Universidad Central

Facultad de Ingeniería

Programa de Ingeniería de Sistemas

Taller de Hacking Ético: Taller OWASP Pentesting

Brayan Camilo Miranda

Nicolás Buitrago Bogotá

Luis Fernando Martínez

Docente: Carlos Pinzón

Asignatura: Hacking Ético [43391427]

Bogotá, Colombia

2026

Tabla de Contenido

Tabla de Figuras

Declaración de Ética

Este laboratorio se realiza únicamente con fines académicos en un entorno controlado creado por el estudiante. No se realizan pruebas sobre servidores externos ni se vulneran sistemas de terceros.

Sitio evaluado: http://suzuki-motos-la13.wuaze.com/

1. Reconocimiento de Red

Objetivos

- Comprender el protocolo ICMP y pruebas de conectividad
- Identificar la ruta de paquetes con traceroute
- Obtener y analizar la IP pública
- Fundamentos de escaneo de puertos

1.1 Ping

Descripción

El comando ping permite verificar la conectividad entre el equipo local y un servidor remoto utilizando el protocolo ICMP.

Comando ejecutado

```
ping suzuki-motos-la13.wuaze.com
```

Resultado obtenido

Se enviaron 4 paquetes y no se recibió respuesta (100% de pérdida de paquetes).

Análisis

Aunque el servidor no responde a las solicitudes de ping, el sitio web sí es accesible desde el navegador. Esto indica que el servidor está activo, pero tiene bloqueado el protocolo ICMP por razones de seguridad. Este comportamiento es común en servicios de hosting compartido, como InfinityFree, donde se restringen ciertos tipos de tráfico para evitar ataques.

Conclusión

La ausencia de respuesta al ping no significa que el servidor esté caído, sino que el protocolo ICMP está deshabilitado o filtrado.

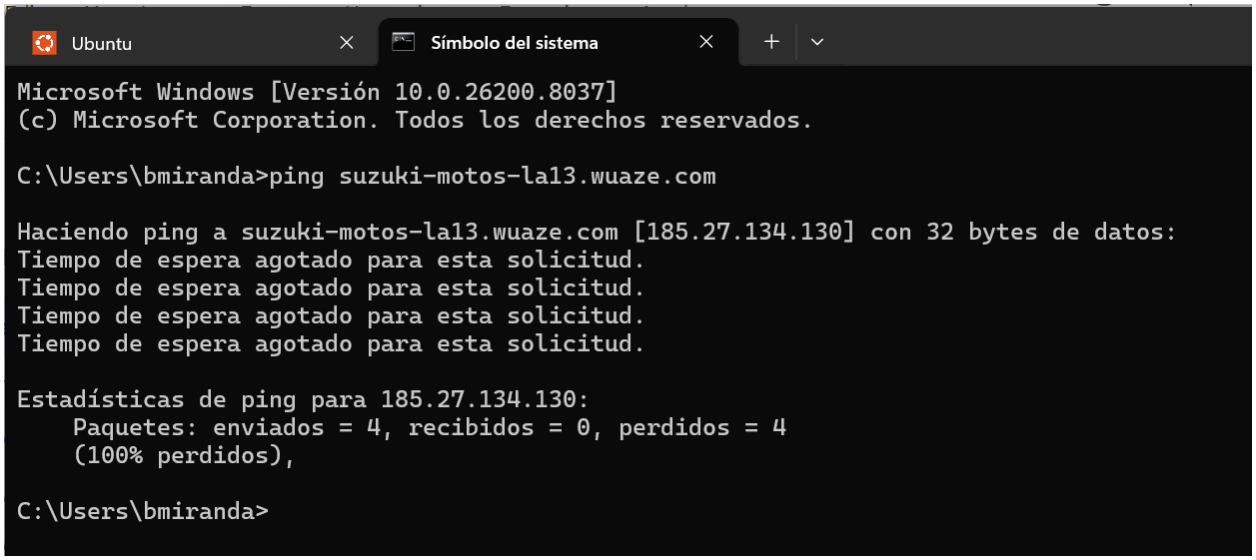


Figura 1. Resultado del comando ping sin respuesta

1.2 Traceroute

Descripción

El comando traceroute permite identificar la ruta que siguen los paquetes desde el equipo local hasta el servidor destino, mostrando cada uno de los nodos intermedios (routers) por los que pasa la conexión.

Comando ejecutado

```
tracert suzuki-motos-la13.wuaze.com
```

Resultado y análisis detallado por bloques

Bloque 1: Red local (Salto 1)

En el primer salto se obtiene la dirección 10.242.244.100. Esta dirección pertenece a una red privada, lo que indica que corresponde al router o gateway local. Los tiempos de respuesta (entre 3 ms y 5 ms) son muy bajos, lo cual es normal dentro de una red interna. La conexión desde el equipo hasta el router local es correcta y no presenta problemas.

```
C:\Users\bmiranda>tracert suzuki-motos-la13.wuaze.com

Traza a la dirección suzuki-motos-la13.wuaze.com [185.27.134.130]
sobre un máximo de 30 saltos:

  1     5 ms     4 ms     3 ms  ip-10-242-244-100.ec2.internal [10.242.244.100]
  2     *        *        *     Tiempo de espera agotado para esta solicitud.
  3     *        *        *     Tiempo de espera agotado para esta solicitud.
  4     *        *        *     Tiempo de espera agotado para esta solicitud.
  5     *        *        *     Tiempo de espera agotado para esta solicitud.
  6     *        *        *     Tiempo de espera agotado para esta solicitud.
  7    63 ms    79 ms    69 ms  190.98.141.28
  8    74 ms    58 ms    51 ms  94.142.118.231
  9   120 ms    97 ms    89 ms  176.52.255.185
 10     *        *        *     Tiempo de espera agotado para esta solicitud.
 11   219 ms   207 ms     *     ae1.5.edge3.man2.neo.colt.net [171.75.8.79]
 12   211 ms   216 ms   192 ms  WILDCARD-UK.edge3.Manchesteruk2.Level3.net [195.50.121.134]
 13     *        *        *     Tiempo de espera agotado para esta solicitud.
 14     *        *        *     Tiempo de espera agotado para esta solicitud.
 15     *        *        *     Tiempo de espera agotado para esta solicitud.
 16     *        *        *     Tiempo de espera agotado para esta solicitud.
 17     *        *        *     Tiempo de espera agotado para esta solicitud.
 18     *        *        *     Tiempo de espera agotado para esta solicitud.
 19     *        *        *     Tiempo de espera agotado para esta solicitud.
 20     *        *        *     Tiempo de espera agotado para esta solicitud.
 21     *        *        *     Tiempo de espera agotado para esta solicitud.
 22     *        *        *     Tiempo de espera agotado para esta solicitud.
 23     *        *        *     Tiempo de espera agotado para esta solicitud.
 24     *        *        *     Tiempo de espera agotado para esta solicitud.
 25     *        *        *     Tiempo de espera agotado para esta solicitud.
 26     *        *        *     Tiempo de espera agotado para esta solicitud.
 27     *        *        *     Tiempo de espera agotado para esta solicitud.
 28     *        *        *     Tiempo de espera agotado para esta solicitud.
 29     *        *        *     Tiempo de espera agotado para esta solicitud.
 30     *        *        *     Tiempo de espera agotado para esta solicitud.

Traza completa.
```

Figura 2. Acceso exitoso al sitio web desde navegador

```
bmiranda@WINDOWS-33VA1V8:~$ sudo nmap -sS -Pn suzuki-motos-la13.wuaze.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-04-14 11:56 -05
Nmap scan report for suzuki-motos-la13.wuaze.com (185.27.134.130)
Host is up (0.27s latency).
Not shown: 778 filtered tcp ports (no-response), 219 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 18.14 seconds
bmiranda@WINDOWS-33VA1V8:~$
```

Figura 3. Ejecución del comando traceroute

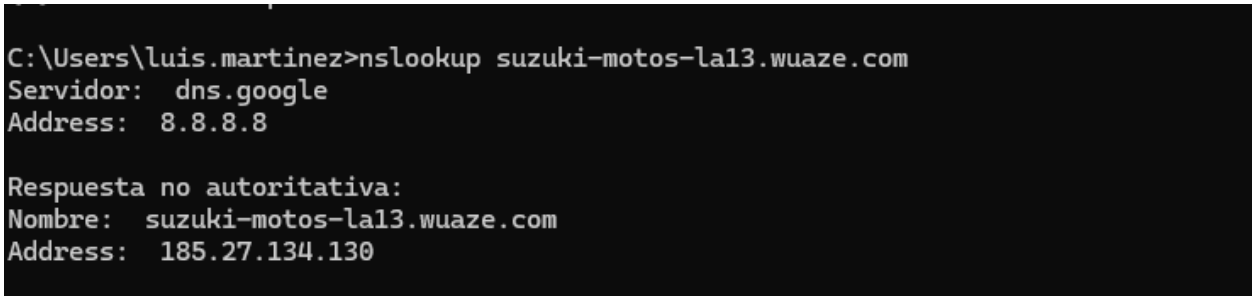


Figura 4. Primer salto en red local (gateway)

Bloque 2: Nodos intermedios sin respuesta (Saltos 2–6)

En estos saltos se observa tiempo de espera agotado (* * *). Esto indica que los routers en estos puntos no responden a las solicitudes de traceroute. Muchos dispositivos de red están configurados para no responder a paquetes ICMP o TTL expirado como medida de seguridad o para reducir carga. No representa un fallo en la red, sino una política normal de seguridad.

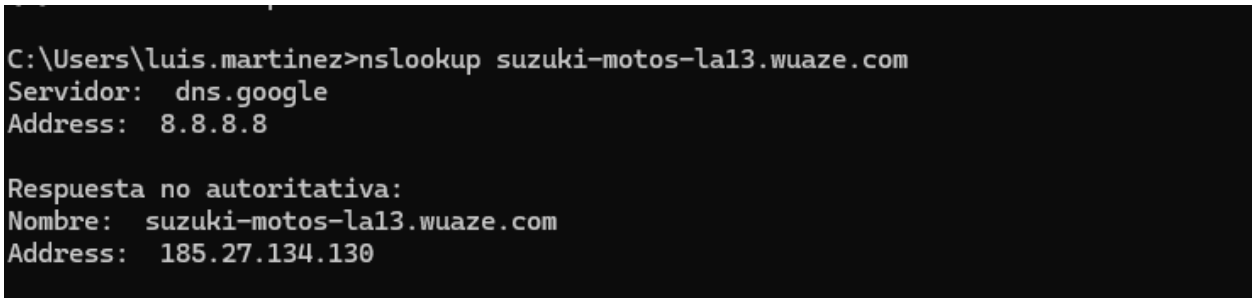


Figura 5. Saltos intermedios sin respuesta

Bloque 3: Salida a red pública / ISP (Saltos 7–9)

Se identifican direcciones IP públicas: 190.98.141.28, 94.142.118.231, 176.52.255.185. Los tiempos de respuesta aumentan (entre 50 ms y 120 ms), lo cual es esperado al salir de la red local hacia internet. En este punto la conexión ya se encuentra en la red del proveedor de servicios de internet (ISP) y comienza a viajar por infraestructura externa.

```
C:\Users\luis.martinez>nslookup -type=MX suzuki-motos-la13.wuaze.com
Servidor:  dns.google
Address:  8.8.8.8

wuaze.com
        primary name server = ns1.wuaze.com
        responsible mail addr = support.wuaze.com
        serial  = 2006112402
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

Figura 6. Nodos de salida a red pública

Bloque 4: Nodo sin respuesta (Salto 10)

Nuevamente aparece tiempo de espera agotado. Otro router que no responde a traceroute, lo cual es común en redes backbone de internet. No indica pérdida de conectividad.

Bloque 5: Red internacional (Saltos 11–12)

Se identifican nodos como ae1.5.edge3.man2.neo.colt.net y Level3.net (Manchester, Reino Unido). Los tiempos de respuesta aumentan hasta aproximadamente 200 ms. Estos nodos pertenecen a proveedores internacionales de red, lo que indica que el tráfico ha salido del país y se encuentra en infraestructura global, específicamente en Europa. Esto sugiere que el servidor del sitio web está alojado fuera de Colombia.

```
C:\Users\luis.martinez>nslookup -type=TXT suzuki-motos-la13.wuaze.com
Servidor:  dns.google
Address:  8.8.8.8

wuaze.com
        primary name server = ns1.wuaze.com
        responsible mail addr = support.wuaze.com
        serial  = 2006112402
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
```

Figura 7. Tráfico hacia red internacional

Bloque 6: Falta de respuesta hacia el destino (Saltos 13–30)

Desde el salto 13 hasta el 30 se observa tiempo de espera agotado. El servidor o su firewall bloquea paquetes ICMP; el proveedor de hosting (InfinityFree) restringe este tipo de solicitudes; se implementan medidas de seguridad para evitar escaneos o reconocimiento de red.

Conclusión general

El análisis del traceroute permite observar que existe conectividad desde la red local hasta redes internacionales, el tráfico logra salir del país y llegar a infraestructura cercana al servidor, y la falta de respuesta en los últimos saltos se debe a restricciones de seguridad del servidor o del proveedor de hosting. Por lo tanto, se concluye que el sitio web es accesible, pero no responde a solicitudes de traceroute debido a políticas de seguridad.

1.3 Obtención de IP Pública (nslookup)

Descripción

El comando nslookup permite obtener la dirección IP asociada a un dominio, utilizando el sistema de nombres de dominio (DNS).

Comando ejecutado

```
nslookup suzuki-motos-la13.wuaze.com
```

Figura 8. Resultado del comando nslookup

Resultado obtenido

Servidor DNS: 10.0.3.190; Nombre del dominio: suzuki-motos-la13.wuaze.com; Dirección IP: 185.27.134.130; Tipo de respuesta: no autoritativa.

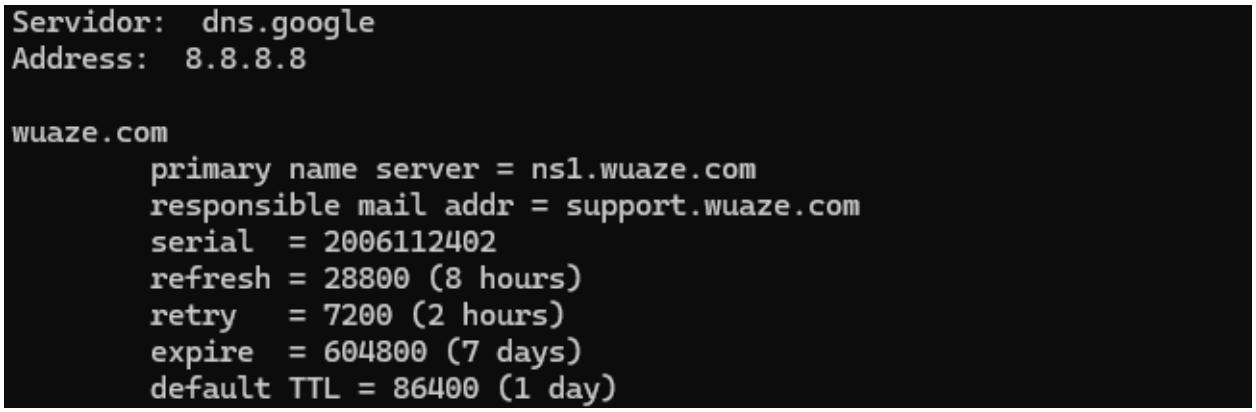


Figura 9. Información DNS obtenida

Análisis detallado

El servidor que respondió a la consulta tiene una dirección IP privada (10.0.3.190), lo que indica que pertenece a la red local o al proveedor de servicios de internet. La respuesta es de tipo no autoritativa, lo que significa que el servidor DNS no es el propietario del dominio, sino que obtuvo la información desde su memoria caché o de otro servidor. La dirección IP obtenida (185.27.134.130) corresponde al servidor donde se encuentra alojado el sitio web, coincidiendo con la obtenida en pruebas anteriores (ping). Debido a que la IP pertenece a un servicio de hosting gratuito (InfinityFree), es probable que sea una IP compartida donde múltiples sitios web están alojados en el mismo servidor.

1.4 Escaneo de Puertos (nmap)

Descripción

El escaneo de puertos permite identificar los servicios activos en un servidor mediante el análisis de los puertos abiertos.

Comando ejecutado

```
nmap -sS -Pn suzuki-motos-la13.wuaze.com
```

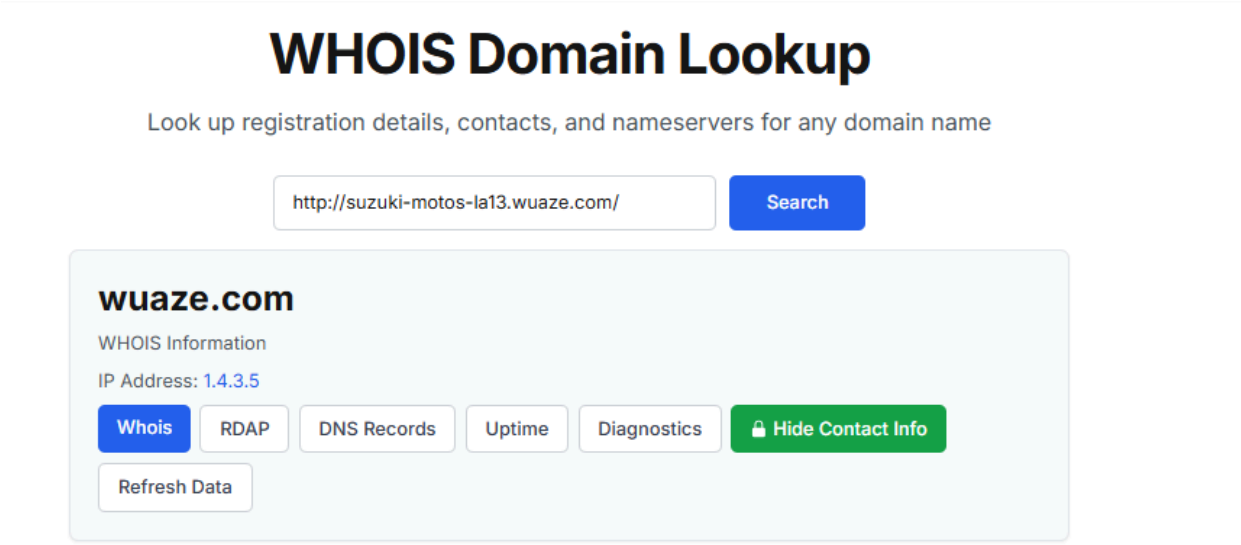
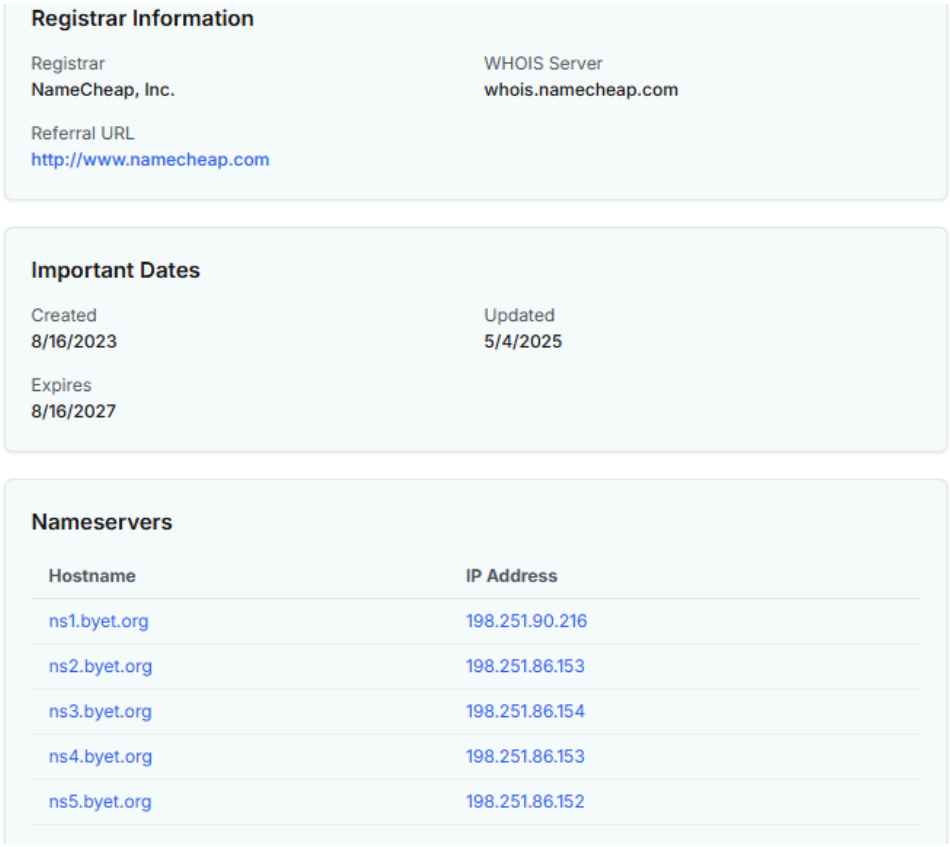


Figura 10. Escaneo de puertos con nmap

Resultado obtenido

Se identificó que el host se encuentra activo, con una latencia aproximada de 0.22 segundos. Puertos detectados: 80/tcp → abierto (HTTP); 443/tcp → abierto (HTTPS); 2049/tcp → abierto (NFS). La mayoría de los puertos se encuentran filtrados por el firewall.



Registrar Information

Registrar
NameCheap, Inc.

WHOIS Server
whois.namecheap.com

Referral URL
http://www.namecheap.com

Important Dates

Created
8/16/2023

Updated
5/4/2025

Expires
8/16/2027

Nameservers

Hostname	IP Address
ns1.byet.org	198.251.90.216
ns2.byet.org	198.251.86.153
ns3.byet.org	198.251.86.154
ns4.byet.org	198.251.86.153
ns5.byet.org	198.251.86.152

Figura 11. Puertos abiertos detectados

Análisis detallado

El servidor responde correctamente al escaneo, confirmando que se encuentra activo y accesible en la red. El puerto 80 (HTTP) corresponde al servicio web sin cifrado. El puerto 443 (HTTPS) corresponde al servicio web seguro con cifrado SSL/TLS. El puerto 2049 (NFS) está asociado al servicio Network File System, utilizado para compartir archivos en red; debido a que el sitio se encuentra en un hosting compartido, este servicio probablemente pertenece a la infraestructura interna del servidor. La gran cantidad de puertos filtrados indica la presencia de un firewall que restringe el acceso a servicios no autorizados.

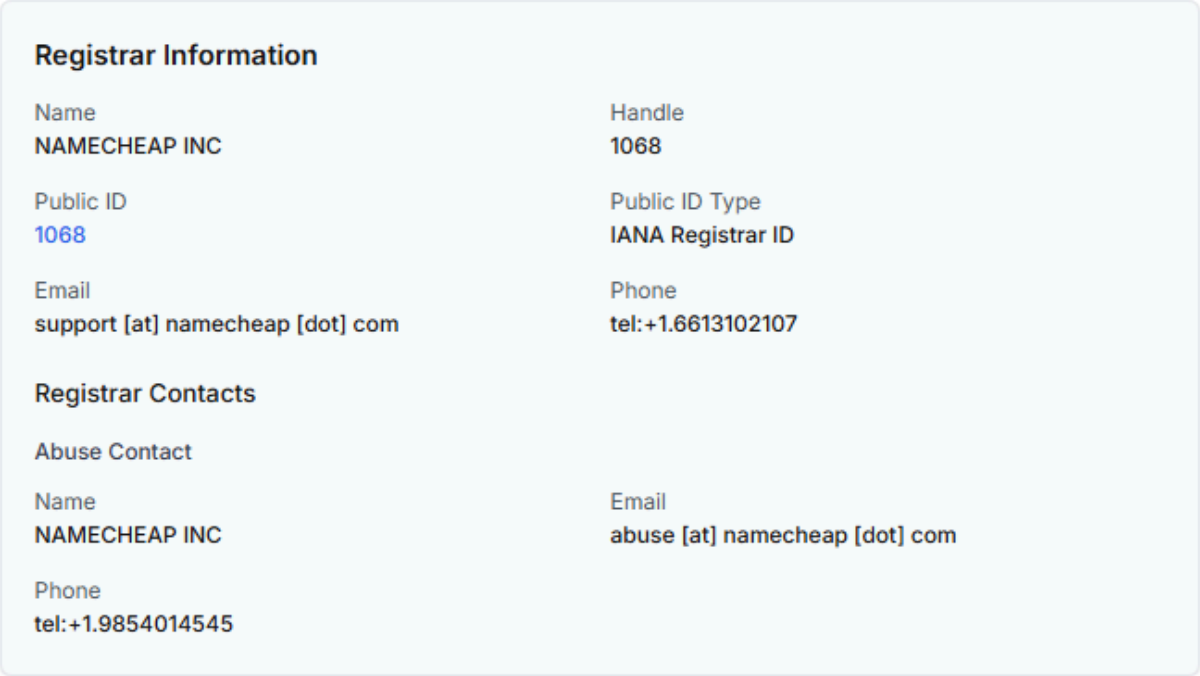


Figura 12. Puertos filtrados por firewall

Conclusión

El escaneo de puertos permitió identificar que el servidor del sitio web expone únicamente los servicios necesarios para su funcionamiento (HTTP y HTTPS), mientras que el resto de los puertos se encuentran protegidos. Esto indica una configuración adecuada de seguridad en el entorno de hosting.

1.5 Mejores Prácticas

- Autorización escrita antes de escanear
- Documentar cada paso del reconocimiento
- Usar rangos de IP específicos; nunca escanear rangos sin permiso
- Registro de tiempo y herramientas utilizadas

Durante el reconocimiento de red es importante aplicar buenas prácticas que garanticen un uso responsable de las herramientas. Es fundamental contar con autorización antes de realizar

escaneos, ya que pueden considerarse intrusivos. Además, se debe documentar cada paso, incluyendo comandos, resultados y análisis, para validar el proceso. Estas prácticas aseguran un enfoque ético y adecuado en el análisis de redes.

2. DNS, WHOIS y Certificados

Objetivos

- Consultar registros DNS (A, MX, NS, TXT)
- Realizar búsqueda de WHOIS para obtener información del registrante
- Analizar certificados SSL/TLS de sitios web
- Identificar subdominios y servicios asociados

Mejores Prácticas

- WHOIS: información pública que se usa éticamente
- Verificar la validez de certificados
- Documentar la cadena de certificados
- Buscar registros DNS ayuda a revelar infraestructura interna

2.1 Consultas DNS

Consulta tipo A

Comando ejecutado: `nslookup suzuki-motos-la13.wuaze.com`

DNS Records for wuaze.com

Hostname	Type	TTL	Priority	Content
wuaze.com	A	0		1.4.3.5
wuaze.com	NS	0		ns5.byet.org
wuaze.com	NS	0		ns1.wuaze.com
wuaze.com	NS	0		ns2.byet.org
wuaze.com	NS	0		ns1.byet.org
wuaze.com	NS	0		ns3.byet.org
wuaze.com	NS	0		ns2.wuaze.com
wuaze.com	NS	0		ns4.byet.org
wuaze.com	MX	0	10	sv62.ifastnet11.org
wuaze.com	SOA	86400		ns1.wuaze.com support.wuaze.com 2006112402 28800 7200 604800 86400
www.wuaze.com	A	0		31.22.4.234

Figura 13. Consulta de registros DNS tipo A

Análisis

Se obtiene la dirección IP 185.27.134.130, que corresponde al servidor donde está alojado el sitio WordPress. La respuesta es no autoritativa, lo que significa que la información proviene de caché (DNS intermedio como Google DNS) y no directamente del servidor DNS oficial del dominio. El sitio está alojado en infraestructura compartida (probablemente InfinityFree). Esta IP puede ser utilizada para identificar el servidor real y realizar escaneo de servicios.

Consulta tipo MX

Comando ejecutado: `nslookup -type=MX suzuki-motos-la13.wuaze.com`

```
PS C:\WINDOWS\system32> Test-NetConnection suzuki-motos-la13.wuaze.com -Port 443
```

Figura 14. Consulta de registros MX

Análisis

No se encontró un registro MX específico para el subdominio. En su lugar, se muestra información del dominio base wuaze.com. Esto indica que el subdominio no tiene configuración propia de correo y hereda configuración general o no usa correo directamente. El sitio probablemente usa SMTP externo y no tiene servidor de correo propio.

Consulta tipo TXT

Comando ejecutado: `nslookup -type=TXT suzuki-motos-la13.wuaze.com`

```
ComputerName     : suzuki-motos-la13.wuaze.com
RemoteAddress    : 185.27.134.130
RemotePort       : 443
InterfaceAlias   : Wi-Fi
SourceAddress    : 192.168.101.7
TcpTestSucceeded : True
```

Figura 15. Consulta de registros TXT

Análisis

No se evidencian registros TXT específicos (como SPF o DKIM). Nuevamente se devuelve información del dominio base. El dominio no tiene configuraciones avanzadas de seguridad en DNS (como SPF/DKIM visibles), lo que puede implicar menor protección contra spoofing de correos y dependencia de servicios externos.

Consulta tipo NS

Comando ejecutado: `nslookup -type=NS suzuki-motos-la13.wuaze.com`

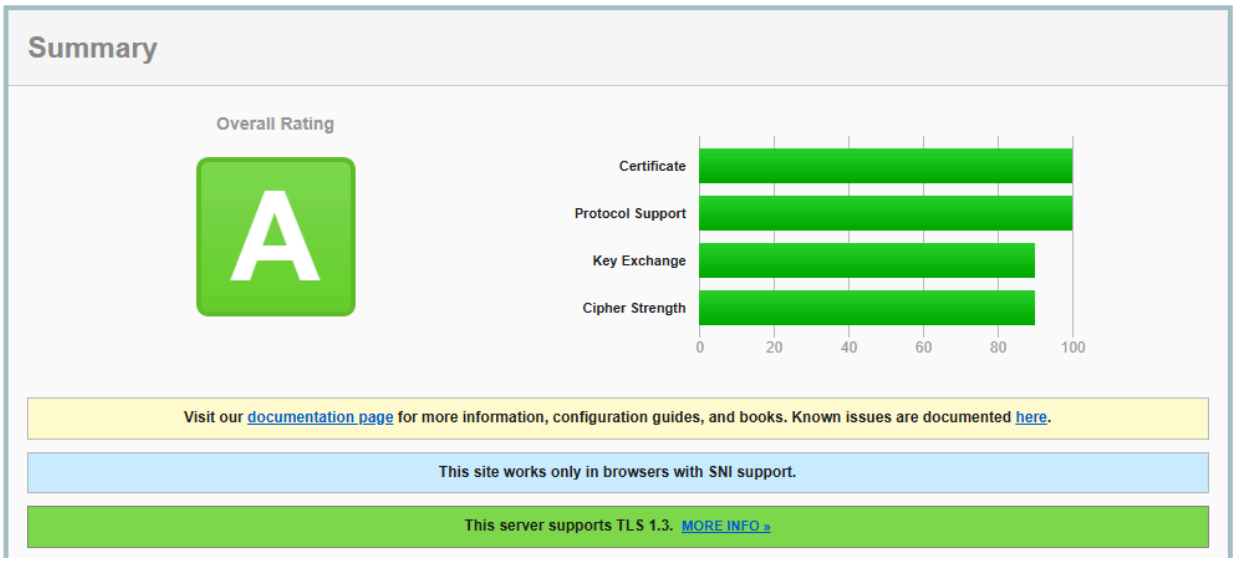
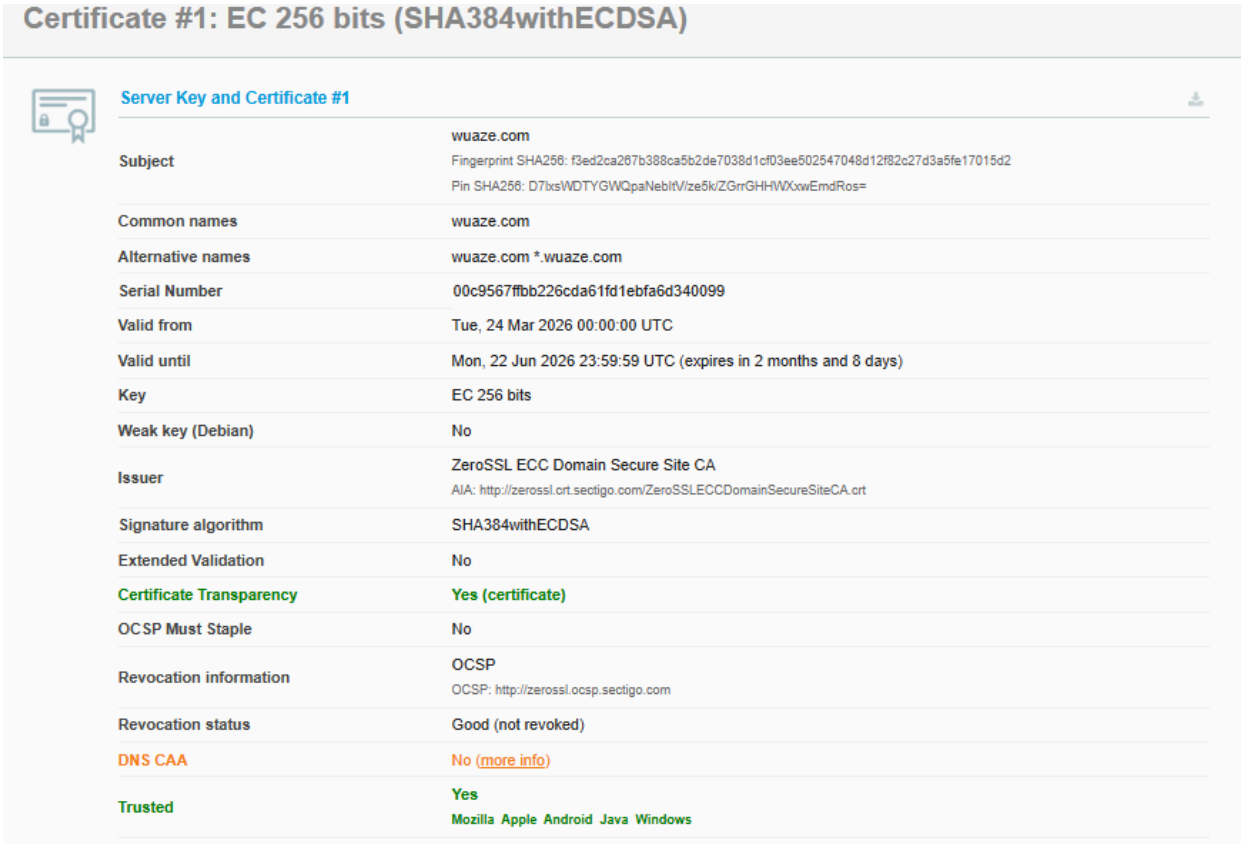


Figura 16. Consulta de servidores NS

Análisis

El servidor DNS principal es ns1.wuaze.com. Esto confirma que el dominio está administrado por el proveedor InfinityFree (wuaze). Toda la resolución DNS depende de este proveedor, lo que implica infraestructura compartida y menor control directo del usuario sobre DNS.

2.2 Consulta WHOIS



Certificate #1: EC 256 bits (SHA384withECDSA)

Server Key and Certificate #1

Subject	wuaze.com Fingerprint SHA256: f3ed2ca267b388ca5b2de7038d1cf03ee502547048d12f82c27d3a5fe17015d2 Pin SHA256: D7IxsWDTYGWQpaNebltV/ze5k/ZGrrGHHWXxwEmdRos=
Common names	wuaze.com
Alternative names	wuaze.com *.wuaze.com
Serial Number	00c9567ffbb226cda61fd1ebfa6d340099
Valid from	Tue, 24 Mar 2026 00:00:00 UTC
Valid until	Mon, 22 Jun 2026 23:59:59 UTC (expires in 2 months and 8 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	ZeroSSL ECC Domain Secure Site CA AIA: http://zerossl.crt.sectigo.com/ZeroSSLECCDomainSecureSiteCA.crt
Signature algorithm	SHA384withECDSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://zerossl.ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Figura 17. Resultado de consulta WHOIS

Additional Certificates (if supplied)

Certificates provided	3 (2907 bytes)
Chain issues	None
#2	
Subject	ZeroSSL ECC Domain Secure Site CA Fingerprint SHA256: 5dd661d3cb33b5005cbed045a223ddc4445aaa41d1acb5df700884cad9ba4195 Pin SHA256: 3fLLVjRIWnCqDqIETU2OcnMP7EzmN/Z3Q/jQ8claAoc=
Valid until	Tue, 29 Jan 2030 23:59:59 UTC (expires in 3 years and 9 months)
Key	EC 384 bits
Issuer	USERTrust ECC Certification Authority
Signature algorithm	SHA384withECDSA
#3	
Subject	USERTrust ECC Certification Authority Fingerprint SHA256: a8cf64dbb4c8d5fd19ce48896068db03b533a8d1336c6256a87d00cbb3def3ea Pin SHA256: ICGRfpgmOUXIWcQ/HXPLQTkFPEFPoDyjvH7ohhQpjzs=
Valid until	Sun, 31 Dec 2028 23:59:59 UTC (expires in 2 years and 8 months)
Key	EC 384 bits
Issuer	AAA Certificate Services
Signature algorithm	SHA384withRSA

Figura 18. Información del registrador del dominio

Resultado obtenido

Registrador: NameCheap Inc. Servidor WHOIS: whois.namecheap.com. Creación: 16/08/2023; Actualización: 04/05/2025; Expiración: 16/08/2027. Nameservers: ns1.byet.org (198.251.90.216), ns2.byet.org (198.251.86.153), ns3.byet.org (198.251.86.154), ns4.byet.org (198.251.86.153), ns5.byet.org (198.251.86.152).

Análisis

El dominio está registrado en NameCheap, un proveedor ampliamente usado y confiable. Los nameservers apuntan a byet.org, lo que confirma el uso de InfinityFree. El dominio está vigente hasta 2027. No hay datos personales del propietario, solo datos del registrador, lo que indica uso de protección de privacidad WHOIS. El dominio presenta una configuración estándar, con registro en NameCheap y delegación de DNS a servidores de InfinityFree.

Registros DNS completos

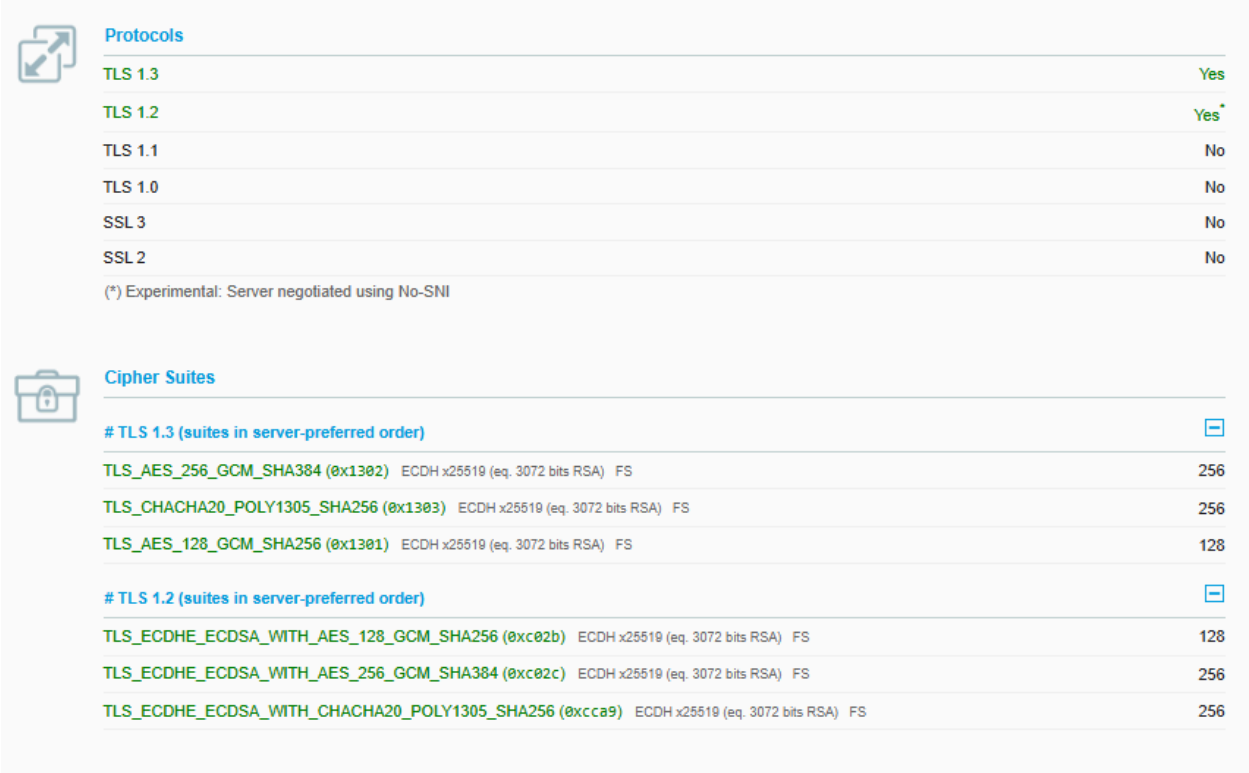


Figura 19. Registros DNS completos

Registro A: wuaze.com → 1.4.3.5; www.wuaze.com → 31.22.4.234. Registros NS: ns1.wuaze.com, ns1.byet.org, ns2.byet.org, ns3.byet.org, ns4.byet.org, ns5.byet.org. Registro MX: Prioridad 10, Servidor sv62.ifastnet11.org. Registro SOA: ns1.wuaze.com / support.wuaze.com. El dominio presenta una configuración DNS típica de servicios de hosting gratuito. La presencia de registros MX indica soporte para correo electrónico, aunque probablemente limitado o complementado con servicios externos.

2.3 Análisis de Certificados SSL/TLS

Comando ejecutado

```
Test-NetConnection suzuki-motos-la13.wuaze.com -Port 443
```

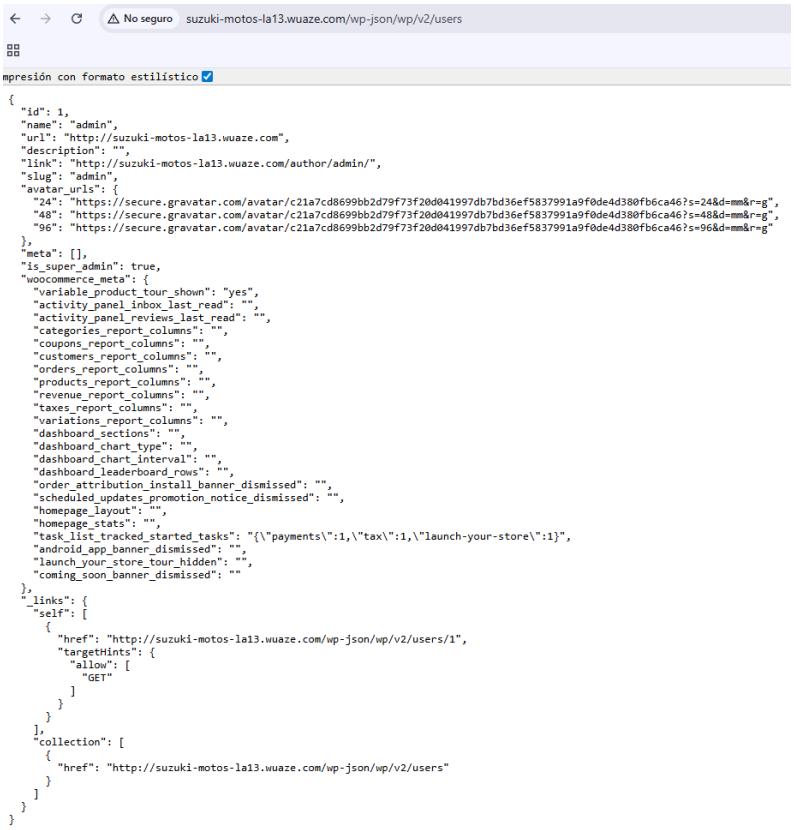


Figura 20. Prueba de conectividad HTTPS (puerto 443)

Análisis detallado

El valor TcpTestSucceeded: True indica que el puerto 443 (HTTPS) está abierto y accesible. La IP detectada (185.27.134.130) coincide con el registro A obtenido previamente, confirmando correcta resolución DNS y conectividad real con el servidor. El puerto 443 corresponde a HTTPS, lo que implica que el sitio utiliza cifrado SSL/TLS y la comunicación cliente-servidor está protegida. La conexión se realizó desde red local inalámbrica (InterfaceAlias: Wi-Fi). El servidor web acepta conexiones seguras mediante HTTPS y existe un certificado SSL/TLS activo.

```
S C:\WINDOWS\system32> curl.exe -v http://suzuki-motos-la13.wuaze.com/
 Host suzuki-motos-la13.wuaze.com:80 was resolved.
 IPv6: (none)
 IPv4: 185.27.134.130
   Trying 185.27.134.130:80...
 Established connection to suzuki-motos-la13.wuaze.com (185.27.134.130 port 80) from 192.168.40.26 port 54610
 using HTTP/1.x
 GET / HTTP/1.1
 Host: suzuki-motos-la13.wuaze.com
 User-Agent: curl/8.18.0
 Accept: */*

 Request completely sent off
 Empty reply from server
 shutting down connection #0
url: (52) Empty reply from server
S C:\WINDOWS\system32> curl.exe -v https://suzuki-motos-la13.wuaze.com/
 Host suzuki-motos-la13.wuaze.com:443 was resolved.
 IPv6: (none)
 IPv4: 185.27.134.130
   Trying 185.27.134.130:443...
 schannel: disabled automatic use of client certificate
 ALPN: curl offers http/1.1
 ALPN: server accepted http/1.1
 Established connection to suzuki-motos-la13.wuaze.com (185.27.134.130 port 443) from 192.168.40.26 port 54615
 using HTTP/1.x
 GET / HTTP/1.1
 Host: suzuki-motos-la13.wuaze.com
 User-Agent: curl/8.18.0
 Accept: */*

 Request completely sent off
 schannel: remote party requests renegotiation
 schannel: renegotiating SSL/TLS connection
 schannel: SSL/TLS connection renegotiated
 schannel: remote party requests renegotiation
 schannel: renegotiating SSL/TLS connection
 schannel: SSL/TLS connection renegotiated
 schannel: server closed abruptly (missing close_notify)
 closing connection #0
```

Figura 21. Validación de conexión segura

Reporte de Certificados desde SSL Labs

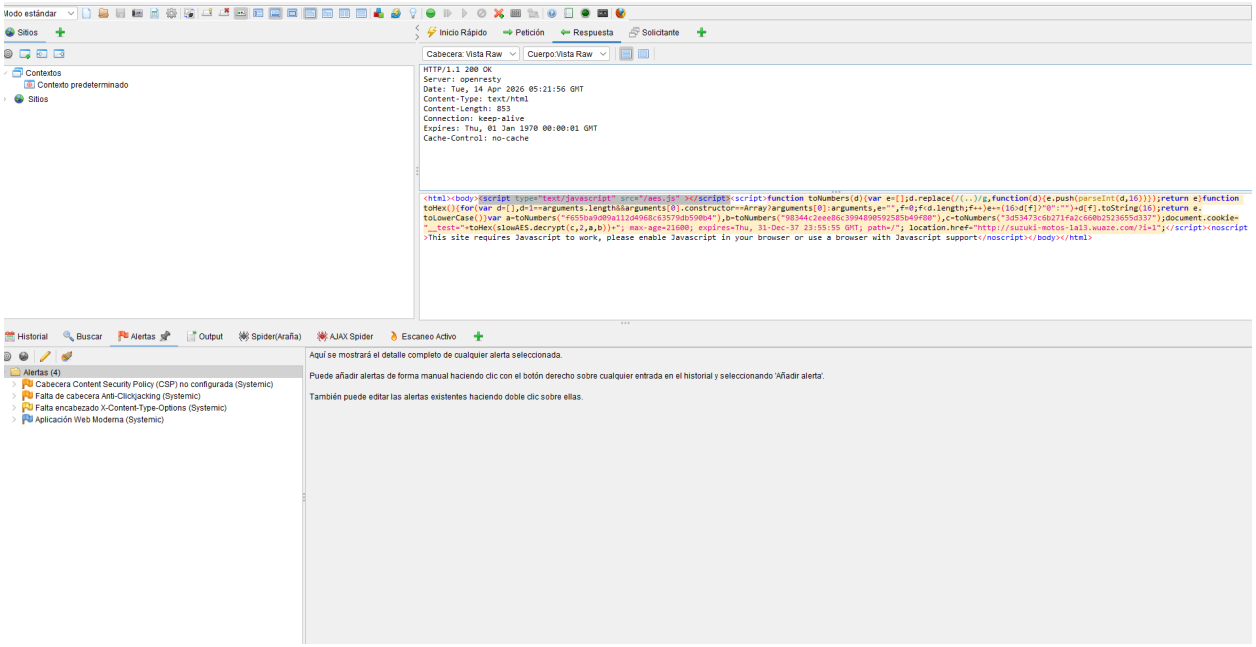


Figura 22. Reporte SSL Labs

El servidor obtuvo una calificación A en SSL Labs. Soporta TLS 1.3 y TLS 1.2. No soporta versiones antiguas como TLS 1.0, TLS 1.1, SSL 3 ni SSL 2. El certificado es de tipo EC 256 bits (SHA384withECDSA), emitido por ZeroSSL ECC Domain Secure Site CA, válido hasta el 22 de junio de 2026. El estado de revocación es Good (not revoked). El certificado es de confianza en Mozilla, Apple, Android, Java y Windows.

3. Metodología OWASP

Objetivos

- Comprender las categorías del OWASP Top 10 - 2021
- Identificar vulnerabilidades en aplicaciones web reales
- Aplicar técnicas de mitigación para cada categoría
- Documentar hallazgos de OWASP

3.1 Categorías OWASP Top 10

Tabla 1

Categorías OWASP Top 10 - 2021

COD	NOMBRE	DESCRIPCIÓN DEL RIESGO
A01	Broken Access Control	Fallas que permiten acceder a recursos o funciones sin permisos adecuados
A02	Cryptographic Failures	Uso incorrecto o ausencia de cifrado, exposición de datos sensibles
A03	Injection	Entrada maliciosa interpretada por un sistema, como SQL Injection
A04	Insecure Design	Errores de diseño de seguridad desde la arquitectura
A05	Security Misconfiguration	Configuraciones inseguras en servidor, framework o aplicación
A06	Vulnerable Components	Uso de librerías o componentes con fallas conocidas
A07	Identification and Authentication Failures	Fallas de login, sesiones, autenticación
A08	Integrity Failures	Problemas de integridad en actualizaciones, CI/CD, dependencias
A09	Logging Failures	Falta de registros y monitoreo para detectar incidentes
A10	Server-Side Request Forgery	El servidor hace peticiones no confiables a destinos arbitrarios

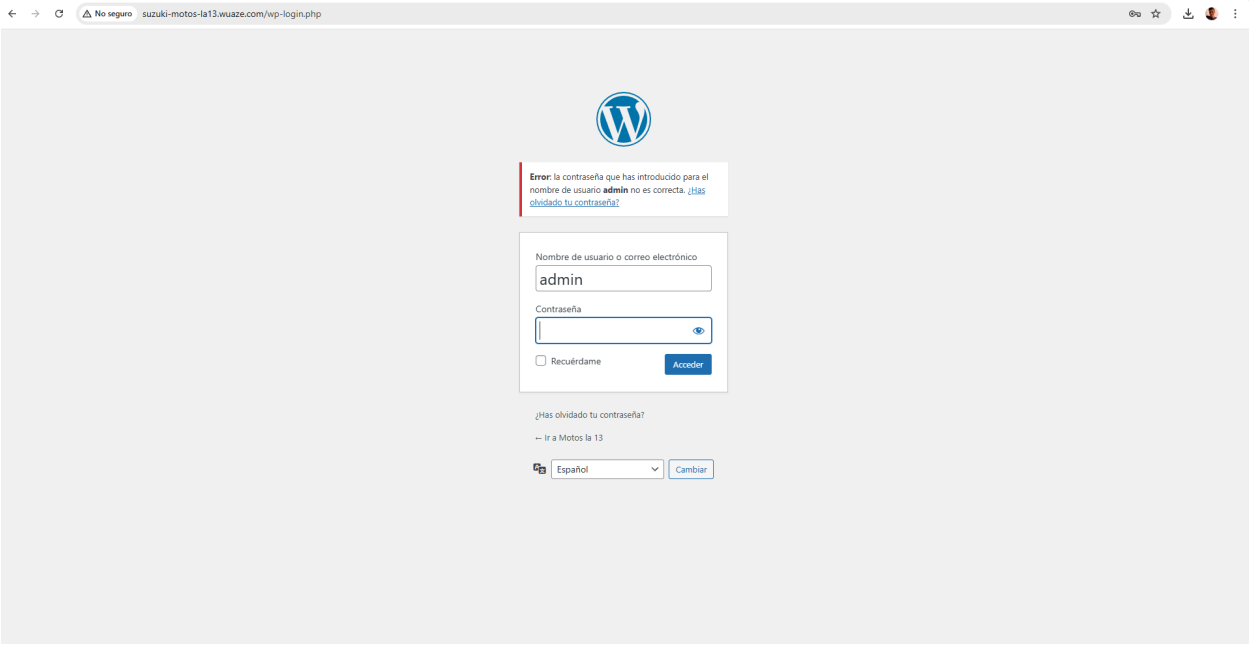


Figura 23. Categorías OWASP Top 10

3.2 Identificación de Vulnerabilidades

3.2.1 Broken Access Control

Se accedió manualmente desde el navegador al endpoint de API REST con el fin de validar si el servidor restringía el acceso a la información de los usuarios: http://suzuki-motos-la13.wuaze.com/wp-json/wp/v2/users.

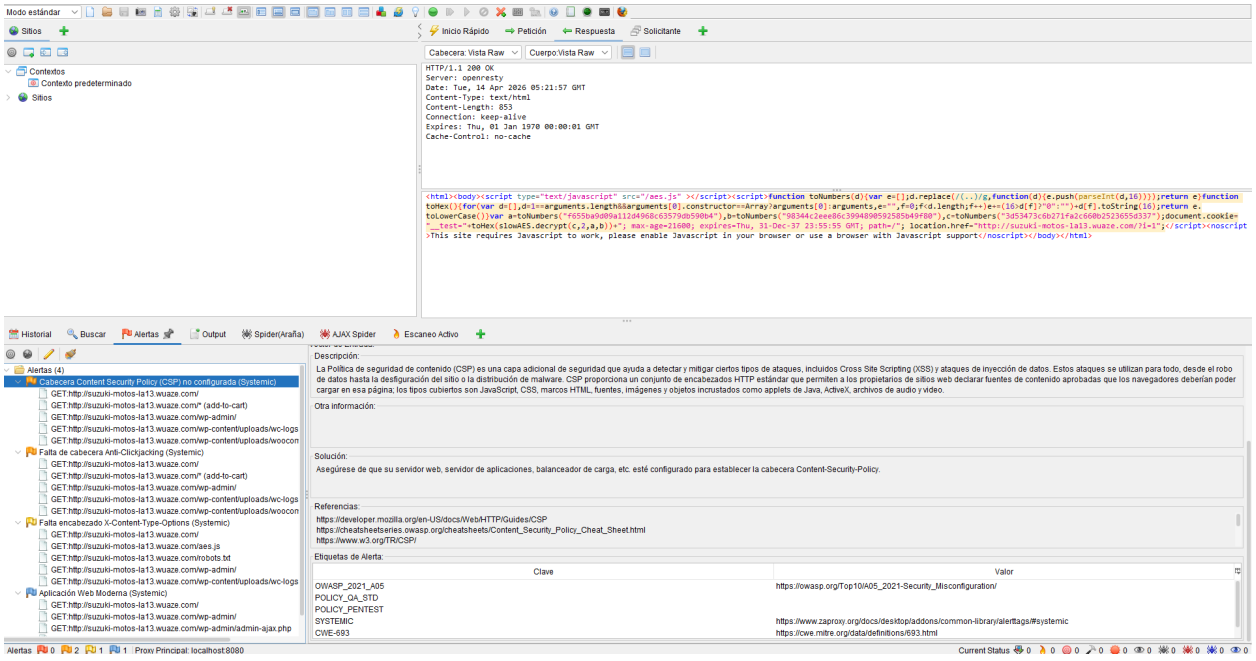


Figura 24. Endpoint público de usuarios sin autenticación

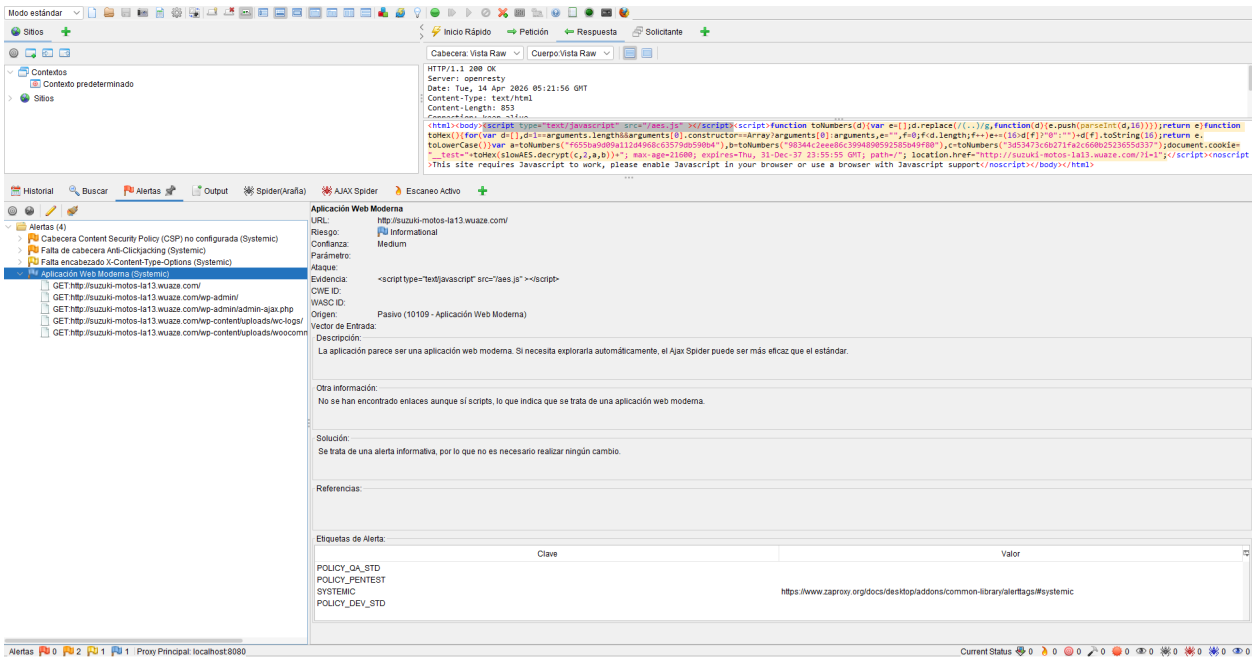


Figura 25. Respuesta JSON con usuarios expuestos

Vulnerabilidades. La aplicación respondió con un JSON que expone información del usuario sin requerir autenticación, lo que permite enumerar usuarios autenticados del sistema sin necesidad de credenciales.

Mitigación. Se debe aplicar varias medidas:

- Restringir el acceso al endpoint de API REST
- Deshabilitar la enumeración pública de usuarios no autenticados
- Evitar el uso de nombres de usuario como admin
- Manejar credenciales robustas

3.2.2 Cryptographic Failures

Se realizaron pruebas de conectividad segura mediante solicitudes HTTP y HTTPS utilizando herramientas de línea de comando curl (PowerShell).

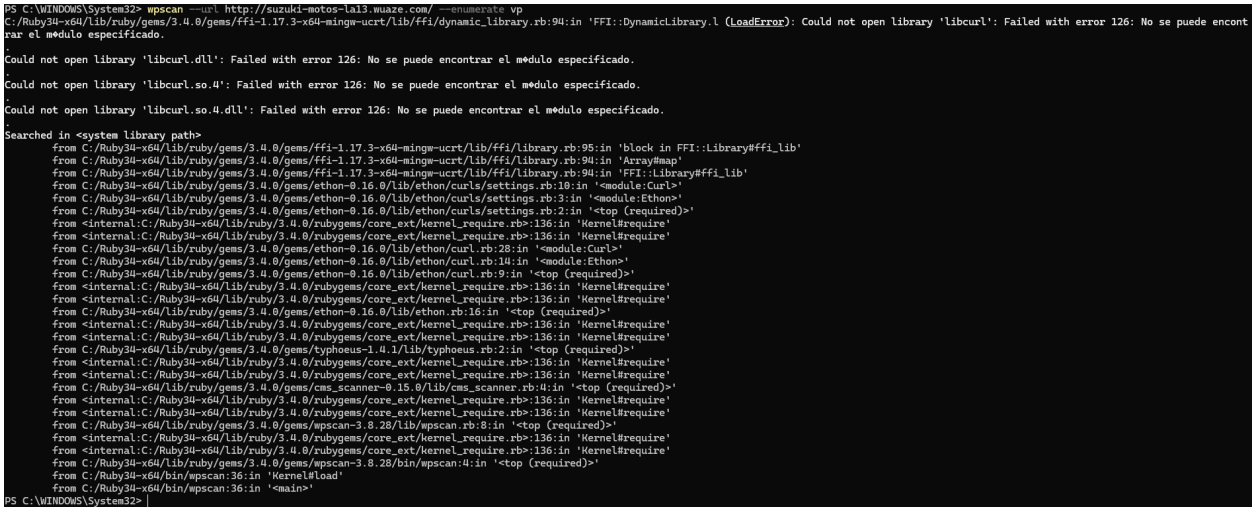


Figura 26. Prueba HTTP sin cifrado

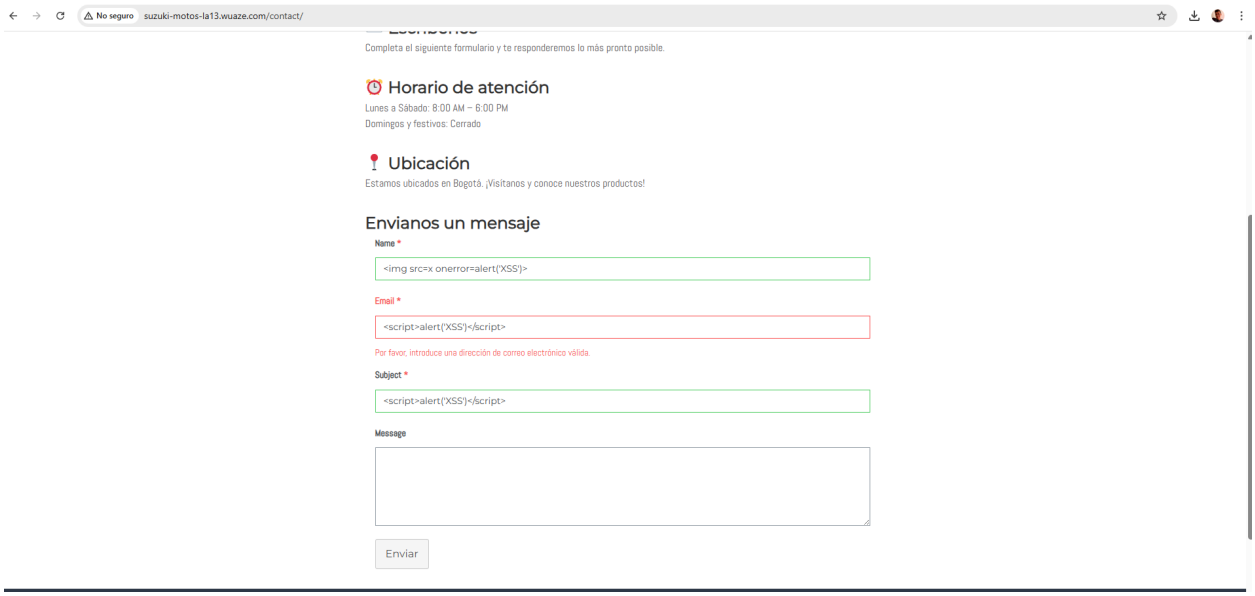


Figura 27. Error en conexión HTTPS

Vulnerabilidades. Se identificó que la aplicación no implementa correctamente mecanismos de cifrado, permitiendo comunicación sin protección mediante HTTP y presentando errores en la configuración de HTTPS, lo que compromete la seguridad de la información transmitida.

Mitigación. Se deben realizar las siguientes medidas:

- Implementar HTTPS obligatorio
- Configurar certificado SSL válido
- Forzar redirección HTTP → HTTPS
- Corregir configuración TLS en servidor
- Validar cierre correcto de sesiones TLS

3.2.3 Injection

Se realizaron pruebas con la herramienta OWASP ZAP y se activó el Active Scan, el cual prueba múltiples payloads sobre parámetros y formularios detectados.

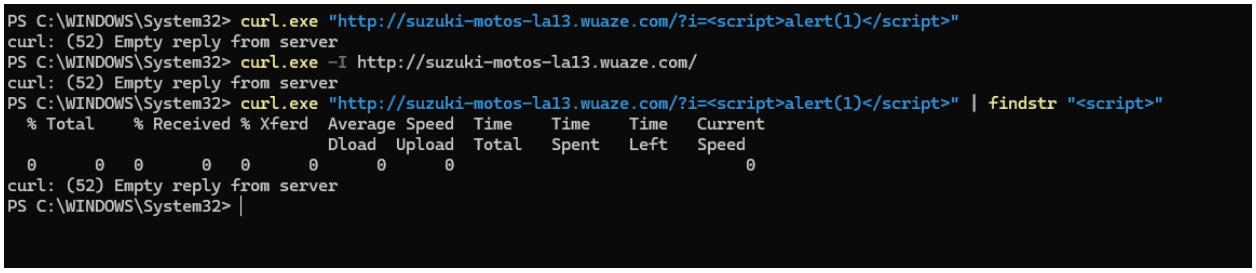


Figura 28. Escaneo OWASP ZAP

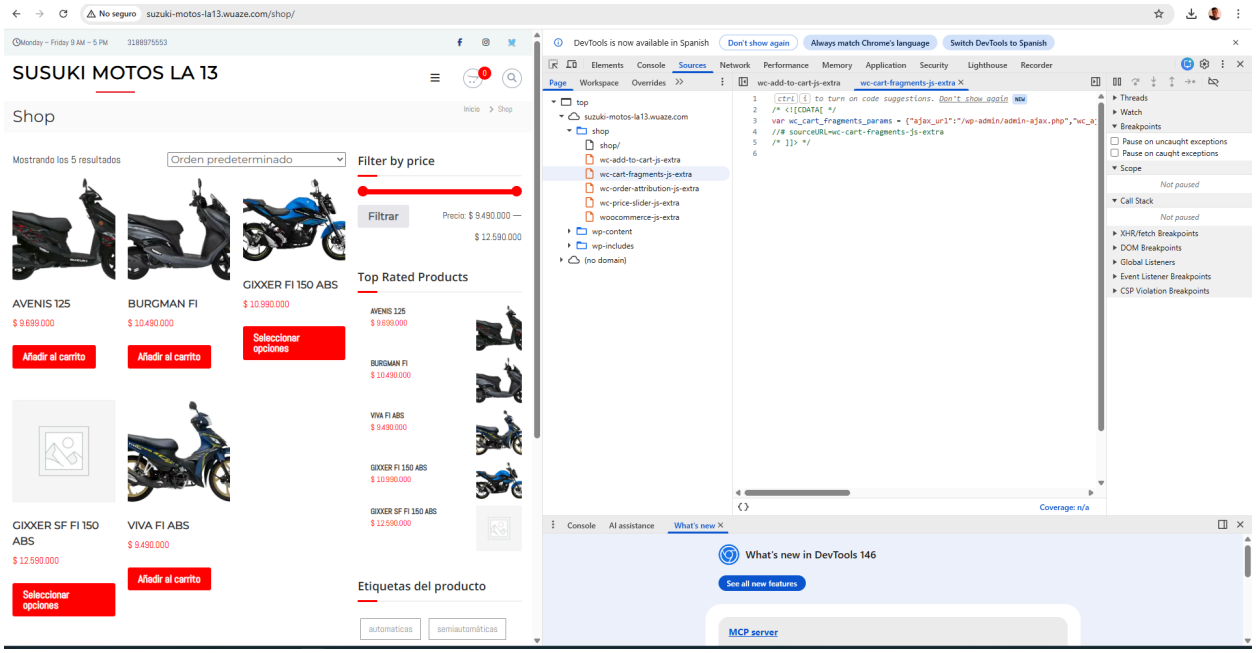


Figura 29. Resultados de análisis automatizado

Vulnerabilidades. No se identificaron vulnerabilidades de inyección SQL en la aplicación tras realizar pruebas automatizadas con OWASP ZAP, lo que sugiere que los mecanismos de validación de entradas están funcionando correctamente en los puntos evaluados.

Mitigación. Aunque no hay vulnerabilidad directa, se recomienda:

- Mantener validación de entradas
- Usar consultas parametrizadas
- Evitar concatenación directa en SQL

3.2.4 Insecure Design

Se realizó un análisis de forma manual del comportamiento de la aplicación web, ingresando a http://suzuki-motos-la13.wuaze.com/wp-login.php, donde ya se evidenció la enumeración de usuarios (A01) y se permiten varios intentos de acceso.

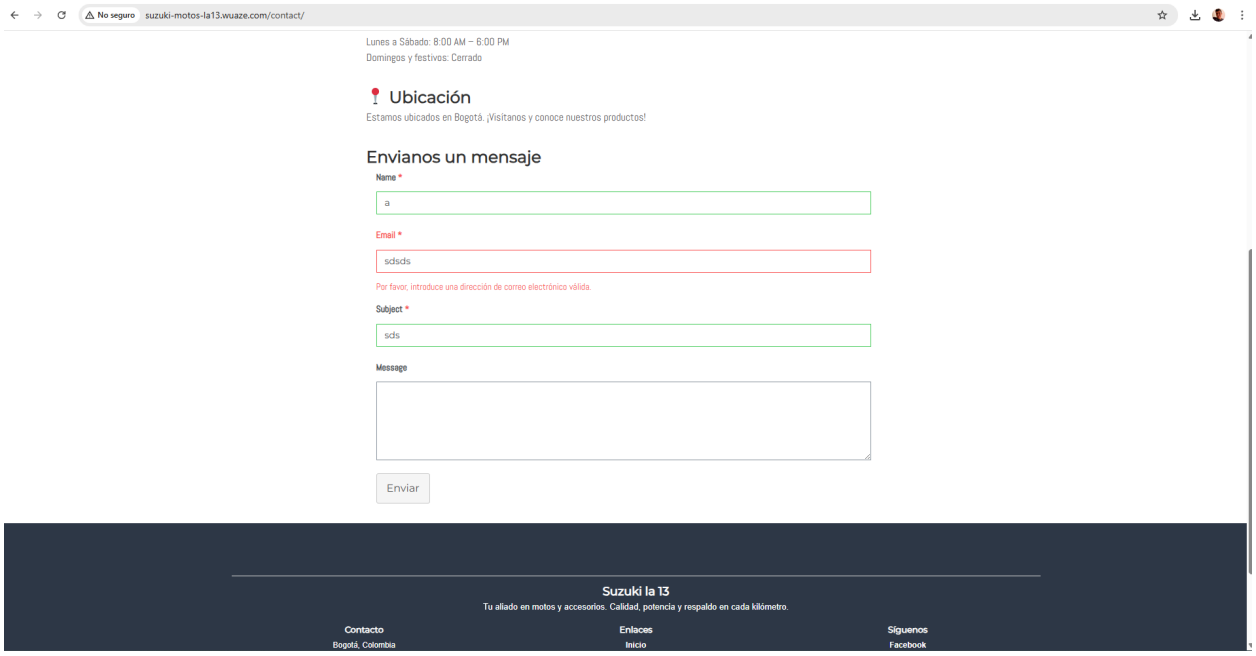


Figura 30. Página de login expuesta

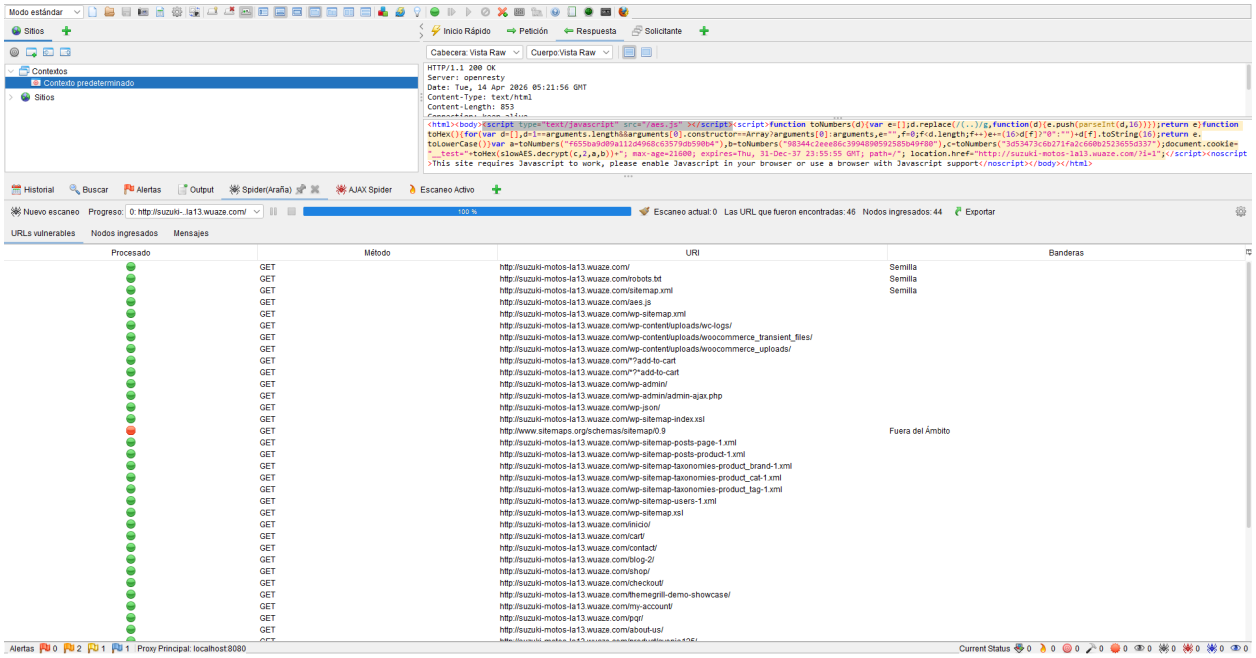


Figura 31. Intentos múltiples de autenticación

Vulnerabilidades. Se identificó que la aplicación no implementa controles de seguridad adecuados en el diseño del sistema de autenticación, permitiendo la exposición del formulario de login sin mecanismos de protección contra ataques como captcha, bloqueo de intentos fallidos y MFA.

Mitigación. Se recomienda:

- Implementar CAPTCHA en login
- Limitar intentos de autenticación
- Implementar bloqueo temporal por intentos fallidos
- Habilitar autenticación multifactor (MFA)
- Evitar uso de usuario admin

3.2.5 Security Misconfiguration

Se realizó la validación mediante OWASP ZAP para la validación de los cabeceros de seguridad de la aplicación.

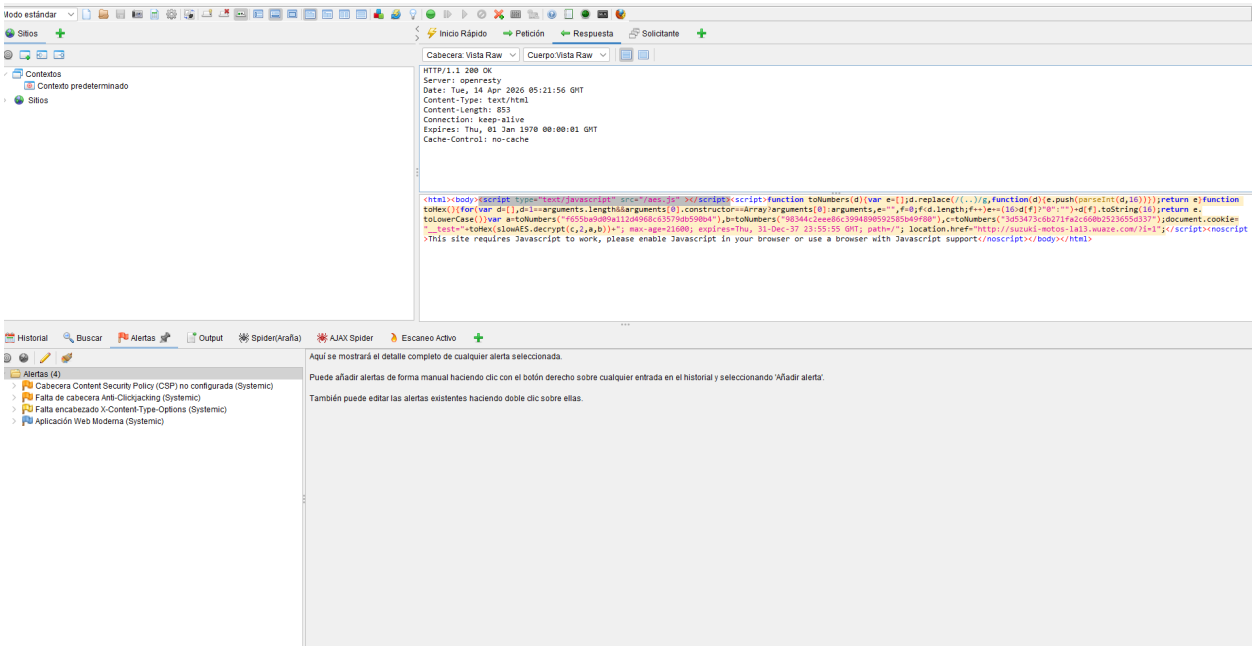


Figura 32. Resultados de cabeceras HTTP

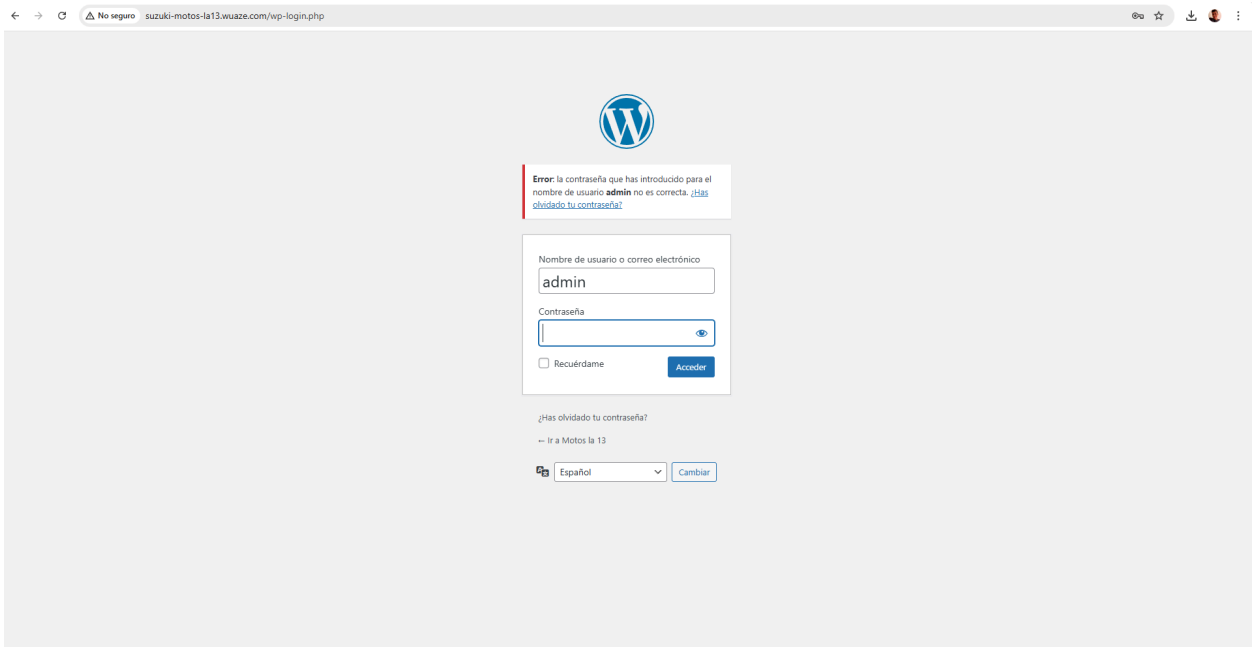


Figura 33. Configuración insegura detectada

Vulnerabilidades. Se identificaron múltiples configuraciones inseguras en el servidor y la aplicación, incluyendo la ausencia de cabeceras de seguridad HTTP y un comportamiento incorrecto en la implementación de HTTP y HTTPS. Estas deficiencias pueden facilitar ataques, inyección de contenido y explotación de vulnerabilidades del navegador.

Mitigación. Se recomienda:

- Configurar correctamente SSL/TLS
- Validar certificado
- Corregir cierre de conexión TLS
- Revisar configuración en hosting (Wuaze)
- Asegurar respuestas HTTP válidas
- Eliminar configuraciones por defecto inseguras

3.2.6 Vulnerable Components

Se validó con OWASP ZAP y con WPScan la revisión manual de respuestas HTTP para identificar tecnologías y comportamientos del servidor.

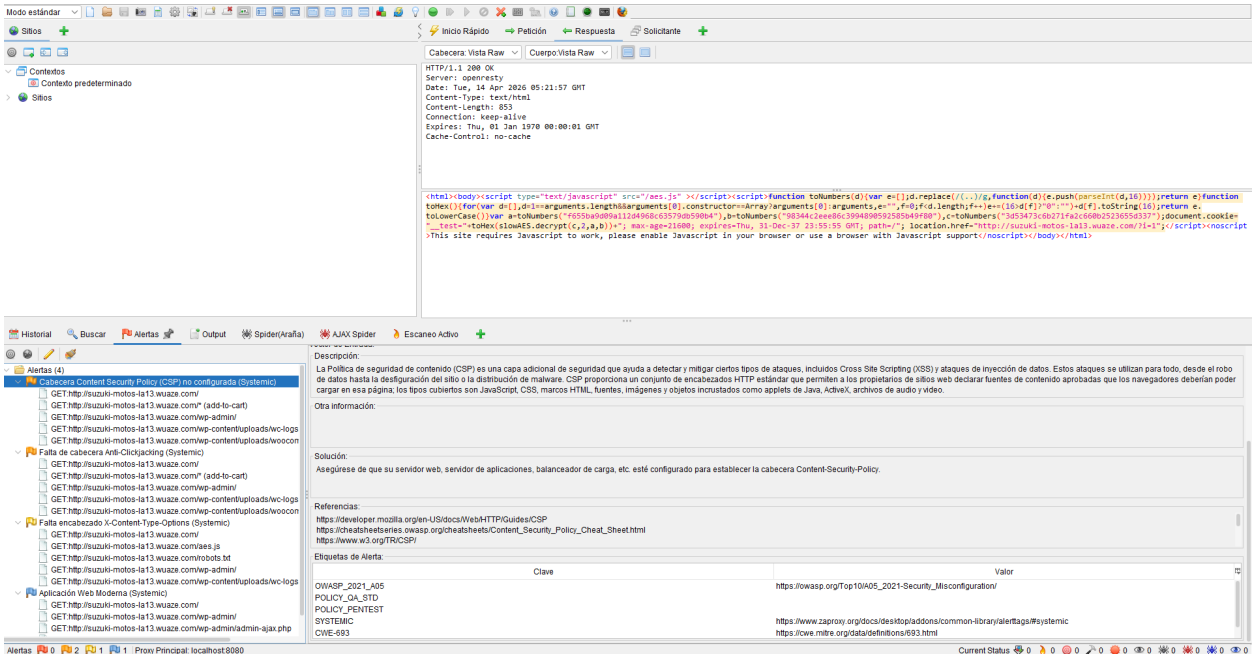


Figura 34. Identificación de tecnologías web

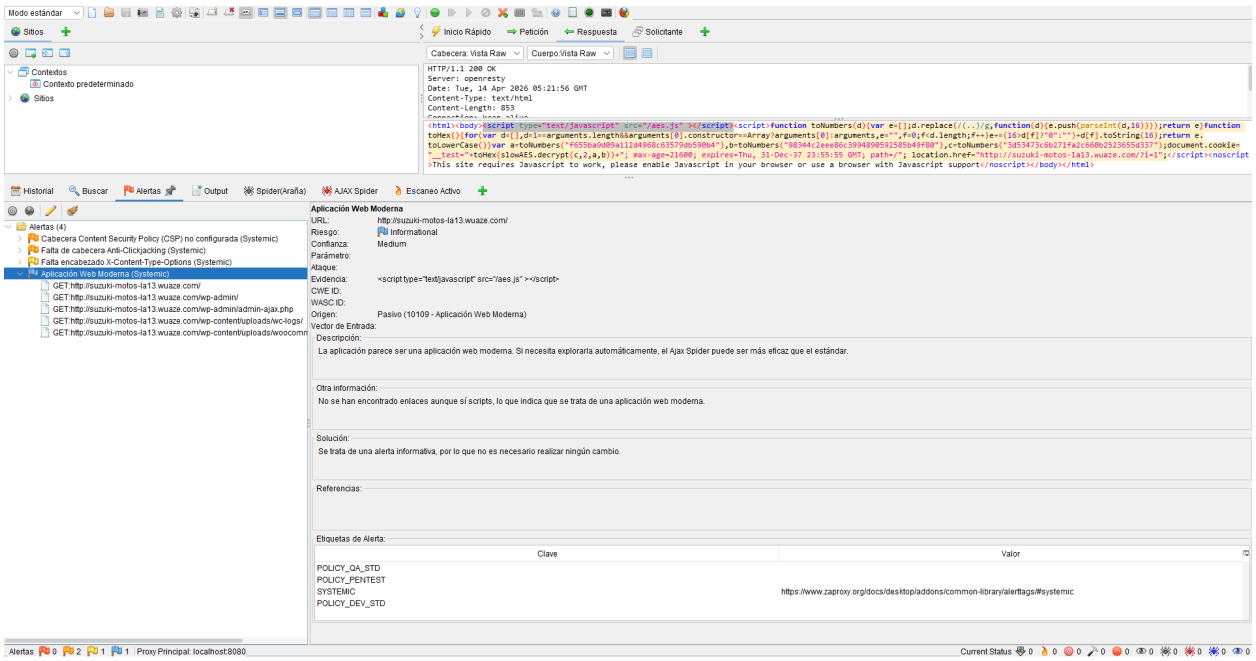


Figura 35. Error de herramienta WPScan

Vulnerabilidades. Se identificó que la aplicación utiliza múltiples componentes tecnológicos como WordPress, OpenResty y librerías del lado cliente. No se evidenció directamente el uso de

versiones vulnerables; sin embargo, la falta de control sobre actualizaciones y dependencias puede representar un riesgo potencial si no se gestionan adecuadamente.

Se intentó realizar un análisis automatizado mediante la herramienta WPScan con el fin de identificar componentes vulnerables en la aplicación WordPress. Sin embargo, durante la ejecución se presentó un error relacionado con dependencias del entorno (libcurl), lo que impidió completar el análisis.

Mitigación. Se recomienda:

- Mantener WordPress actualizado
- Actualizar plugins y temas
- Eliminar plugins innecesarios
- Ocultar versión del servidor
- Implementar escaneo periódico de vulnerabilidades

3.2.7 Identification and Authentication Failures

Se realizaron pruebas manuales introduciendo payloads de XSS en distintos campos de entrada del sitio web como formularios de contacto y campos de búsqueda.

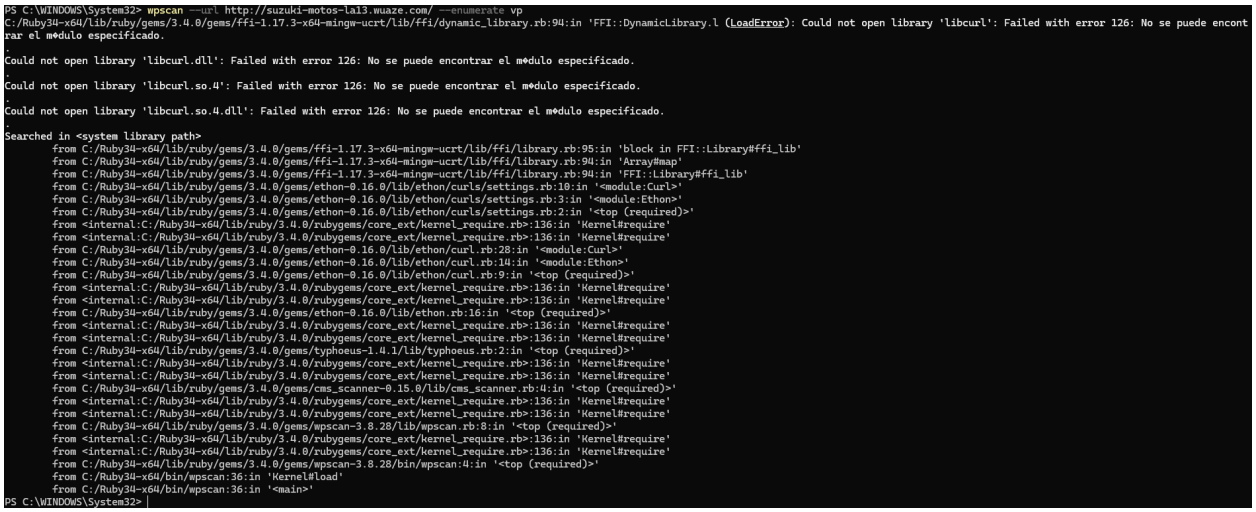


Figura 36. Prueba XSS en formulario web

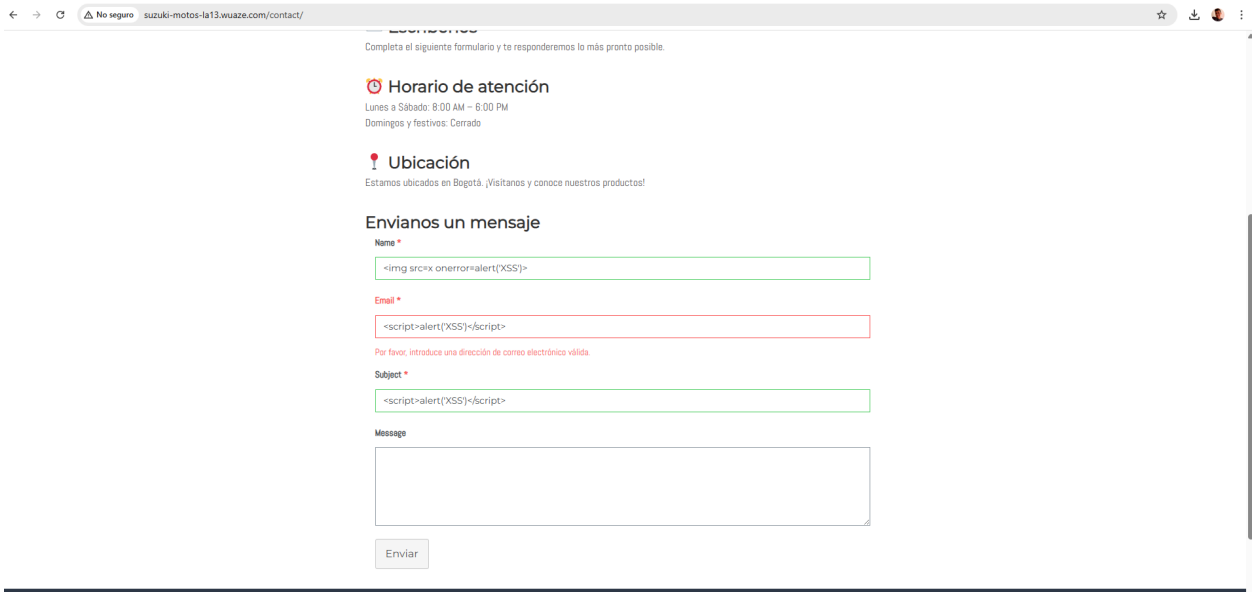


Figura 37. Validación de entradas en formulario

Vulnerabilidades. Se realizaron pruebas de inyección de código JavaScript en el formulario de contacto mediante distintos payloads XSS. No se evidenció ejecución de scripts en el navegador, lo que indica que la aplicación implementa mecanismos de validación y/o sanitización de entradas.

Se realizaron pruebas complementarias mediante solicitudes HTTP desde consola utilizando payloads XSS, con el fin de verificar si la aplicación reflejaba entradas maliciosas en sus respuestas.

```
PS C:\WINDOWS\System32> curl.exe "http://suzuki-motos-la13.wuaze.com/?i=<script>alert(1)</script>"
curl: (52) Empty reply from server
PS C:\WINDOWS\System32> curl.exe -I http://suzuki-motos-la13.wuaze.com/
curl: (52) Empty reply from server
PS C:\WINDOWS\System32> curl.exe "http://suzuki-motos-la13.wuaze.com/?i=<script>alert(1)</script>" | findstr "<script>"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0                              0
curl: (52) Empty reply from server
PS C:\WINDOWS\System32>
```

Figura 38. Prueba XSS desde consola

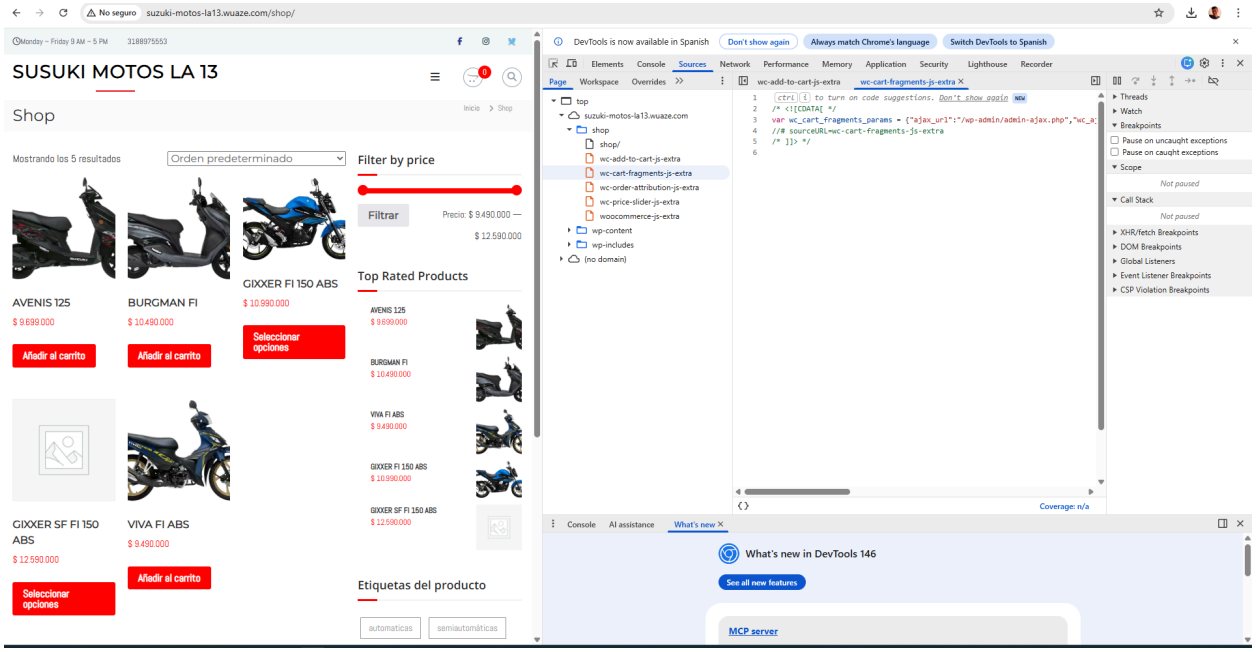


Figura 39. Respuesta sin ejecución de scripts

Mitigación. Se observó validación en el campo de correo electrónico, lo que evidencia controles adicionales en ciertos inputs, reforzando la seguridad del formulario.

3.2.8 Integrity Failures

Se realizó la inspección de código con la opción inspeccionar y la revisión de respuestas del ZAP.

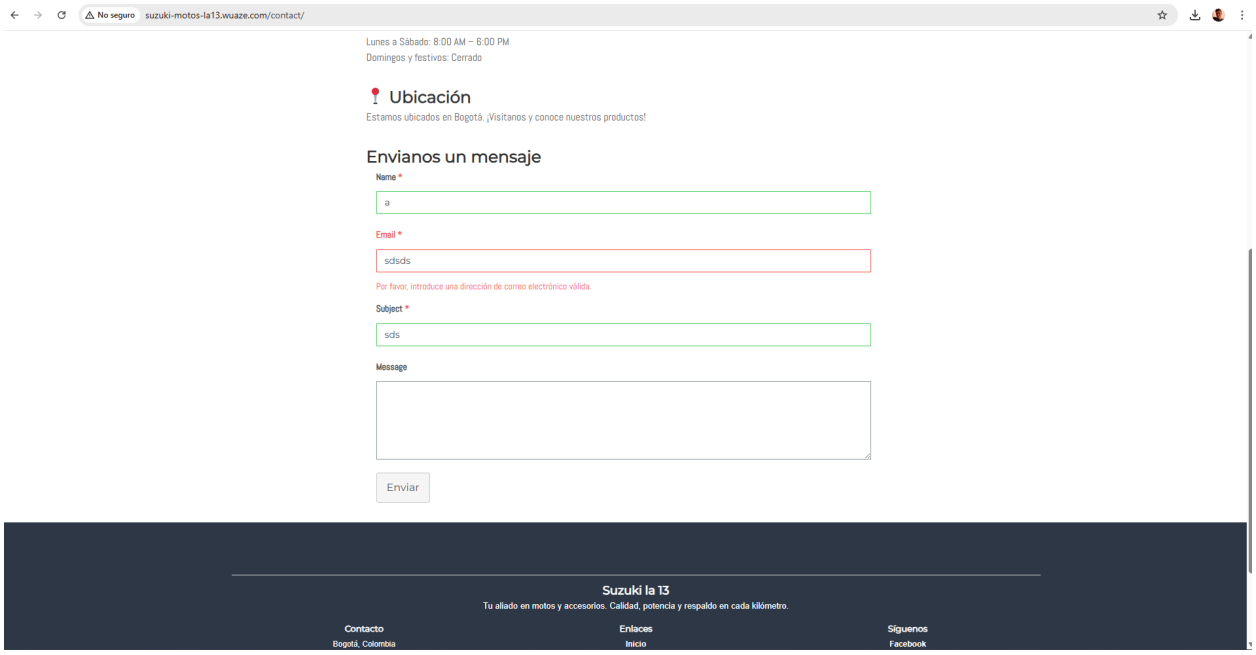


Figura 40. Scripts cargados sin integridad

Vulnerabilidades. Se identificó que la aplicación carga múltiples scripts JavaScript asociados a WordPress y WooCommerce sin mecanismos visibles de verificación de integridad, como Subresource Integrity (SRI), ni restricciones mediante políticas de seguridad de contenido (CSP).

Mitigación. Se recomienda:

- Implementar CSP
- Usar Subresource Integrity (SRI)
- Controlar scripts cargados
- Limitar dependencias innecesarias
- Mantener plugins actualizados

3.2.9 Logging Failures

Se realizaron varios intentos de envío de formulario con datos inválidos, se realizó prueba de inyección y validación de comportamiento de la web ante posibles errores.

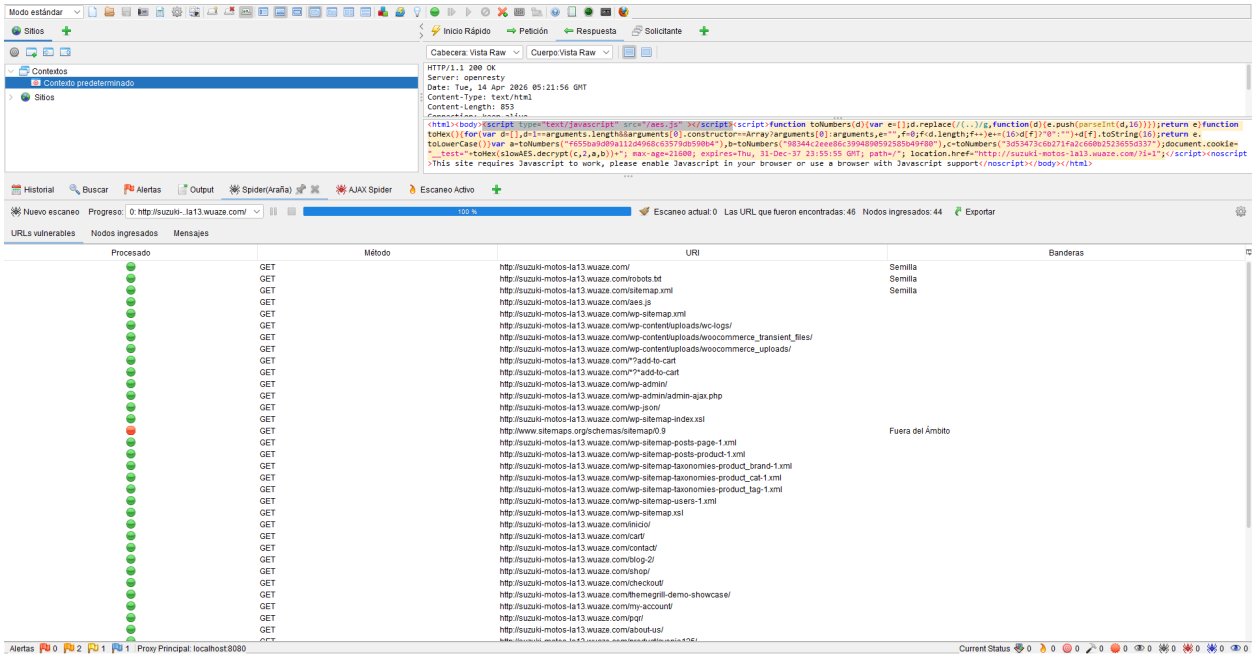


Figura 41. Falta de monitoreo de eventos

Vulnerabilidades. No se evidenciaron mecanismos de registro ni monitoreo de eventos de seguridad en la aplicación. Las pruebas realizadas no generaron alertas visibles, bloqueos ni registros de actividad sospechosa, lo que podría dificultar la detección de ataques o incidentes de seguridad.

Mitigación. Se recomienda:

- Implementar logging de eventos críticos: login, errores, intentos fallidos
- Monitoreo en tiempo real
- Alertas de seguridad
- Centralización de logs

3.2.10 Server-Side Request Forgery (SSRF)

Se realizó un análisis manual de la aplicación, incluyendo: revisión de funcionalidades visibles (formulario de contacto, tienda WooCommerce, navegación general); búsqueda de

parámetros en URL (?i=1 y otros posibles parámetros dinámicos); observación del tráfico con navegador (DevTools) y OWASP ZAP.

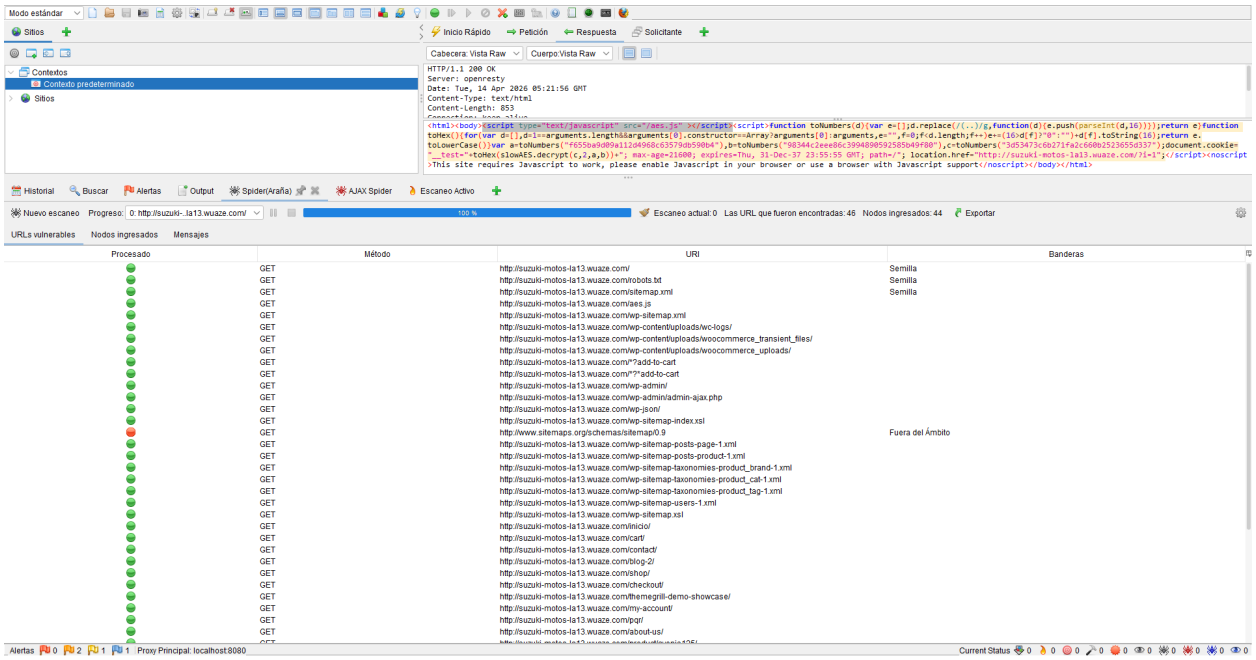


Figura 42. Análisis SSRF sin evidencia de vulnerabilidad

Hallazgo. No se identificaron vulnerabilidades de tipo SSRF en la aplicación, ya que no se encontraron funcionalidades que permitan al usuario influir en solicitudes realizadas por el servidor hacia recursos internos o externos.

Posible mitigación. Aunque no se detectó vulnerabilidad, se recomienda:

- Validar URLs de entrada
- Restringir conexiones salientes del servidor
- Usar listas blancas (whitelist)
- Bloquear acceso a IPs internas
- Implementar firewalls de aplicación (WAF)

Referencias

ICANN. (s. f.). *WHOIS lookup*. https://lookup.icann.org/

OWASP Foundation. (2021). *OWASP Top 10: The ten most critical web application security risks*. OWASP. https://owasp.org/www-project-top-ten/

OWASP Foundation. (2023). *OWASP Web Security Testing Guide*. OWASP. https://owasp.org/www-project-web-security-testing-guide/

OWASP Foundation. (2023). *OWASP Zed Attack Proxy (ZAP)*. OWASP. https://owasp.org/www-project-zap/

Qualys, Inc. (s. f.). *SSL Server Test*. SSL Labs. https://www.ssllabs.com/ssltest/

WordPress Foundation. (2023). *WordPress security white paper*. WordPress.org. https://wordpress.org/about/security/