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.

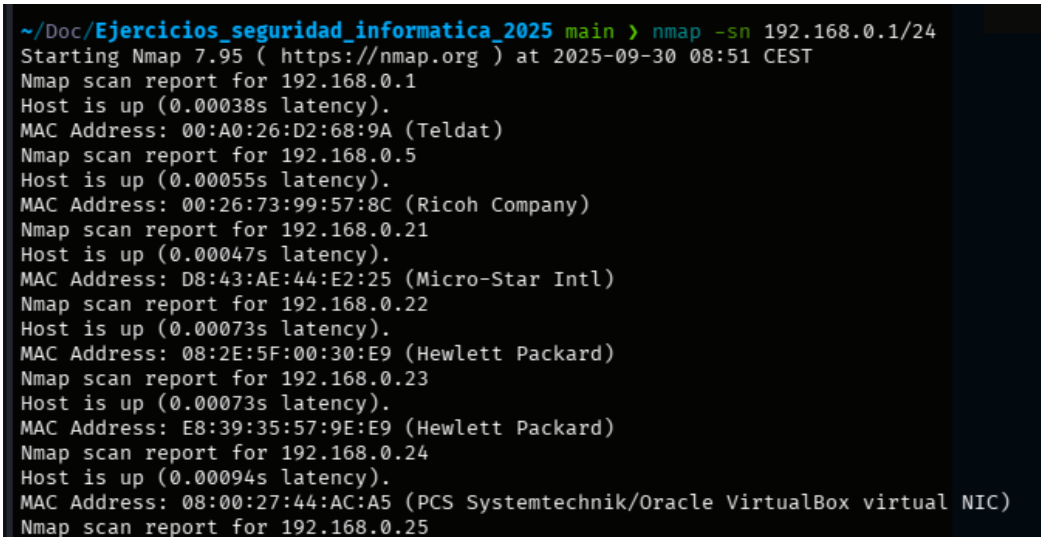
Material necesario

- 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:

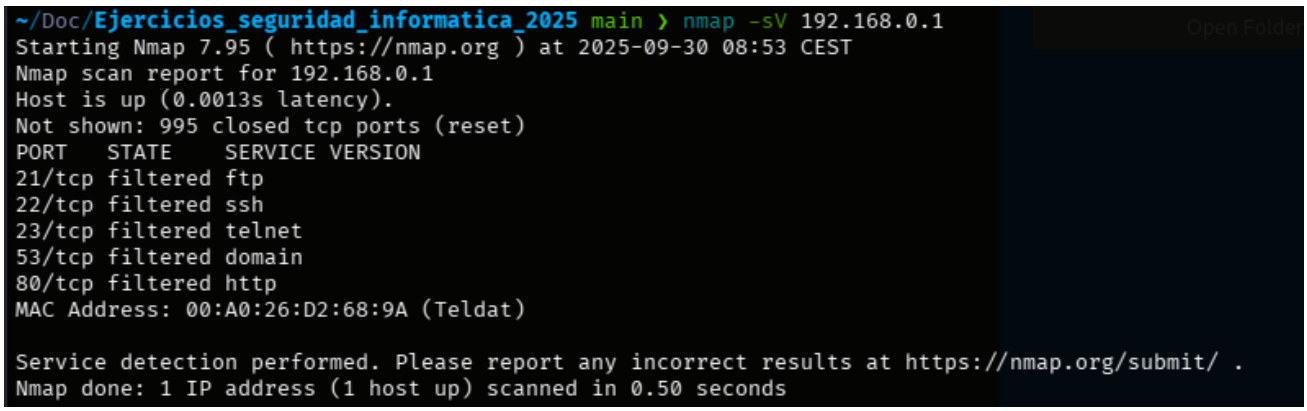
   ### nmap -sn 192.168.1.0/24



(ajusta el rango según la red del aula).

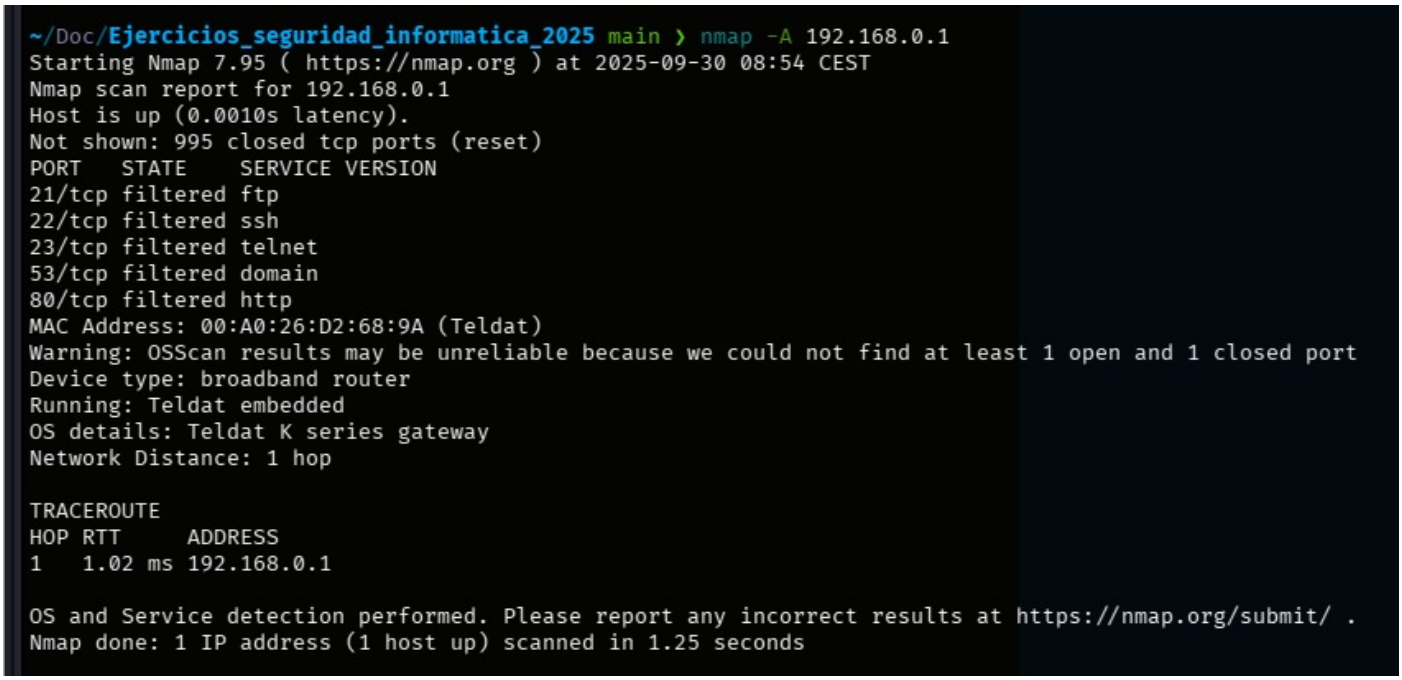
2. Elige un host detectado (por ejemplo, la IP 192.168.1.20) y haz un escaneo de puertos:

   ### nmap -sV 192.168.1.20



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

   nmap -A 192.168.1.20



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:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-09-30 08:59:39 (GMT2)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /EGAxqvVr.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
+ /EGAxqvVr.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-96B8-444553540000], 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-96B8-444553540000], 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

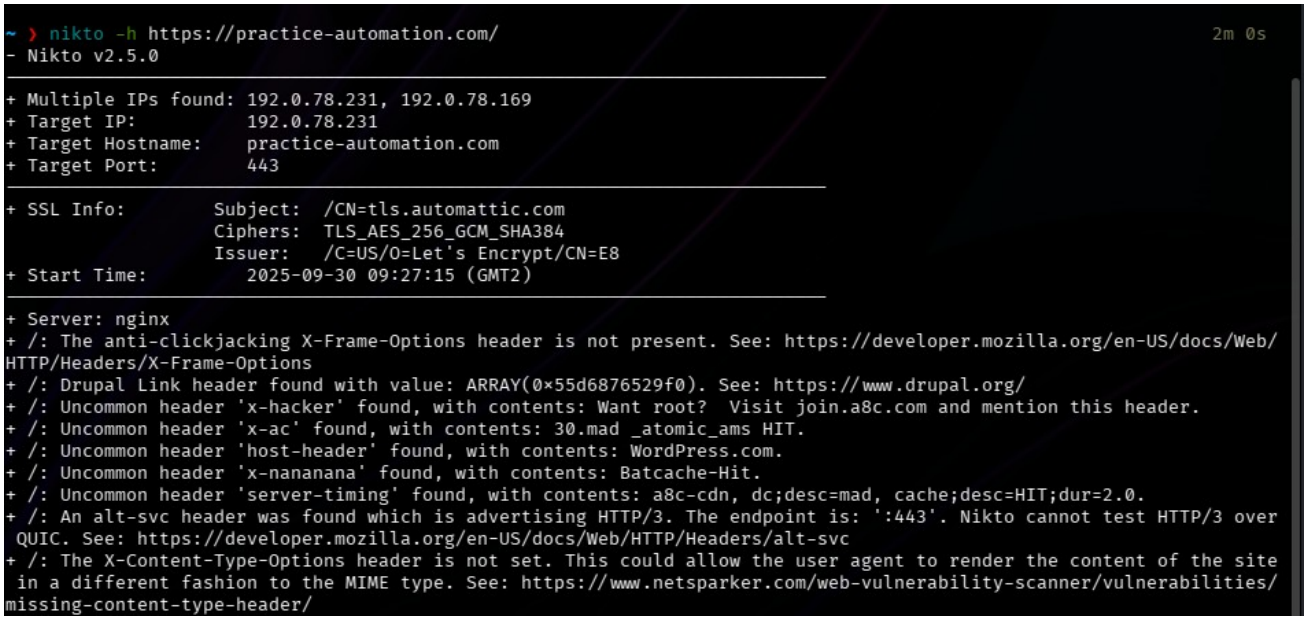
- Informe de posibles vulnerabilidades (cabeceras inseguras, directorios ocultos, configuraciones por defecto).
- Identificación de tecnologías utilizadas en la web (PHP, Apache, etc.).
- Detección (si la hay) de parámetros vulnerables a inyección SQL.

```
~ ❯ sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --batch                    1m 22s
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.9#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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/
[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/

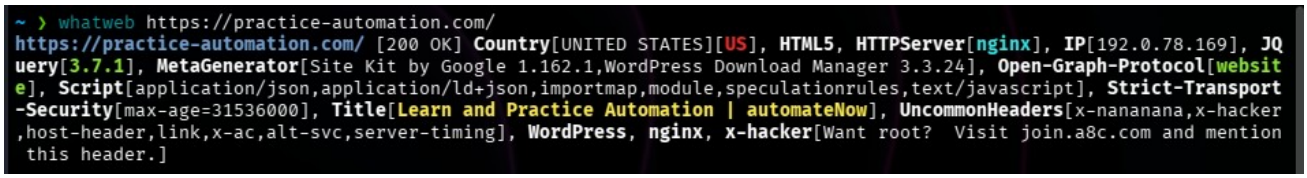


Hallazgos y observaciones

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 (Automattic/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/

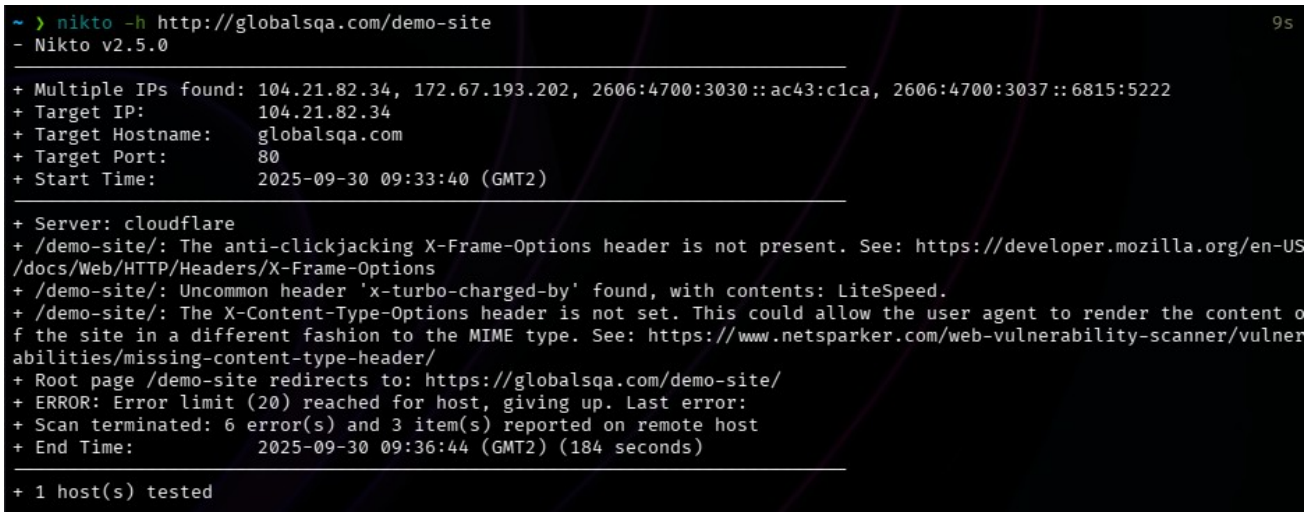


Este sitio web:

- 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



🛡️ 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
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
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

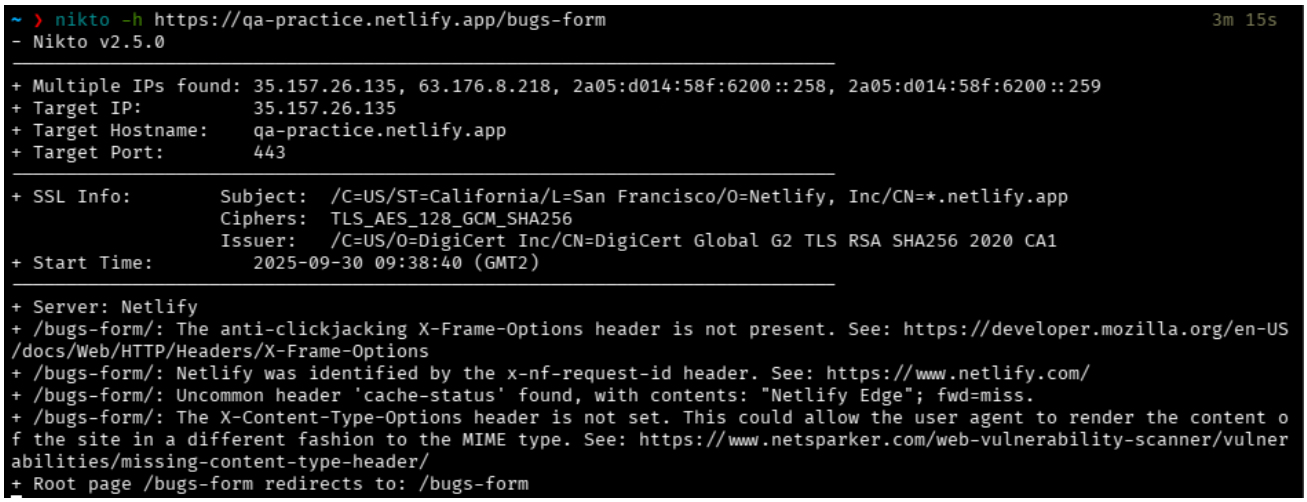
```
~ ❯ whatweb http://globalsqa.com/demo-site
http://globalsqa.com/demo-site [301 Moved Permanently] Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], IP
[104.21.82.34], RedirectLocation[https://globalsqa.com/demo-site], Title[301 Moved Permanently][Title element contai
ns newline(s)!], UncommonHeaders[nel,x-turbo-charged-by,cf-cache-status,report-to,cf-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,re
ferrer-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



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)

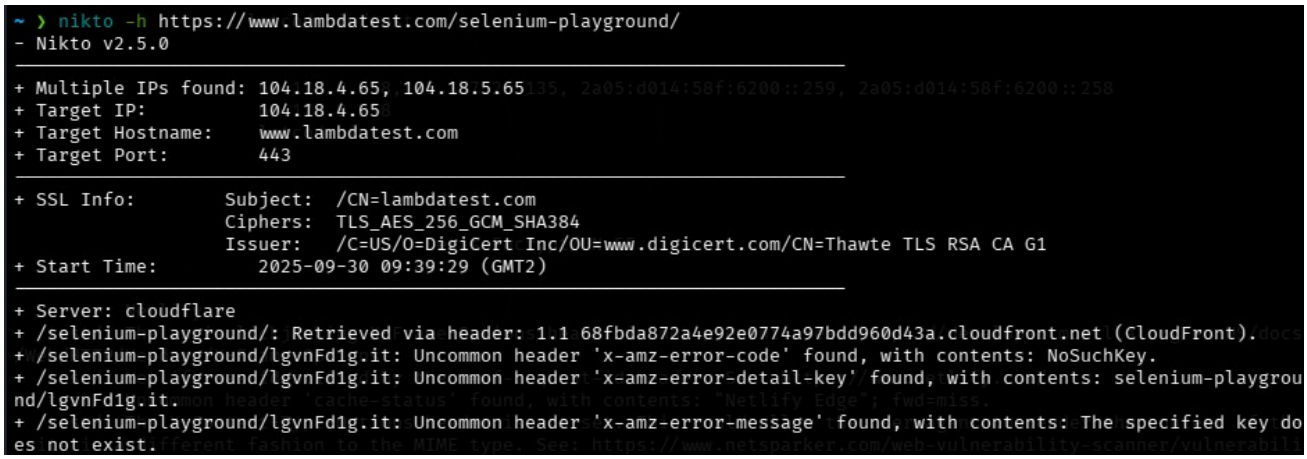
Hallazgos y observaciones

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

WEB 4

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



SSL/TLS

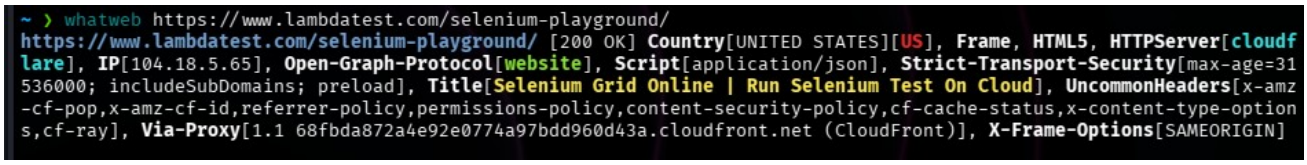
- Certificado válido para lambdatest.com
- Cifrado fuerte: TLS_AES_256_GCM_SHA384 (TLS 1.3)
- Emisor: DigiCert (entidad certificadora confiable)

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.

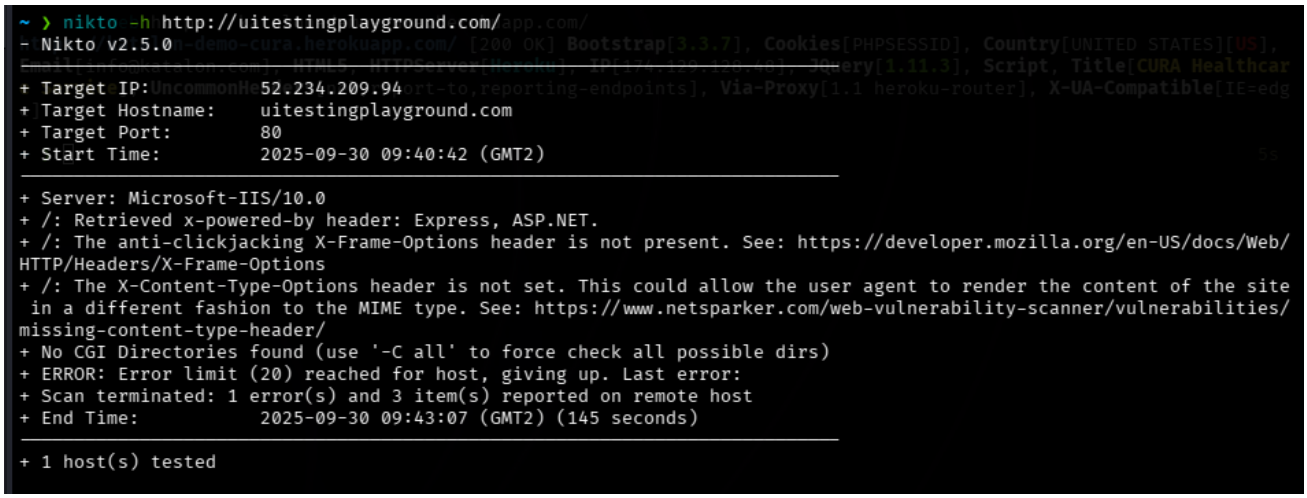
Esto significa que Nikto intentó acceder a un recurso (archivo) en un bucket S3 que no existe o fue eliminado.

whatweb https://www.lambdatest.com/selenium-playground/



WEB 5

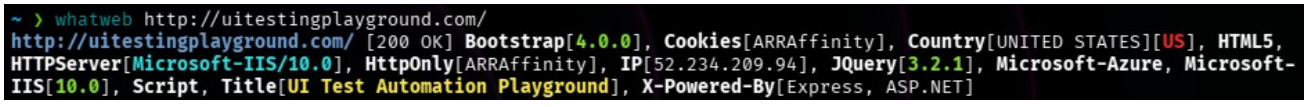
nikto -h http://uitestingplayground.com/



🛡️ Vulnerabilidades y observaciones:

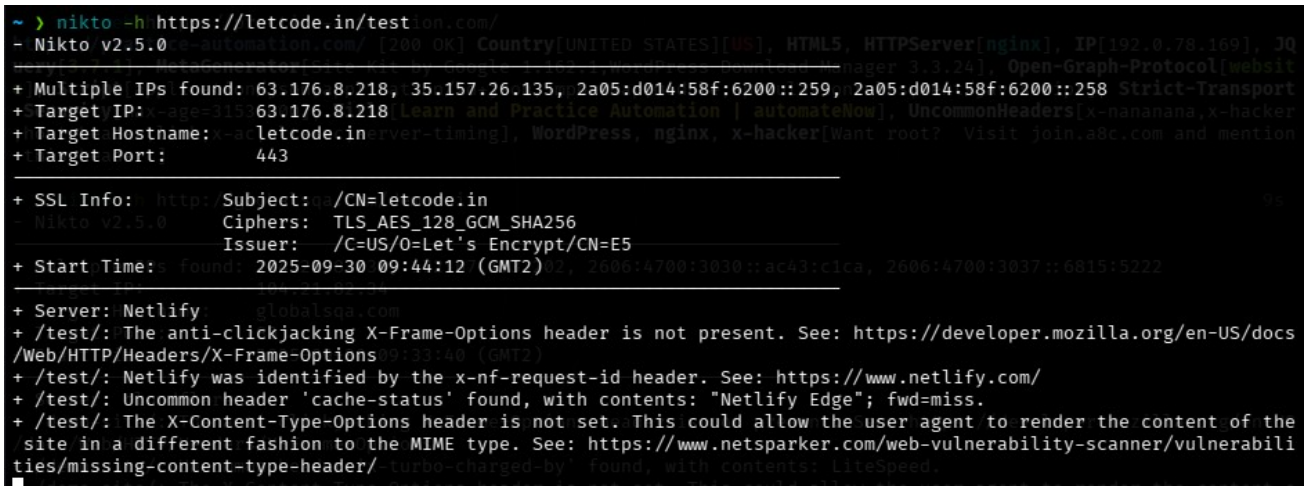
1. **Encabezado x-powered-by detectado**
   - La página devuelve la cabecera x-powered-by con valores **Express** y **ASP.NET**.
   - Esto indica qué tecnologías/frameworks están en uso, algo que en términos de seguridad es mejor ocultar para no dar pistas a posibles atacantes.
2. **Falta el encabezado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



WEB 6

nikto -h https://letcode.in/test



🔐 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)

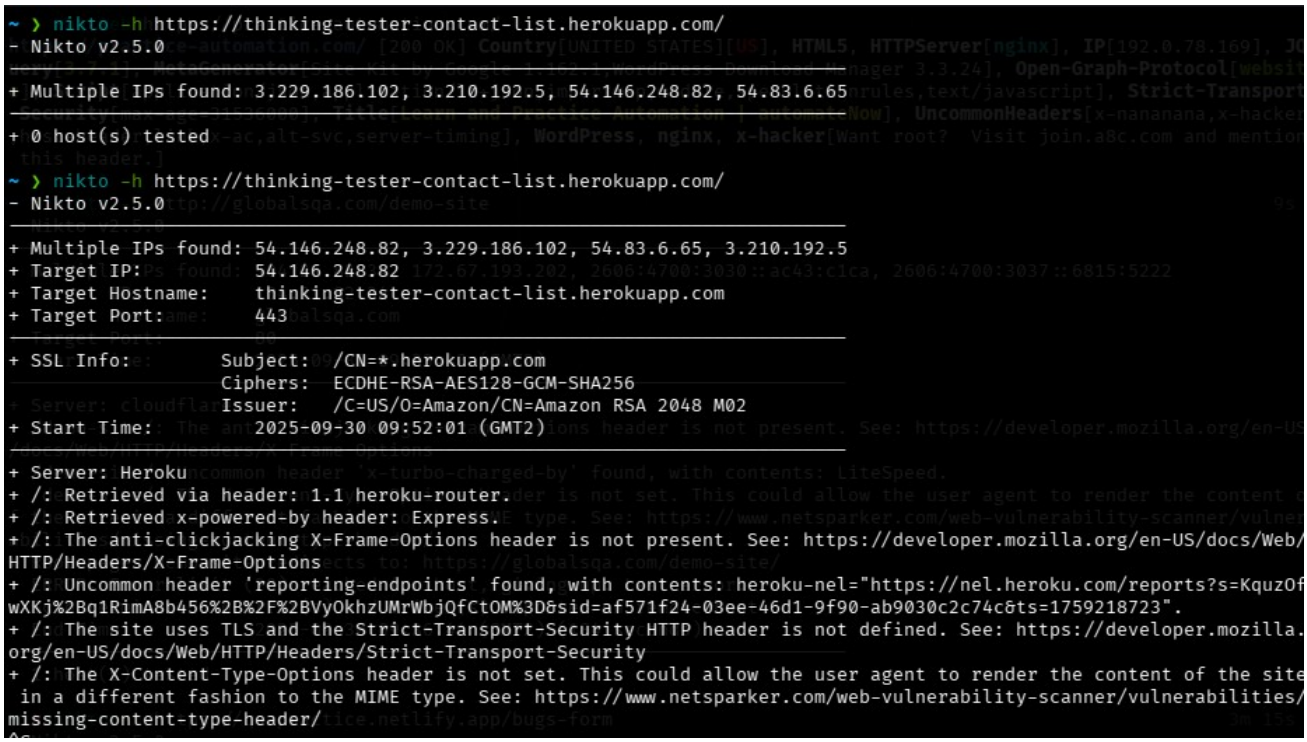
🛡️ Vulnerabilidades y observaciones:

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

WEB 7

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



🔐 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:

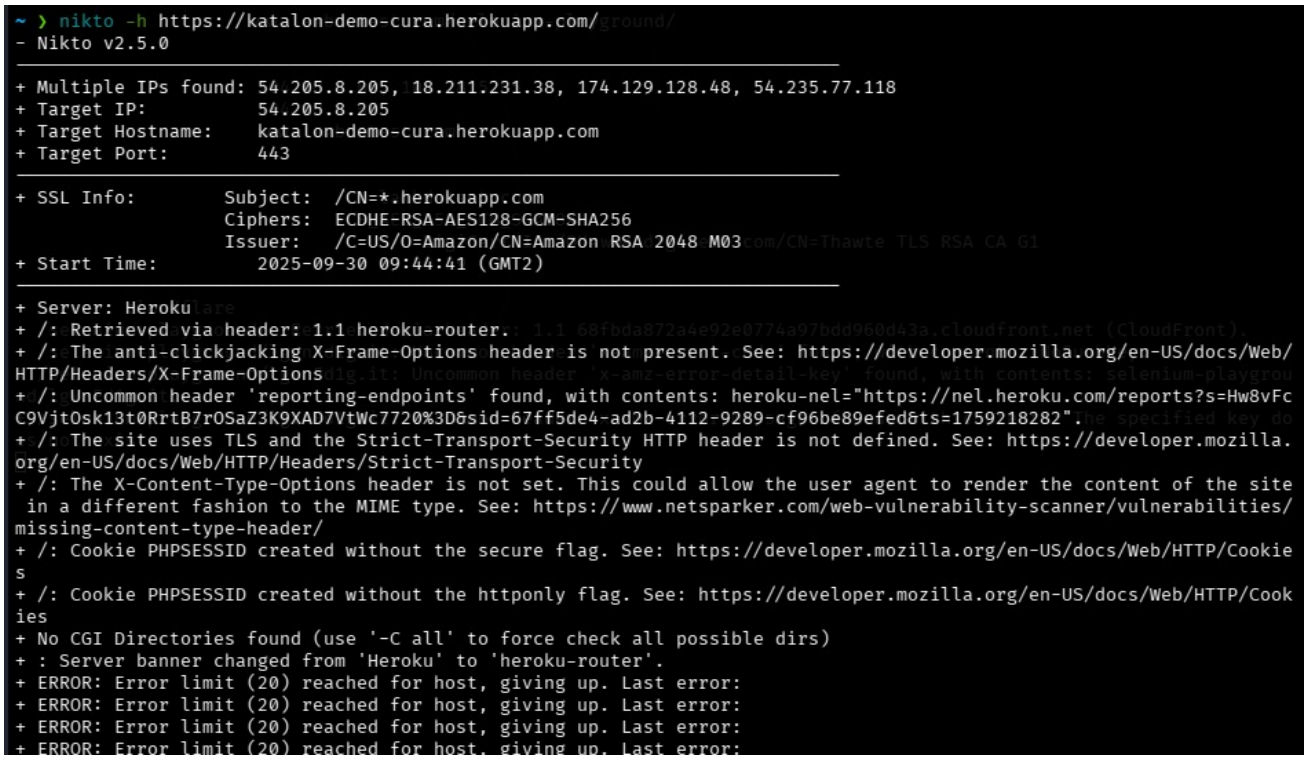
1. **Encabezado x-powered-by detectado**
   - Valor: **Express** (framework Node.js).
   - Esto revela tecnología usada, que es preferible ocultar por seguridad.
2. **Falta el encabezado anti-clickjacking X-Frame-Options**
   - No está presente, lo que expone a riesgos de clickjacking.
   - Más info
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/

WEB 8

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



🔐 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:

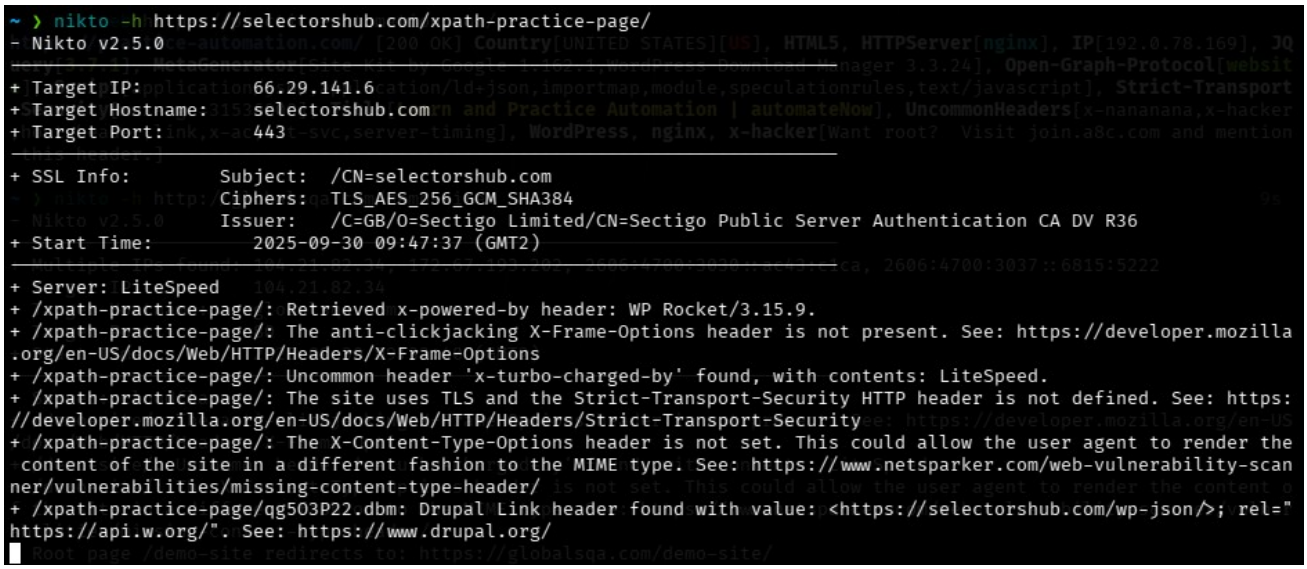
1. **Falta el encabezado anti-clickjacking X-Frame-Options**
   - El sitio no envía esta cabecera, lo que expone a ataques de *clickjacking*.
   - Más info: X-Frame-Options - MDN
2. **Encabezado poco común reporting-endpoints detectado**
   - Contiene enlace para Network Error Logging (NEL) de Heroku, 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/

WEB 9

nikto -h https://selectorshub.com/xpath-practice-page/



🔐 Información SSL/TLS:

- **Certificado SSL:**
  - Common Name (CN): selectorshub.com
  - Cifrado: TLS_AES_256_GCM_SHA384 (TLS 1.3, seguro)
  - Emisor: Sectigo Public Server Authentication CA DV R36 (Entidad certificadora confiable)

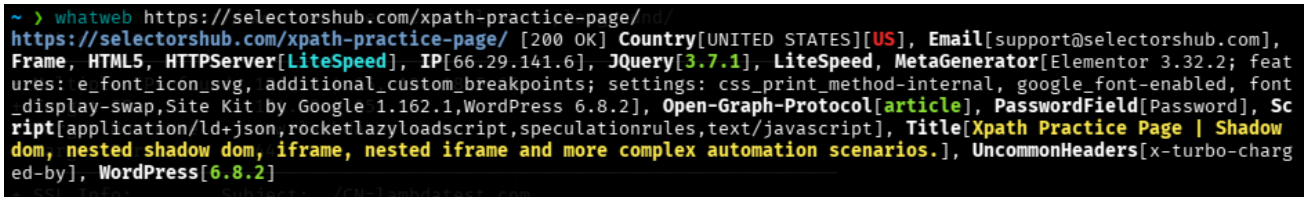
🛡️ Vulnerabilidades y observaciones:

1. **Encabezado X-Powered-By detectado:**
   - Valor: WP Rocket/3.15.9 (plugin de optimización para WordPress)
2. **Falta el encabezado anti-clickjacking X-Frame-Options**
   - No está presente en la URL /xpath-practice-page/, dejando la página vulnerable a ataques de clickjacking.
   - Más info: X-Frame-Options - MDN
3. **Encabezado poco común x-turbo-charged-by detectado:**
   - Contenido: LiteSpeed (indica que el servidor está acelerado por LiteSpeed Cache o similar).
4. **Falta la cabecera Strict-Transport-Security (HSTS)**
   - No se ha configurado HSTS, lo que podría permitir ataques man-in-the-middle o downgrade.
   - Más info: Strict-Transport-Security - MDN
5. **Falta la cabecera X-Content-Type-Options**
   - Sin esta cabecera, los navegadores pueden interpretar tipos MIME incorrectamente, causando vulnerabilidades.
   - Más info: Missing Content-Type Header - Netsparker

6. **Drupal Link header encontrado:**

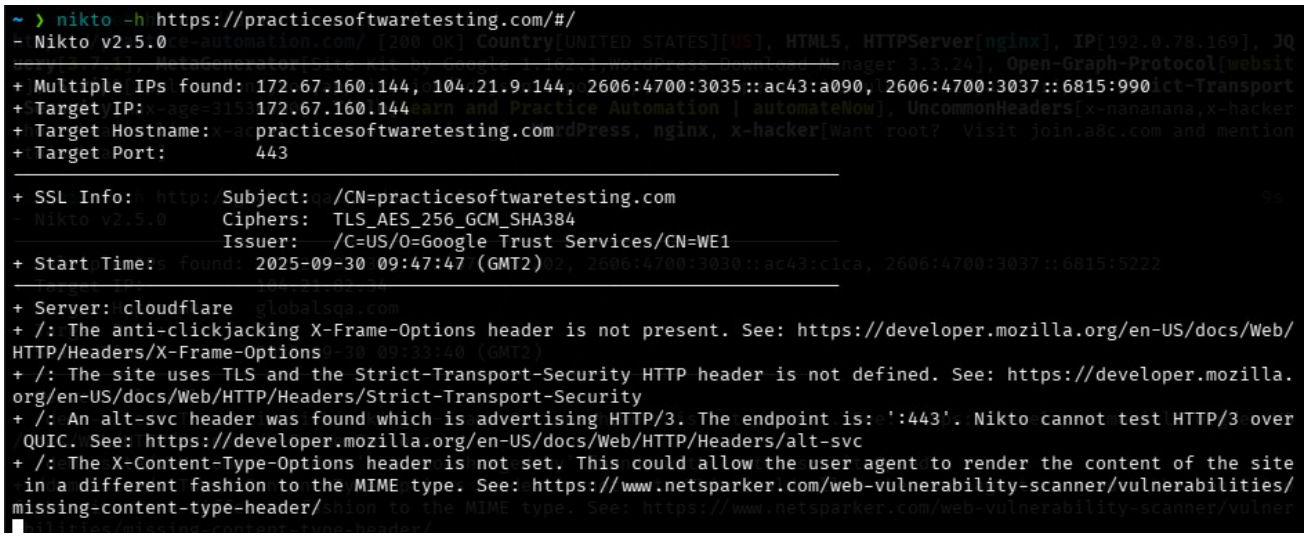
   - En la ruta /xpath-practice-page/qg5O3P22.dbm aparece un header Link que apunta a: <https://selectorshub.com/wp-json/> con relación a la API de WordPress (similar a Drupal).
   - Esto puede dar pistas sobre la tecnología usada (WordPress con REST API activa).

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



WEB 10

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



🔐 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
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
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
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

whatweb https://practicesoftwaretesting.com/#/