

# Ejercicio 1: Auditoría de seguridad activa con test de intrusión (Red local)

**Objetivo:** Detectar equipos y puertos abiertos en una red local, como primer paso de un test de intrusión.

## Material necesario

- Kali Linux.
- Acceso a una red local con al menos otro equipo conectado (puede ser una máquina virtual o el propio router).

## Pasos

1. Escanea la red local para descubrir hosts activos:

**nmap -sn 192.168.1.0/24**

```
~/Doc/Ejercicios_seguridad_informatica_2025 main > nmap -sn 192.168.0.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 08:51 CEST
Nmap scan report for 192.168.0.1
Host is up (0.00038s latency).
MAC Address: 00:A0:26:D2:68:9A (Teldat)
Nmap scan report for 192.168.0.5
Host is up (0.00055s latency).
MAC Address: 00:26:73:99:57:8C (Ricoh Company)
Nmap scan report for 192.168.0.21
Host is up (0.00047s latency).
MAC Address: D8:43:AE:44:E2:25 (Micro-Star Intl)
Nmap scan report for 192.168.0.22
Host is up (0.00073s latency).
MAC Address: 08:2E:5F:00:30:E9 (Hewlett Packard)
Nmap scan report for 192.168.0.23
Host is up (0.00073s latency).
MAC Address: E8:39:35:57:9E:E9 (Hewlett Packard)
Nmap scan report for 192.168.0.24
Host is up (0.00094s latency).
MAC Address: 08:00:27:44:AC:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.25
```

(ajusta el rango según la red del aula).

2. Elige un host detectado (por ejemplo, la IP 192.168.1.20) y haz un escaneo de puertos:

**nmap -sV 192.168.1.20**

```
~/Doc/Ejercicios_seguridad_informatica_2025 main > nmap -sV 192.168.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 08:53 CEST
Nmap scan report for 192.168.0.1
Host is up (0.0013s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    filtered  domain
80/tcp    filtered  http
MAC Address: 00:A0:26:D2:68:9A (Teldat)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

3. Opcional: Haz un escaneo más detallado incluyendo detección de sistema operativo:

**nmap -A 192.168.1.20**

```
~/Doc/Ejercicios_seguridad_informatica_2025 main > nmap -A 192.168.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 08:54 CEST
Nmap scan report for 192.168.0.1
Host is up (0.0010s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    filtered  domain
80/tcp    filtered  http
MAC Address: 00:A0:26:D2:68:9A (Teldat)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: broadband router
Running: Teldat embedded
OS details: Teldat K series gateway
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   1.02 ms  192.168.0.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
```

## Resultado esperado

- Listado de **IP activas** en la red.
- Identificación de **puertos abiertos** y servicios que están en ejecución.
- Información inicial sobre posibles puntos de entrada para un atacante.



## Ejercicio 2: Auditoría básica de páginas web

**Objetivo:** Analizar vulnerabilidades comunes en una página web usando herramientas incluidas en Kali Linux.

### Material necesario

- Kali Linux.
- Una página web de pruebas (puede ser una aplicación vulnerable en local, como DVWA o WebGoat, o un sitio autorizado para prácticas, como **testphp.vulnweb.com**).

### Pasos

1. Haz un escaneo con **Nikto** para identificar configuraciones inseguras y vulnerabilidades:

## nikto -h <http://testphp.vulnweb.com>

```
~ > nikto -h http://testphp.vulnweb.com
- Nikto v2.5.0

+ Target IP: 7.95 ( 44.228.249.3 ) at 2025-09-30 08:55 CEST
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2025-09-30 08:59:39 (GMT2)

+ Server: No banner retrieved
+ /EGAxqVr.gz: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /EGAxqVr.gz: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

2. Analiza con **WhatWeb** qué tecnologías usa el sitio (servidor, CMS, etc.):

## whatweb <http://testphp.vulnweb.com>

```
~ > whatweb http://testphp.vulnweb.com
^[[3http://testphp.vulnweb.com [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-44453540000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.com], HTTPServer[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0][clsid:D27CDB6E-AE6D-11cf-96B8-44453540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[text/JavaScript], Title[Home of Acunetix Art], X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]
```

3. Opcional: Haz un escaneo con **sqlmap** para comprobar si un formulario es vulnerable a inyección SQL:

## sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --batch

### Resultado esperado

- Informe de posibles vulnerabilidades (cabeceras inseguras, directorios ocultos, configuraciones por defecto).
- Identificación de tecnologías utilizadas en la web (PHP, Apache, etc.).
- Detección (si la hay) de parámetros vulnerables a inyección SQL.

```
~ > sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --batch
[!] 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 @ 09:01:53 /2025-09-30/
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 08:55 CEST
[09:01:53] [INFO] testing connection to the target URL
[09:01:55] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:01:55] [INFO] testing if the target URL content is stable
[09:01:56] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[09:01:56] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[09:01:56] [INFO] target URL content is stable
[09:01:56] [INFO] testing if GET parameter 'artist' is dynamic
[09:01:57] [INFO] GET parameter 'artist' appears to be dynamic
[09:01:57] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[09:01:57] [INFO] heuristic (XSS) test shows that GET parameter 'artist' might be vulnerable to cross-site scripting (XSS) attacks
[09:01:57] [INFO] testing for SQL injection on GET parameter 'artist'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
```

# https://qarmy.ar/webs-practicas-testing/

## WEB 1

nikto -h <https://practice-automation.com/>

```
~ > nikto -h https://practice-automation.com/ 2m 0s
- Nikto v2.5.0

+ Multiple IPs found: 192.0.78.231, 192.0.78.169
+ Target IP: 192.0.78.231
+ Target Hostname: practice-automation.com
+ Target Port: 443

+ SSL Info: Subject: /CN=tl.s.automattic.com
            Ciphers: TLS_AES_256_GCM_SHA384
            Issuer: /C=US/O=Let's Encrypt/CN=E8
+ Start Time: 2025-09-30 09:27:15 (GMT2)

+ Server: nginx
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Drupal Link header found with value: ARRAY(0x55d6876529f0). See: https://www.drupal.org/
+ /: Uncommon header 'x-hacker' found, with contents: Want root? Visit join.a8c.com and mention this header.
+ /: Uncommon header 'x-ac' found, with contents: 30.mad _atomic_ams HIT.
+ /: Uncommon header 'host-header' found, with contents: WordPress.com.
+ /: Uncommon header 'x-nananana' found, with contents: Batcache-Hit.
+ /: Uncommon header 'server-timing' found, with contents: a8c-cdn, dc;desc=mad, cache;desc=HIT;dur=2.0.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

### Hallazgos y observaciones

#### 1. Falta cabecera X-Frame-Options

- No está presente la cabecera anti-clickjacking, por lo que la página podría ser vulnerable a ataques de clickjacking.
- Más info: [X-Frame-Options - MDN](#)

#### 2. Cabecera Drupal Link con valor extraño:

- Se detectó un encabezado "Drupal Link" con valor ARRAY(0x559587e90900), lo cual parece un error o un valor no formateado correctamente.

#### 3. Headers poco comunes:

- server-timing: Contiene métricas internas de tiempo y estado (a8c-cdn, dc;desc=mad, cache;desc=STALE;dur=2.0).
- x-nananana: Valor Batcache-Hit. Probablemente relacionado con caché interna.
- x-ac: Valor 30.mad \_atomic\_ams STALE. Podría ser otra información interna o de caché.
- host-header: Valor WordPress.com.
- x-hacker: Valor curioso que dice:

"Want root? Visit join.a8c.com and mention this header."  
Esto es un "easter egg" o mensaje divertido dejado por los desarrolladores (Automatic/WordPress).

#### 4. Cabecera alt-svc anunciando HTTP/3:

- Indica que el servidor soporta HTTP/3 sobre QUIC, pero Nikto no puede analizar esta versión aún.

#### 5. Falta cabecera X-Content-Type-Options

- No está definida, lo que puede permitir que el navegador interprete contenido con tipos MIME incorrectos, aumentando riesgos de seguridad.

## whatweb <https://practice-automation.com/>

```
~ > whatweb https://practice-automation.com/  
https://practice-automation.com/ [200 OK] Country[UNITED STATES][US], HTML5, HTTPServer[nginx], IP[192.0.78.169], JQ  
uery[3.7.1], MetaGenerator[Site Kit by Google 1.162.1,WordPress Download Manager 3.3.24], Open-Graph-Protocol[websit  
e], Script[application/json,application/ld+json,importmap,module,speculationrules,text/javascript], Strict-Transport  
-Security[max-age=31536000], Title[Learn and Practice Automation | automateNow], UncommonHeaders[x-nananana,x-hacker  
,host-header,link,x-ac,alt-svc,server-timing], WordPress, nginx, x-hacker[Want root? Visit join.a8c.com and mention  
this header.]
```

Este sitio web:

- Está construido con **WordPress**, usando plugins de Google y gestión de descargas.
- Está alojado en **Estados Unidos**, con servidor **nginx**.
- Usa tecnologías web modernas (HTML5, JS moderno, SEO estructurado).
- Tiene medidas de seguridad activas (como HSTS).
- Está probablemente **alojado en WordPress.com o en servidores gestionados por Automattic** (por la cabecera x-hacker).



# WEB 2

nikto -h <http://globalsqa.com/demo-site>

```
~ > nikto -h http://globalsqa.com/demo-site
- Nikto v2.5.0

+ Multiple IPs found: 104.21.82.34, 172.67.193.202, 2606:4700:3030::ac43:c1ca, 2606:4700:3037::6815:5222
+ Target IP: 104.21.82.34
+ Target Hostname: globalsqa.com
+ Target Port: 80
+ Start Time: 2025-09-30 09:33:40 (GMT2)

+ Server: cloudflare
+ /demo-site/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /demo-site/: Uncommon header 'x-turbo-charged-by' found, with contents: LiteSpeed.
+ /demo-site/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /demo-site redirects to: https://globalsqa.com/demo-site/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 6 error(s) and 3 item(s) reported on remote host
+ End Time: 2025-09-30 09:36:44 (GMT2) (184 seconds)

+ 1 host(s) tested
```

🛡️ Vulnerabilidades y observaciones encontradas:

## 1. Falta el encabezado X-Frame-Options (anti-clickjacking)

- El servidor **no envía el header X-Frame-Options**, que es importante para proteger la web contra ataques de *clickjacking* (evitar que otros sitios embeban tu página en un iframe y hagan click fraudulento).
- Referencia: [MDN X-Frame-Options](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

## 2. Encabezado poco común x-turbo-charged-by con valor "LiteSpeed"

- Esto indica que se está usando tecnología o caché relacionada con **LiteSpeed** (un servidor web o sistema de caché/optimización). No es un problema grave, pero es una firma que puede ayudar a atacantes a saber qué tecnologías usas.

## 3. Falta el encabezado X-Content-Type-Options

- El servidor **no envía X-Content-Type-Options**, que es un header de seguridad para evitar que el navegador interprete el contenido con un tipo MIME diferente al declarado, previniendo ataques de tipo *MIME sniffing*.
- Esto puede facilitar ataques donde contenido malicioso se ejecute por error.
- Más info: [Netsparker Missing Content-Type Header](https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/)

## 4. Redirección detectada

- La página /demo-site redirige a <https://globalsqa.com/demo-site/> (como ya viste antes, HTTP → HTTPS y añadir barra final).

## whatweb http://globalsqa.com/demo-site

```
~ > whatweb http://globalsqa.com/demo-site
http://globalsqa.com/demo-site [301 Moved Permanently] Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], IP
[104.21.82.34], RedirectLocation[https://globalsqa.com/demo-site], Title[301 Moved Permanently][Title element contain
s newline(s)!], UncommonHeaders[nel,x-turbo-charged-by,cf-cache-status,report-to,cf-ray]
https://globalsqa.com/demo-site [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[cloudflare], IP[104.2
1.82.34], RedirectLocation[https://www.globalsqa.com/demo-site/], UncommonHeaders[x-redirect-by,x-litespeed-cache,ref
errer-policy,x-turbo-charged-by,cf-cache-status,nel,report-to,cf-ray]
https://www.globalsqa.com/demo-site/ [200 OK] Country[UNITED STATES][US], Google-Analytics[Universal][UA-67337609-1]
, HTML5, HTTPServer[cloudflare], IP[104.21.82.34], JQuery, MetaGenerator[Elementor 3.18.0; features: e_dom_optimizat
ion, e_optimized_assets_loading, e_optimized_css_loading, e_font_icon_svg, additional_custom_breakpoints, block_edit
or_assets_optimize, e_image_loading_optimization; settings: css_print_method-external, google_font-enabled, font_dis
play-swap,Site Kit by Google 1.158.0,WordPress 6.7.3], Open-Graph-Protocol[article], Script[application/json,applica
tion/ld+json,importmap,module,text/javascript], Title[Demo Testing Site - GlobalsQA], UncommonHeaders[link,x-litespe
ed-cache,nel,referrer-policy,x-turbo-charged-by,report-to,cf-cache-status,cf-ray], WordPress[6.7.3]
```

Resumen global de esta cadena:

- **La URL inicial sin HTTPS redirige a la versión segura (HTTPS).**
- Luego la versión sin www redirige a la versión con www y barra final, por temas de SEO y consistencia.
- La versión final con HTTPS y www entrega el contenido.
- Está alojado detrás de **Cloudflare** para protección y aceleración.
- Usa **WordPress + Elementor + varios plugins para optimización y analítica.**
- Está bien configurado para redes sociales (Open Graph).
- Usa caché y políticas de seguridad modernas.

# WEB 3

## nikto -h <https://qa-practice.netlify.app/bugs-form>

```
~ > nikto -h https://qa-practice.netlify.app/bugs-form 3m 15s
- Nikto v2.5.0

+ Multiple IPs found: 35.157.26.135, 63.176.8.218, 2a05:d014:58f:6200::258, 2a05:d014:58f:6200::259
+ Target IP: 35.157.26.135
+ Target Hostname: qa-practice.netlify.app
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Netlify, Inc/CN=*.netlify.app
           Ciphers: TLS_AES_128_GCM_SHA256
           Issuer: /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
+ Start Time: 2025-09-30 09:38:40 (GMT2)

+ Server: Netlify
+ /bugs-form/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /bugs-form/: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/
+ /bugs-form/: Uncommon header 'cache-status' found, with contents: "Netlify Edge"; fwd=miss.
+ /bugs-form/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /bugs-form redirects to: /bugs-form
```

### SSL/TLS

- Certificado válido para \*.netlify.app
- Cifrado: TLS\_AES\_128\_GCM\_SHA256 (TLS 1.3)
- Emisor: DigiCert Global G2 TLS RSA SHA256 2020 CA1 (entidad confiable)

### Hallazgos y observaciones

#### 1. Falta cabecera X-Frame-Options en /bugs-form

- No está presente, lo que puede dejar la página vulnerable a ataques de clickjacking.
- Más info: [X-Frame-Options - MDN](#)

#### 2. Cabecera poco común cache-status con valor "Netlify Edge"; fwd=miss

- Indica que el contenido fue servido directamente desde el borde de Netlify y no desde caché.

#### 3. Falta la cabecera X-Content-Type-Options en /bugs-form

- Esto puede permitir que el navegador interprete mal el tipo MIME y abra la puerta a vulnerabilidades.
- Más info: [Missing Content-Type Header - Netsparker](#)

#### 4. La ruta raíz /bugs-form redirige a sí misma

- Posible configuración de redirección que puede generar bucles o problemas si no está controlada.

## whatweb <https://qa-practice.netlify.app/bugs-form>

```
~ > whatweb https://qa-practice.netlify.app/bugs-form 16s
https://qa-practice.netlify.app/bugs-form [200 OK] Bootstrap[4.1.0], Country[UNITED STATES][US], HTML5, HTTPServer[Netlify], IP[63.176.8.218], Script[text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[QA Practice | Learn with RV], UncommonHeaders[cache-status,x-nf-request-id], X-UA-Compatible[IE=edge]
```



# WEB 4

**nikto -h <https://www.lambdatest.com/selenium-playground/>**

```
~ > nikto -h https://www.lambdatest.com/selenium-playground/
- Nikto v2.5.0

+ Multiple IPs found: 104.18.4.65, 104.18.5.65, 2a05:d014:58f:6200::259, 2a05:d014:58f:6200::258
+ Target IP: 104.18.4.65
+ Target Hostname: www.lambdatest.com
+ Target Port: 443

+ SSL Info: Subject: /CN=lambdatest.com
Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=Thawte TLS RSA CA G1
+ Start Time: 2025-09-30 09:39:29 (GMT2)

+ Server: cloudflare
+ /selenium-playground/: Retrieved via header: 1.1 68fbda872a4e92e0774a97bdd960d43a.cloudfront.net (CloudFront).doca
+ /selenium-playground/lgvnFd1g.it: Uncommon header 'x-amz-error-code' found, with contents: NoSuchKey.
+ /selenium-playground/lgvnFd1g.it: Uncommon header 'x-amz-error-detail-key' found, with contents: selenium-playgrou
nd/lgvnFd1g.it.
+ /selenium-playground/lgvnFd1g.it: Uncommon header 'cache-status' found, with contents: 'Netlify Edge'; fwd=miss.
+ /selenium-playground/lgvnFd1g.it: Uncommon header 'x-amz-error-message' found, with contents: The specified key do
es not exist.
+ /selenium-playground/lgvnFd1g.it: Uncommon header 'x-amz-error-message' found, with contents: The specified key do
es not exist.
```

## SSL/TLS

- Certificado válido para lambdatest.com
- Cifrado fuerte: TLS\_AES\_256\_GCM\_SHA384 (TLS 1.3)
- Emisor: DigiCert (entidad certificadora confiable)

## Observaciones y hallazgos importantes

- **Cabecera Via indica que detrás del servidor hay un CDN CloudFront (Amazon).**
- En la ruta /selenium-playground/lgvnFd1g.it se encontraron varios encabezados poco comunes relacionados con errores de Amazon S3:
  - x-amz-error-code: NoSuchKey
  - x-amz-error-detail-key: selenium-playground/lgvnFd1g.it
  - x-amz-error-message: The specified key does not exist.

Esto significa que Nikto intentó acceder a un recurso (archivo) en un bucket S3 que no existe o fue eliminado.

**whatweb <https://www.lambdatest.com/selenium-playground/>**

```
~ > whatweb https://www.lambdatest.com/selenium-playground/
https://www.lambdatest.com/selenium-playground/ [200 OK] Country[UNITED STATES][US], Frame, HTML5, HTTPServer[cloudf
lare], IP[104.18.5.65], Open-Graph-Protocol[website], Script[application/json], Strict-Transport-Security[max-age=31
536000; includeSubDomains; preload], Title[Selenium Grid Online | Run Selenium Test On Cloud], UncommonHeaders[x-amz
-cf-pop,x-amz-cf-id,referrer-policy,permissions-policy,content-security-policy,cf-cache-status,x-content-type-option
s,cf-ray], Via-Proxy[1.1 68fbda872a4e92e0774a97bdd960d43a.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN]
```

# WEB 5

nikto -h <http://uitestingplayground.com/>

```
~ > nikto -h http://uitestingplayground.com/ -pp.com/
- Nikto v2.5.0 - demo-cura.herokuapp.com/ [200 OK] Bootstrap[3.3.7], Cookies[PHPSESSID], Country[UNITED STATES][US],
+ Target IP: UncommonHe52.234.209.94 [rt-to,reporting-endpoints], Via-Proxy[1.1 heroku-router], X-UA-Compatible[IE=edge]
+ Target Hostname: uitestingplayground.com
+ Target Port: 80
+ Start Time: 2025-09-30 09:40:42 (GMT2)

+ Server: Microsoft-IIS/10.0
+ /: Retrieved x-powered-by header: Express, ASP.NET.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 1 error(s) and 3 item(s) reported on remote host
+ End Time: 2025-09-30 09:43:07 (GMT2) (145 seconds)

+ 1 host(s) tested
```

## Vulnerabilidades y observaciones:

### 1. Encabezado x-powered-by detectado

- La página devuelve la cabecera x-powered-by con valores **Express** y **ASP.NET**.
- Esto indica qué tecnologías/frameworks están en uso, algo que en términos de seguridad es mejor ocultar para no dar pistas a posibles atacantes.

### 2. Falta el encabezado anti-clickjacking X-Frame-Options

- El servidor **no envía el header X-Frame-Options**, lo que significa que el sitio es vulnerable a ataques de *clickjacking*.
- [Referencia](#)

### 3. Falta el encabezado X-Content-Type-Options

- No se ha configurado X-Content-Type-Options, que previene que los navegadores interpreten incorrectamente los tipos MIME.
- Esto podría permitir ejecución de contenido malicioso.
- Más info: [Netsparker sobre este header](#)

### 4. No se encontraron directorios CGI

- No se detectaron directorios CGI expuestos (normalmente usados para scripts, pueden ser un vector de ataque).

whatweb <http://uitestingplayground.com/>

```
~ > whatweb http://uitestingplayground.com/
http://uitestingplayground.com/ [200 OK] Bootstrap[4.0.0], Cookies[ARRAffinity], Country[UNITED STATES][US], HTML5,
HTTPServer[Microsoft-IIS/10.0], HttpOnly[ARRAffinity], IP[52.234.209.94], JQuery[3.2.1], Microsoft-Azure, Microsoft-
IIS[10.0], Script, Title[UI Test Automation Playground], X-Powered-By[Express, ASP.NET]
```

# WEB 6

## nikto -h <https://letcode.in/test>

```
~ > nikto -h https://letcode.in/test
- Nikto v2.5.0
+ Multiple IPs found: 63.176.8.218, 35.157.26.135, 2a05:d014:58f:6200::259, 2a05:d014:58f:6200::258 Strict-Transport
+ Target/IP: x-age=31536000 63.176.8.218 Learn and Practice Automation | automatenow], UncommonHeaders[x-nananana,x-hacker
+ Target Hostname: x-letcode.inserver-timing], WordPress, nginx, x-hacker[Want root? Visit join.a8c.com and mention
+ Target Port: 443

+ SSL Info: http: Subject: /CN=letcode.in
+ Nikto v2.5.0 Ciphers: TLS_AES_128_GCM_SHA256
+ Issuer: /C=US/O=Let's Encrypt/CN=E5
+ Start Time: found: 2025-09-30 09:44:12 (GMT2)02, 2606:4700:3030::ac43:c1ca, 2606:4700:3037::6815:5222

+ Server: Netlify global.sga.com
+ /test/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs
/Web/HTTP/Headers/X-Frame-Options
+ /test/: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/
+ /test/: Uncommon header 'cache-status' found, with contents: "Netlify Edge"; fwd=miss.
+ /test/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabili
ties/missing-content-type-header/
+ turbo-charged-by: found, with contents: LiteSpeed.
```

### Información SSL/TLS:

#### • Certificado SSL:

- Common Name (CN): letcode.in
- Cifrado: TLS\_AES\_128\_GCM\_SHA256 (protocolo TLS 1.3 seguro)
- Emisor: Let's Encrypt (certificado gratuito y confiable)

### Vulnerabilidades y observaciones:

#### 1. Falta el encabezado anti-clickjacking X-Frame-Options

- No está presente en la ruta /test/, dejando la web vulnerable a ataques de clickjacking.
- Más info: [X-Frame-Options - MDN](#)

#### 2. Encabezado poco común cache-status detectado

- Valor: "Netlify Edge"; fwd=miss — indica el estado de la cache en la CDN de Netlify (se indica que no había contenido cacheado en el borde).
- Esto es típico y normal para una CDN.

#### 3. Falta el encabezado X-Content-Type-Options

- No está configurado, lo que puede permitir a los navegadores interpretar el contenido con un tipo MIME diferente al esperado, potencialmente causando problemas de seguridad.
- Más info: [Missing Content-Type Header - Netsparker](#)

#### 4. Netlify identificado mediante x-nf-request-id

- Este header es un identificador único de la petición en la infraestructura de Netlify.

## whatweb <https://letcode.in/test>

```
~ > whatweb https://letcode.in/test
https://letcode.in/test [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Netlify], IP[35.157.26.135],
RedirectLocation[/test/], Strict-Transport-Security[max-age=31536000], Title[Document moved], UncommonHeaders[cache-
status,x-nf-request-id]
https://letcode.in/test/ [200 OK] Country[UNITED STATES][US], HTML5, HTTPServer[Netlify], IP[35.157.26.135], Open-Gr
aph-Protocol, Script[application/json,module,text/javascript], Strict-Transport-Security[max-age=31536000], Title[Wo
rkspace | LetCode with Koushik], UncommonHeaders[cache-status,x-nf-request-id]
```

# WEB 7

nikto -h <https://thinking-tester-contact-list.herokuapp.com/>

```
~ > nikto -h https://thinking-tester-contact-list.herokuapp.com/
- Nikto v2.5.0 e-automation.com [200 OK] Country[UNITED STATES][US], HTML5, HTTPServer[nginx], IP[192.0.78.169], J
+ Multiple IPs found: 3.229.186.102, 3.210.192.5, 54.146.248.82, 54.83.6.65
+ 0 host(s) tested: -ac,alt-svc,server-timing], WordPress, nginx, x-hacker[Want root? Visit join.a8c.com and mention
this header.]
~ > nikto -h https://thinking-tester-contact-list.herokuapp.com/
- Nikto v2.5.0 http://globalsqa.com/demo-site
+ Multiple IPs found: 54.146.248.82, 3.229.186.102, 54.83.6.65, 3.210.192.5
+ Target IP: 54.146.248.82
+ Target Hostname: thinking-tester-contact-list.herokuapp.com
+ Target Port: 443
+ SSL Info: Subject: /CN=*.herokuapp.com
Ciphers: ECDHE-RSA-AES128-GCM-SHA256
Server: cloudflare Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M02
+ Start Time: 2025-09-30 09:52:01 (GMT2)
+ Server: Heroku
+ /: Retrieved via header: 1.1 heroku-router
+ /: Retrieved x-powered-by header: Express
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'reporting-endpoints' found, with contents: heroku-nel="https://nel.heroku.com/reports?s=KquzOf
wXKj%2Bq1RimA8b456%2B%2F%2BvYokhzUMrWbjQfCtOM%3D&sid=af571f24-03ee-46d1-9f90-ab9030c2c74c&ts=1759218723".
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

## 🔒 Información SSL/TLS:

### • Certificado SSL:

- Common Name (CN): \*.herokuapp.com (certificado comodín para herokuapp.com)
- Cifrado usado: ECDHE-RSA-AES128-GCM-SHA256 (seguro)
- Emisor: Amazon RSA 2048 M02

## 🛡️ Vulnerabilidades y observaciones:

### 1. Encabezado x-powered-by detectado

- Valor: **Express** (framework Node.js).
- Esto revela tecnología usada, que es preferible ocultar por seguridad.

### 2. Falta el encabezado anti-clickjacking X-Frame-Options

- No está presente, lo que expone a riesgos de clickjacking.
- [Más info](#)

### 3. Encabezado poco común reporting-endpoints encontrado

- Contiene: heroku-nel="https://nel.heroku.com/reports?s=..."
- Esto está relacionado con Network Error Logging (NEL), para monitorizar errores de red en clientes.

### 4. No se definió la cabecera Strict-Transport-Security (HSTS)

- Esta cabecera obliga a los navegadores a usar siempre HTTPS.
- Su ausencia es una debilidad en la política de seguridad HTTPS.
- [Más info](#)

## 5. Falta el encabezado X-Content-Type-Options

- No está configurado el header para evitar que el navegador interprete contenido con un tipo MIME diferente al declarado.
- Esto puede facilitar ataques de ejecución de contenido malicioso.
- [Más info](#)

**whatweb https://thinking-tester-contact-list.herokuapp.com/**

```
~ > whatweb https://thinking-tester-contact-list.herokuapp.com/  
https://thinking-tester-contact-list.herokuapp.com/ [200 OK] Country[UNITED STATES][US], HTML5, HTTPServer[Heroku],  
IP[3.229.186.102], PasswordField, Script, Title[Contact List App], UncommonHeaders[nel,report-to,reporting-endpoints  
1. Via-Proxy[1.1.heroku-router]. X-Powered-By[Express]
```



# WEB 8

nikto -h <https://katalon-demo-cura.herokuapp.com/>

```
~ > nikto -h https://katalon-demo-cura.herokuapp.com/ground/
- Nikto v2.5.0

+ Multiple IPs found: 54.205.8.205, 18.211.231.38, 174.129.128.48, 54.235.77.118
+ Target IP: 54.205.8.205
+ Target Hostname: katalon-demo-cura.herokuapp.com
+ Target Port: 443

+ SSL Info: Subject: /CN=*.herokuapp.com
Ciphers: ECDHE-RSA-AES128-GCM-SHA256
Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M03.com/CN=Thawte TLS RSA CA G1
+ Start Time: 2025-09-30 09:44:41 (GMT2)

+ Server: Heroku/are
+ /: Retrieved via header: 1.1 heroku-router.: 1.1 68fnda872a4e92e8774a97hdd968d43a.cloudflare.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie PHPSESSID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'Heroku' to 'heroku-router'.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
```

## 🔒 Información SSL/TLS:

### • Certificado SSL:

- Common Name (CN): \*.herokuapp.com
- Cifrado: ECDHE-RSA-AES128-GCM-SHA256 (seguro)
- Emisor: Amazon RSA 2048 M03

## 🛡️ Vulnerabilidades y observaciones:

### 1. Falta el encabezado anti-clickjacking X-Frame-Options

- El sitio no envía esta cabecera, lo que expone a ataques de *clickjacking*.
- Más info: [X-Frame-Options - MDN](#)

### 2. Encabezado poco común reporting-endpoints detectado

- Contiene enlace para Network Error Logging (NEL) de Heroku, útil para monitoreo de errores.

### 3. No está configurada la cabecera Strict-Transport-Security (HSTS)

- La ausencia de HSTS implica que los navegadores no están forzados a usar HTTPS siempre, lo que puede facilitar ataques de tipo downgrade o man-in-the-middle.
- Más info: [Strict-Transport-Security - MDN](#)

### 4. Falta el encabezado X-Content-Type-Options

- Sin este header, el navegador puede interpretar contenido con tipos MIME incorrectos, facilitando ataques.
- Más info: [Netsparker Missing Content-Type Header](#)

## 5. Cookies PHPSESSID sin flags secure y httponly

- La cookie de sesión PHP (PHPSESSID) se crea sin el flag Secure, lo que implica que puede enviarse por HTTP en lugar de solo HTTPS, aumentando el riesgo de interceptación.
- Tampoco tiene el flag HttpOnly, que previene acceso a la cookie vía JavaScript (evitando ataques XSS).
- Más info:
  - [Secure flag - MDN](#)
  - [HttpOnly flag - MDN](#)

## 6. No se encontraron directorios CGI

- Esto es positivo, ya que no se detectaron posibles puntos de ejecución de scripts CGI vulnerables.

## 7. Cambio en el banner del servidor

- El banner cambió de 'Heroku' a 'heroku-router', lo que indica una capa de proxy/redirect en la infraestructura.

**whatweb https://katalon-demo-cura.herokuapp.com/**

```
~ > whatweb https://katalon-demo-cura.herokuapp.com/ [200 OK] Bootstrap[3.3.7], Cookies[PHPSESSID], Country[UNITED STATES][US],  
https://katalon-demo-cura.herokuapp.com/ [200 OK] Bootstrap[3.3.7], Cookies[PHPSESSID], Country[UNITED STATES][US],  
Email[info@katalon.com], HTML5, HTTPServer[Heroku], IP[174.129.128.48], JQuery[1.11.3], Script, Title[CURA Healthcar  
e Service], UncommonHeaders[nel,report-to,reporting-endpoints], Via-Proxy[1.1 heroku-router], X-UA-Compatible[IE=edg  
e]Target IP: 104.18.4.65
```



## 6. Drupal Link header encontrado:

- En la ruta /xpath-practice-page/qg5O3P22.dbm aparece un header Link que apunta a: <https://selectorshub.com/wp-json/> con relación a la API de WordPress (similar a Drupal).
- Esto puede dar pistas sobre la tecnología usada (WordPress con REST API activa).

**whatweb https://selectorshub.com/xpath-practice-page/**

```
~ > whatweb https://selectorshub.com/xpath-practice-page/
https://selectorshub.com/xpath-practice-page/ [200 OK] Country[UNITED STATES][US], Email[support@selectorshub.com],
Frame, HTML5, HTTPServer[LiteSpeed], IP[66.29.141.6], JQuery[3.7.1], LiteSpeed, MetaGenerator[Elementor 3.32.2; feat
ures: e_font_icon_svg, additional_custom_breakpoints; settings: css_print_method-internal, google_font-enabled, font
_display-swap, Site Kit by Google 1.162.1, WordPress 6.8.2], Open-Graph-Protocol[article], PasswordField[Password], Sc
ript[application/ld+json, rocketlazyloadscript, speculationrules, text/javascript], Title[Xpath Practice Page | Shadow
dom, nested shadow dom, iframe, nested iframe and more complex automation scenarios.], UncommonHeaders[x-turbo-charg
ed-by], WordPress[6.8.2]
```

# WEB 10

nikto -h <https://practicesoftwaretesting.com/#/>

```
~ > nikto -h https://practicesoftwaretesting.com/#/
- Nikto v2.5.0 - automation.com/ [200 OK] Country[UNITED STATES][US], HTML5, HTTPServer[nginx], IP[192.8.78.169], JQ
+ Multiple IPs found: 172.67.160.144, 104.21.9.144, 2606:4700:3035::ac43:a090, 2606:4700:3037::6815:990 [ct-Transport
+ Target IP: x-age=3153172.67.160.144 Earn and Practice Automation | automateNow], UncommonHeaders[x-nananana,x-hacker
+ Target Hostname: x-acpracticesoftwaretesting.comrdPress, nginx, x-hacker[Want root? Visit join.a8c.com and mention
+ Target Port: 443

+ SSL Info: http: Subject: /CN=practicesoftwaretesting.com
- Nikto v2.5.0 Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Google Trust Services/CN=WE1
+ Start Time: Found: 2025-09-30 09:47:47 (GMT2)82, 2606:4700:3038::ac43:c1ca, 2606:4700:3037::6815:5222

+ Server: cloudflare globalssl.com
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/
HTTP/Headers/X-Frame-Options9-30 09:53:00 (GMT2)
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.
org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is:':443'. Nikto cannot test HTTP/3 over
QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
missing-content-type-header/shion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulner
```

## 🔒 Información SSL/TLS:

### • Certificado SSL:

- Common Name (CN): practicesoftwaretesting.com
- Cifrado: TLS\_AES\_256\_GCM\_SHA384 (TLS 1.3, seguro)
- Emisor: Google Trust Services (entidad confiable)

## 🛡️ Vulnerabilidades y observaciones:

### 1. Falta la cabecera anti-clickjacking X-Frame-Options

- No presente, lo que puede dejar la web vulnerable a ataques de clickjacking.
- Más info: [X-Frame-Options - MDN](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

### 2. Falta el encabezado Strict-Transport-Security (HSTS)

- No está configurado, lo que puede facilitar ataques de tipo man-in-the-middle o downgrade de HTTPS.
- Más info: [Strict-Transport-Security - MDN](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

### 3. Se detectó encabezado alt-svc anunciando HTTP/3

- El sitio anuncia soporte para HTTP/3 en el puerto 443. Nikto no puede escanear HTTP/3 por limitaciones técnicas.
- Más info: [alt-svc header - MDN](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc)

### 4. Falta la cabecera X-Content-Type-Options

- Sin esta cabecera, el navegador podría interpretar mal el tipo MIME del contenido, lo que puede abrir la puerta a vulnerabilidades.
- Más info: [Missing Content-Type Header - Netsparker](https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/)

whatweb <https://practicesoftwaretesting.com/#/>

```
~ > whatweb https://practicesoftwaretesting.com/#/
https://practicesoftwaretesting.com/#/ [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[cloudflare], IP[172.67.160.144], Open-Graph-Protocol, Script[module], Title[Practice Software Testing - Toolshop - v5.0], UncommonHeaders[cf-cache-status,nel,report-to,cf-ray,alt-svc] ..0.00
```