

OSINT Ofensivo

ReadMe :

Este documento comenzará con una breve descripción de qué es OSINT y cómo su uso complementa las actividades de un equipo de red team en pentesting y hacking ético. Posteriormente, presentaré una de mis metodologías para realizar OSINT en el reconocimiento de aplicaciones web, junto con las herramientas que utilizo.

¿Qué es OSINT?

OSINT (Open Source Intelligence) se refiere al conjunto de técnicas y herramientas que se utilizan para recopilar información pública disponible en fuentes abiertas (sitios web, dns, dorks, bases de datos, registros públicos gubernamentales, etc), analizar los datos obtenidos y relacionarlos para generar inteligencia útil. Posteriormente se utilizará esta información de inteligencia para planificar la etapa de prueba de penetración.

OSINT en un Red Team para Pentesting Web

Un Red Team (Equipo Rojo) es un equipo de personas que utilizan las mismas técnicas y herramientas de los hackers o ciber atacantes para evadir la detección y poner a prueba la seguridad de las aplicaciones, software, servidores, sistemas informáticos, políticas de seguridad, capital humano, etc.

En un equipo de **Red Team**, OSINT es una fase clave del **reconocimiento** (reconnaissance), ya que permite identificar posibles vectores de ataque antes de ejecutar penetraciones en sitios específicos de los sistemas. Así es como OSINT se complementa con el pentesting web:

[1] *Identificación de Objetivos y Tecnologías:*

Se recopilan dominios, subdominios y direcciones IP asociadas a la empresa.

Se identifican tecnologías utilizadas en los servidores web (**CMS, frameworks, servidores, bases de datos**).

[2] *Recolección de Credenciales Filtradas:*

Se buscan credenciales expuestas en filtraciones de datos mediante herramientas y bases de datos de breaches.

Se analiza el uso de **contraseñas débiles o reutilizadas**.

[3] *Descubrimiento de Subdominios y Servicios Web Expuestos:*

Se utilizan herramientas de consola o servicios web para encontrar subdominios.

Se buscan endpoints, API expuestos o paneles administrativos sin protección.

[4] *Análisis de Metadatos y Documentos Públicos:*

Se extraen metadatos de documentos en línea (**PDF, DOCX, imágenes**) que pueden revelar nombres de usuarios, versiones de software o estructuras internas.

[5] *Enumeración de Empleados:*

Se recopila información sobre empleados en LinkedIn o redes sociales para diseñar ataques de phishing dirigidos.

También se enumeran los empleados para tener un conocimiento de cómo está jerarquizada la empresa en base al personal de trabajo e identificar puestos claves (**CEO, CTO, gerente, administración, desarrolladores**).

[6] *Búsqueda de Vulnerabilidades Conocidas:*

Se analizan versiones de software utilizadas y se cruzan con bases de datos de vulnerabilidades como **CVE, Exploit-DB, searchsploit, github**.

[7] *Monitoreo de Exposición y Dark Web:*

Se investiga en foros clandestinos y la Dark Web con herramientas específicas en busca de información filtrada o credenciales en venta. Esto lo hacemos con la intención de validar si hay datos filtrados sobre un objetivo y aprovecharnos de esa información.

[📄] *Metodología de OSINT Ofensivo*

La siguiente metodología se divide en 5 etapas de acuerdo a la investigación que iremos haciendo en el software y la empresa/organización.

[?] WHOIS

- | -> Información de tecnologías
- | -> Información de consultas DNS
- | -> Geolocalización IP de servidores

[🔍] INSPECCIONAR WEB

- | -> Navegación y funcionalidad de la web
- | -> Hover sobre componentes de la web
- | -> Inspeccionar contenido HTML (Ctrl+u)
- | -> Analizar metadatos en la cabecera del HTML
- | -> Buscar versiones y autores de la web
- | -> Inspeccionar flujo de archivos del Network browser tool (proxy)
- | -> Buscar palabras claves en la Debbuger browser tool
- | -> Buscar paneles de login
- | -> Analizar redirecciones href
- | -> Escanear y analizar las URLs de la web
- | -> Fuzzing de archivos y directorios
- | -> Descubrimiento de puertos activos

[🌐] SUBDOMINIOS

- | -> Buscar subdominios con herramientas de consola
- | -> Buscar subdominios con herramientas web
- | -> Buscar subdominios con herramientas de interfaz API
- | -> Buscar subdominios con dorks

| -> Buscar subdominios por certificados CA/SSL/TLS

[✉] Emails

| -> Buscar direcciones emails con herramientas web

| -> Buscar direcciones emails con dorks

| -> Buscar direcciones emails con scripts

[👤] Linkedin

| -> Buscar empleados con Linkedin

| -> Buscar empleados en redes sociales

| -> Buscar empleados con dorks

| -> Buscar empleados con scripts

[🕷] SCRAPING DE TRÁFICO HTTP

| -> Network browser tool (proxy)

| -> Proxy http (Burpsuit, Mitmproxy)

| -> Inspección de archivos sensibles (conf.js, app.js, scrips.js)

[🗺] MAPA DE INTELIGENCIA

| -> Ordenar y plasmar la estructura informática

| -> Generar un workflow de esquema de relaciones

[🔪] Técnicas y herramientas para OSINT Ofensivo

A continuación, se especificarán técnicas y herramientas que utilizo para ejecutar OSINT en etapa de reconocimiento para pentesting web.

[?] WHOIS

La etapa “whois” involucra obtener datos acerca de la infraestructura y las aplicaciones web. Podemos obtener datos sobre las tecnologías utilizadas para crear las aplicaciones web, datos relacionados al registro de dominios, cantidad de dominios registrados, quien registro los dominios, ubicación del servidor, proveedor del servicio de hosting, dirección IP del servidor web, información de los servidores DNS (registros MX, configuración de protocolos de seguridad SPF, DKIM, DMARK).

● [Información de consultas DNS]

[🔪] whois

Install: sudo apt install whois

```
└─$ whois oca.com.ar > whois.txt

domain:                oca.com.ar
registrant:            [REDACTED]
registrar:             nicar
registered:            1996-01-01 00:00:00
changed:               2024-11-07 17:07:08.989798
expire:               2025-12-01 00:00:00

contact:               [REDACTED]
name:                 OCA LOG S.A.
registrar:            nicar
created:              2021-11-12 11:28:12.407904
changed:              2025-01-29 13:58:53.008705

ns1:                  dns1.advance.com.ar ([REDACTED])
ns2:                  dns2.advance.com.ar ([REDACTED])
registrar:            nicar
created:              2016-06-30 22:57:32.387639
```

[🐞] Centralops

Link: <https://centralops.net/co/>

Central Ops .net		Advanced online Internet utilities	
Utilities		DNS records	
Domain Dossier	Domain Check	name	class type data
Email Dossier	Browser Mirror	oca.com.ar	IN CAA [no interpretation available] 00 05 69 73 73 75 65 6C ..issue1 hex dump: 65 74 73 65 66 63 72 79 etsenory (22 bytes) 79 74 2E 6F 72 67 pt.org
Ping	Traceroute	oca.com.ar	IN CAA [no interpretation available] 00 05 69 73 73 75 65 73 ..issues hex dump: 65 63 74 69 67 6F 2E 63 ectigo.c (18 bytes) 6F 6D om
NSlookup / Dig		oca.com.ar	IN CAA [no interpretation available] 00 09 69 73 73 75 65 77 ..issuew hex dump: 09 6C 64 73 65 63 74 69 ildsecti (22 bytes) 67 6F 2E 63 6F 6D go.com
		oca.com.ar	IN A [redacted]
		oca.com.ar	IN TXT v=spf1 a mx ip4:[redacted] ip4:[redacted] ip4:[redacted] include:spf:[redacted] include:spf:[redacted] include:_spf:[redacted] ~all
		oca.com.ar	IN TXT k=rsa, t=s; p=MIGfMA0GCsqGSIb3DQEBAQUAA4GNADCBiQKBgQDPtW5iwpXVPiH5FzJ7Nr18USzuY9zqqzJE0D1r04xDN6qwiDnmgcFNNfMewVKNZD1O+2J9N14hRprzByFwFQW76yoh54Xu3uSbQ
		oca.com.ar	IN TXT MS=ms41493589
		oca.com.ar	IN TXT MS=ms51223267
		oca.com.ar	IN TXT sophos-domain-verification=343eea39ed4e78305cbf0777382b458e2a4476ed
		oca.com.ar	IN TXT R0hlyozMzG215+jAYeD5kPR8RXRHauwKONYmUSM0BgCy15UyBdLCBkPEdZG5cKGfmBNkVojCGdliMOQTtEqmg==
		oca.com.ar	IN SOA server: dns1.advance.com.ar email: dominios@advance.com.ar

[🐞] Dnsdumpster

Link: <https://dnsdumpster.com>

MX Records			
5 oca-com-	[redacted]	ASN: 8875	MICROSOFT-CORP-MSN-AS-BLOCK
ar.mail.protection.outlook.com	mail-	52.96.0.0/12	United States
	colpr85cu@201.inbound.pro		
	tection.outlook.com		
NS Records			
dns2.advance.com.ar	[redacted]	ASN: 10834	Telefonica de Argentina, AR
		209.13.0.0/16	Argentina
dns1.advance.com.ar	[redacted]	ASN: 10834	Telefonica de Argentina, AR
		209.13.0.0/16	Argentina
TXT Records			
"k=rsa; t=s; p=MIGfMA0GCsqGSIb3DQEBAQUAA4GNADCBiQKBgQDPtW5iwpXVPiH5FzJ7Nr18USzuY9zqqzJE0D1r04xDN6qwiDnmgcFNNfMewVKNZD1O+2J9N14hRprzByFwFQW76yoh54Xu3uSbQ3JP0A7k8o8GutRF8zbFUA8n0ZH2y0cIEjM1ixY4W4LwPA7m4q00bmV5jhd6309d8z1XkUbwIDAQAB"			
"MS=ms51223267"			
"sophos-domain-verification=343eea39ed4e78305cbf0777382b458e2a4476ed"			
"MS=ms41493589"			
"v=spf1 a mx ip4:[redacted] ip4:[redacted] ip4:[redacted] ip4:[redacted] include:spf:[redacted] include:[redacted] include:_spf.embluemail.com ~all"			
"R0hlyozMzG215+jAYeD5kPR8RXRHauwKONYmUSM0BgCy15UyBdLCBkPEdZG5cKGfmBNkVojCGd1/iMOQTtEqmg=="			

[🔪] dnsrecon

```
└─$ dnsrecon -d oca.com.ar
[*] std: Performing General Enumeration against: oca.com.ar ...
[-] DNSSEC is not configured for oca.com.ar
[*] SOA dns1.advance.com.ar 209.
[*] NS dns2.advance.com.ar 209.
[*] Bind Version for 209. disclosed"
[*] NS dns1.advance.com.ar 209.
[*] Bind Version for 209. disclosed"
[*] MX oca-com-ar.mail.protection.outlook.com 52.
[*] MX oca-com-ar.mail.protection.outlook.com 52.
[*] MX oca-com-ar.mail.protection.outlook.com 52.
[*] MX oca-com-ar.mail.protection.outlook.com 52.
[*] A oca.com.ar 200.
[*] TXT oca.com.ar sophos-domain-verification=343eea39ed4e78305cbf0777382b458e2a4476ed
[*] TXT oca.com.ar R0hlyozMzG215+jAYeD5kPR8RXRHauwKONYmUSM0BgCvL5UYbDLcBkPEdZG5cKGfmBNkV
[*] TXT oca.com.ar v=spf1 a mx ip4: ip4: ip4:
bluemail.com ~all
[*] TXT oca.com.ar k=rsa; t=s; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDPtW5iwpXVPiH5FzJ
tRF8zbFUA8n0ZH2y0cIEjMliXY4W4LwPA7m4q00bmVsjhd6309d8z1XkUBwIDAQAB
[*] TXT oca.com.ar MS=ms41493589
[*] TXT oca.com.ar MS=ms51223267
[*] TXT _dmarc.oca.com.ar v=DMARC1; p=quarantine
[*] Enumerating SRV Records
[+] SRV _sipfederationtls._tcp.oca.com.ar sipfed.online.lync.com 443
[+] SRV _autodiscover._tcp.oca.com.ar correo.oca.com.ar 200. 443
[+] 2 Records Found
```

🔴 [INFORMACIÓN DE TECNOLOGÍAS]

[🔪] whatweb

Install: sudo apt install whatweb

```
.$$$ $$.
$$$$ $$. .$$$ $$$ .$$$$$. .$$$$$$$$$. $$$ $$. .$$$$$. .$$$$$.
$ $$ $$$ $ $$$ $$$ $ $$$$$$. $$$$ $$$$$$ $ $ $$$ $ $$$ $$.
$ ` $ $$$ $ ` $ $$$ $ ` $ $$$ $ $ ' $ ` $ ` $ $ ` $ $$$ $ ` $ $$$'
$. $ $$$ $. $$$$$$ $. $$$$$$ ` $ $. $ : ' $. $ $$$ $. $$$ $ $. $$$$.
$: : $ . $$$ $: : $ $$$ $: : $ $$$ $: : $ $$$ $: : $ $$$ $: : $ $$$
$ ; ; $ $$$ $$$ $ ; ; $ $$$ $ ; ; $ $$$ $ ; ; $ $$$ $$$ $ ; ; $ $$$
$$$$$$$ $$$$$$ $$$$ $$$ $$$$ $$$ $$$$ $$$$$$ $$$$$$ $$$$$$ $$$$$$'
```

```

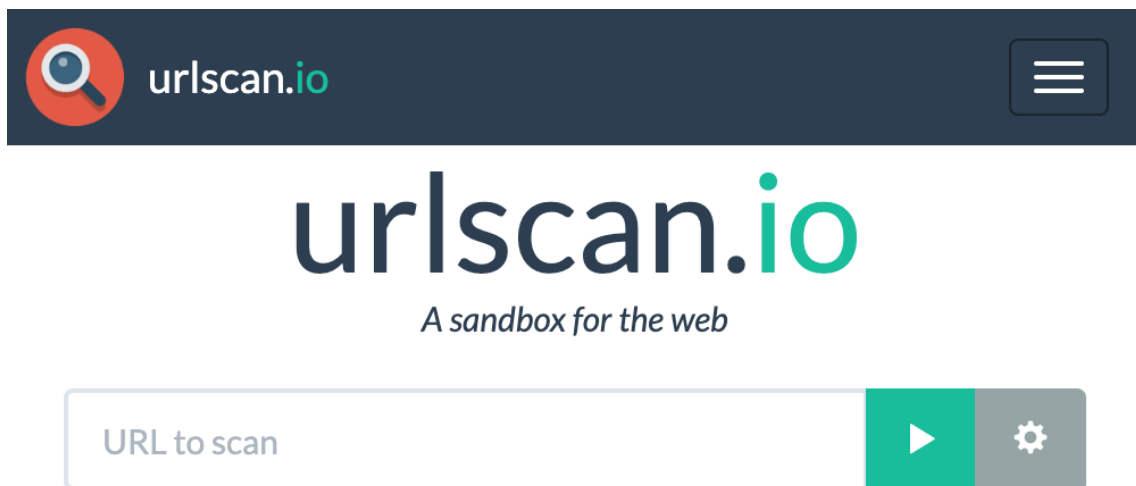
└─$ whatweb --color=never oca.com.ar | tr ',' '\n' | awk 'NF {print $NF}' > whatweb.txt

└─(sonic@sonic)~[/Public]
└─$ cat whatweb.txt
Country[ARGENTINA][AR]
HTTPServer[elb]
IP[200.10.96.107]
RedirectLocation[https://oca.com.ar:443/]
Permanently]
ASP.NET[4.0.30319][MVC5.3]
Bootstrap
Country[ARGENTINA][AR]
Frame
HTML5
HTTPServer[elb]
IP[200.10.96.107]
jQuery[3.5.1]
[IDENTIFICADOR-FACEBOOK]
Script[text/javascript]
llegan]
UncommonHeaders[x-aspnetmvc-version]
X-Powered-By[ASP.NET]

```

[🔗] **urlScan** (API)

Link: <https://urlscan.io/>



Realizar petición POST a la API:

```

└─$ curl -sX POST "https://urlscan.io/api/v1/scan/" -H "Content-Type: application/json" -H
"API-Key: your-api-key-here" -d '{"url": "$domain", "visibility": "public", "tags":
["demotag1", "demotag2"]}' > urlScan_uuid.txt

```


Obtener el "uuid" del archivo: urlScan_uuid.txt

```
{
  "message": "Submission successful",
  "uuid": "61a3ba41-[REDACTED]",
  "result": "https://urlscan.io/result/61a3ba41-[REDACTED]",
  "api": "https://urlscan.io/api/v1/result/61a3ba41-[REDACTED]",
  "visibility": "public",
  "options": {},
  "url": "[REDACTED]"
}
```

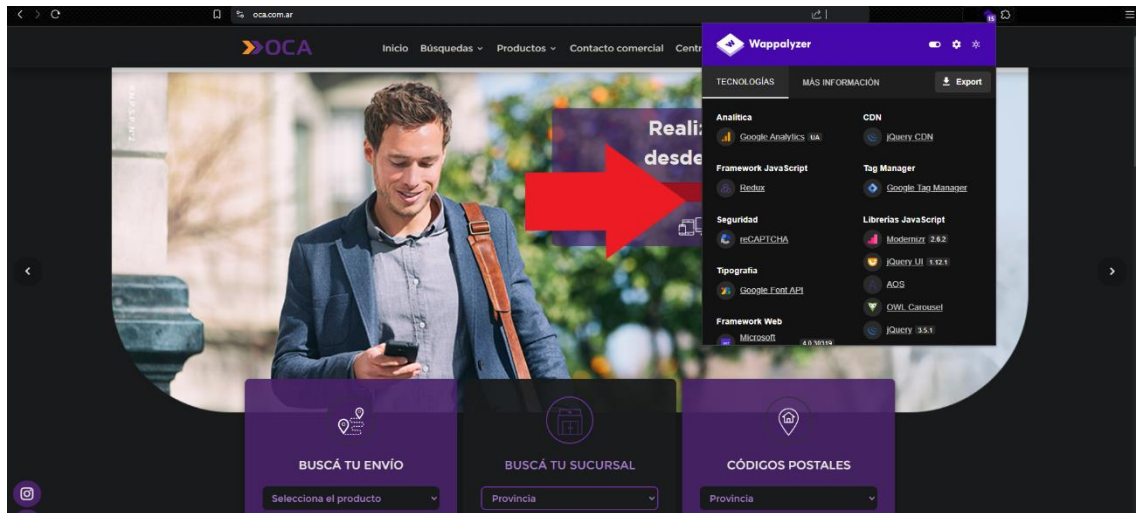
Realizar petición GET con el "uuid"

```
$ curl -s "https://urlscan.io/api/v1/result/your-uuid-here/" >> urlScan_result.txt
```

Resultado de tecnología del sitio web objetivo:

```
"servers": [
  "Microsoft-IIS/8.5",
  "nginx",
  "Golfe2",
  "ESF",
  "sffe",
  "Google Tag Manager",
  "cafe",
  "cloudflare",
  "AmazonS3"
],
"Server": "Microsoft-IIS/8.5",
"X-Powered-By": "ASP.NET"
```

[🔧] wappalyzer



● [Geolocalización IP de servidores]

[🔧] Hackertarget

```
$ curl -s "https://api.hackertarget.com/geoiip/?q=target-ip-here" > geoIP.txt
```

```
$ cat geoIP.txt
IP: 200.51.200.157
Country: Argentina
State: Buenos Aires
City: Rafael Castillo
Latitude: -34.7122
Longitude: -58.6112
```

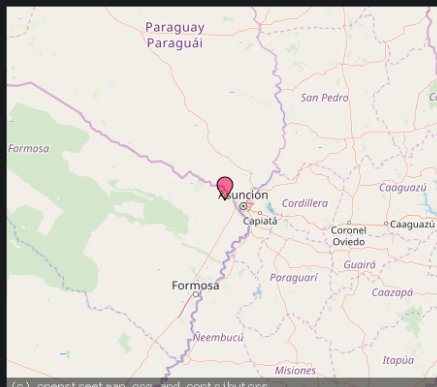
[🔧] Dnslytics

Link: <https://search.dnslytics.com>

IP 200.10.32.137

Summary

Description	HUAWEI TECH INVESTMENT CO LTD
PTR record	107.host.advance.com.ar
Provider	Telefonica de Argentina (AR 🇦🇷)
AS Number	10834 (AS10834/ASN10834)
IP range	200.10.32.0 - 200.10.32.255
On DNS Blacklist	No
Checked 23 DNSBL listings	
Number of domains hosted	4
Number of mail servers hosted	0
Number of name servers hosted	0
IP location	Clorinda, Formosa, Argentina (AR) 🇦🇷



[INSPECCIONAR WEB]

[🐞] Contenido HTML (Ctrl+u)

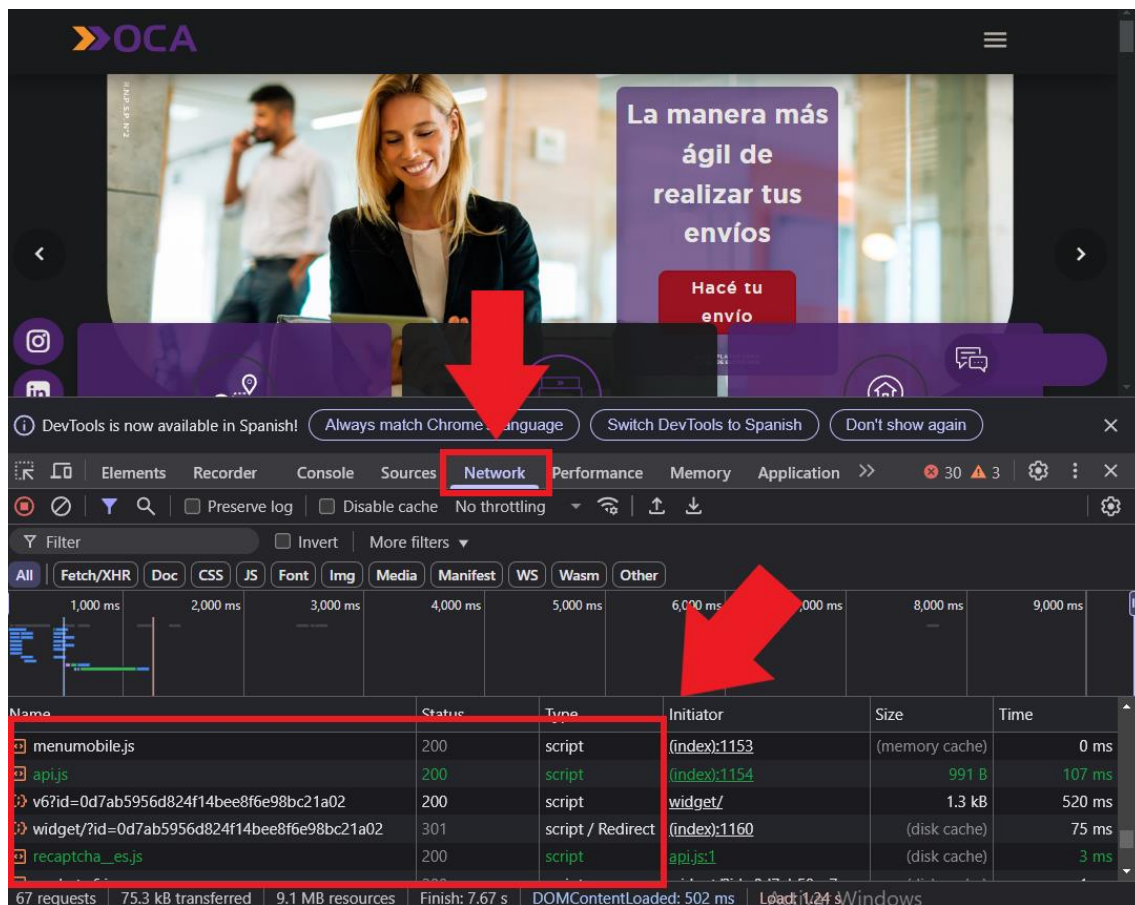
```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0">

  <link rel="icon" href="https://www.oca.com.ar/favicon-oca-32x32.png" sizes="32x32" />

  <title>Inicio - OCA - Las buenas noticias llegan</title>
  <meta name="description" content="Te damos la bienvenida a OCA, el correo privado m&#225;s grande del pa&#237;s. I

  <!-- Google Tag Manager -->
  <script>
  (function (w, d, s, l, i) {
    w[l] = w[l] || []; w[l].push({
      'gtm.start':
        new Date().getTime(), event: 'gtm.js'
    }); var f = d.getElementsByTagName(s)[0],
    j = d.createElement(s), dl = l != 'dataLayer' ? '&l=' + l : ''; j.async = true; j.src =
      'https://www.googletagmanager.com/gtm.js?id=' + i + dl; f.parentNode.insertBefore(j, f);
  })(window, document, 'script', 'dataLayer', 'GTM-TV7R9MZW');</script>
  <!-- End Google Tag Manager -->
  <!-- Facebook Tag -->
  <meta property="fb:admins" content="IDENTIFICADOR-FACEBOOK" />
  <meta property="og:title" content="Inicio - OCA - Las buenas noticias llegan" />
  <meta property="og:type" content="website" />
  <meta property="og:image" content="http://200.32.52.139/Content/oca_violeta.png" />
  <meta property="og:url" content="https://www.oca.com.ar" />
  <meta property="og:site_name" content="OCA" />
  <meta property="og:description" content="Te damos la bienvenida a OCA, el correo privado m&#225;s grande del pa&#237;s. I
```

[🐞] Network browser tool (proxy)



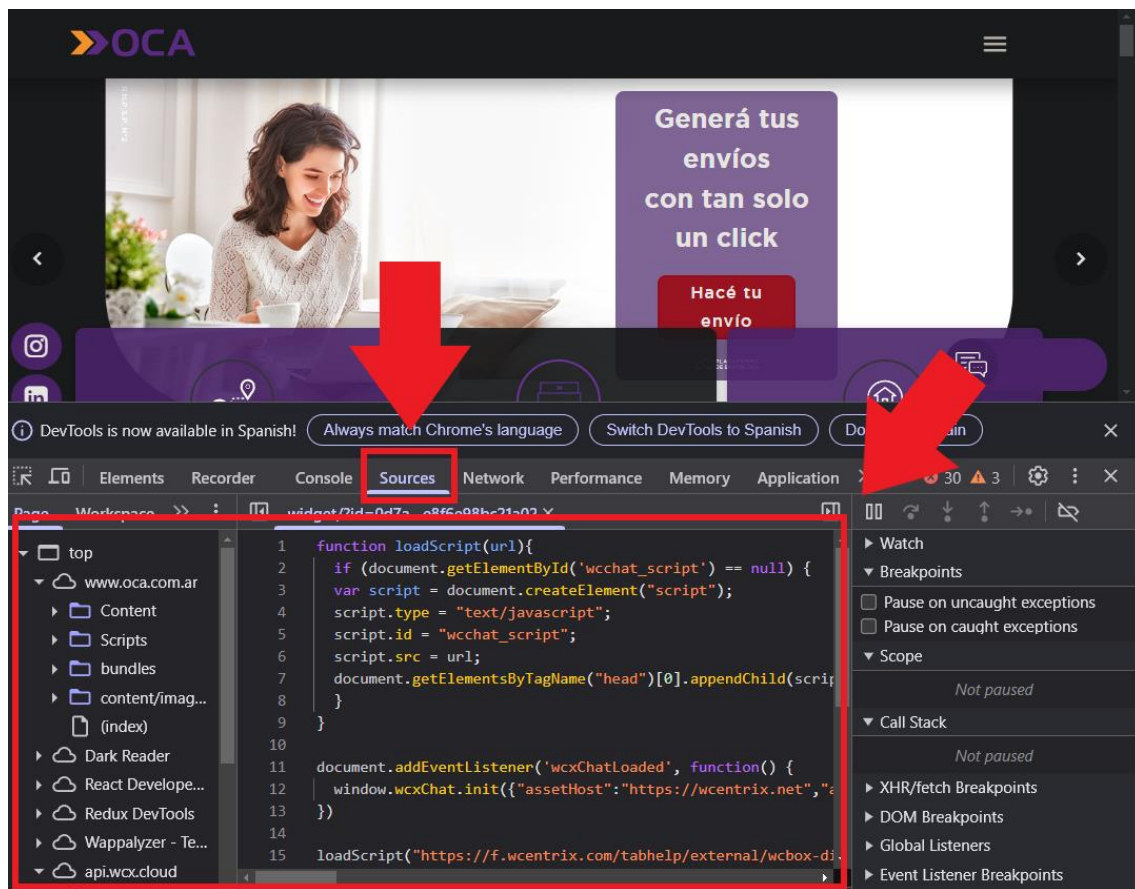
Podes utilizar las herramientas de desarrollo del navegador web apretando la combinación de teclas `ctrl+shift+c`.

Nos enfocaremos en utilizar la herramienta “network” de la consola del navegador.

Aquí analizaremos el trafico http que circula por las peticiones al dominio en cuestión.

Deberemos analizar y seleccionar los archivos que nos llamen la atención de forma manual para posteriormente inspeccionarlos en búsqueda de credenciales o información útil.

[🐞] Debugger browser tool



[🐞] Phonebook.cz

Phonebook.cz

Phonebook lists all domains, email addresses, or URLs for the given input domain. Wildcards such as *.gov.uk are allowed. You are searching 34 billion records.

netflix.com

Try: [cia.gov](#), [cnn.com](#), [netflix.com](#), [*.ru](#), [*.gov.uk](#), [solarwinds.com](#)

- ☐ Domains
☒ Email Addresses
☐ URLs

[roelofvanzwol@netflix.com](#)
[hsteck@netflix.com](#)
[xamatrain@netflix.com](#)
[chaos@netflix.com](#)
[rbachwani@netflix.com](#)
[jbennett@netflix.com](#)
[anorkin@netflix.com](#)
[zli@netflix.com](#)
[jbasilico@netflix.com](#)
[yramond@netflix.com](#)
[alex1@netflix.com](#)
[flixpac@netflix.com](#)
[bennett@netflix.com](#)
[barrys@netflix.com](#)
[phishing@netflix.com](#)
[rse@netflix.com](#)
[discship@netflix.com](#)
[paypal@netflix.com](#)
[hari@netflix.com](#)

[🔍] Way Back Machine

URL:

https://web.archive.org/cdx/search/cdx?url=oca.com.ar/*&collapse=urlkey&output=txt&fl=original

```
http://www.oca.com.ar:80/cdo/recomendar.asp
http://www.oca.com.ar:80/cdo/soft.asp
http://www.oca.com.ar:80/cdo/Tarifa.asp
http://www.oca.com.ar:80/cdo/terminos.asp
http://www.oca.com.ar/CentroDeAyuda
http://www.oca.com.ar/ChAI8M7eiwYQ8PCK3s3orIZHEicABsArpjgsqdo9qy6zqx0JpVy/qP2xcKSu9MSLmWU0fMsbWf2Ra6YaAsBX
http://www.oca.com.ar:80/chalchaleros98.htm
http://www.oca.com.ar/chalchaleros_98.gif
http://www.oca.com.ar/change._change
http://www.oca.com.ar/click._change
http://www.oca.com.ar/click.dismiss
http://www.oca.com.ar/click.magnificPopup
http://www.oca.com.ar:80/clientes
https://www3.oca.com.ar/Clientes/App_Themes/MiTheme/Estilos/main.css
https://www3.oca.com.ar/Clientes/App_Themes/MiTheme/Estilos/skin.css
http://www3.oca.com.ar:80/Clientes/BusyBoxDotNet.axd?res=maskBG.png
https://www.oca.com.ar/clientes/default.aspx?IdModulo=20
https://www.oca.com.ar/clientes/default.aspx?IdModulo=29
https://www.oca.com.ar/clientes/default.aspx?IdModulo=54
http://www.oca.com.ar:80/Clientes/Inicio.aspx?
http://www3.oca.com.ar:80/Clientes/Inicio.aspx?data=W38UsDNwMbqbQ00FP8JP+VzJ/KThjroi9adT1dSHQiuukV0jHh1KP8DgJ96WJ1RmJ7
https://www.oca.com.ar/Clientes/Inicio.aspx?data=W38UsDNwMbqbQ00FP8JP%2bVzJ%2fKThjroi9adT1dSHQiuukV0jHh1KP8DgJ96WJ1RmK
https://www3.oca.com.ar/Clientes/LogOut/Contenidos/CD_Faq.htm
https://www3.oca.com.ar/Clientes/LogOut/Contenidos/imagenes/cd_faq_001.gif
https://www3.oca.com.ar/Clientes/LogOut/Contenidos/imagenes/cd_faq_002.gif
https://www3.oca.com.ar/Clientes/LogOut/Contenidos/imagenes/spacer.gif
http://www.oca.com.ar:80/codigopostal.asp
http://www.oca.com.ar:80/codigopostal_archivos/editdata.mso
http://www.oca.com.ar:80/codigopostal_archivos/filelist.xml
http://www.oca.com.ar:80/comfecha.asp
http://www.oca.com.ar:80/comments/feed/
http://www.oca.com.ar:80/como_buscar_envio/2024.htm
http://www.oca.com.ar:80/como_buscar_envio/acuse.htm
http://www.oca.com.ar:80/como_buscar_envio/carta_documento.htm
http://www.oca.com.ar:80/como_buscar_envio/confronte.htm
http://www.oca.com.ar:80/como_buscar_envio/confronte_notarial.htm
http://www.oca.com.ar:80/como_buscar_envio/confronte_notarial_mediacion.htm
http://www.oca.com.ar:80/como_buscar_envio/home.htm
http://www.oca.com.ar:80/como_buscar_envio/images/pixel.gif
```

[🔍] Escaneo de puertos http

```
└─$ for port in $(seq 1 65535); do curl -s --connect-timeout 2 http://200.***.***.***:$port -o /dev/null && echo "200.***.***.*** - Puerto: [$port] activo" || echo "200.***.***.*** - Puerto: [$port] cerrado"; done
```

[🔍] Escaneo de puertos con Nmap

```
└─$ nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 200.***.***.*** -oG ports
```

🔴 [SUBDOMINIOS]

[🔍] urlScan

Link: <https://urlscan.io/>



urlscan.io



```
└─$ cat urlScan_result.txt | grep -A 50 '"sanList"' | awk '/"sanList"/ {flag=1} flag; /\n/,/\n/{flag=0}' | grep "$name" | sort | uniq | tr -d('",";') | tr -d(' ')
```

```
sftp.oca.com.ar
squalo.oca.com.ar
tc.oca.com.ar
test2.oca.com.ar
test.oca.com.ar
webservice.oca.com.ar
www1.oca.com.ar
www2.oca.com.ar
www3.oca.com.ar
www4.oca.com.ar
www5.oca.com.ar
www6.oca.com.ar
www7.oca.com.ar
www8.oca.com.ar
www9.oca.com.ar
www.autodiscover.oca.com.ar
www.epakoca.com.ar
www.oca.com.ar
wxw.oca.com.ar
x.oca.com.ar
```

[🔗] CRT

Link: <https://crt.sh/>

```
└─$ curl -sX GET "https://crt.sh?q=oca.com.ar" | grep '<TD>' | grep ".oca.com.ar" | tr -d '<TD>/' | sed 's/BR/ /g' | tr ' ' '\n' | sort | uniq
```

```
auth.oca.com.ar
autodiscover.oca.com.ar
correo.oca.com.ar
cross.oca.com.ar
developers.oca.com.ar
ecommerce.oca.com.ar
est.oca.com.ar
ext.oca.com.ar
int.oca.com.ar
marketing.oca.com.ar
mda.oca.com.ar
mesadeayuda.oca.com.ar
nas.oca.com.ar
oca.com.ar
ocaepak.oca.com.ar
prod.ext.oca.com.ar
producto.oca.com.ar
productos.oca.com.ar
qa-cross.oca.com.ar
rev.oca.com.ar
```

[🔍] Merklemap

Link: <https://merklemap.com/searchh?query=oca.com.ar&page=0>

www.mutuallaroca.com.ar	mutuallaroca.com.ar	3/23/2025
kip-moca.com.ar ielbb.com	kip-moca.com.ar ielbb.com	3/19/2025
barriolaboca.com.ar	barriolaboca.com.ar	3/18/2025
hoteldelrrioroca.com.ar	hoteldelrrioroca.com.ar	3/17/2025
*.hoteldelrrioroca.com.ar	hoteldelrrioroca.com.ar	3/17/2025
tiendaloca.com.ar	tiendaloca.com.ar	3/11/2025
*.tiendaloca.com.ar	tiendaloca.com.ar	3/11/2025
cross.oca.com.ar	cross.oca.com.ar	3/11/2025
*.maquinasroca.com.ar	maquinasroca.com.ar	3/10/2025
maquinasroca.com.ar	maquinasroca.com.ar	3/10/2025
*.cuoredipannaroca.com.ar	cuoredipannaroca.com.ar	3/6/2025
cuoredipannaroca.com.ar	cuoredipannaroca.com.ar	3/6/2025
moyanobrunoroca.com.ar	moyanobrunoroca.com.ar	3/6/2025
*.moyanobrunoroca.com.ar	moyanobrunoroca.com.ar	3/6/2025
www.moyanobrunoroca.com.ar	moyanobrunoroca.com.ar	3/6/2025
www.lanaderoca.com.ar	webdisk.lanaderoca.com.ar	3/5/2025
lanaderoca.com.ar	webdisk.lanaderoca.com.ar	3/5/2025

[🔍] Dnsdumpster

Link: <https://dnsdumpster.com/>

Host	IP	ASN	ASN Name	Open Services (from DB)
auth.oca.com.ar	119.8.73.73 ecs-119-8-73-73.compute.h wclouds-dns.com	ASN:136907 119.8.72.0/21	HWCLLOUDS-AS-AP HUANEI CLOUDS, HK Argentina	https: Microsoft-IIS/10.0 title: Outlook cn: oca.com.ar o: OCA LOG S.A. tech: Microsoft ASP.NET IIS:10.0 Windows Server Outlook Web App:15.1.2507
correo.oca.com.ar	200.41.237.250 correo.oca.com.ar	ASN:10834 200.41.224.0/20	Telefonica de Argentina, AR Argentina	
developers.oca.com.ar	200.10.108.133 133.host.advance.com.ar	ASN:10834 200.10.96.0/19	Telefonica de Argentina, AR Argentina	http: Microsoft-HTTPAPI/2.0 title: Not Found tech: Microsoft HTTPAPI:2.0 https: Microsoft-HTTPAPI/2.0 title: Not Found cn: oca.com.ar o: OCA LOG S.A. tech: Microsoft HTTPAPI:2.0 http8080: Apache/2.4.52 (Ubuntu) title: Index of / tech: Apache HTTP Server:2.4.52 Ubuntu

[🐞] Sslmate

Link: https://sslmate.com/ct_search_api/

Enter a domain to try it out:

oca.com.ar

o search sub-domains ☒ Show DNS names ☒ Show issuer ☒ Show revocation info ☒ Show problem reporting instructions ☒ Show certificate data

```
GET https://api.certspotter.com/v1/issuances?domain=oca.com.ar&expand=dns_names&expand=issuer&expand=revocation&expand=problem_reporting&expand=cert_der
```

```
{
  "id": "7421551393",
  "tbs_sha256": "158973ec216bd56b8b22cb175d46a0b0d12bda795507761f73b79626fc8514d2",
  "cert_sha256": "5ad900e6aff543dc584d98ef6a4eb4edffdb380a0840d137f34d764e62a7e259",
  "dns_names": ["auth.oca.com.ar", "autodiscover.oca.com.ar", "correo.oca.com.ar", "developers.oca.com.ar", "ext.oca.com.ar", "i
  "pubkey_sha256": "d14c23b20b665ba9b9076a23d888778cfb9d032d456a4f67f598b100384d3495",
  "issuer": {"friendly_name": "Sectigo", "pubkey_sha256": "4648564dc7c901037f631391d765643e8f8f86622849f59dfc9564838e1e8a76",
  "not_before": "2024-05-31T00:00:00Z",
  "not_after": "2025-07-01T23:59:59Z",
  "revoked": false,
  "revocation": {"time": null, "reason": null, "checked_at": "2025-03-26T15:00:01Z"},
  "problem_reporting": "To revoke one or more certificates issued by Sectigo for which you (i) are the Subscriber or (ii) c
  "cert_der": "MIIIImzCCB40gAwIBAgIRAKPWcKt0KEEH27zXHN2ZykwDQYJKoZIhvcNAQELBQAwgZUXCzAJBgNVBAYTAkdCMRswGQYDVQQIEXJHcmVhdGVy
}
```

```
"dns_names": ["auth.oca.com.ar", "autodiscover.oca.com.ar", "correo.oca.com.ar", "developer
s.oca.com.ar", "ext.oca.com.ar", "int.oca.com.ar", "nas.oca.com.ar", "oca.com.ar", "ocageo.c
om.ar", "rev.oca.com.ar", "sftp.oca.com.ar", "squalo.oca.com.ar", "test2.oca.com.ar", "test.
oca.com.ar", "webservice.oca.com.ar", "www1.oca.com.ar", "www2.oca.com.ar", "www3.oca.com.a
r", "www4.oca.com.ar", "www5.oca.com.ar", "www6.oca.com.ar", "www7.oca.com.ar", "www8.oca.co
m.ar", "www9.oca.com.ar", "www.oca.com.ar", "www.ocageo.com.ar"],
```

[🐞] Osint.sh

Link: <https://osint.sh/subdomains/>

OSINT.SH

HOME ALL TOOLS - ABOUT API TERMS CONTACT SPONSOR

SUBDOMAIN FINDER

The fastest way to discover subdomains in your DNS recon

example.com



CHECK NOW

[🔍] Dorks



Link: <https://google.com>

site:*oca.com.ar site:oca.com.ar -www site:*.oca.com.*



All Shopping Videos Images Short videos News Forums More

 OCA Developers
<https://developers.oca.com.ar> · [Translate this page](#) · 



OCA Developers
Optimizamos las gestiones de tus envíos · Seguimiento de envíos en cada etapa. · Buscador de puntos y sucursales. · Buscador de códigos postales online.

 OCA
<http://webservice.oca.com.ar> · ePak... · [Translate this page](#) · 



Oep_Tracking Web Service
Devuelve Listado de codigos postales asignados para cada agencia.
GetDatosDeEtiquetasPorOrdenOrNumeroEnvio. Obtiene el código fuente de las etiquetas ...

 OCA
<http://webservice.oca.com.ar> · oep_... · [Translate this page](#) · 

Oep_Tracking Web Service
Devuelve todos los servicios por cada Centros de Imposición existentes por provincia.
IngresoOR. Ingreso de archivo de OR. List_Envios. Dado el CUIT del cliente ...

 OCA
<http://webservice.oca.com.ar> · oep_... · [Translate this page](#) · 

Oep_Tracking Web Service
Obtiene el código fuente de las etiquetas pertenecientes a la orden de retiro con operativa especial con formato para Etiquetadoras. (idOrdenRetiro es requerido ...

 OCA
<https://test.oca.com.ar> · [Translate this page](#) · 

Untitled
OCA - TEST.OCA.COM.AR.

● [EMAILS]

[🔍] Phonebook.cz

Phonebook.cz

Phonebook lists all domains, email addresses, or URLs for the given input domain. Wildcards such as *.gov.uk are allowed. You are searching 34 billion records.

netflix.com


Try: [cia.gov](#), [cnn.com](#), [netflix.com](#), [*.ru](#), [*.gov.uk](#), [solarwinds.com](#)

- ☐ Domains
☒ Email Addresses
☐ URLs

[roelofvanzwol@netflix.com](#)
[hsteck@netflix.com](#)
[xamatrain@netflix.com](#)
[chaos@netflix.com](#)
[rbachwani@netflix.com](#)
[jbennett@netflix.com](#)
[anorkin@netflix.com](#)
[zli@netflix.com](#)
[jbasilico@netflix.com](#)
[yramond@netflix.com](#)
[alex1@netflix.com](#)
[flixfac@netflix.com](#)
[bennett@netflix.com](#)
[barrys@netflix.com](#)
[phishing@netflix.com](#)
[xrs@netflix.com](#)
[discship@netflix.com](#)
[paypal@netflix.com](#)
[hari@netflix.com](#)


[🔍] Dorks

"email" "contacto" "@oca.com.ar" Feedback

 OCA
<https://www6.oca.com.ar> > Contacto [Translate this page](#)


contactanos

Regístrate · REGISTRATE · **CONTACTO**. CONTACTANOS. Nombre. Apellido. Provincia. Teléfono.
Email. Mensaje. Atención al cliente: 0800-999-7700 de lunes a viernes de ...

 OCA - Las buenas noticias llegan
<https://www3.oca.com.ar> > contactese [Translate this page](#)


Contáctese

... **contacto** con usted. Nombre y Apellido, *. **Email**, *. Teléfono, *. Producto. Seleccione ...
Email: ocawebconsulta@oca.com.ar. Casa Central OCA La Rioja 301 (1214) ...

 x.com
<https://x.com> > ocacorreook [Translate this page](#)


Correo OCA (@OCACorreoOK) / X

Para acceder al descuento tenés que enviarnos un **email** a oferton@oca.com.ar, incluyendo tu nombre completo, D.N.I. y teléfono de **contacto**. Además te ...

 enal.com.ar
<https://enal.com.ar> > Otros [Translate this page](#)

Cómo puedo enviar un correo a OCA en Río Grande - Enal

Feb 6, 2025 — ✓ Contactá a OCA Río Grande por **email** a: rio.grande@oca.com.ar. ... **contacto** donde publican su información de **contacto**, incluyendo direcciones de ...

 Protectomet
<https://protectomet.com.ar> > como... [Translate this page](#)

Cómo enviar un correo a OCA en Comodoro Rivadavia

Nov 22, 2024 — ... **contacto** disponibles: Tipo de **contacto**, Información, Teléfono, 0800-555-1234.
Email, **contacto**@oca.com.ar. Horario de atención, Lunes a Viernes, ...

[🦋] Script

Mi script de python: <https://github.com/FeathersMcgr4w/emails-from-domain>

OSINT Search emails from company domains

Python script to search for emails from a specific company domain and subdomians.

--> **Use:** python3 find-emails-employees.py example-domain.com

--> **Example:** python3 find-emails-employees.py telefonica.com

```
$ cat emails_employees.txt
last@coto.com.ar
vmartino@coto.com.ar
JSmith@coto.com.ar
John.Smith@coto.com.ar
John_Smith@coto.com.ar
Info@coto.com.ar
info@coto.com.ar
info@coto.com.ar
atracciondetalentos@coto.com.ar
atracciondetalentos@coto.com.ar
```



"software developer" "Soporte IT" "Recursos Humanos" "oca.com.ar" "linkedin"

(without quotes):



LinkedIn · Sara M.

240+ followers



Sara M. - Full Stack Developer - OCA GLOBAL

Sabadell, Cataluña, España · Full Stack Developer · OCA GLOBAL

Software Engineer · Experiencia: OCA GLOBAL · Educación: Universitat Politècnica de Catalunya (UPC) · Ubicación: Sabadell · 248 contactos en LinkedIn.



LinkedIn · OCA

190.4K+ followers



OCA

Somos **OCA**, una empresa de servicio logístico en Argentina. Desde hace más de 60 años llegamos a cada rincón del país. Contamos con más de 150 sucursales, ...

Missing: ~~developer~~ | Show results with: [developer](#)



LinkedIn · Carla Crespo

540+ followers



Carla Crespo - OCA

Buenos Aires, Provincia de Buenos Aires, Argentina · OCA

Soy una Tester con experiencia en Análisis de documentos funcionales, casos de uso... · Experiencia:

OCA · Educación: Talento Tech · Ubicación: Buenos Aires ...



LinkedIn · Juan Pablo Bortolini

830+ followers



Juan Pablo Bortolini - Senior Software Developer

San Jorge, Santa Fe, Argentina · Senior Software Developer · Allied Group

Senior **Software Developer** in Allied Group · +15 años en la industria del desarrollo de software. +9 años trabajando con equipos distribuidos para clientes ...



LinkedIn Colombia

<https://co.linkedin.com/company/ocatpa>



OCA

[🐞] Script

Mi script de python: <https://github.com/FeathersMcgr4w/find-linkedin-employees>

OSINT Find LinkedIn Employees

Python script to search for employees on LinkedIn for a company using a domain.

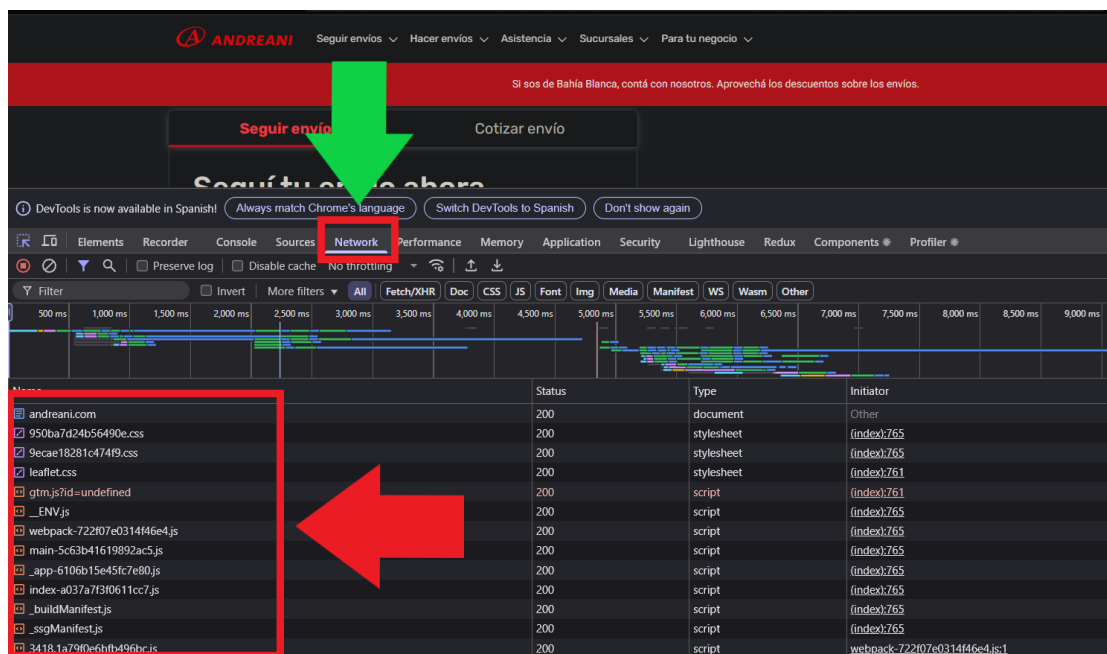
--> Use: `python3 find-linkedin-employees.py example-domain.com`

--> Example: `python3 find-linkedin-employees.py telefonica.com`

```
└─$ cat linkedin_employees.txt
software developer: Ariel Rodriguez | Perfil profesional - LinkedIn - https://ar.linkedin.com/in/ariel-rodriguez-5a1ba34a
Recursos Humanos: COTO | LinkedIn - https://in.linkedin.com/company/coto-cicsa
Recursos Humanos: Agostina Biggeri en LinkedIn: Buenos días! mi nombre es Agostina y ... - https://es.linkedin.com/posts/agostina-biggeri-73b3ba1b2_buenos-d%C3%ADas-mi-nombre-es-agostina-y-estoy-activity-7157688993772449794-7XcF
Recursos Humanos: valentina bevilacqua on LinkedIn: Curriculum Grupo Arcor COTO ... - https://www.linkedin.com/posts/valentina-bevilacqua-45974928a_curriculum-grupo-arcor-coto-open-engish-activity-7184004847812177921-yvfe
Recursos Humanos: Brenda Moya en LinkedIn: #trabajo - https://es.linkedin.com/posts/brenda-moya-2888a1235_trabajo-activity-6946167187048947712-wc3U
Recursos Humanos: Anabela Cassia en LinkedIn: Job Search | Indeed | 13 comentarios - https://hn.linkedin.com/posts/anabela-cassia-061b7819a_job-search-indeed-activity-6832118611927158784-0yAE?trk=public_profile_like_view
Recursos Humanos: COTO LANZÓ UNA CAMPAÑA POR SU 48 ANIVERSARIO - https://es.linkedin.com/pulse/coto-lanz%C3%B3-una-campa%C3%B1a-por-su-48-aniversario-christian-selva
```

● [Scraping web]

[🐞] Network browser tool (proxy)



The screenshot shows a web browser with the DevTools network tab open. A green arrow points to the 'Network' tab. A red arrow points to the list of network requests. The list shows various resources loaded from andreani.com, including CSS files, JavaScript files, and a manifest file.

Name	Status	Type	Initiator
andreani.com	200	document	Other
950ba7d24b56490e.css	200	stylesheet	(index):765
9ecae18281c474f9.css	200	stylesheet	(index):765
leaflet.css	200	stylesheet	(index):761
gtm.js?id=undefined	200	script	(index):761
_ENV.js	200	script	(index):765
webpack-722f07a0314f46e4.js	200	script	(index):765
main-5c63b41619892ac5.js	200	script	(index):765
_app-6106b15e45fc7e80.js	200	script	(index):765
index-a037a7f3f0611cc7.js	200	script	(index):765
_buildManifest.js	200	script	(index):765
_ssgManifest.js	200	script	(index):765
34181a790e6b1d496bc.js	200	script	webpack-722f07a0314f46e4.js:1

Analizar archivos del tráfico http:

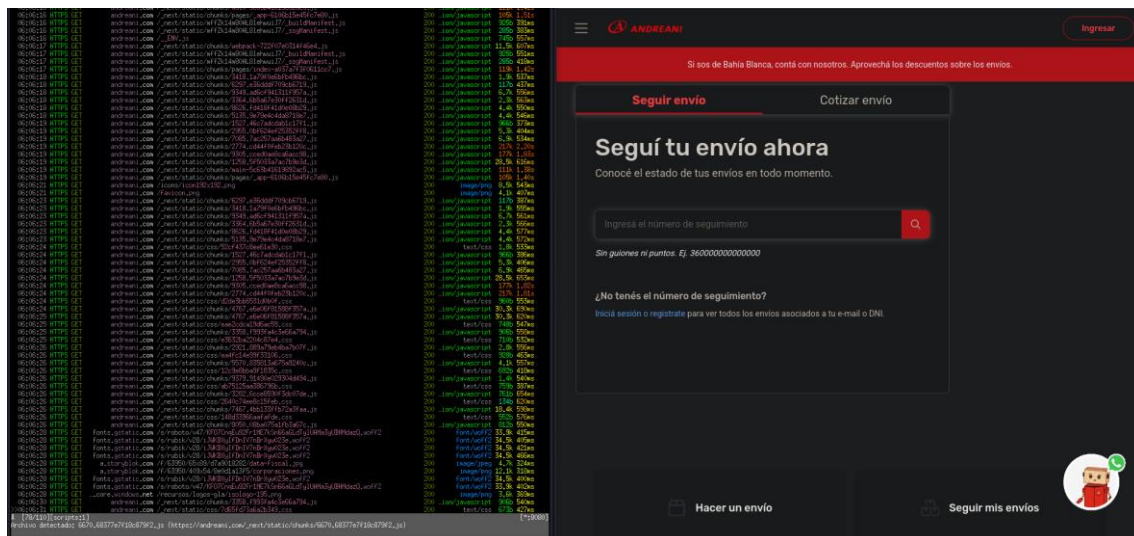
```
< > C andreani.com/_ENV.js

globalThis._ENV = Object.assign({}, globalThis._ENV,
{"NEXT_PUBLIC_ACTIVE_APM":"true","NEXT_PUBLIC_ONBOARDING_HOST":"https://onboarding.andreani.com",
"NEXT_PUBLIC_MFE_SEGUIMIENTO":"seguimiento@https://traza-
microfrontend.andreani.com/next/static/chunks/remoteEntry.js","NEXT_PUBLIC_STORYBLOK_TOKEN":"gi
1ARVAUWeZrLL1MxIPziQtt","NEXT_PUBLIC_URL_NORLOG":"http://www.norlog.com.ar/","NEXT_PUBLIC_ONBOAR
DING_URL":"https://onboarding.andreani.com","NEXT_PUBLIC_URL_API_PWA":"https://apidestinatarios.
andreani.com","NEXT_PUBLIC_API_PYMES_URL":"https://pymes-
api.andreani.com/api/v1/","NEXT_PUBLIC_LOGIN_CORPORATIVO":"https://login.andreani.com/login?
client_id=13_1mxjhhrz6zb4w8s88ssc0o80048csc4c8w8kwc544scos8o48s&redirect_uri=http://andreanionli
ne.com/oauth-check","NEXT_PUBLIC_GOOGLETAGMANAGER_ID":"GTM-
KBWJPZJC","NEXT_PUBLIC_ENV_APM":"Production","NEXT_PUBLIC_URL_COTIZADOR":"https://pymes.andreani
.com/cotizador","NEXT_PUBLIC_CHAT_BOT_URL":"https://bit.ly/3UaHDee","NEXT_PUBLIC_API_SUGGEST_HER
E_KEY":"8PeZn45qSTYQkmRcm9nydzWJkfgZpfk_ZrLndIHoxYe","NEXT_PUBLIC_GA_MEASUREMENT_ID":"GTM-
KBWJPZJC","REACT_ENV_PREFIX":"NEXT_PUBLIC"});
```

De esta forma podemos encontrar dominios, subdominios, tokens, claves, usuarios, contraseñas, servicios, comentarios, urls, puertos, endpoints, apis.

 **Mitmproxy** (proxy)

Use: mitmproxy -p 8080



Analizar los archivos del tráfico web por medio de la herramienta de consola mitmproxy. Luego analizar y seleccionar manualmente los archivos web que nos interesen para posteriormente inspeccionarlos más detenidamente en busca de credenciales o rutas.

[🦋] OsintTool

Mi herramienta de osint para Linux (próximamente en mi github) automatiza la tarea de capturar el tráfico http mediante “mitmproxy” y un script en Python que guarda el tráfico y posteriormente identifica archivos sensibles.

```
└─$ ./osintTool.sh -h
*****
*                                     *
*                                     *
*  O S I N T T O O L  : ( ) : ( )  *
*                                     *
*                                     *
*  osintTool.sh v1.0                *
*  Author: feathersMcgraw           *
*  Automated Osint Pentesting Web   *
*                                     *
*****

Optional argument:
    [-h]    show this help menu

Main parameters:
    [-m]    Mode [ whois ] - [ extractUrls ] - [ subdomains ] - [ emails ] - [ linkedin ] - [ httpTraffic ]
```

```
└─$ ./osintTool.sh -m httpTraffic -d andreani.com
```

```
[*] ::: SNIFFING DATA FROM HTTP TRAFFIC ::: ...
[+] Opening Mitmproxy - please wait ...

::: _____ :::
::: INSTRUCTIONS :::
::: _____ :::

[1] Open your browser and upload the mitmproxy-ca-cert.pem in settings → certificates
[2] Configure foxyproxy in port 8080
[3] Search your domain in the nav bar Example: https://www.domain.com
[4] The mitmproxy is going to sniff the traffic
[5] When finished, close the xterm shell, to continue the program!
```


Captura de trafico http:

URL: https://staticcdn.duckduckgo.com/trackerblocking/v6/current/extension-tds.js

URL: https://andreani.com/_next/static/css/950ba7d24b56490e.css

URL: https://unpkg.com/leaflet@1.9.4/dist/leaflet.css

URL: https://andreani.com/__ENV.js

URL: https://andreani.com/_next/static/css/9ecae18281c474f9.css

URL: https://andreani.com/_next/static/chunks/webpack-722f07e0314f46e4.js

URL: https://andreani.com/_next/static/mffZk14m80AL8lehwuiJ7/_buildManifest.js

URL: https://andreani.com/_next/static/mffZk14m80AL8lehwuiJ7/_ssgManifest.js

URL: https://andreani.com/_next/static/chunks/pages/index-a037a7f3f0611cc7.js

URL: https://andreani.com/_next/static/chunks/main-5c63b41619892ac5.js

URL: https://andreani.com/_next/static/chunks/pages/_app-6106b15e45fc7e80.js

URL: https://andreani.com/_next/static/chunks/6297.e36dddf709cb6719.js

URL: https://andreani.com/_next/static/chunks/9349.ad6cf941311f957a.js

URL: https://andreani.com/_next/static/chunks/3364.6b5a67e30ff2631d.js

URL: https://andreani.com/_next/static/chunks/3418.1a79f0e6bfb496bc.js

URL: https://andreani.com/_next/static/chunks/5135.9e79e4c4da8718e7.js

URL: https://andreani.com/_next/static/chunks/8626.fd418f41d0e08b29.js

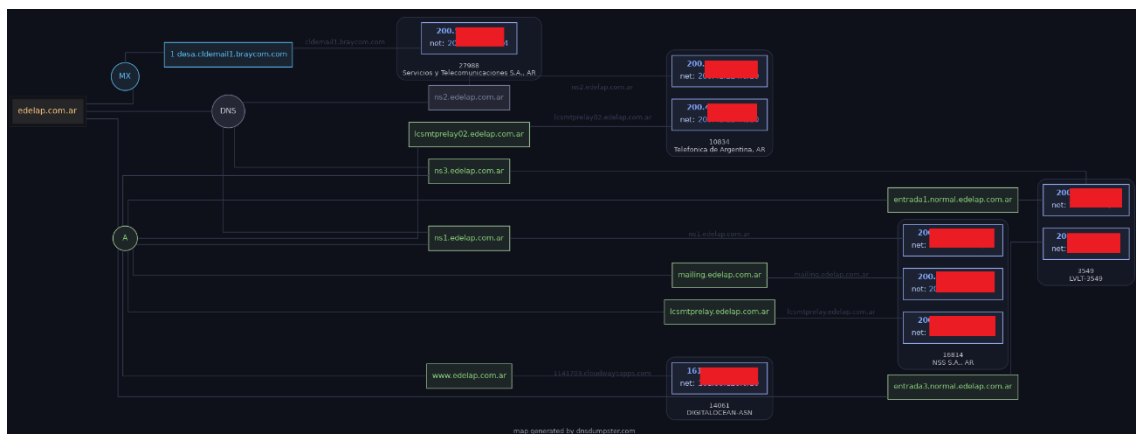
Obtención automatizada de archivos sensibles:

```
URL: https://andreani.com/__ENV.js

globalThis.__ENV = Object.assign({}, globalThis.__ENV, {"NEXT_PUBLIC_ACTIVE_APM":"true","NEXT_PUBLIC_ONBOARDING_HOST":"https://onboarding.andreani.com","NEXT_PUBLIC_MFE_SEGUIMIENTO":"seguimiento@https://traza-microfrontend.andreani.com/_next/static/chunks/remoteEntry.js","NEXT_PUBLIC_STORYBLOK_TOKEN":"gi1ARVAUWeZrLL1MxIPziQt","NEXT_PUBLIC_URL_NORLOG":"http://www.norlog.com.ar/","NEXT_PUBLIC_ONBOARDING_URL":"https://onboarding.andreani.com","NEXT_PUBLIC_URL_API_PWA":"https://apidestinatarios.andreani.com","NEXT_PUBLIC_API_PYMES_URL":"https://pymes-api.andreani.com/api/v1/","NEXT_PUBLIC_LOGIN_CORPORATIVO":"https://login.andreani.com/login?client_id=13_1mxjhhr6zb4w8s88ssc0o80048csc4c8w8kwc44scos8o48s&redirect_uri=http://andreanionline.com/oauth-check","NEXT_PUBLIC_GOOGLETAGMANAGER_ID":"GTM-KBWJPZJC","NEXT_PUBLIC_ENV_APM":"Production","NEXT_PUBLIC_URL_COTIZADOR":"https://pymes.andreani.com/cotizador","NEXT_PUBLIC_API_SUGGEST_HERE_KEY":"8PezN45qSTYQkmRcm9nydzWJkfgZpfk ZrLnd1HoXyE","NEXT_PUBLIC_CHAT_BOT_URL":"https://bit.ly/3UaHDee","NEXT_PUBLIC_GA_MEASUREMENT_ID":"GTM-KBWJPZJC","REACT_ENV_PREFIX":"NEXT_PUBLIC"});
```

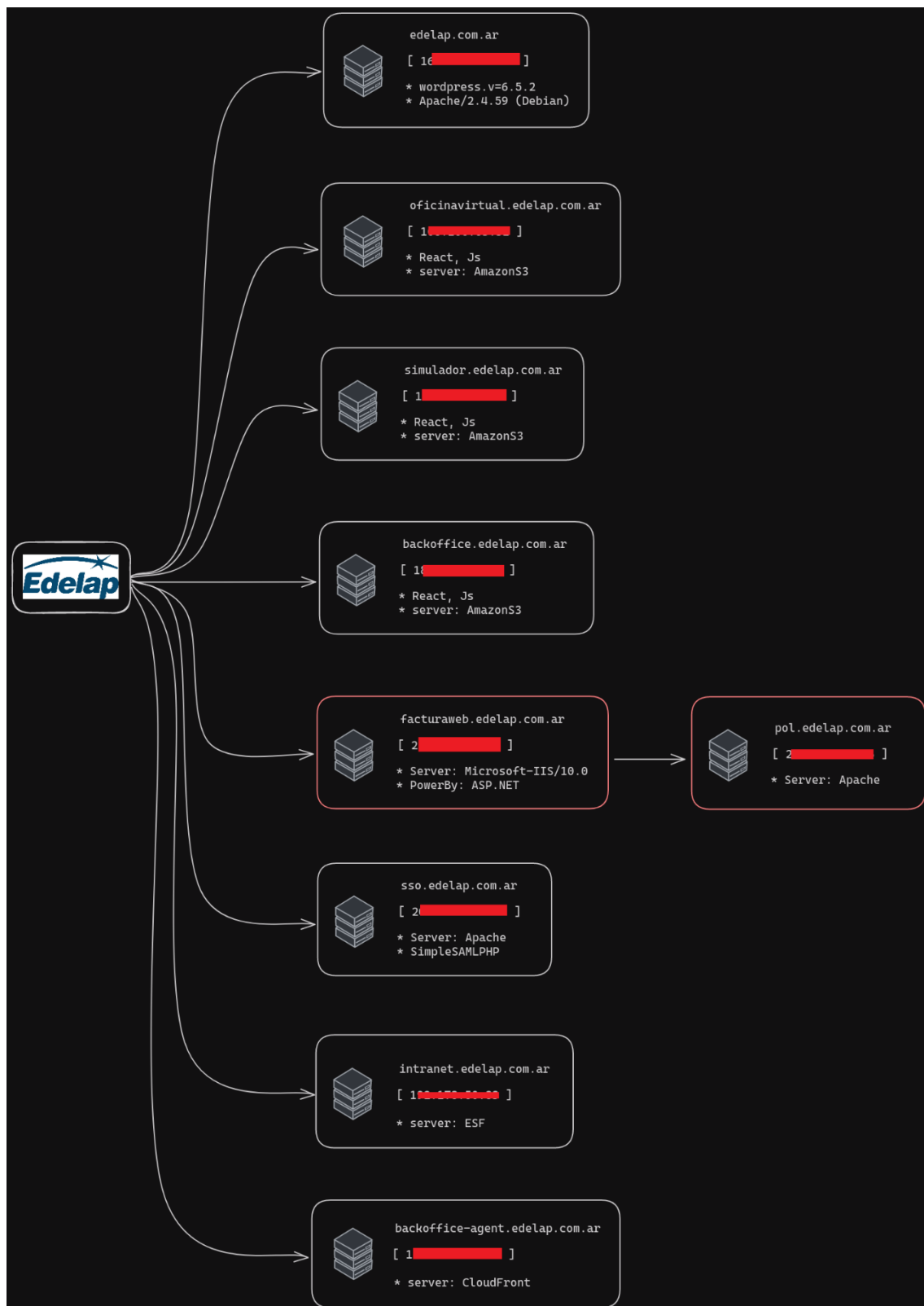
MAPA DE INTELIGENCIA

[🕒] Mapa dnsdumpster



El siguiente mapa de relaciones de los diferentes servicios dns y servidores web, lo podemos obtener de manera automatizada mediante la herramienta online dnsdumpster.com.

[🗺️] Mapa Excalidraw



Mediante la herramienta online “excalidraw” podemos crear nuestros propios mapas de inteligencia utilizando elementos gráficos para luego exportarlos en otro formato.

[🚦] Conclusión

Hemos llegado al final de este documento. A lo largo de este contenido, he explicado qué es OSINT y cómo se integra en ejercicios de red team dentro del hacking ético. También he mostrado una parte de mi metodología y las herramientas que empleo para realizar OSINT durante la fase de reconocimiento en un ejercicio de pentesting web. Una vez recopilados los datos en las etapas anteriores, es fundamental analizarlos y procesarlos para obtener información útil, la cual se entregará al equipo de pentesters para iniciar la fase de penetración en las aplicaciones web y buscar posibles vulnerabilidades explotables.

[👤] Contacto

[🔗] <https://www.linkedin.com/in/david-padron-9a74aa323/>

[🔗] <https://github.com/FeathersMcgr4w>

[🔗] <https://feathersmcgr4w.github.io/cyber-portfolio/>