

Reto 1

Ciberseguridad básica

Randy Villanueva Guzman
THINCRS

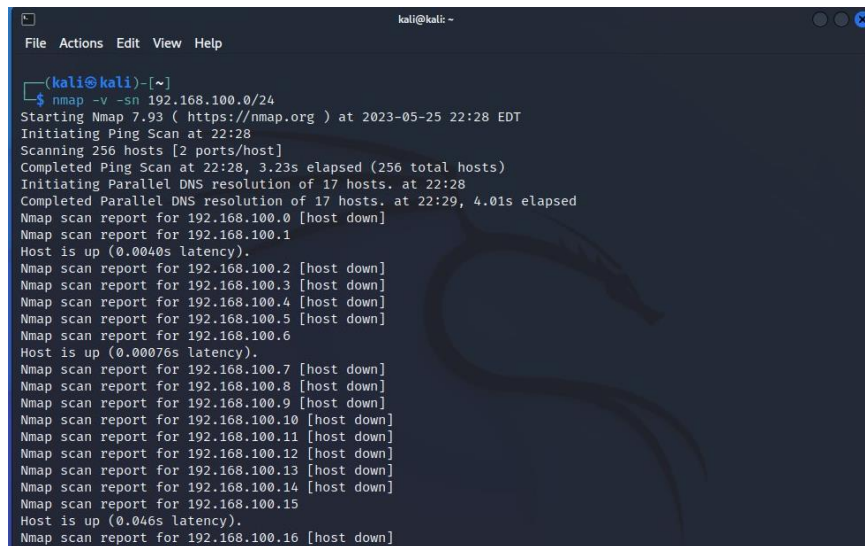
Contents

Detección de dirección IP de equipos.....	2
Recopilar Información de sitios web	4
Maltego – CaseFile	4
OWASP	5
Identificar el tipo de sitio web	8

Detección de dirección IP de equipos

Para la detección de direcciones IP usamos la herramienta de la línea de comandos en Linux (en este caso usando Kali) NMAP la cual nos permite realizar un análisis y monitoreo de la red a la cual estamos conectados. Con esto podemos identificar que hosts están activos, para así, hacer un análisis a cada uno lo que nos ayudara a identificar diferentes datos como: sistema operativo, puertos y servicios abiertos.

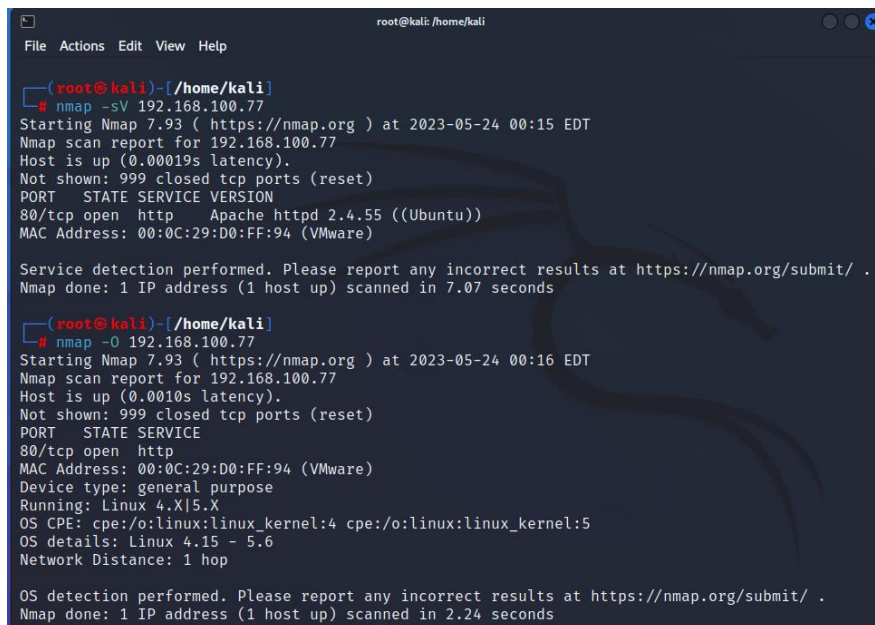
1. Escáner la red para ver la lista de host activos en nuestra red



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ nmap -v -sn 192.168.100.0/24  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 22:28 EDT  
Initiating Ping Scan at 22:28  
Scanning 256 hosts [2 ports/host]  
Completed Ping Scan at 22:28, 3.23s elapsed (256 total hosts)  
Initiating Parallel DNS resolution of 17 hosts. at 22:28  
Completed Parallel DNS resolution of 17 hosts. at 22:29, 4.01s elapsed  
Nmap scan report for 192.168.100.0 [host down]  
Nmap scan report for 192.168.100.1  
Host is up (0.0040s latency).  
Nmap scan report for 192.168.100.2 [host down]  
Nmap scan report for 192.168.100.3 [host down]  
Nmap scan report for 192.168.100.4 [host down]  
Nmap scan report for 192.168.100.5 [host down]  
Nmap scan report for 192.168.100.6  
Host is up (0.00076s latency).  
Nmap scan report for 192.168.100.7 [host down]  
Nmap scan report for 192.168.100.8 [host down]  
Nmap scan report for 192.168.100.9 [host down]  
Nmap scan report for 192.168.100.10 [host down]  
Nmap scan report for 192.168.100.11 [host down]  
Nmap scan report for 192.168.100.12 [host down]  
Nmap scan report for 192.168.100.13 [host down]  
Nmap scan report for 192.168.100.14 [host down]  
Nmap scan report for 192.168.100.15  
Host is up (0.046s latency).  
Nmap scan report for 192.168.100.16 [host down]
```

Figura 1. Escaneo a la red para identificar hosts activos

2. Una vez identificados podemos de nuevo usar la herramienta NMAP con diferentes opciones, para escanear un host en específico como se muestra en la imagen 2,3 y 4.



```
root@kali: /home/kali  
File Actions Edit View Help  
  
(root@kali)~/home/kali  
# nmap -sV 192.168.100.77  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 00:15 EDT  
Nmap scan report for 192.168.100.77  
Host is up (0.00019s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
80/tcp open  http   Apache httpd 2.4.55 ((Ubuntu))  
MAC Address: 00:0C:29:D0:FF:94 (VMware)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds  
  
(root@kali)~/home/kali  
# nmap -O 192.168.100.77  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 00:16 EDT  
Nmap scan report for 192.168.100.77  
Host is up (0.0010s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp open  http  
MAC Address: 00:0C:29:D0:FF:94 (VMware)  
Device type: general purpose  
Running: Linux 4.X|5.X  
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5  
OS details: Linux 4.15 - 5.6  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
```

Figura 2. Escaneo a host 192.168.100.77 con SO Ubuntu

```
root@kali: /home/kali
File Actions Edit View Help
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 00:19 EDT
Nmap scan report for 192.168.100.111
Host is up (0.0023s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind 2-4 (RPC #100000)
3306/tcp  open  mysql   MySQL 5.5.47-0+deb8u1
MAC Address: 00:0C:29:2D:B6:70 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.18 seconds

(root@kali)-[/home/kali]
# nmap -O 192.168.100.111
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 00:19 EDT
Nmap scan report for 192.168.100.111
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
3306/tcp  open  mysql
MAC Address: 00:0C:29:2D:B6:70 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds

(root@kali)-[/home/kali]
#
```

Figura 4. Escaneo a host 192.168.100.11 con SO Debian

```
root@kali: /home/kali
File Actions Edit View Help
# nmap -sV 192.168.100.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 00:33 EDT
Nmap scan report for 192.168.100.112
Host is up (0.00087s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:0C:29:43:67:36 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds

(root@kali)-[/home/kali]
# nmap -O 192.168.100.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 00:33 EDT
Nmap scan report for 192.168.100.112
Host is up (0.00097s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:43:67:36 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): AVtech embedded (87%)
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds

(root@kali)-[/home/kali]
#
```

Figura 5. Escaneo a host 192.168.100.113 con SO Windows

Recopilar Información de sitios web

Para el análisis y recuperación de información de sitios web podemos hacer el uso de las siguientes herramientas: Maltego - CaseFile y Owasp.

Maltego – CaseFile

Maltego es una biblioteca enfocada para la seguridad informática y pentesting la cual tiene como objetivo proporcionar un conjunto de transformaciones para el descubrimiento de datos que después se pueden observar en formato grafico para un mejor análisis.

En este caso en particular usamos la sub-herramienta CaseFile la cual nos permite analizar sitios web que nos puede ayudar a determinar las relaciones entre un link y los sitios físicos a los que pertenece, así como la generación de reportes.

1. Reporte generado del sitio web de la Escuela Superior de Computo

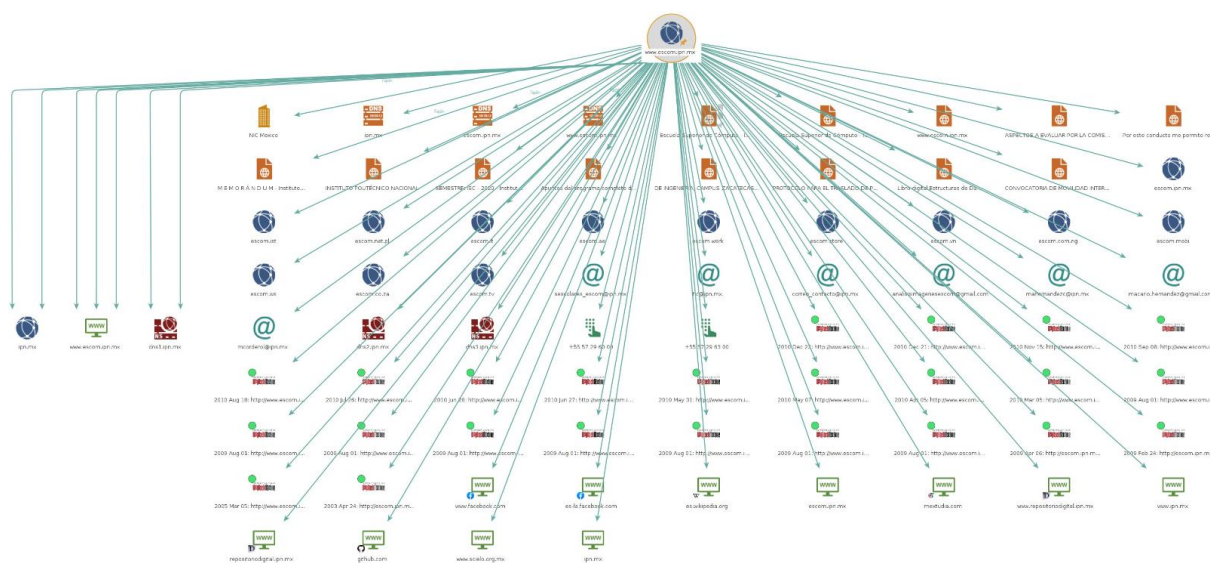


Figura 6. Mapa grafico que establece las relaciones entre los diferentes servicios del sitio

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	Website	www.escom.ipn.mx	3
2	Domain	ipn.mx	2
3	NS Record	dns1.ipn.mx	2
4	Domain	escom.ist	1
5	Domain	escom.net.pl	1
6	Domain	escom.it	1
7	Domain	escom.com.ng	1
8	Domain	escom.mobi	1
9	Domain	escom.ws	1
10	Domain	escom.co.za	1

Figura 7. Top 10 Entidades ordenadas por links externos hacia el dominio

Ranked by Outgoing Links			
Rank	Type	Value	Outgoing links
1	Domain	www.escom.ipn.mx	83
2	Website	www.escom.ipn.mx	0
3	Domain	ipn.mx	0
4	NS Record	dns1.ipn.mx	0
5	Domain	escom.ist	0
6	Domain	escom.net.pl	0
7	Domain	escom.it	0
8	Domain	escom.com.ng	0
9	Domain	escom.mobi	0
10	Domain	escom.ws	0

Figura 8. Top 10 Entidades ordenadas por links internos hacia otros dominios

Ranked by Total Links			
Rank	Type	Value	Total links
1	Domain	www.escom.ipn.mx	83
2	Website	www.escom.ipn.mx	3
3	Domain	ipn.mx	2
4	NS Record	dns1.ipn.mx	2
5	Domain	escom.ist	1
6	Domain	escom.net.pl	1
7	Domain	escom.it	1
8	Domain	escom.com.ng	1
9	Domain	escom.mobi	1
10	Domain	escom.ws	1

Figura 9. Top 10 de links en el sitio web

OWASP

Es una herramienta que te permite analizar un sitio web con la finalidad de exponer los problemas de seguridad que este pueda tener, centrándose en los 10 riesgos más importantes:

- Inyección
- Autenticación Rota
- Exposición de datos confidenciales
- Entidades XML externas XXE
- Pérdida de control de acceso
- Mala configuración de seguridad
- Scripting entre sitios
- Deserialización no segura
- Uso de componentes con vulnerabilidades conocidas
- Registro y supervisión insuficientes

1. Análisis de vulnerabilidades del sitio web de la Escuela Superior de Computo

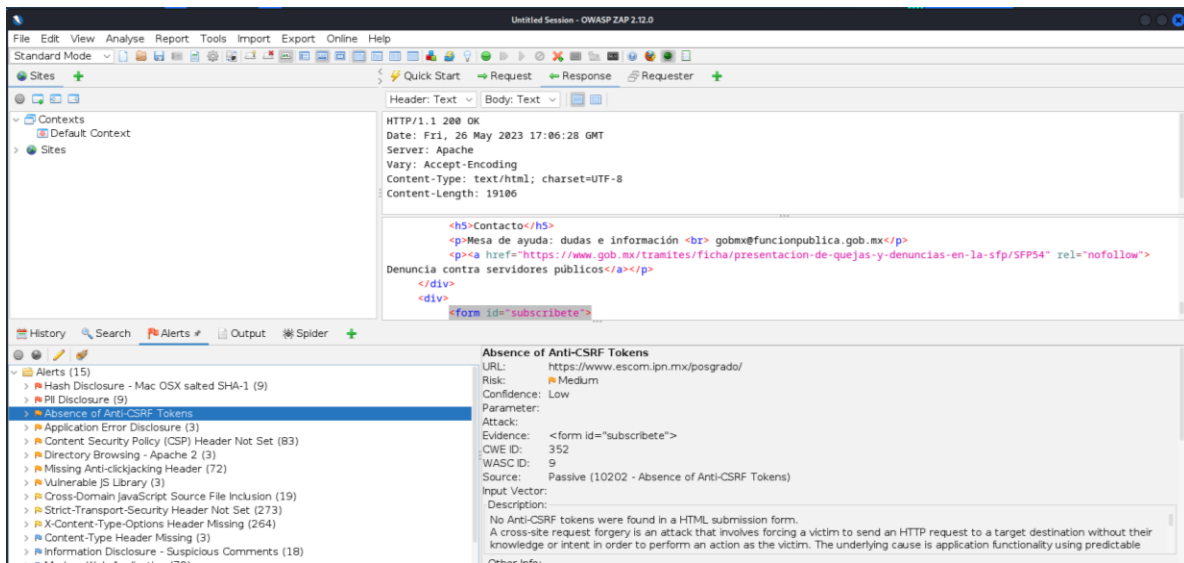


Figura 10. Vulnerabilidad Ausencia de Anti-CSRF tokens

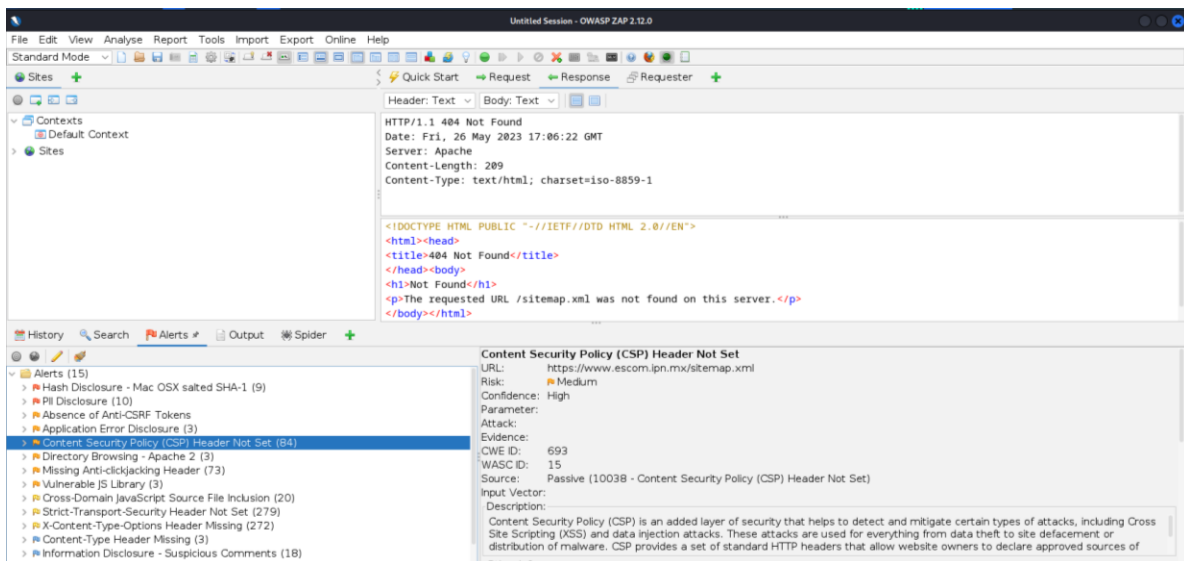


Figura 11. Vulnerabilidad Content Security Policy (CSP) Header Not Set

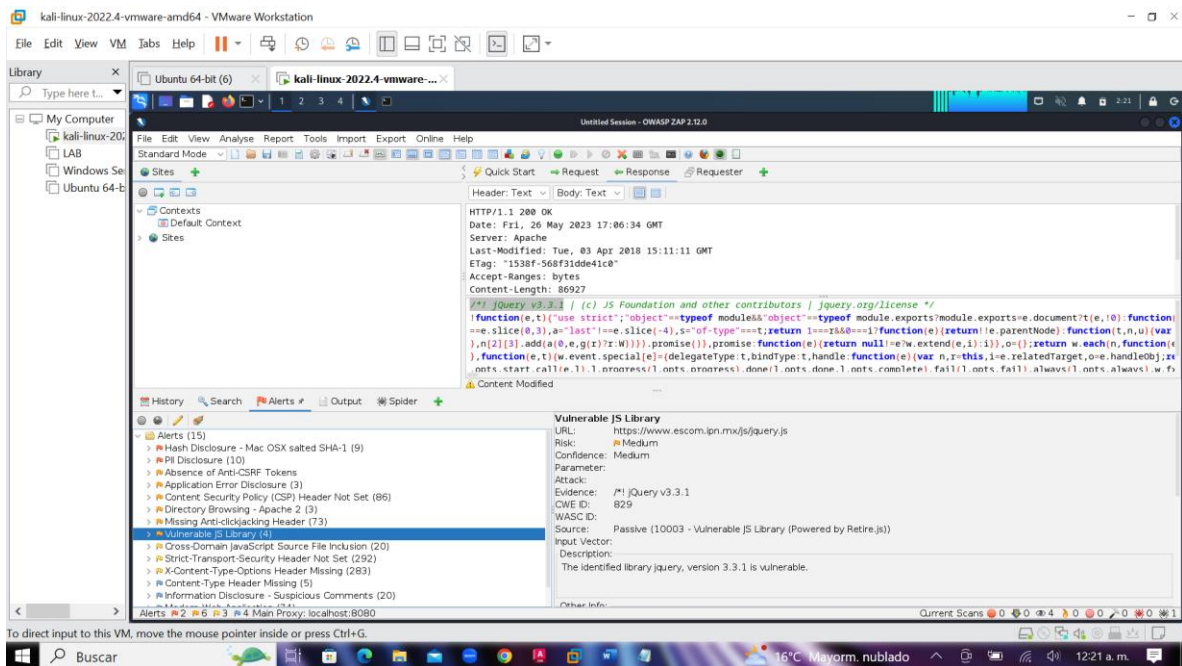


Figura 12. Vulnerabilidad en Biblioteca de JS utilizada

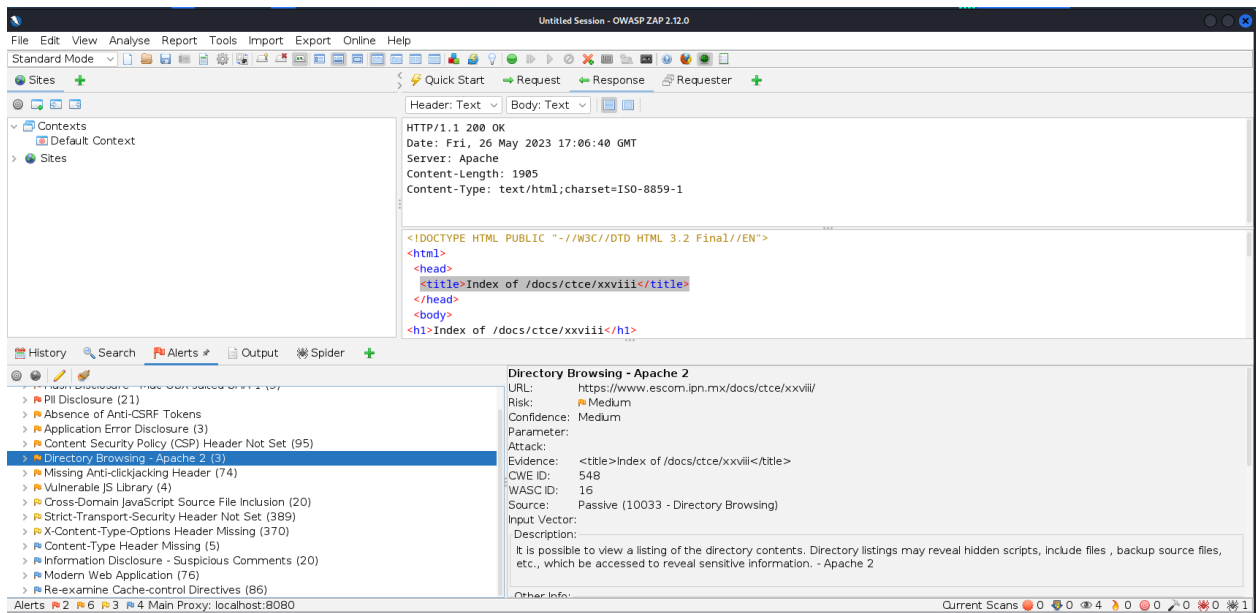


Figura 13. Vulnerabilidad Directory Browsing en Apache 2

Identificar el tipo de sitio web

La identificación de un sitio web se puede realizar con la herramienta builtwith la cual nos ayuda al análisis del sitio proporcionándonos las tecnologías con las cual está construido como: widgets, lenguajes, servicios y estándares. A diferencia de las anteriores es la más fácil e intuitiva ya que no necesitamos instalar nada porque se encuentra disponible como aplicación web.

1. Identificando tipo de sitio de la Escuela Superior de Computo

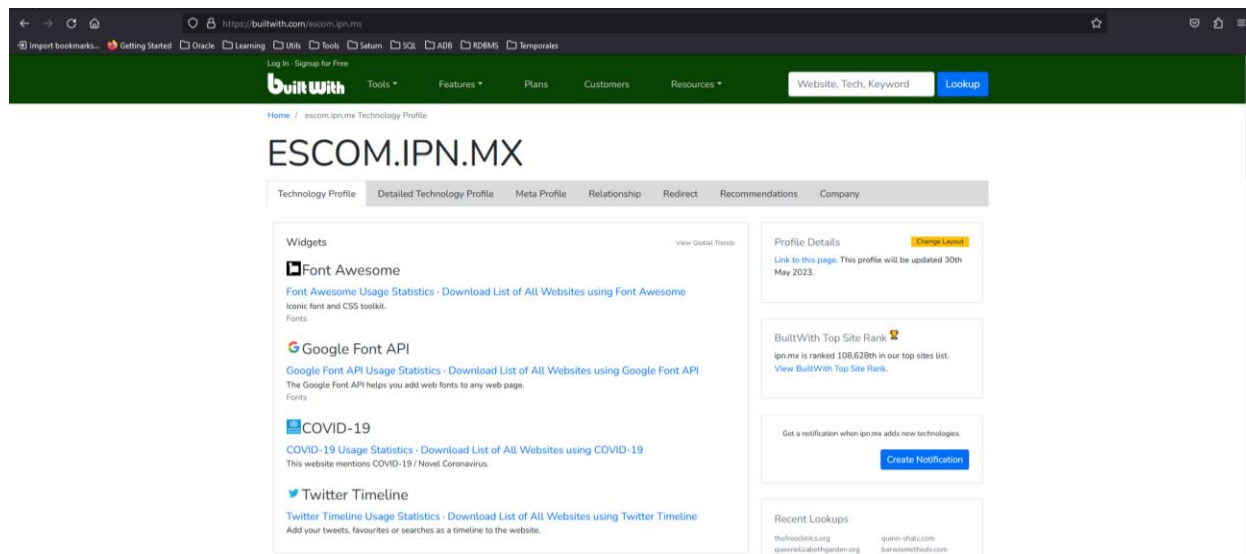


Figura 14. Widgets utilizados en el sitio

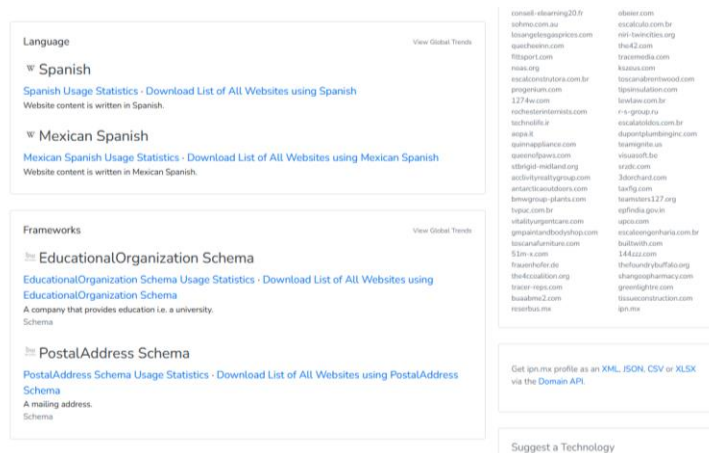


Figura 15. Lenguaje y Framework utilizados en el sitio

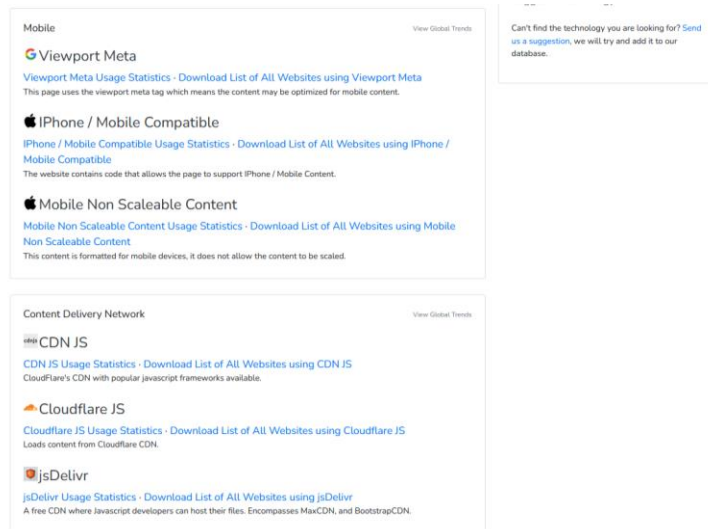


Figura 16. Soporte Móvil y Content Delivery Network utilizados en el sitio

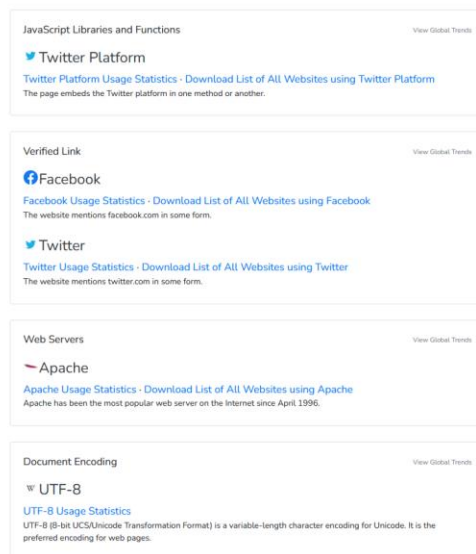






Figura 17. Bibliotecas Javascript, Servidores Web y Document Encoding utilizados en el sitio


Document Standards View Global Trends


 **HTML5 DocType**
[HTML5 DocType Usage Statistics](#)
The DOCTYPE is a required preamble for HTML5 websites.


 **X-UA-Compatible**
[X-UA-Compatible Usage Statistics](#)
Allows a website to define how a page is rendered in Internet Explorer 8, allowing a website to decide to use IE7 style rendering over IE8 rendering.

 **Google Chrome IE Frame**
[Google Chrome IE Frame Usage Statistics](#)
Frames Google Chrome window into Internet Explorer for HTML 5 compatibility.

 **Meta Description**
[Meta Description Usage Statistics](#)
The description attribute provides a concise explanation of the page content.

 **Open Graph Protocol**
[Open Graph Protocol Usage Statistics](#)
The Open Graph protocol enables any web page to become a rich object in a social graph, a open protocol supported by Facebook.

 **Twitter Cards**
[Twitter Cards Usage Statistics](#)
Twitter cards make it possible for you to attach media experiences to Tweets that link to your content.

 **Cascading Style Sheets**
[Cascading Style Sheets Usage Statistics](#)
Cascading Style Sheets (CSS) is a stylesheet language used to describe the presentation of a document written in a markup language. Its most common application is to style web pages written in HTML.


 **Twitter Bootstrap**

Figura 18. Estándares utilizados en el sitio