

# TRABAJO AUDITORIA

## DANIEL VARGAS



© 2025 Daniel Vargas de Miguel. Todos los derechos reservados.

# INFORME DE AUDITORÍA - ELFERIAL.ES

1. ¿QUÉ VAMOS A HACER?

2. ¿CUÁL ES EL OBJETIVO DE ESTA AUDITORÍA?

3. ¿QUÉ HERRAMIENTAS USAREMOS Y PARA QUÉ SIRVEN?

4. EMPEZAMOS CON EL ANÁLISIS

4.1 NMAP

4.2 ZAPROXY

4.3 SQLMAP

4.4 THEHARVESTER

4.5 SHODAN

4.6 NESSUS

5. INFORMES OBTENIDOS: VULNERABILIDADES, PUNTOS FUERTES Y ASPECTOS A MEJORAR

5.1 NMAP

5.2 ZAPROXY

5.3 SQLMAP

5.4 THEHARVESTER

5.5 SHODAN

5.6 NESSUS

---

## *1- ¿Qué vamos a hacer?*

Vamos a realizar un análisis técnico de una página web y realizar una auditoría técnica completa. Evaluaremos su rendimiento, vulnerabilidades, puntos fuertes, puntos débiles, etc. También evaluaremos su accesibilidad su SEO técnico y la arquitectura de la información y navegación. Para ello necesitaremos diferentes herramientas como: NMAP, ZAP, SQLMAP, TheHarvester.

---

## *2-¿Cuál es el objetivo de esta auditoría?*

El objetivo de esta auditoría de seguridad web sobre el sitio <https://www.elferial.es/> es identificar posibles vulnerabilidades técnicas que puedan comprometer la confidencialidad, integridad o disponibilidad de la información gestionada por la página. A través de un análisis estructurado, se evaluarán aspectos clave como la configuración del servidor, el manejo de datos de usuarios, la exposición de información sensible, el cumplimiento de buenas prácticas de desarrollo seguro y la resistencia ante ataques comunes como inyecciones, XSS o fallos de autenticación. El fin último es proporcionar un diagnóstico claro que permita fortalecer la seguridad de la plataforma, proteger la experiencia de los usuarios y reducir los riesgos operativos.

---

---

## *3-¿Qué herramientas usaremos y para qué sirven?*

- *NMAP*

Nmap (Network Mapper) es una herramienta de código abierto utilizada para el escaneo y auditoría de redes. Permite descubrir hosts y servicios en una red mediante el envío de paquetes personalizados. Es muy útil para detectar puertos abiertos, sistemas operativos y versiones de software. Se emplea en análisis de seguridad, evaluación de vulnerabilidades y recopilación de información. Admite escaneos rápidos o detallados, según los parámetros configurados. Soporta scripts NSE (Nmap Scripting Engine) para automatizar tareas avanzadas. Es compatible con múltiples protocolos como TCP, UDP, ICMP, entre

otros.Nmap funciona en sistemas Linux, Windows y macOS.Puede generar informes en formatos como XML, HTML o texto plano.Es una herramienta clave en cualquier informe de ciberseguridad y pentesting.

## ● *ZAPROXY*

OWASP ZAP (Zed Attack Proxy) es una herramienta gratuita y de código abierto para pruebas de seguridad en aplicaciones web.Su objetivo principal es detectar vulnerabilidades como XSS, inyecciones SQL, problemas de autenticación y configuraciones inseguras.

Funciona como proxy entre el navegador y la web, permitiendo interceptar, modificar y analizar tráfico HTTP/HTTPS.Incluye escaneos automáticos y manuales, ideal tanto para principiantes como para expertos.Permite crear scripts personalizados y automatizar pruebas repetitivas.

Se integra fácilmente en entornos CI/CD para pruebas en desarrollo continuo.También puede mapear la estructura de una web y encontrar recursos ocultos.Conclusión: es una herramienta clave en pentesting web, eficaz y fácil de usar.Recomendada para análisis regulares de seguridad en entornos de desarrollo y producción.Complementa otras herramientas como Burp Suite o Nikto en auditorías completas.

## ● *SQLMAP*

SQLmap es una herramienta de seguridad de código abierto diseñada para automatizar la detección y explotación de vulnerabilidades de inyección SQL en aplicaciones web. Su principal función es identificar fallos en bases de datos, permitiendo a los pentesters y auditores de seguridad extraer información sensible (como credenciales, tablas o datos confidenciales), ejecutar comandos remotos e incluso tomar control del servidor vulnerable si las condiciones lo permiten. Aunque es ampliamente utilizada en pruebas de penetración legales y auditorías de seguridad, su mal uso puede tener consecuencias legales, por lo que siempre debe emplearse con autorización explícita sobre sistemas objetivo.

## • THE HARVESTER

TheHarvester es una herramienta de código abierto utilizada para la recolección de información (reconocimiento pasivo) en fases iniciales de pruebas de penetración y análisis de seguridad. Su principal función es obtener correos electrónicos, nombres de empleados, subdominios, direcciones IP y hosts relacionados con un dominio específico. Utiliza fuentes públicas como buscadores (Google, Bing, Baidu), redes sociales, bases de datos como Shodan o PGP, y servicios DNS. Es muy útil para footprinting sin alertar al objetivo, ya que no interactúa directamente con los sistemas del mismo. TheHarvester permite personalizar las búsquedas, guardar resultados y exportarlos en distintos formatos. Su interfaz por línea de comandos facilita la integración con otras herramientas de seguridad. Ayuda a los analistas a identificar vectores de ataque potenciales. Es comúnmente utilizado en auditorías de seguridad, ejercicios de red teaming y pruebas de caja negra. Su uso debe cumplir con normativas éticas y legales.

## • SHODAN

Shodan es un motor de búsqueda especializado en dispositivos conectados a internet, como servidores, cámaras, routers y sistemas IoT. Permite a usuarios encontrar equipos vulnerables o mal configurados mediante filtros como puertos, protocolos o ubicación. Es útil para pentesters y administradores de red para identificar fallos de seguridad, pero también puede ser usado por atacantes para encontrar objetivos. Ofrece datos técnicos como banners, servicios activos y versiones de software. Su uso responsable ayuda a fortalecer la ciberseguridad, aunque requiere ética para evitar actividades malintencionadas.

## • NESSUS

Nessus es una herramienta de escaneo de vulnerabilidades ampliamente utilizada en ciberseguridad para identificar fallos en sistemas, redes y aplicaciones. Desarrollada por Tenable, permite detectar configuraciones inseguras, parches faltantes y posibles brechas de seguridad mediante análisis automatizados. Su base de datos de vulnerabilidades se actualiza constantemente, facilitando la evaluación de riesgos y el cumplimiento de

normativas. Nessus es empleado por profesionales para auditorías, pentesting y reforzamiento de defensas, generando informes detallados que ayudan a priorizar y mitigar amenazas. Su versatilidad lo hace útil tanto en entornos corporativos como en pruebas de seguridad proactivas.

---

## 4-EMPEZAMOS CON EL ANÁLISIS

Vamos a empezar con el análisis de la web de <https://www.elferial.es/> yo voy a utilizar una máquina virtual de kali linux para hacer las pruebas. Vamos con la primera herramienta del análisis que es NMAP

### 4-1 NMAP



El primer paso es instalar nmap con el siguiente comando `sudo apt install nmap`.

```

root@kali:~/home/kali]
# sudo apt install nmap
nmap ya está en su versión más reciente (7.95+dfsg-1kali1).
Fijado nmap como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
imagemagick-7-common libdc1394-25 libimath-3-1-29t64 liblqr-1-0 libmagickcore-7.q16-10-extra libmpcdec6 libonnxit64 libpthreadpool0 libsrtp2-1 libxnnpack0
libabsl20230802 libdca0 libjxl0.10 liblrdf0 libmagicwand-7.q16-10 libmpeg2encpp-2.1-0t64 libopenexr-3-1-30 libraptor2-0 libvo-acenc0 libvajl2
libavt0 libfaad2 libjxr-tools libltc11 libmjpegutils-2.1-0t64 libmplex2-2.1-0t64 libopenh264-7 libraw23t64 libvo-amvbenc0 libzbar0t64
libcpufifo0 libfuse2-3 libjxr0t64 libmagickcore-7.q16-10 libmodplug1 libmeon27t64 libopenp2-0 libsoundtouch1 libwmidid2 libzxing3
Utilece «sudo apt autoremove» para eliminarlos.

Summary: Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

```

El primer escaneo es hacer un escaneo básico para ver los puertos abiertos ls  
*nmap -v -sS -p- -T4 -oN escaneo\_basico.txt www.elferial.es*

```

└─(root㉿kali)-[~/home/kali/dani/final]
# nmap -v -sS -p- -T4 -oN escaneo_basico.txt www.elferial.es
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 17:35 CEST
Initiating Ping Scan at 17:35
Scanning www.elferial.es (217.116.16.122) [4 ports]
Completed Ping Scan at 17:35, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:35
Completed Parallel DNS resolution of 1 host. at 17:35, 0.00s elapsed
Initiating SYN Stealth Scan at 17:35
Scanning www.elferial.es (217.116.16.122) [65535 ports]
Discovered open port 21/tcp on 217.116.16.122
Discovered open port 25/tcp on 217.116.16.122
Discovered open port 993/tcp on 217.116.16.122
Discovered open port 143/tcp on 217.116.16.122
Discovered open port 587/tcp on 217.116.16.122
Discovered open port 995/tcp on 217.116.16.122
Discovered open port 110/tcp on 217.116.16.122
Discovered open port 80/tcp on 217.116.16.122
Discovered open port 443/tcp on 217.116.16.122
SYN Stealth Scan Timing: About 0.38% done
Discovered open port 8008/tcp on 217.116.16.122
SYN Stealth Scan Timing: About 6.28% done; ETC: 17:51 (0:15:10 remaining)
SYN Stealth Scan Timing: About 57.89% done; ETC: 17:38 (0:01:06 remaining)
Completed SYN Stealth Scan at 17:37, 100.82s elapsed (65535 total ports)
Nmap scan report for www.elferial.es (217.116.16.122)
Host is up (0.028s latency).
rDNS record for 217.116.16.122: mailing.myfocus.es
Not shown: 60231 filtered tcp ports (net-unreach), 5291 filtered tcp ports (no-response)
PORT      STATE     SERVICE
21/tcp    open      ftp
25/tcp    open      smtp
80/tcp    open      http
110/tcp   open      pop3
113/tcp   closed   ident
143/tcp   open      imap
443/tcp   open      https
587/tcp   open      submission
993/tcp   open      imaps
995/tcp   open      pop3s
8008/tcp  open      http
49247/tcp closed   unknown
49799/tcp closed   unknown

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 101.09 seconds
Raw packets sent: 102761 (4.521MB) | Rcvd: 96973 (5.980MB)

```

El segundo escaneo es para ver las vulnerabilidades de la página web *nmap --dns-servers 8.8.8.8 --script vuln -p 80,443 -oN escaneo\_vulnerabilidades.txt*  
**217.116.16.122**

```
# nmap -dns-servers 8.8.8.8 --script vuln -p 80,443 -oN escaneo_vulnerabilidades.txt 217.116.16.122
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 17:50 CEST
Nmap scan report for 217.116.16.122
Host is up (0.0015s latency).

PORT      STATE SERVICE
80/tcp    open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-cross-domain-policy:
|   VULNERABLE:
|     Cross-domain and Client Access policies.
|       State: LIKELY VULNERABLE
|         A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader, etc. use to access data across different domains. A client access policy file is similar to cross-domain policy but is used for MS Silverlight applications. Overly permissive configurations enables Cross-site Request Forgery attacks, and may allow third parties to access sensitive data meant for the user.
|     Check results:
|       /crossdomain.xml:
|         <?xml version="1.0" ?>
|         <cross-domain-policy>
|           <allow-access-from domain="www.elferial.es" />
|         </cross-domain-policy>

Extra information:
Trusted domains:elferial.es

References:
https://www.adobe.com/devnet/articles/crossdomain_policy_file_spec.html
http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
http://acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file
http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/CrossDomain_PolicyFile_Specification.pdf
https://www.owasp.org/index.php/Test_RIA_cross_domain_policy_%28OTG-CONFIG-008%29
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| http-cookie-flags:
|   :
|   PHPSESSID:
|     httponly flag not set
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

Nmap done: 1 IP address (1 host up) scanned in 231.96 seconds
```

El tercer escaneo y último es un escaneo completo (tarda mas pero puede aportarnos más información) para ello pondremos el comando:

```
nmap -sS -sU -T4 -A -v -Pn -p- --script=default,vuln,auth,discovery,brute -O --osscan-limit  
--max-retries 3 --min-rate 5000 --max-rtt-timeout 1000ms --min-hostgroup 64 --open -oN  
scanscan-ultra-complete.txt 217.116.16.128
```

```
root@kali:~/Downloads/finmap# ./finmap -a 192.168.1.1 -p 21-443 --script=script.default,vuln.auth.discovery.brute -O --osscan-limit --max-retries 3 --min-rate 5000 --max-rtt-timeout 1000ms --min-hostgroup 64 --open -oN escaneo_ultra_completo.txt 217.116.16.122
Host discovery disabled (-Ph). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 17:59 CEST
NSE: Starting multi-threaded port scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:59
NSE: [shodan-api] Error: Please specify your ShodanGT key with the shodan-api.apikey argument
NSE: [http-nse] [http-nse] Need to be executed for IPv4.
NSE: [targets-lvvv-maptool] This script is IPv6 only.
NSE: [intrace] A source IP must be provided through Fromip argument.
No preprint devices in the subnet
Completed NSE at 17:59; 10.94s elapsed
Initiating NSE at 17:59
Completed NSE at 17:59; 0.08s elapsed
Initiating NSE at 17:59
Completed NSE at 17:59; 0.08s elapsed
Initiating NSE at 17:59
Completed NSE at 17:59; 0.08s elapsed
NSE: Multi-threaded script results:
[!]multicasts-nsfnet-discovery: 0
Targets-asn:
[!]targets-asn-asn is a mandatory parameter
[!]http-notext-share: The http-notext-share module is temporarily disabled due to changes in Robtex's API. See https://www.robtex.com/api/
[!]http-headers: The http-headers module is temporarily disabled due to changes in Robtex's API. See https://www.robtex.com/api/
Initiating Parallel DNS resolution of 1 host at 17:59
Completed Parallel DNS resolution of 1 host at 17:59; 0.01s elapsed
Initiating OS detection scan at 17:59
Completed OS detection (217.116.16.122) [65535 ports]
Discovered open port 110/tcp on 217.116.16.122
Discovered open port 21/tcp on 217.116.16.122
Discovered open port 22/tcp on 217.116.16.122
Discovered open port 80/https on 217.116.16.122
Discovered open port 80/HTTP on 217.116.16.122
Discovered open port 8015/tcp on 217.116.16.122
```

Estos tres escaneos nos darán como resultados un informe cada uno que luego nos leeremos, exploraremos mejoras y utilizaremos la ia para ver qué nos recomienda

```
[root@kali]~[~/home/kali/dani/final/nmap]
# ls
escaneo_basico.txt  escaneo_ultra_completo.txt  escaneo_vulnerabilidades.txt
```

## 4.2 ZAPROXY



Al igual que nmap vamos a proceder con la instalación de zaproxy en kali linux para ello vamos a instalarlo paso por paso lo primero es el comprando de instalación sudo

```
apt install zaproxy
```

```
root@kali: /home/kali
# apt install zaproxy

Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libmagick-7-common libdc1394-25 libimath-3-29764 liblqr-1-0 libmagickcore7-q16-10-extra libmpcdec6 libbonnxt64 libpthreadpool0 libsrtp2-1 libvpx-acenc0 libwxonpack0
libmagickx-7-common libdci1394-25 liblqrdf0 libmagickwand-7-q16-10 libmpeg2encpp2-1-0t64 libopenexr3-1-30 libraptor2-0 libvo-acenc0 libuyajl2
libihavt0 libfaad2 libjxr-tools liblbtcl libmjngutells-2-1-0t64 libmplex2-2-1-0t64 libopenh264-7 libraw23t64 libvo-amvbenc0 libzbar0t64
libcpufifo0 libfuse3-3 libjxr0t64 libmagickcore7-q16-10 libmodplug1 libneon27t64 libopenh2-0 libsoundtouch1 libwldmid12 libzxing3

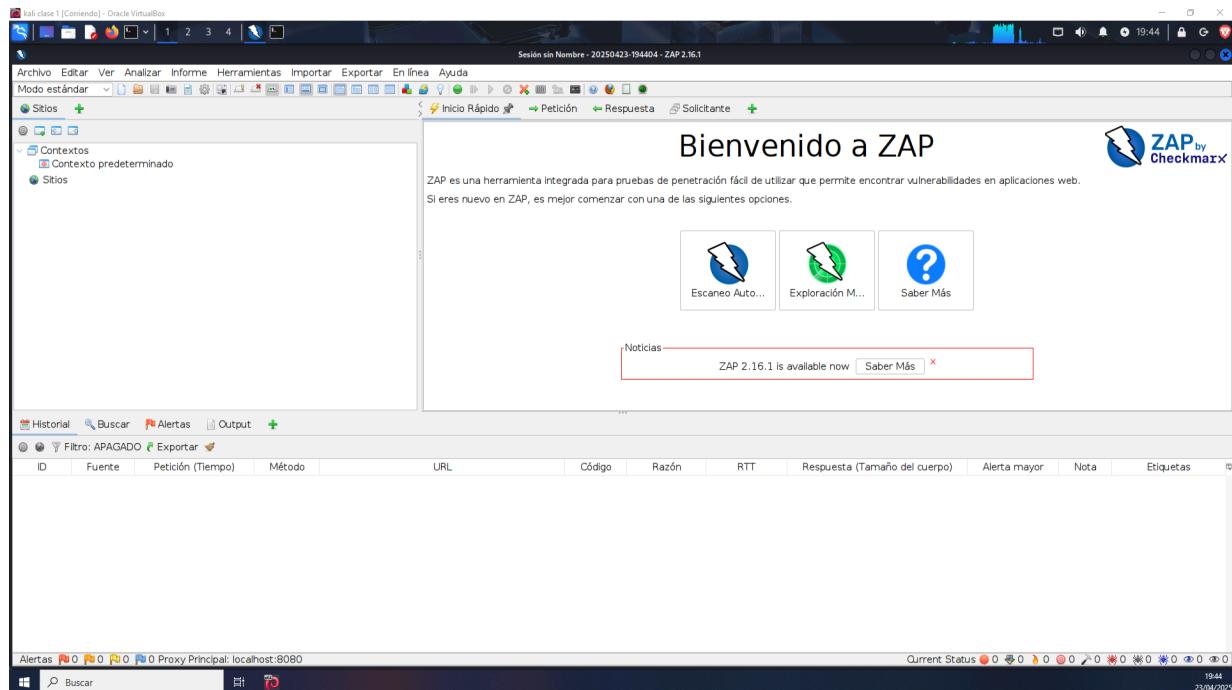
Utilice «sudo apt autoremove» para eliminarlos.

Installing:
zaproxy

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1
Download size: 214 MB
Space needed: 271 MB / 51,4 GB available

Des: https://mirrors.as.cdn.perfprod.com/kali/kali-rolling/main amd64 zaproxy all 2.16.1-0kali11 [214 MB]
Descargados 214 MB en 4s (49,1 MB/s).
Selezionando el paquete zaproxy previamente no seleccionado.
(Leyendo la base de datos ... 438885 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../aproxy_2.16.1-0kali11_all.deb ...
Desempaquetando zaproxy (2.16.1-0kali1) ...
Configurando zaproxy (2.16.1-0kali1) ...
Procesando disparadores para kali-menu (2029.2.0) ...
```

Para ejecutarlo simplemente ponemos zaproxy y nos saldra la interfaz grafica que es muy intuitiva y fácil de usar



Para hacer un escaneo simplemente tenemos que irnos a escaneo automatico (el rayito azul) una vez dentro nos pedira poner la web y el navegador preferido. Vamos a rellenarlo para ver como queda:

Ayuda



Inicio Rápido Petición Respuesta Solicitante +

# Escaneo Automatizado

Esta pantalla le permite iniciar un escaneo automático contra una aplicación: simplemente ingrese su URL a continuación y presione 'Atacar'. Tenga en cuenta que solo debe atacar aplicaciones para las cuales ha recibido previamente una clara autorización.

URL a atacar:

Usar el spider tradicional:

Usar el spider ajax:  Sí es Moderno  No

Progreso: No iniciado

Le damos a atacar y empieza el analisis

Una vez terminado el análisis nos sacará un informe para eso nos vamos arriba a la pestaña informes

guardamos el informe(es un html con lo cual se nos abrirá una ventana web nueva) y como se ve en las siguientes imágenes todo estará perfecto

kali clase 1 [Corriendo] - Oracle VirtualBox

```
(root㉿kali)-[~/home/kali/dani/final/zaproxy]
# ls
Zaproxy_elferial.html

(root㉿kali)-[~/home/kali/dani/final/zaproxy]
#
```

Vista clase 1 [Corriendo] - Oracle VirtualBox

zaproxy.xml ZAP EL FERIAL ZAP EL FERIAL 20:00

Archivo /home/kali/dani/final/zaproxy/Zaproxy\_elferial.html#about-this-report

## ZAP EL FERIAL

Generated with on mié 23 abr 2025, at 19:52:43

ZAP Versión: 2.16.1

ZAP by [Checkmarx](#)

**Contents**

- [About this report](#)
  - [Report parameters](#)
- [Summaries](#)
  - [Alert counts by risk and confidence](#)
  - [Alert counts by size and risk](#)
  - [Alert counts by alert type](#)
- [Alerts](#)
  - [Risk=Alto, Confidence=Media \(1\)](#)
  - [Risk=Medio, Confidence=Alta \(1\)](#)
  - [Risk=Medio, Confidence=Media \(3\)](#)
  - [Risk=Medio, Confidence=Baja \(1\)](#)
  - [Risk=Bajo, Confidence=Media \(1\)](#)
  - [Risk=Informativo, Confidence=Media \(3\)](#)
  - [Risk=Informativo, Confidence=Baja \(3\)](#)
- [Appendix](#)
  - [Alert types](#)

**About this report**

**Report parameters**

**Contexts**

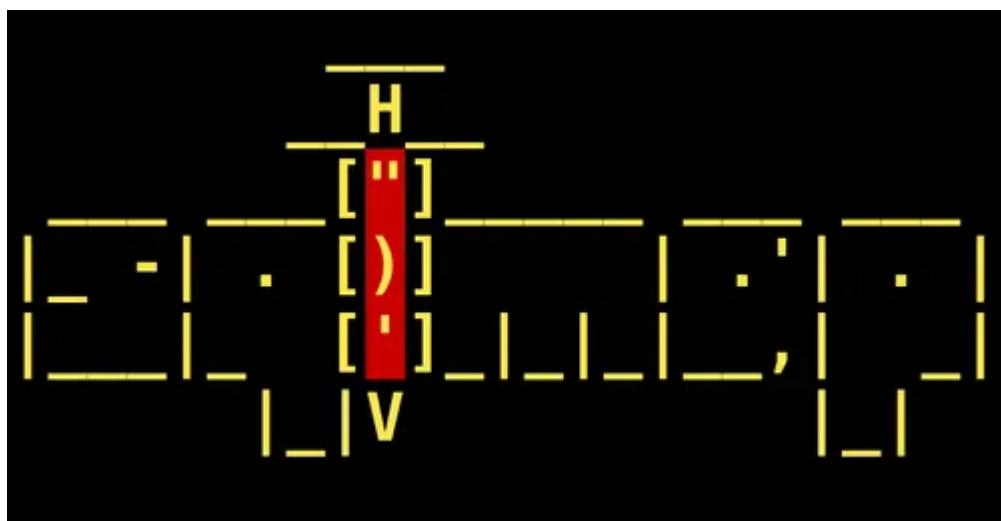
No contexts were selected, so all contexts were included by default.

**Sites**

The following sites were included:

- http://www.elferial.es
- https://www.elferial.es

## 4.3 SQLMAP



El tercer programa que vamos a ejecutar es sqlmap para ver las vulnerabilidades de inyección de sql. Para ello vamos a instalar el programa. Vamos a proceder a instalarlo con el siguiente comando: `sudo apt install sqlmap`

una vez instalado vamos a proceder a analizar la web con el siguiente comando

```
sqlmap -u "https://www.elferial.es/" --batch --crawl=2 --level=3 --risk=2  
--output-dir=elferial sqlmap report
```

```

root@kali:~/home/kali/elferlal.es#
# sqlmap -u "https://www.elferlal.es/" --batch --crawl=2 --level=3 --risk=2 --output-dir=elferlal_sqlmap_report
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 17:36:33 /2025-08-24/
[17:36:33] [WARNING] using '/home/kali/elferlal_sqlmap_report' as the output directory
do you want to check for the existence of site's sitemap.xml? [y/N] N
[17:36:33] [INFO] starting crawler for target url: 'https://www.elferlal.es/'
[17:36:33] [INFO] searching for links with depth 2
[17:36:34] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[17:36:34] [WARNING] running in a single-thread mode. This could take a while
[17:36:34] [INFO] 71/130 links visited (55%)
[17:36:42] [INFO] got a 301 redirect to 'https://www.elferlal.es/'. Do you want to follow? [y/n] Y
[17:36:42] [INFO] 71/130 links visited (55%)
[17:36:42] [WARNING] potential CAPTCHA protection mechanism detected
do you want to never stop injecting results? [y/n] N
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N
[17:36:42] URL:
GET https://www.elferlal.es/noticias-y-eventos?year=current
do you want to test this URL? [y/n] Y
[17:36:42] [INFO] testing URL: 'https://www.elferlal.es/noticias-y-eventos?year=current'
[17:36:42] [INFO] using '/home/kali/elferlal_sqlmap_report/results-04242025_0536pm.csv' as the CSV results file in multiple targets mode
[17:36:42] [INFO] testing connection to the target URL
you can set your own proxy by setting the environment variable 'HTTP_PROXY' or 'HTTPS_PROXY'. If you want to set its own ('IP:PORT') do you want to use those [y/N] Y
[17:36:42] [INFO] checking if the target is protected by some kind of WAF/IPS
[17:36:42] [INFO] testing if the target URL content is stable
[17:36:42] [INFO] target URL content is stable
[17:36:42] [INFO] testing if GET parameter 'year' is dynamic
[17:36:42] [WARNING] GET parameter 'year' does not appear to be dynamic
[17:36:52] [WARNING] heuristic (basic) test shows that GET parameter 'year' might not be injectable
[17:36:52] [INFO] testing for SQL injection on GET parameter 'year'
[17:36:59] [INFO] testing for AND boolean-based blind - WHERE or HAVING clause

```

Cuando termine nos sacará un informe de que ha encontrado como se muestra en la imagen

```

root@kali:~/home/kali/dani/final/sqlmap#
# ls
sqlmap.txt
# 

```

## 4.4 THE HARVESTER



theHarvester

Vamos a usar el harvester para ver correos y demás información (siempre de forma ética) suele venir instalado en kali linux pero vamos a instalarlo de nuevo

```
sudo apt install theharvester
```

```
[Archivos] [Acciones] [Editor] [Vista] [Ayuda]
root@kali: /home/kali/dani/final/sqlmap
# sudo apt install theharvester
theharvester ya está en su versión más reciente (4.7.0-0kali2).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
imageMagick-7-common libbd1394-25 libmath-3-1-29164 liblqr-1-0 libmagiccore-7.q16-10-extra libmpcdec6 libbonnxt64 libpthreadpool0 libsttp2-1 libxnpack0
libabfs20230802 libdcad libjxl10.10 liblrdf0 libmagickwand-7.q16-10 libmpeg2encpp-2.1-0t64 libopenexr-3-1-30 libraptor2-0 libvo-acenc0 libuya12
libavif2 libfaad2 libfrxr-tools libltc1 libmjpegutils-2.1-0t64 libopenh264-7 libraw23t64 libvo-amrenc0 libybar0t64
libdcpinfo0 libopus3-3 libvpx10t64 libmagiccore-7.q16-10 libmuplugi libone21t64 libopenni2-0 libsoundtouch1 libwlm0m10i2 libxzhang3
Utilice «sudo apt autoremove» para eliminarlos.

Summary:
 Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
root@kali: /home/kali/dani/final/sqlmap
#
```

Ahora vamos a proceder a analizar la web de elferial.es con el siguiente comando

como no nos ha encontrado nada lo que haremos es no guardar informe. Pero utilizaremos otro programa que podemos usar es <https://hunter.io> buscamos la web del ferial y esto es lo que nos saca

**Domain Search** ⓘ

Upload a list of domains to search

elferiel.es 4 results × Filters Q

Type Department Show only results with

4 results for your search

Export Find by name

info@elferiel.es Support Save as lead Add to a campaign  
99% Verify email address 13 sources

rmpolo@elferiel.es Save as lead Add to a campaign  
78% Verify email address 5 sources

gerente@elferiel.es Save as lead Add to a campaign  
76% Verify email address 2 sources

emprendimiento@elferiel.es Save as lead Add to a campaign  
75% Verify email address 1 source

Follow CC El Ferial for updates  
Get notified when CC El Ferial opens new jobs, raises funds, and more.  
Follow this company

Company CC El Ferial  
CC El Ferial is a Shopping Mall that offers a complete range of services with over 60 stores and a free parking lot with 1,700 ... more  
Social:

Technologies

Similar companies

También nos da más información de las herramientas que utiliza la página web

1 company matches your filters

Save companies Find email addresses 1 company

Company CC El Ferial elferiel.es 4 email addresses Follow Find email addresses

Description  
CC El Ferial is a Shopping Mall that offers a complete range of services with over 60 stores and a free parking lot with 1,700 spaces.

Details  
Website: [elferiel.es](#) Social:   
Keywords: shopping mall, retail, commercial real estate, parking facilities

Email addresses Technologies Signals

Technologies used on elferiel.es  
Powered by TechLc

Data Visualization

Programming Framework  
 Bootstrap  
 jQuery  
 Modernizr

Programming Language  
 PHP

Security  
 HSTS

Web Servers  
 Apache HTTP Server

Website Optimization  
 OWL Carousel

## 4.5 SHODAN

Es un sitio web que nos va a dar mucha información de la página en mi opinión muy útil y es una de las mejores páginas de ciberseguridad y más visitada al día. Para empezar el análisis nos registramos y buscamos arriba la web que queremos analizar  
En la barra de buscador ponemos net dos puntos y la ip del sitio que queremos analizar  
(En mi caso es net:217.116.16.122)



Una vez analizado estos son los resultados que nos muestra sobre nuestra página de el feriaL. Como curiosidad no solo nos muestran los puertos abiertos también una información general de la web y lo mas interesante las tecnologías usadas y las vulnerabilidades que ha tenido lo cual lo hace muy interesante

This screenshot shows the detailed search results for the IP address 217.116.16.122. The results are organized into several sections:

- General Information:** Lists hostnames (centrocomercialgorbel.com, www.centrocomercialgorbel.com, mailing.myfocus.es, panel.polarik.com, correo.trdimension.com), domains (centrocomercialgorbel.com, myfocus.es, polarik.com, trdimension.com), country (Spain), city (Madrid), organization (MyFOCUS), ISP (acens Technologies, S.L.), and ASN (AS16371).
- Open Ports:** Shows a grid of 14 open ports: 21, 25, 80, 110, 143, 443, 587, 993, 995, and 2222.
- Protocols:** Displays a list of protocols and commands, including:
  - 22B 217.116.16.122:2233 FTP server ready
  - 53B Login incorrect.
  - 214-The following commands are recognized (\* =)\*'s unimplemented:
  - 214-CMD XCWD XCUP XCPN SWIN? QUIT PORT PWD
  - 214-EPST EPSV ALLOV REINV REINV REINV RRD
  - 214-XWD XWD XWD XWD SITE LIST HELP
  - 214-NORD FEAT OPTS AUTH CCCP\* COM\* ENC\* MCIC\*
  - 214-PBSZ PROT TYPESTRU MODE RETR STOR STOU
  - 214-APPF REST ABOR USER PASS ACC\* REIN\* LIST
  - 214-STAT SITE MLSD RLST
  - 214-Direct comments to root@127.0.0.1:1
  - 211-Features:
  - MOTM
  - SITE RWDR
  - SSCN
  - TWS
  - MFTP
  - SIZE
  - PROT
  - CCC
  - SITE INDIR
  - PRZC
  - AUTH TLS
  - LANG ko-KR;it-IT;fr-FR;zh-TW;es-ES;ru-RU;zh-CN;bg-BG;en-US;ja-JP
  - NFS modify;UNIX,DOS;UNIX,mode;
- Web Technologies:** Lists JavaScript Libraries (jQuery, Angular.js) and UI Frameworks (React.js, Angular.js).

**Vulnerabilities**

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

**2020 (2)**

**CVE-2020-11023** **6.9** In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

**CVE-2020-11022** **6.9** In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

**2019 (1)**

**CVE-2019-11358** **6.1** jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable \_\_proto\_\_ property, it could extend the native Object.prototype.

**2015 (1)**

**CVE-2015-9251** **6.1** jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

## 4.6 NESSUS

Nessus es una herramienta para analizar fallos y vulnerabilidades de distintos sistemas el problema que tiene esta herramienta es que es un poco compleja de instalar debido a que te pide una cuenta de trabajo para el trial o premium con dinero pero vamos a probar con la trial para ello tenemos que meternos en la pagina web oficial y descargarlo

<https://www.tenable.com/products/nessus/nessus-essentials>

## Tenable Nessus® Essentials

Nessus Essentials is a free product from Tenable that provides high-speed, in-depth vulnerability scanning for up to 16 IP addresses per scanner.

**Limitations:** Nessus Essentials does not support unlimited scanning, compliance checks, content audits, Live Results, configurable reports, or the Nessus virtual appliance. For access to these features and more, upgrade to Nessus Professional.

**For Students & Educators:** If you're using Nessus Essentials for education, register through the [Tenable for Education](#) program to get started.

**Learn Nessus:** Our [on-demand Nessus Fundamentals course](#) covers everything from asset discovery to compliance, helping you master Nessus for effective vulnerability assessment in various business use cases.

**Register for an Activation Code**

You are registering for a 1-year Nessus Essentials license.

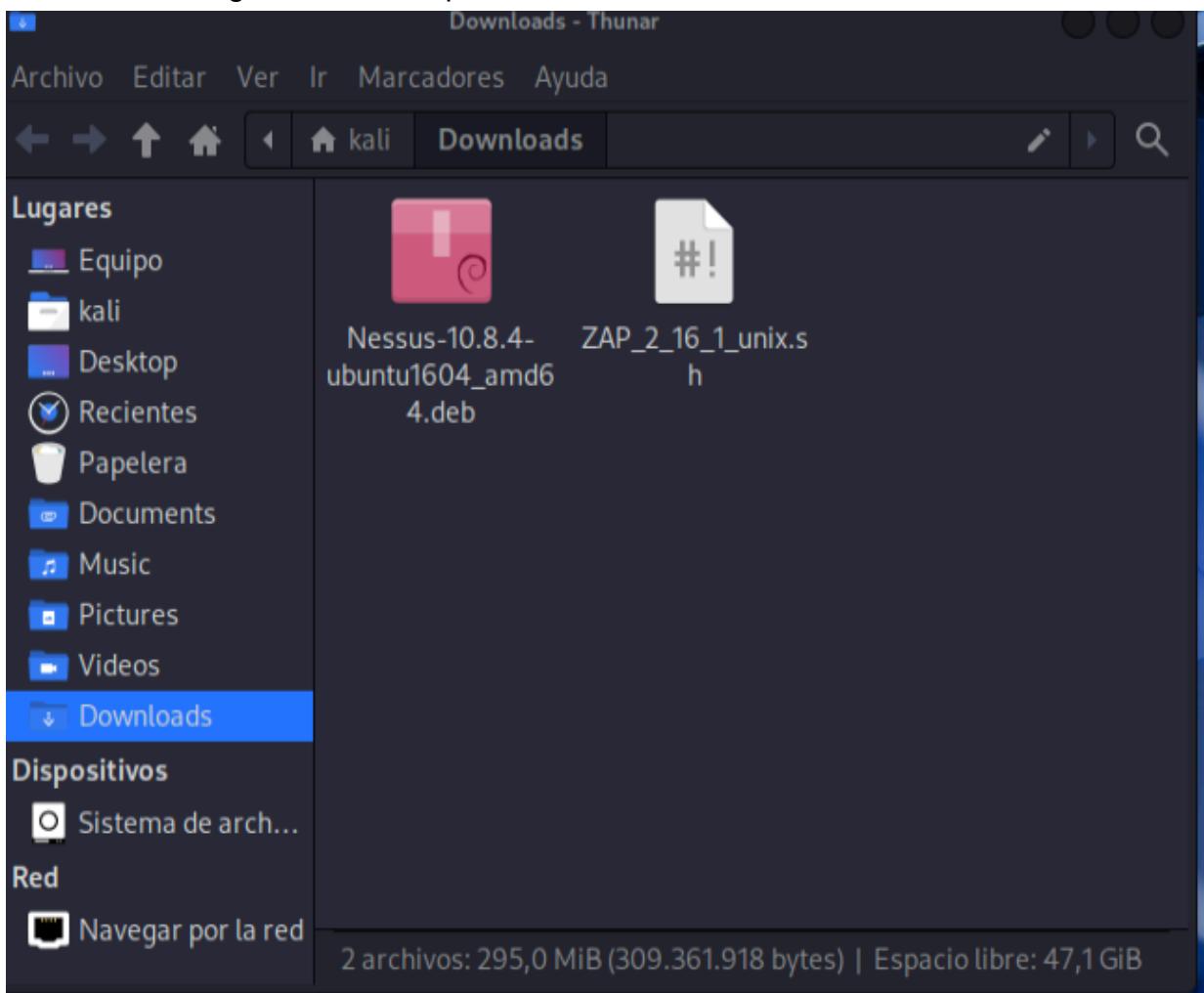
First Name
  Last Name

 Business Email
 

Check to receive updates from Tenable  
Tenable will only process your personal data in accordance with its [Privacy Policy](#).

[Get Started](#)

Una vez descargado tenemos que



con el dpkg lo descomprimiremos con el siguiente comando

```
sudo dpkg -i Nessus-10.8.4-ubuntu1604_amd64.deb
```

```
[sudo] contrasena para kali:          Kali Forums  Kali Nethunter  Exploit-DB  Google Hacking DB  OffSec
└─[root@kali]─[~/home/kali/Downloads]
# sudo dpkg -i Nessus-10.8.4-ubuntu1604_amd64.deb
Seleccionando el paquete nessus previamente no seleccionado.
(Leyendo la base de datos ... 439043 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar Nessus-10.8.4-ubuntu1604_amd64.deb ...
Desempaquetando nessus (10.8.4) ...
Configurando nessus (10.8.4) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

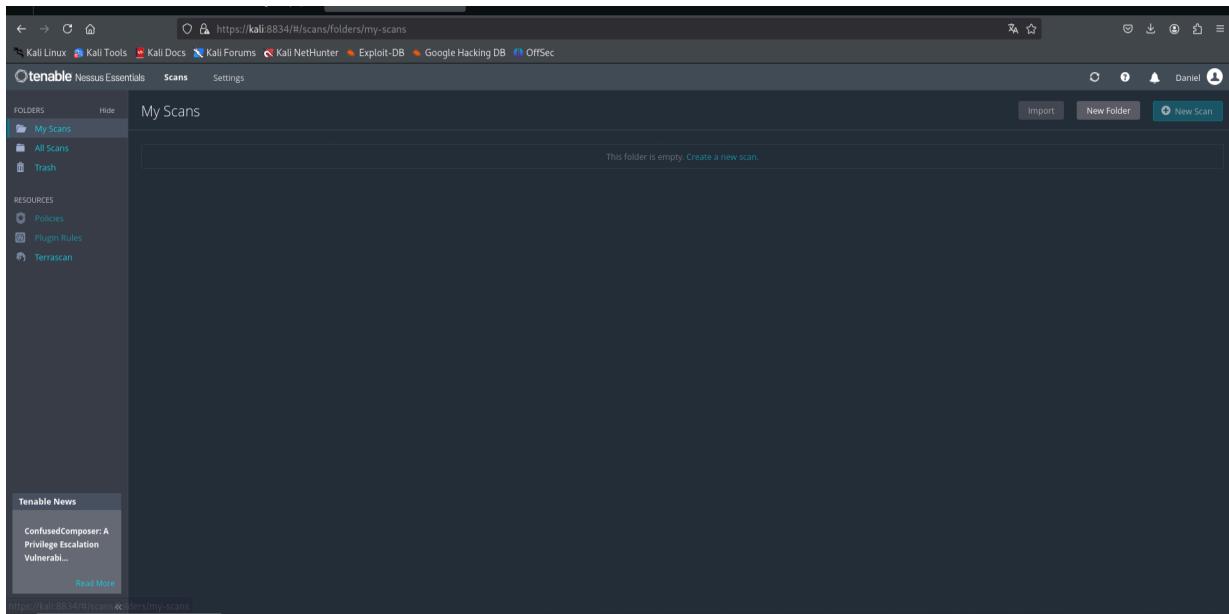
Una vez terminado tenemos que seguir los comandos que nos pone primero

`/bin/systemctl start nessusd.service`

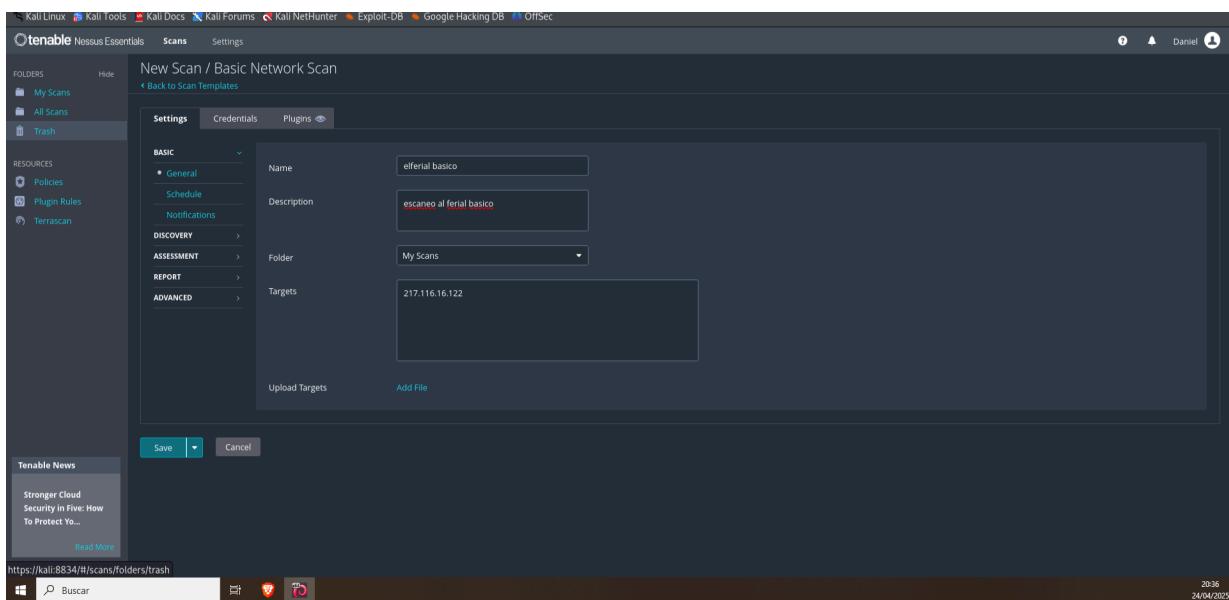
Y entrar en el siguiente url en mi caso es este:

`https://kali:8834/`

Una vez configurado todo el programa necesitará actualizarse e instalar la licencia,plugins y componentes. Debemos esperar hasta que termine para empezar el escáner



Configuraremos los datos para el escáner y vamos a hacer dos: Uno básico y uno completo. Empezaremos por el basico y despues el avanzado



**Tenable Nessus Essentials** | **Scans** | **Settings**

**escaneo completo elederal**

Hosts 1 | Vulnerabilities 18 | History 1

Filter ▾ Search Hosts 1 Host

Host Vulnerabilities

217.116.16.122 2 27

**Scan Details**

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS 3.0
- Scanner: Local Scanner
- Start: Today at 4:31 PM
- End: Today at 4:58 PM
- Elapsed: 27 minutes

**Vulnerabilities**

Critical: 1  
High: 1  
Medium: 1  
Low: 1  
Info: 15

**Tenable News**

Verizon 2025 DBIR: Tenable Research Collaboration ... [Read More](#)

Buscar 17:34 25/04/2025

**Tenable Nessus Essentials** | **Scans** | **Settings**

**escaneo completo elederal**

Hosts 1 | Vulnerabilities 18 | History 1

Filter ▾ Search Hosts 1 Host

Host Vulnerabilities

217.116.16.122 2 27

**Scan Details**

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 4:31 PM
- End: Today at 4:58 PM
- Elapsed: 27 minutes

**Vulnerabilities**

Critical: 1  
High: 1  
Medium: 1  
Low: 1  
Info: 15

**Tenable News**

OpenAI SearchGPT Results Tampering with Prompt Inj... [Read More](#)

Buscar 17:34 25/04/2025

**Tenable Nessus Essentials** | **Scans** | **Settings**

**escaneo completo elederal**

Hosts 1 | Vulnerabilities 18 | History 1

Filter ▾ Search Vulnerabilities 18 Vulnerabilities

Family	Count	Actions
Service detection	4	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
General	5	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
General	2	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
Port scanners	4	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
General	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
Device Type	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
General	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
Settings	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
General	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
Service detection	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
General	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
Misc.	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
Content detection	1	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>

**Scan Details**

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 4:31 PM
- End: Today at 4:58 PM
- Elapsed: 27 minutes

**Vulnerabilities**

Critical: 1  
High: 1  
Medium: 1  
Low: 1  
Info: 15

**Tenable News**

Progress WhatsUp Gold Unauthenticated Wireless MAC... [Read More](#)

Buscar 17:34 25/04/2025

Ambos escáner muestran el mismo resultado vamos a bajarlo para tener un informe mas completo y luego en el siguiente punto lo analizaremos

## *5-INFORMES OBTENIDOS VULNERABILIDADES, PUNTOS FUERTES Y ASPECTOS A MEJORAR*

### *5.1 NMAP*

#### *VULNERABILIDADES*

Viendo el análisis de estos 3 documentos podemos ver que el puerto 80 (HTTP) y HTTPS 443 ambos están abiertos y accesibles. No se han detectado vulnerabilidades de CSRF(), XSS almacenado o basado en DOM(). Ha encontrado una **VULNERABILIDAD**

**CRITICA** que se basa en **crossdomain.xml**(permite acceso desde www.elferial.es sin restricciones suficientes, lo que podría facilitar ataques CSRF o acceso no autorizado a datos).La falta de flag HttpOnly en la cookie PHPSESSID, lo que aumenta el riesgo de robo de sesión mediante XSS.También tiene otros puertos FTP(21/tcp), SMTP(25/tcp), POP3(110/tcp) IMAP(143/tcp) que podrían ser motivos de ataque si no estan bien securizados.

### *PUNTOS FUERTES*

El firewall ha bloqueado diferentes scripts de nmap y además se han marcado como filtered con lo cual indica que el firewall ha bloqueado bien esos intentos.Se usan los puertos IMAPS (993/tcp) y POP3S(995/tcp) para servicios de correo que son puertos cifrados lo cual es un punto a favor.No se encontraron evidencias de XSS y CSRF

### *ASPECTOS A MEJORAR*

Muy importante arreglar la configuracion del crossdomain.xml restringiendo el acceso solo a dominios específicos necesarios o evitando permisos genéricos.Añadir el flag HttpOnly y Secure a las cookies (especialmente PHPSESSID) para mitigar robo de sesión. Cerrar los puertos no esenciales y actualizar el servidor web de PHP a la última versión.

## *5.2 ZAPROXY*

### *VULNERABILIDADES*

Se han detectado diversas vulnerabilidades la más importante trata sobre la Librería JS ya que se detectó el uso de una versión antigua de jquery-validation (v1.13.0), con múltiples CVEs asociados (por ejemplo, CVE-2022-31147, CVE-2021-43306, etc) y permite explotarla para entrar al sistema. Además de esta vulnerabilidad crítica tenemos también la Ausencia de Tokens Anti-CSRF y Falta de CSP (Content Security Policy) y mas librerías de js que generan vulnerabilidades. Al igual que nmap nos muestra problemas con las cookies sin flags (HttpOnly, Secure, Same Site) y Falta del encabezado X-Content-Type-Options.

### *PUNTOS FUERTES*

Los puntos fuertes según este informe son el uso de HTTPS con cabeceras como Strict-Transport-Security,el servidor responde correctamente con códigos 200 y buena estructura de recursos y la página parece bien estructurada como una SPA moderna (detectada como “Aplicación Web Moderna”).

### *ASPECTOS A MEJORAR*

Estos es en lo que yo me centraria en corregir y que me parece más necesario: Actualizar librerías JS a versiones libres de vulnerabilidades (especialmente jQueryValidation)Configurar cabeceras de seguridad(Content-Security-Policy,X-Frame-Options y X-Content-Type-Options),Incluir tokens CSRF en formularios sensibles.Configurar correctamente las cookies (HttpOnly, Secure, SameSite).Automatizar análisis de seguridad periódicos. Implementar pruebas de penetración internas para validar mitigaciones.Revisar dependencias de terceros e implementar un sistema de gestión de componentes vulnerables.Aplicar políticas de Zero Trust para mejorar seguridad en capas.

## 5.3 SQLMAP

### VULNERABILIDADES

El análisis con sqlmap no encontró vulnerabilidades explotables de inyección SQL. Sin embargo, se detectó un posible mecanismo de protección CAPTCHA, lo que sugiere que el sitio podría estar implementando medidas de seguridad adicionales para prevenir ataques automatizados. Aunque no se identificaron vulnerabilidades críticas, es importante seguir monitoreando otros parámetros y endpoints, ya que el escaneo fue interrumpido antes de completar todas las pruebas.

### PUNTOS FUERTES

El sitio web mostró estabilidad en el contenido durante las pruebas, lo que indica un buen manejo de las solicitudes. Además, la redirección 301 detectada sugiere que el sitio sigue prácticas adecuadas de gestión de URLs. La presencia de un posible CAPTCHA refleja una conciencia de seguridad, lo que puede disuadir ataques automatizados. El parámetro year no mostró dinamismo inesperado, lo que reduce el riesgo de inyección SQL en esa área específica.

### ASPECTOS A MEJORAR

Aunque el escaneo no reveló vulnerabilidades graves, se recomienda realizar pruebas más exhaustivas en otros parámetros y secciones del sitio, ya que el análisis fue interrumpido prematuramente. Además, sería beneficioso investigar el funcionamiento del posible CAPTCHA para asegurar que no pueda ser eludido fácilmente. También se sugiere revisar manualmente el código y las consultas SQL asociadas al parámetro year para descartar falsos negativos. Por último, mantener actualizadas las herramientas de análisis y repetir las pruebas periódicamente ayudaría a identificar nuevas vulnerabilidades que puedan surgir.

## 5.4 THEHARVESTER Y HUNTER

Cuando analizamos la página web con theharvester no nos dio nada de información pero luego con la aplicación de hunter si que obtuvimos información importante. Vamos a analizar las dos

capturas de pantalla para ver que podemos analizar. Actualizar los plugins del CSM. También tiene medidas de seguridad como CAPTCHA y WAF que indican la conciencia de la ciberseguridad. Un buen sistema por roles que mejora la seguridad..