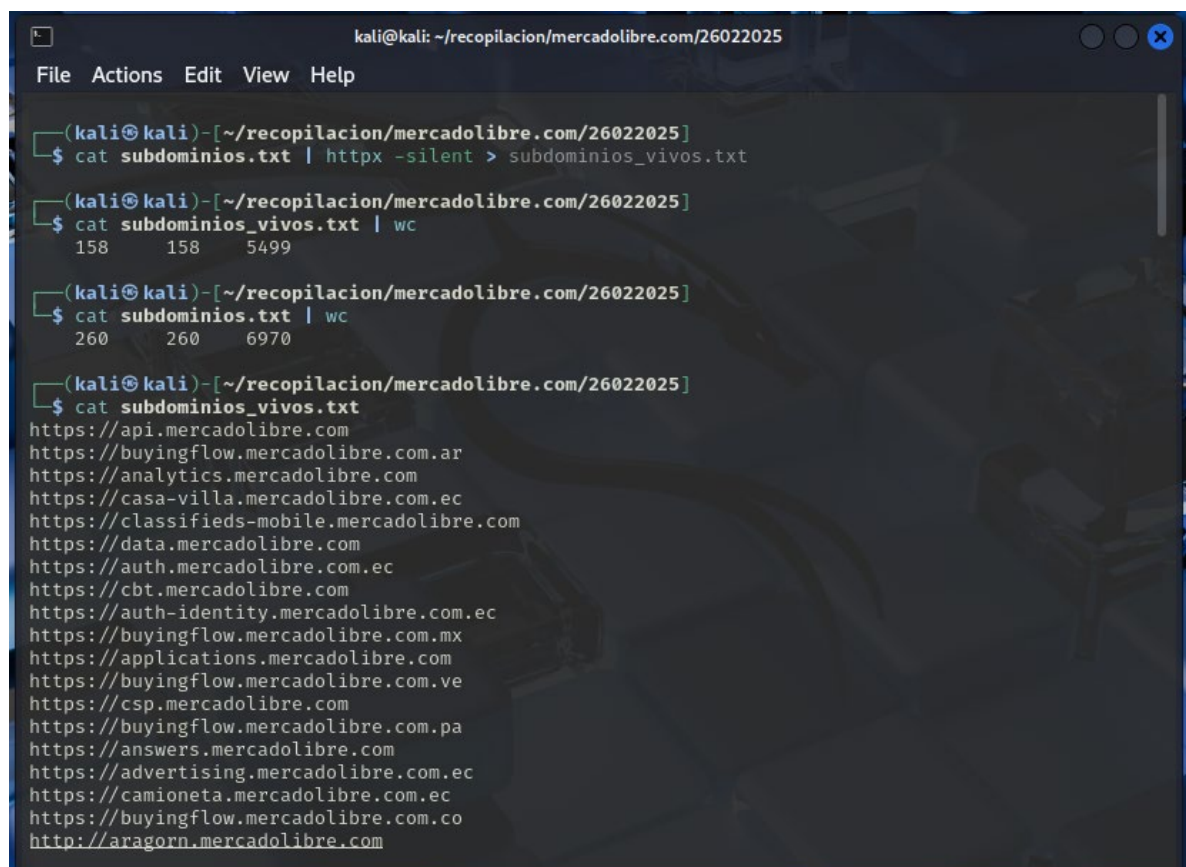
*Ilustración 8 AlterX - dnsX*

### 3. TECNICAS DE FINGERPRINTING

El Fingerprinting es un conjunto de técnicas utilizadas para identificar características específicas de un sistema, servicio o aplicación web. Su objetivo es determinar información detallada sobre la tecnología y configuración utilizada en un objetivo, como versiones de software, sistemas operativos, frameworks y servicios expuestos.

#### 3.1. Identificación de Subdominios – httpx

httpx es una herramienta utilizada para verificar la accesibilidad y estado de subdominios a través de peticiones HTTP/HTTPS. Se utiliza comúnmente después de la enumeración de subdominios para filtrar aquellos que están activos y responden correctamente.

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~/recopilacion/mercadolibre.com/26022025'. The terminal shows a series of commands and their outputs. First, the command 'cat subdominios.txt | httpx -silent > subdominios\_vivos.txt' is executed. Then, 'cat subdominios\_vivos.txt | wc' is run, showing '158 158 5499'. Next, 'cat subdominios.txt | wc' is run, showing '260 260 6970'. Finally, 'cat subdominios\_vivos.txt' is run, displaying a list of URLs including 'https://api.mercadolibre.com', 'https://buyingflow.mercadolibre.com.ar', 'https://analytics.mercadolibre.com', 'https://casa-villa.mercadolibre.com.ec', 'https://classifieds-mobile.mercadolibre.com', 'https://data.mercadolibre.com', 'https://auth.mercadolibre.com.ec', 'https://cvt.mercadolibre.com', 'https://auth-identity.mercadolibre.com.ec', 'https://buyingflow.mercadolibre.com.mx', 'https://applications.mercadolibre.com', 'https://buyingflow.mercadolibre.com.ve', 'https://csp.mercadolibre.com', 'https://buyingflow.mercadolibre.com.pa', 'https://answers.mercadolibre.com', 'https://advertising.mercadolibre.com.ec', 'https://camioneta.mercadolibre.com.ec', 'https://buyingflow.mercadolibre.com.co', and 'http://aragorn.mercadolibre.com'.

```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat subdominios.txt | httpx -silent > subdominios_vivos.txt

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat subdominios_vivos.txt | wc
158      158      5499

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat subdominios.txt | wc
260      260      6970

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ cat subdominios_vivos.txt
https://api.mercadolibre.com
https://buyingflow.mercadolibre.com.ar
https://analytics.mercadolibre.com
https://casa-villa.mercadolibre.com.ec
https://classifieds-mobile.mercadolibre.com
https://data.mercadolibre.com
https://auth.mercadolibre.com.ec
https://cvt.mercadolibre.com
https://auth-identity.mercadolibre.com.ec
https://buyingflow.mercadolibre.com.mx
https://applications.mercadolibre.com
https://buyingflow.mercadolibre.com.ve
https://csp.mercadolibre.com
https://buyingflow.mercadolibre.com.pa
https://answers.mercadolibre.com
https://advertising.mercadolibre.com.ec
https://camioneta.mercadolibre.com.ec
https://buyingflow.mercadolibre.com.co
http://aragorn.mercadolibre.com
```

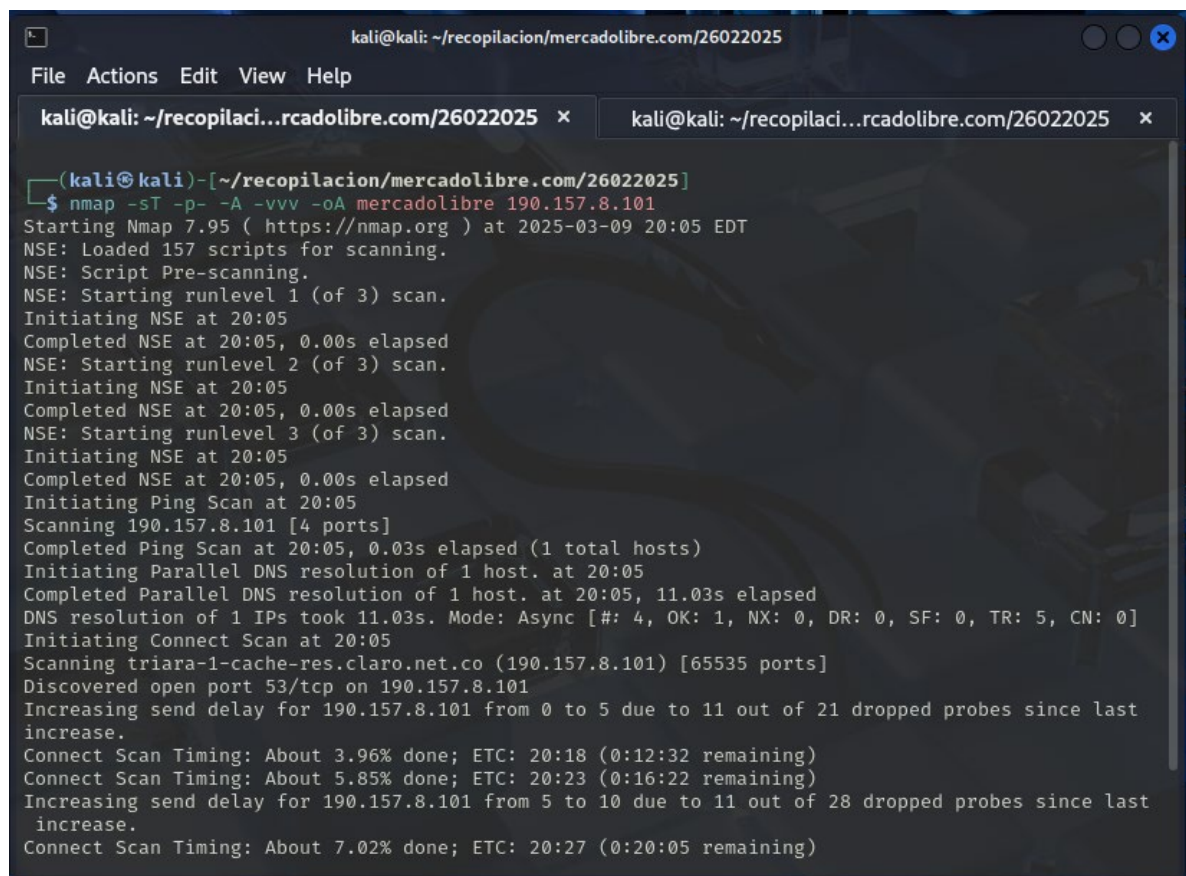
Ilustración 9 Httpx



### 3.2. Escaneo de puertos y detección de servicios – Masscan / Nmap

Nmap (Network Mapper) es una herramienta de escaneo de red utilizada para descubrir hosts, puertos abiertos y servicios en un objetivo.

Masscan es un escáner de puertos que se usa para descubrir servicios abiertos en un rango de IPS. Funciona de manera similar a Nmap, pero con una capacidad de escaneo mucho más rápida al enviar paquetes sin esperar respuestas antes de continuar.

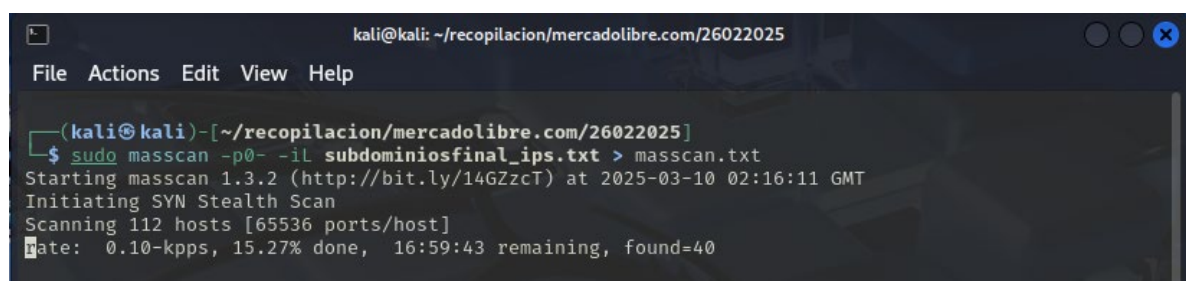


```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

kali@kali: ~/recopilaci...rcadolibre.com/26022025 x kali@kali: ~/recopilaci...rcadolibre.com/26022025 x

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ nmap -sT -p- -A -vvv -oA mercadolibre 190.157.8.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-09 20:05 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:05
Completed NSE at 20:05, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:05
Completed NSE at 20:05, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:05
Completed NSE at 20:05, 0.00s elapsed
Initiating Ping Scan at 20:05
Scanning 190.157.8.101 [4 ports]
Completed Ping Scan at 20:05, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:05
Completed Parallel DNS resolution of 1 host. at 20:05, 11.03s elapsed
DNS resolution of 1 IPs took 11.03s. Mode: Async [#: 4, OK: 1, NX: 0, DR: 0, SF: 0, TR: 5, CN: 0]
Initiating Connect Scan at 20:05
Scanning triara-1-cache-res.claro.net.co (190.157.8.101) [65535 ports]
Discovered open port 53/tcp on 190.157.8.101
Increasing send delay for 190.157.8.101 from 0 to 5 due to 11 out of 21 dropped probes since last increase.
Connect Scan Timing: About 3.96% done; ETC: 20:18 (0:12:32 remaining)
Connect Scan Timing: About 5.85% done; ETC: 20:23 (0:16:22 remaining)
Increasing send delay for 190.157.8.101 from 5 to 10 due to 11 out of 28 dropped probes since last increase.
Connect Scan Timing: About 7.02% done; ETC: 20:27 (0:20:05 remaining)
```

Ilustración 10 Nmap



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ sudo masscan -p0- -il subdominiosfinal_ips.txt > masscan.txt
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-03-10 02:16:11 GMT
Initiating SYN Stealth Scan
Scanning 112 hosts [65536 ports/host]
Rate: 0.10-kpps, 15.27% done, 16:59:43 remaining, found=40
```

Ilustración 11 Masscan

### 3.3. Identificación tecnologías Web – Gowitness/ WhatWeb

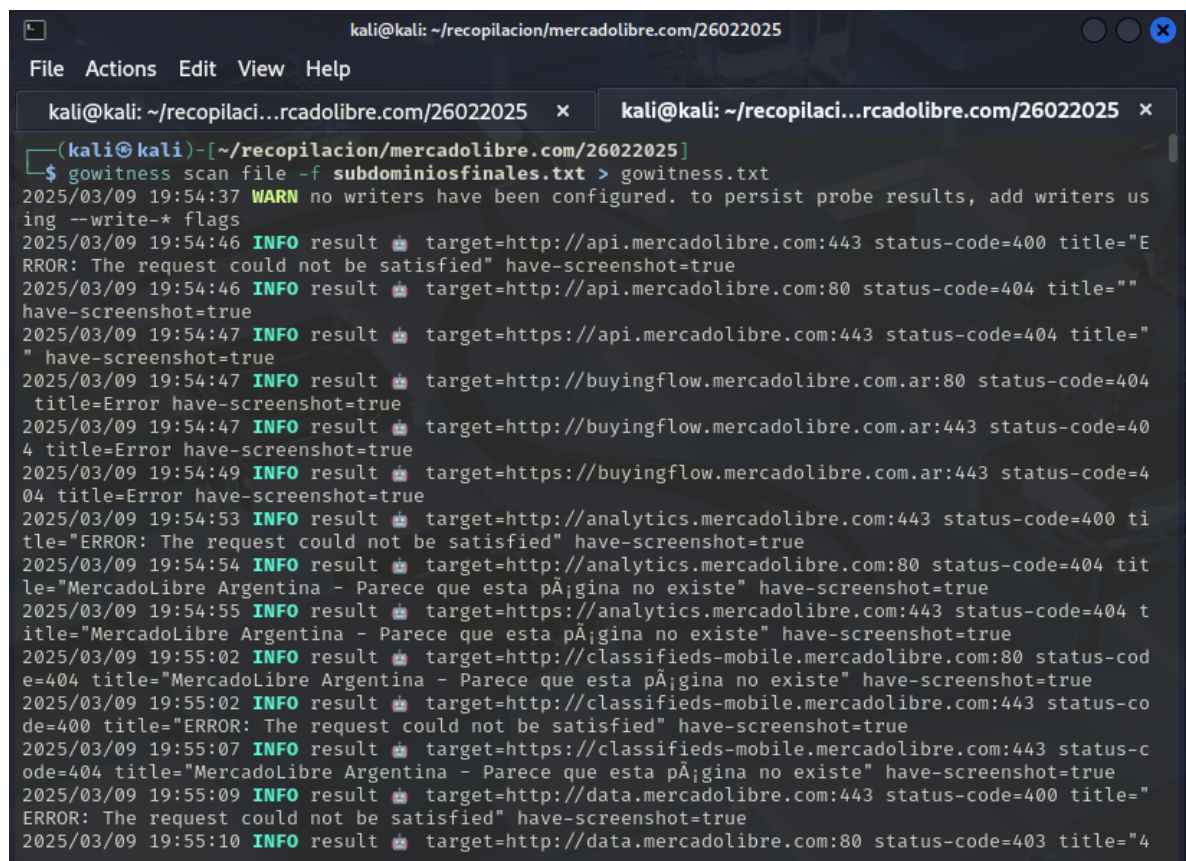
Gowitness es una herramienta utilizada para tomar capturas de pantalla de sitios web y verificar su estado HTTP/HTTPS. Se emplea en el reconocimiento de aplicaciones web para identificar interfaces expuestas, posibles vulnerabilidades visuales y analizar contenido en servidores activos.

WhatWeb es una herramienta utilizada para identificar tecnologías web en un sitio objetivo.

#### Conclusión

El escaneo con Gowitness ha revelado múltiples subdominios activos, restringidos y potencialmente mal configurados. Los subdominios accesibles con código 200 podrían contener información útil para análisis adicionales, mientras que los 403 indican posibles restricciones de acceso.

El sitio mercadolibre.com está protegido por CloudFlare, lo que oculta su infraestructura real y restringe el acceso directo. La presencia de Amazon S3 sugiere que podrían existir archivos almacenados en buckets privados o públicos.



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

kali@kali: ~/recopilaci...rcadolibre.com/26022025 x kali@kali: ~/recopilaci...rcadolibre.com/26022025 x

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ gowitness scan file -f subdominiosfinales.txt > gowitness.txt
2025/03/09 19:54:37 WARN no writers have been configured. to persist probe results, add writers using --write-* flags
2025/03/09 19:54:46 INFO result 🚩 target=http://api.mercadolibre.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/09 19:54:46 INFO result 🚩 target=http://api.mercadolibre.com:80 status-code=404 title="" have-screenshot=true
2025/03/09 19:54:47 INFO result 🚩 target=https://api.mercadolibre.com:443 status-code=404 title="" have-screenshot=true
2025/03/09 19:54:47 INFO result 🚩 target=http://buyingflow.mercadolibre.com.ar:80 status-code=404 title=Error have-screenshot=true
2025/03/09 19:54:47 INFO result 🚩 target=http://buyingflow.mercadolibre.com.ar:443 status-code=404 title=Error have-screenshot=true
2025/03/09 19:54:49 INFO result 🚩 target=https://buyingflow.mercadolibre.com.ar:443 status-code=404 title=Error have-screenshot=true
2025/03/09 19:54:53 INFO result 🚩 target=http://analytics.mercadolibre.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/09 19:54:54 INFO result 🚩 target=http://analytics.mercadolibre.com:80 status-code=404 title="MercadoLibre Argentina - Parece que esta página no existe" have-screenshot=true
2025/03/09 19:54:55 INFO result 🚩 target=https://analytics.mercadolibre.com:443 status-code=404 title="MercadoLibre Argentina - Parece que esta página no existe" have-screenshot=true
2025/03/09 19:55:02 INFO result 🚩 target=http://classifieds-mobile.mercadolibre.com:80 status-code=404 title="MercadoLibre Argentina - Parece que esta página no existe" have-screenshot=true
2025/03/09 19:55:02 INFO result 🚩 target=http://classifieds-mobile.mercadolibre.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/09 19:55:07 INFO result 🚩 target=https://classifieds-mobile.mercadolibre.com:443 status-code=404 title="MercadoLibre Argentina - Parece que esta página no existe" have-screenshot=true
2025/03/09 19:55:09 INFO result 🚩 target=http://data.mercadolibre.com:443 status-code=400 title="ERROR: The request could not be satisfied" have-screenshot=true
2025/03/09 19:55:10 INFO result 🚩 target=http://data.mercadolibre.com:80 status-code=403 title="4
```

Ilustración 12 Gowitness



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help
kali@kali: ~/recopilaci...rcadolibre.com/26022025 x kali@kali: ~/recopilaci...rcadolibre.com/26022025 x

(kali@kali)~/recopilacion/mercadolibre.com/26022025
$ whatweb mercadolibre.com > whatweb.txt

(kali@kali)~/recopilacion/mercadolibre.com/26022025
$ cat whatweb.txt
http://mercadolibre.com [403 Forbidden] CloudFront, Country[UNITED STATES][US], HTML5, HTTPServer[AmazonS3], IP[143.204.23.49], Title[Error! - Mercado Libre], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 c9c5e7596582e81eaf731e0b573c09bc.cloudfront.net (CloudFront)], X-UA-Compatible[IE=edge]

(kali@kali)~/recopilacion/mercadolibre.com/26022025
$
```

Ilustración 13 WhatWeb

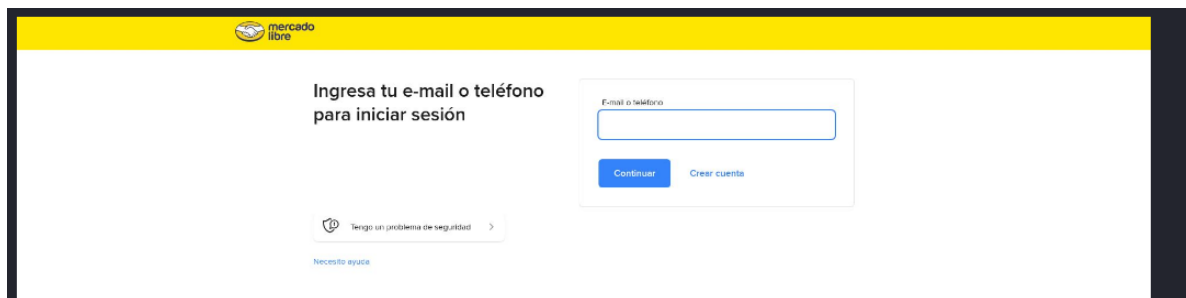


Ilustración 14 eshops.mercadolibre.com

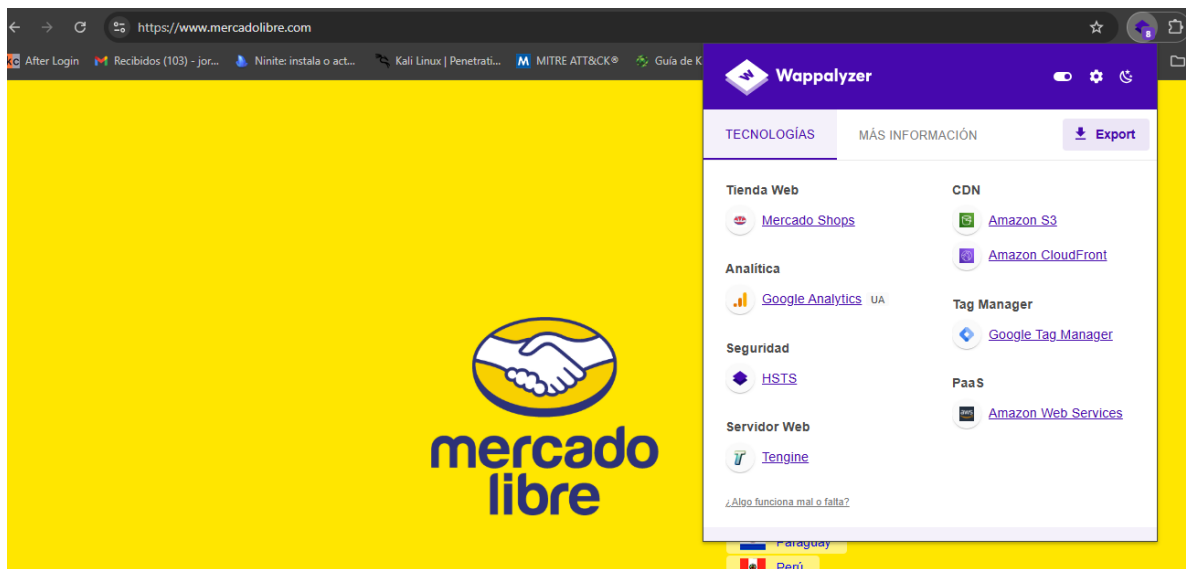


Ilustración 15 Wappalizer



### 3.5. Descubrimiento de contenido / Fuzzing – Ffuf

ffuf (Fast Web Fuzzer) es una herramienta diseñada para enumerar directorios y archivos ocultos en servidores web mediante fuerza bruta. Se basa en diccionarios de nombres de archivos y directorios comunes para detectar recursos que pueden no estar indexados públicamente.

#### **Directorios y archivos relevantes detectados:**

- Posibles archivos de configuración y credenciales:
  - ✓ .bash\_history → Historial de comandos ejecutados en la terminal.
  - ✓ .git/ y .gitignore → Pueden contener información sobre el control de versiones del código fuente.
  - ✓ .env → Suele almacenar variables de entorno, incluyendo credenciales y claves API.
  - ✓ .htaccess y .htpasswd → Configuraciones de acceso y autenticación en Apache.
  - ✓ mysql\_history → Podría contener consultas SQL sensibles.
  - ✓ .ssh/ → Posibles claves SSH o configuraciones de acceso remoto.
- Directorios relacionados con control de versiones y caché:
  - ✓ .cache/, .config/, .cvs/, .svn/ → Podrían exponer datos históricos o configuraciones del proyecto.
  - ✓ CVS/Entries, CVS/Repository → Indican el uso de sistemas de control de versiones antiguos.
- Archivos y directorios administrativos:
  - ✓ Admin/, AdminTools/, Administration/ → Posibles paneles de administración.
  - ✓ ServerAdministrator/, SiteServer/, Super-Admin/ → Directorios que podrían estar protegidos pero accesibles con credenciales.

```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)~[~/recopilacion/mercadolibre.com/26022025]
$ ffuf -w ~/recopilacion/lists/common.txt -t 10 -mc 200,401,403 -u https://mercadolibre.com/FUZZ

v2.1.0-dev

:: Method      : GET
:: URL         : https://mercadolibre.com/FUZZ
:: Wordlist     : FUZZ: /home/kali/recopilacion/lists/common.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 10
:: Matcher     : Response status: 200,401,403

.config      [Status: 403, Size: 13704, Words: 4355, Lines: 217, Duration: 200ms]
.env         [Status: 403, Size: 13704, Words: 4355, Lines: 217, Duration: 226ms]
.cache       [Status: 403, Size: 13704, Words: 4355, Lines: 217, Duration: 223ms]
.cvsignore   [Status: 403, Size: 13704, Words: 4355, Lines: 217, Duration: 231ms]
.git-rewrite [Status: 403, Size: 13704, Words: 4355, Lines: 217, Duration: 232ms]
.forward     [Status: 403, Size: 13704, Words: 4355, Lines: 217, Duration: 227ms]
.cvs         [Status: 403, Size: 13704, Words: 4355, Lines: 217, Duration: 231ms]
.bashrc      [Status: 403, Size: 13704, Words: 4355, Lines: 217, Duration: 230ms]
```

Ilustración 17 ffuf

## 4. ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades es una fase crítica en una evaluación de seguridad, cuyo objetivo es identificar debilidades explotables en los sistemas o aplicaciones dentro del alcance del análisis. Esta sección se basa en la información recolectada durante la fase de reconocimiento y se complementa con herramientas de escaneo de seguridad.

### 4.1. Análisis estándar – Greenbone y Nuclei

El escaneo realizado con Greenbone sobre mercadolibre.com no arrojó vulnerabilidades detectadas. Esto indica que, al menos desde el punto de vista de esta herramienta, el sitio no presenta fallos de seguridad evidentes dentro de los parámetros evaluados.

Conclusión:

Los resultados sugieren que mercadolibre.com tiene un buen nivel de seguridad en los aspectos analizados. Sin embargo, esto no significa que el sitio sea completamente seguro, ya que algunas vulnerabilidades pueden no ser detectadas por esta herramienta o pueden requerir enfoques más específicos para identificarse. Para una evaluación más completa, sería recomendable complementar con otras herramientas o metodologías de análisis.

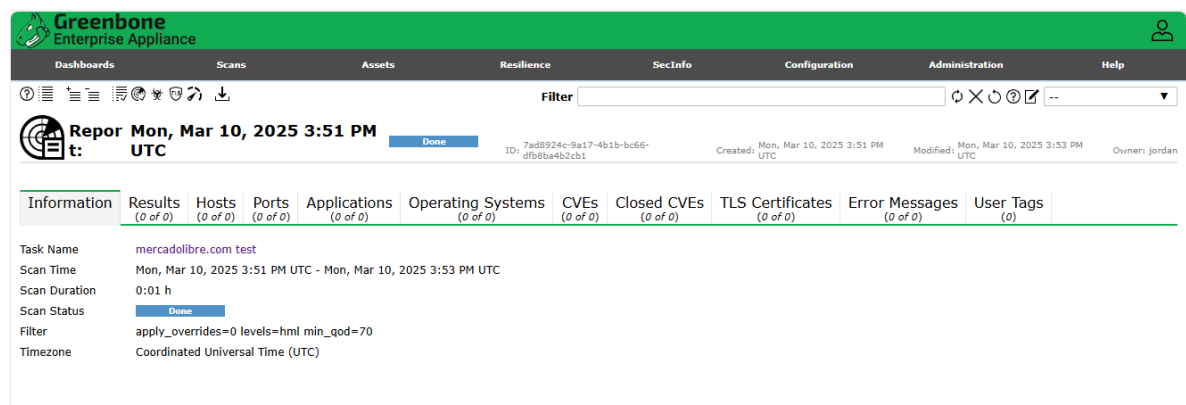


Ilustración 18 Grenbone

```
kali@kali: ~  
File Actions Edit View Help  
+-----+-----+-----+-----+  
[INF] No new updates found for nuclei templates  
  
(kali@kali)-[~]  
$ nuclei -u mercadolibre.com  
WARNING:(ast) sonic only supports go1.17~1.23, but your environment is not suitable  
  
      _ _ _ _ _  
     / / / / /  
    / / / / /  
   / / / / /  
  / / / / /  
 / / / / /  
/ / / / /  
v3.3.9  
projectdiscovery.io  
  
[INF] Current nuclei version: v3.3.9 (outdated)  
[INF] Current nuclei-templates version: v10.1.5 (latest)  
[WRN] Scan results upload to cloud is disabled.  
[INF] New templates added in latest release: 281  
[INF] Templates loaded for current scan: 7756  
[INF] Executing 7567 signed templates from projectdiscovery/nuclei-templates  
[WRN] Loading 189 unsigned templates for scan. Use with caution.  
[INF] Targets loaded for current scan: 1  
[INF] Running httpx on input host  
[INF] Found 1 URL from httpx  
[INF] Templates clustered: 1713 (Reduced 1620 Requests)  
[INF] Using Interactsh Server: oast.fun  
[cookies-without-httponly] [javascript] [info] mercadolibre.com ["_d2id"]  
[azure-domain-tenant] [http] [info] https://login.microsoftonline.com:443/mercadolibre.com/v2.0/.well-known/openid-configuration ["882c0c7c-23db-40e6-9992-5b2c0f064e05"]  
  
(kali@kali)-[~]  
$
```

Ilustración 19 Nuclei

## Conclusión

Investigando un poco sobre el resultado de la URL <https://login.microsoftonline.com:443/mercadolibre.com/v2.0/.well-known/openid-configuration>

La presencia de este endpoint indica que mercadolibre.com utiliza Microsoft Entra ID para gestionar la autenticación y autorización mediante el protocolo OpenID Connect. Este es un enfoque común y seguro cuando se implementa correctamente. No obstante, es crucial que la organización mantenga buenas prácticas de seguridad en la configuración y gestión de su proveedor de identidad para proteger los datos y recursos de sus usuarios.

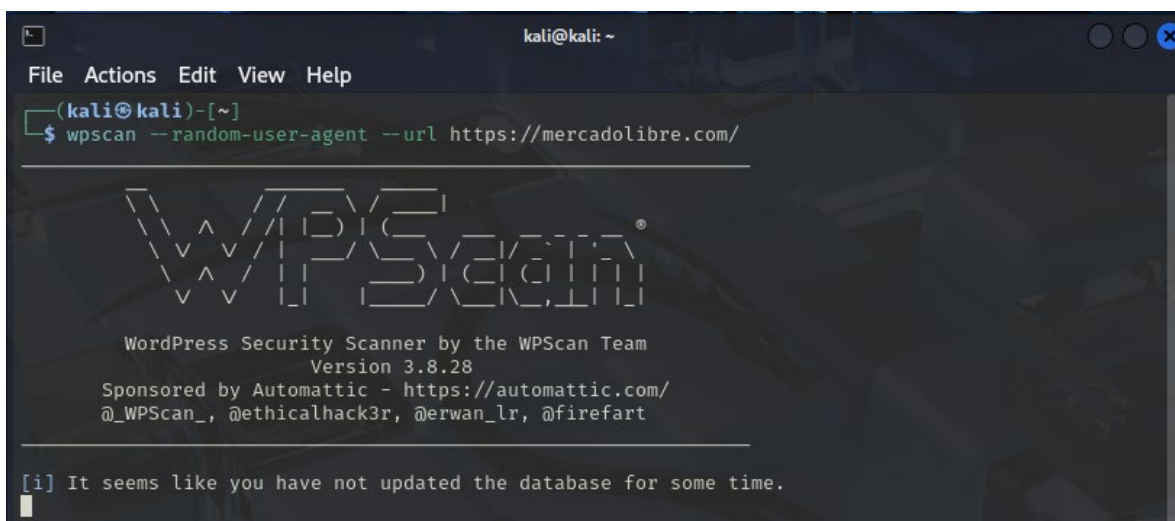


## 4.2. Análisis web – wpscan

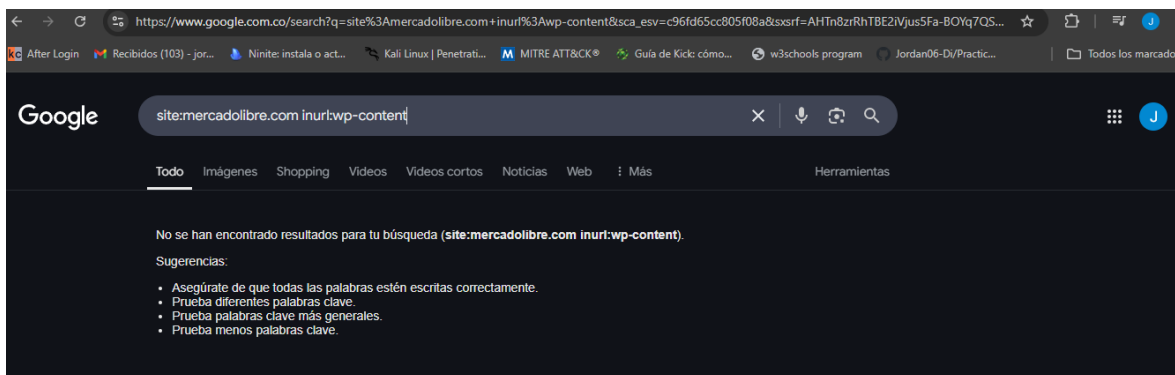
Utilice Wpscan para analizar la presencia de sitios basados en WordPress dentro del dominio, con el objetivo de identificar posibles vulnerabilidades en plugins, temas o configuraciones. Sin embargo, el escaneo no detectó subdominios que utilicen esta tecnología.

## Conclusión

Los resultados indican que el dominio “mercadolibre.com” no tiene implementaciones de WordPress accesibles públicamente.



*Ilustración 20 Wpscan*



*Ilustración 21 wp-content*

### 4.3. Análisis SSL/TLS

Se realizó un análisis de seguridad SSL/TLS utilizando Qualys SSL Labs en dos direcciones IP asociadas a mercadolibre.com. Ambos servidores obtuvieron una calificación B, lo que indica una configuración aceptable, pero con aspectos mejorables.

El principal problema identificado es el soporte de los protocolos TLS 1.0 y TLS 1.1, los cuales están obsoletos y considerados inseguros.

#### Conclusión

Si bien los servidores analizados tienen una configuración SSL adecuada en cuanto a cifrados y certificados, la compatibilidad con versiones antiguas de TLS representa un riesgo de seguridad.

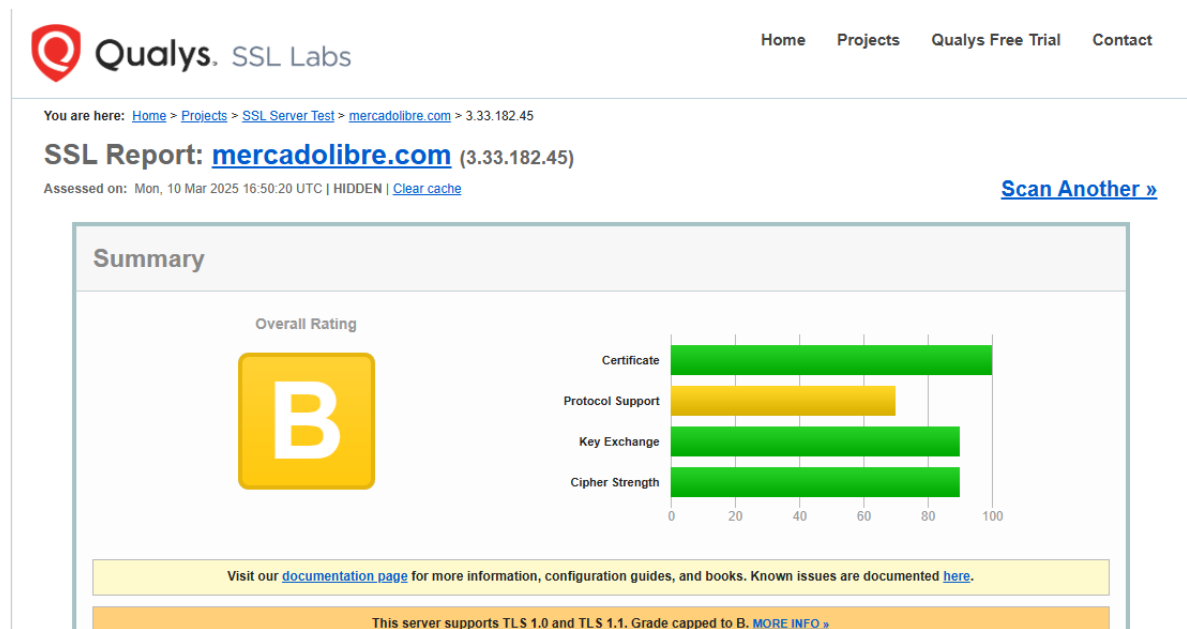


Ilustración 22 SSL





You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [mercadolibre.com](#) > 15.197.170.90

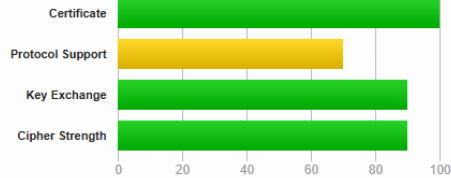
## SSL Report: [mercadolibre.com](#) (15.197.170.90)

Assessed on: Mon, 10 Mar 2025 16:50:20 UTC | [HIDDEN](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

Ilustración 23 SSL 2

```
kali@kali: ~/recopilacion/mercadolibre.com/26022025/testssl.sh
File Actions Edit View Help

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025/testssl.sh]
$ ./testssl.sh mercadolibre.com

#####
testssl.sh version 3.2rc4 from https://testssl.sh/dev/
(f34b81e 2025-03-06 11:16:01)

This program is free software. Distribution and modification under
GPLv2 permitted. USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ https://testssl.sh/bugs/
#####

Using OpenSSL 1.0.2-bad (Sep 1 2022) [-179 ciphers]
on kali:./bin/openssl.Linux.x86_64

Testing all IPv4 addresses (port 443): 143.204.23.45 143.204.23.68 143.204.23.49 143.204.23.119

Start 2025-03-10 13:15:17 —> 143.204.23.45:443 (mercadolibre.com) <—

Further IP addresses: 143.204.23.119 143.204.23.68 143.204.23.49
rDNS (143.204.23.45): server-143-204-23-45.bog50.r.cloudfront.net.
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    offered (OK): final
```

Ilustración 24 Testssl

#### 4.4. Análisis de servidores correo (DMARC/DKIM/SPF)

El análisis de DMARC para el dominio mercadolibre.com muestra que cuenta con una configuración válida y adecuada de sus registros DMARC, SPF y DKIM. Esto significa que el dominio está bien protegido contra ataques de phishing, suplantación de identidad (spoofing) y uso no autorizado para el envío de correos electrónicos maliciosos.

##### Conclusión

El dominio mercadolibre.com tiene una buena configuración de seguridad en su correo electrónico, lo que ayuda a prevenir ataques.

COMPROBAR DOMINIO

**¡Bien hecho! Tiene un registro DMARC válido que le permite ver la totalidad de sus programas de correo electrónico y le ayuda a garantizar que cumple con las mejores prácticas de envío de correo electrónico. Su dominio aprovecha al máximo las protecciones de dominio que ofrece DMARC.**

Las comprobaciones que se realizan aquí son similares a las que realizan los proveedores de buzones de correo, como Google, Yahoo y Microsoft. Los registros DMARC, SPF y DKIM se encuentran en el DNS de su dominio y los utilizan los proveedores de buzones de correo para separar el correo electrónico legítimo del abuso. Según su estricta política DMARC, los receptores de buzones de correo pueden identificar y bloquear de forma fiable el phishing, la suplantación de identidad y el uso no autorizado de su dominio.

EMPEZAR

✓ DMARC

Su dominio tiene un registro DMARC válido y su política DMARC evitará el abuso de su dominio por parte de phishers y spammers.

+ [Detalles](#)

✓ FPS

¡Buen trabajo! Tienes un registro SPF válido, que especifica un error leve (~all).

+ [Detalles](#)

✓ DKIM

Encontramos al menos un registro DKIM válido. Es probable que tengas otros, ya que cada fuente de envío de correo electrónico debe tener sus propias claves DKIM. La visibilidad de DMARC puede ayudarte a descubrir cada una de tus claves DKIM y mucho más.

+ [Detalles](#)

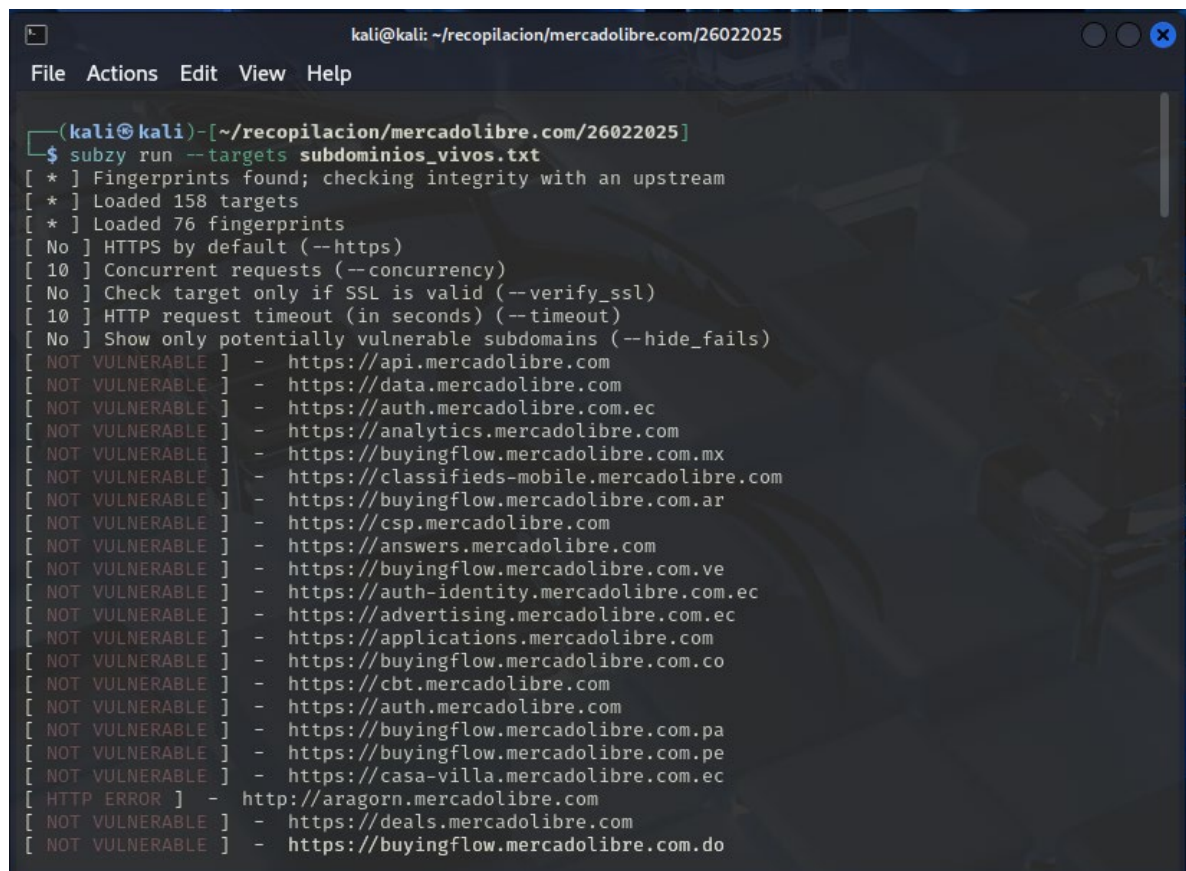
Ilustración 25 Dmarc

#### 4.5. Detección de subdominios takeover (subzy)

Subzy es una herramienta de seguridad utilizada para detectar subdominios huérfanos o mal configurados, los cuales podrían ser secuestrados, en la ejecución de los subdominios de “mercadolibre.com” no se encontraron vulnerabilidades.

Conclusión:

El escaneo realizado con Subzy no encontró subdominios vulnerables a una posible toma de control. Esto indica que la configuración DNS y los servicios asociados a los subdominios de mercadolibre.com están correctamente gestionados.



```
kali@kali: ~/recopilacion/mercadolibre.com/26022025
File Actions Edit View Help

(kali@kali)-[~/recopilacion/mercadolibre.com/26022025]
$ subzy run --targets subdominios_vivos.txt
[ * ] Fingerprints found; checking integrity with an upstream
[ * ] Loaded 158 targets
[ * ] Loaded 76 fingerprints
[ No ] HTTPS by default (--https)
[ 10 ] Concurrent requests (--concurrency)
[ No ] Check target only if SSL is valid (--verify_ssl)
[ 10 ] HTTP request timeout (in seconds) (--timeout)
[ No ] Show only potentially vulnerable subdomains (--hide_fails)
[ NOT VULNERABLE ] - https://api.mercadolibre.com
[ NOT VULNERABLE ] - https://data.mercadolibre.com
[ NOT VULNERABLE ] - https://auth.mercadolibre.com.ec
[ NOT VULNERABLE ] - https://analytics.mercadolibre.com
[ NOT VULNERABLE ] - https://buyingflow.mercadolibre.com.mx
[ NOT VULNERABLE ] - https://classifieds-mobile.mercadolibre.com
[ NOT VULNERABLE ] - https://buyingflow.mercadolibre.com.ar
[ NOT VULNERABLE ] - https://csp.mercadolibre.com
[ NOT VULNERABLE ] - https://answers.mercadolibre.com
[ NOT VULNERABLE ] - https://buyingflow.mercadolibre.com.ve
[ NOT VULNERABLE ] - https://auth-identity.mercadolibre.com.ec
[ NOT VULNERABLE ] - https://advertising.mercadolibre.com.ec
[ NOT VULNERABLE ] - https://applications.mercadolibre.com
[ NOT VULNERABLE ] - https://buyingflow.mercadolibre.com.co
[ NOT VULNERABLE ] - https://cbt.mercadolibre.com
[ NOT VULNERABLE ] - https://auth.mercadolibre.com
[ NOT VULNERABLE ] - https://buyingflow.mercadolibre.com.pa
[ NOT VULNERABLE ] - https://buyingflow.mercadolibre.com.pe
[ NOT VULNERABLE ] - https://casa-villa.mercadolibre.com.ec
[ HTTP ERROR ] - http://aragorn.mercadolibre.com
[ NOT VULNERABLE ] - https://deals.mercadolibre.com
[ NOT VULNERABLE ] - https://buyingflow.mercadolibre.com.do
```

Ilustración 26 Subzy

## 5. TECNICAS OSINT

En esta parte se explotaron técnicas y herramientas OSINT aplicadas a redes sociales relevantes para evaluar el nivel de exposición de “mercadolibre.com” y su posible impacto en la seguridad, la inteligencia de fuentes abiertas (OSINT, Open Source Intelligence) juega un papel crucial en la recopilación de información pública para identificar posibles amenazas y vulnerabilidades.

Las redes sociales son una fuente valiosa dentro de OSINT, ya que permiten analizar la exposición de información sensible, patrones de comportamiento y posibles vectores de ataque.

### MALTEGO

En este caso utilice Maltego para investigar el dominio “mercadolibre.com”, logrando extraer una serie de direcciones de correo electrónico corporativas y un correo personal.

Resultados obtenidos: Se identificaron múltiples direcciones de correo electrónico relacionadas con el dominio mercadolibre.com, además de algunos nombres asociados a esas cuentas:

- Correos corporativos:
  - [pablo.rocco@mercadolibre.com](mailto:pablo.rocco@mercadolibre.com)
  - [luciano.juarez@mercadolibre.com](mailto:luciano.juarez@mercadolibre.com)
  - [lorenzo.ganz@mercadolibre.com](mailto:lorenzo.ganz@mercadolibre.com)
  - [nicolas.videla@mercadolibre.com](mailto:nicolas.videla@mercadolibre.com)
  - [pablo.medic@mercadolibre.com](mailto:pablo.medic@mercadolibre.com)
  - [jonathan.lalana@mercadolibre.com](mailto:jonathan.lalana@mercadolibre.com)
- Personas asociadas:
  - Pablo Rocco
  - Luciano Juarez
  - Marcelo Lorenzo Ganz
  - Nicolás Videla
- Correo personal encontrado:
  - videlanicolas@gmail.com (asociado a Nicolás Videla)

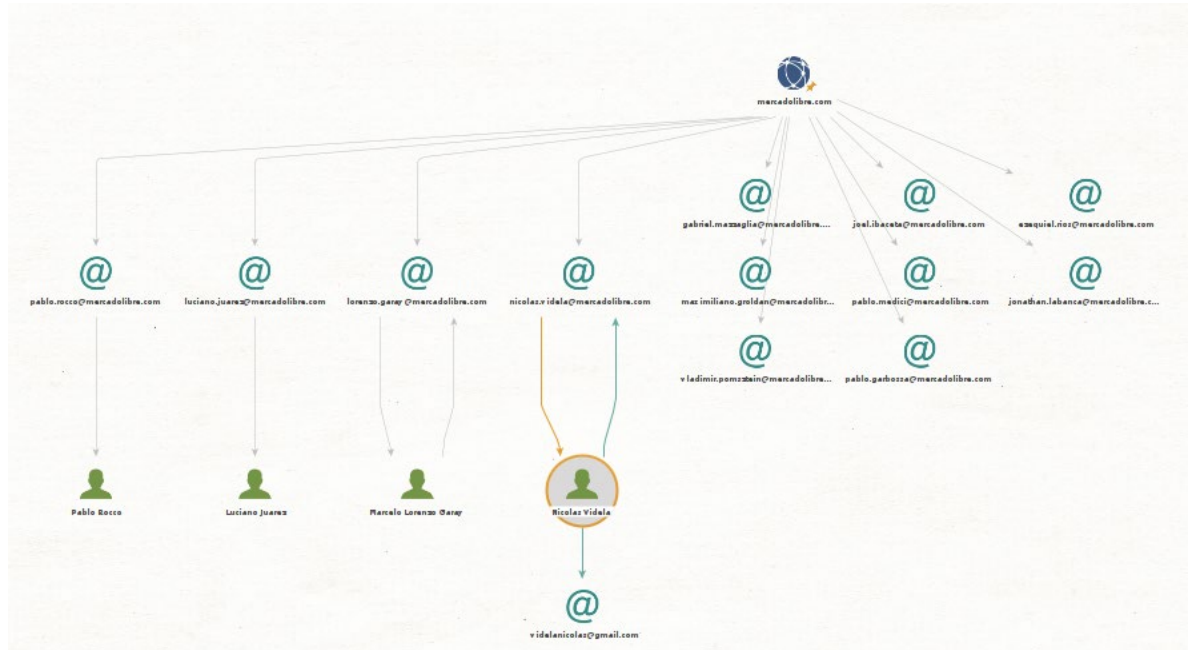




Ilustración 27 Maltego

## REDES SOCIALES (LINKEDING)

Después de realizar una búsqueda con los nombres de los empleados encontrados, se evidencia que dos de ellos tienen perfiles en la red Linkeding y pertenecen al mundo TI, además son ex colaboradores de Mercado Libre.

✓ Pablo Rocco

**Pablo Rocco**  
Senior Technical Security Analyst at Shopify

**Senior Security Compliance Engineer**  
Mercadolibre.com  
may. 2016 - oct. 2018 · 2 años 6 meses  
Argentina

- Policy & process design: redesigned and implemented risk analysis process and incident management process.
- Security incident management: Lead incident coordinator, design and implementation of incident management web application.
- Compliance program: Run PCI DSS program, both operational and assessment support.
- Report & metrics: Security compliance metrics reports using Tableau data visualization tool.


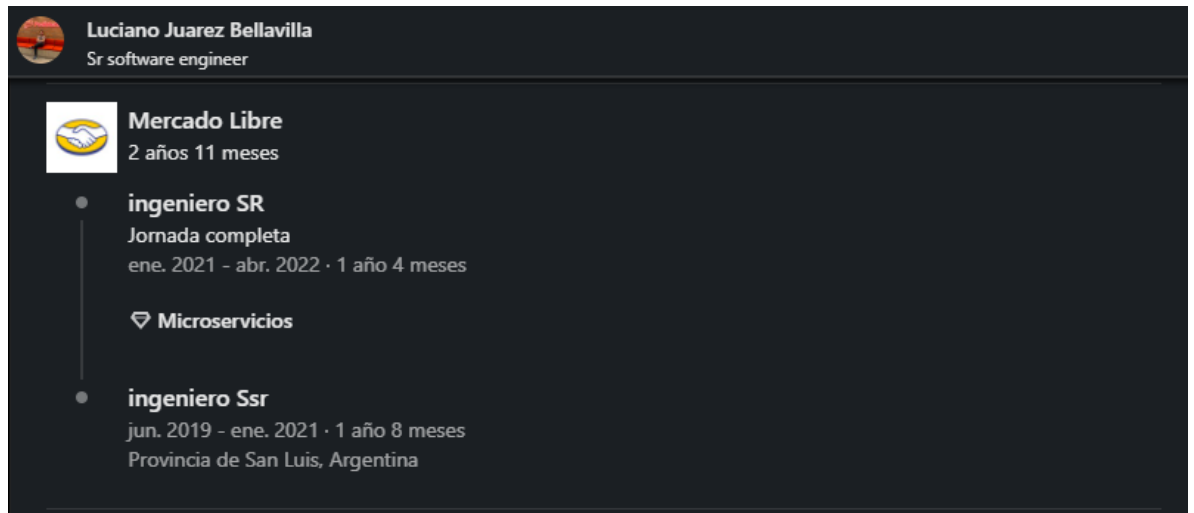
 **Security Monitoring y Analytical Skills**

Ilustración 28 Pablo Rocco

✓ Luciano Juarez



The screenshot shows a LinkedIn profile for Luciano Juarez Bellavilla, a Sr software engineer. The profile includes a profile picture, a cover photo, and a list of work experiences. The first experience is at Mercado Libre, where he worked as an ingeniero SR from January 2021 to April 2022. The second experience is at Microservicios, where he worked as an ingeniero Ssr from June 2019 to January 2021. The profile also shows a location of Provincia de San Luis, Argentina.

**Luciano Juarez Bellavilla**  
Sr software engineer

**Mercado Libre**  
2 años 11 meses

- ingeniero SR**  
Jornada completa  
ene. 2021 - abr. 2022 · 1 año 4 meses
- Microservicios**
- ingeniero Ssr**  
jun. 2019 - ene. 2021 · 1 año 8 meses  
Provincia de San Luis, Argentina

Ilustración 29 Luciano Juarez

## 6. CONCLUSIÓN

El análisis realizado en este informe demuestra cómo, a través de técnicas de Foorprinting, Fingerprinting, análisis de vulnerabilidades y OSINT, es posible recolectar una gran cantidad de información sobre un dominio y su infraestructura asociada.

En la fase de Foorprinting, herramientas como Shuffledns, Katana y Ctfr permitieron identificar subdominios, registros de certificados y contenido indexado, facilitando la comprensión del ecosistema digital del objetivo. Posteriormente, en el Fingerprinting, herramientas como Masscan, Nmap y Wappalyzer ayudaron a perfilar los servicios y tecnologías en uso, incluyendo la detección de posibles WAFS y contenidos ocultos mediante Fuzzing.

En la fase de análisis de vulnerabilidades, se utilizaron herramientas como Greenbone, Nuclei y Wpscan, detectando posibles fallos de seguridad en la infraestructura web y en la configuración de SSL/TLS y servidores de correo. Además, con Subzy.

Finalmente, la aplicación de técnicas de OSINT y el uso de Maltego evidenciaron cómo la información expuesta en fuentes abiertas y redes sociales puede ser utilizada por atacantes para realizar ataques dirigidos, demostrando la importancia de una correcta gestión de la información pública y credenciales filtradas.

En conclusión, este informe refuerza la necesidad de una estrategia integral de ciberseguridad, combinando auditorías periódicas, configuración segura de servicios, monitoreo constante y concienciación en seguridad digital.

## 7. REFERENCIAS Y BIBLIOGRAFIA

- Herramientas explicadas en GitHub
- ChatGPT IA