EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://linuxshopv2.site.je/	Checks	9 pruebas
Dominio	linuxshopv2.site.je	Hallazgos	44 totales
Fecha	3 de septiembre de 2026 a las 01:05	Problemas	15 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre linuxshopv2.site.je arroja una puntuación de 61/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 comprobaciones pasivas, obteniendo 6 resultados satisfactorios, 0 advertencias y 3 fallos críticos en la configuración. El sitio presenta deficiencias graves en la implementación de políticas de seguridad y en la gestión del tráfico cifrado, al no forzar conexiones seguras. A pesar de tener un certificado SSL válido, la falta de cabeceras de protección básicas hace que el sitio se considere vulnerable ante ataques comunes. No se ejecutó un pentest activo en este escaneo.

Resumen de Riesgos

0	5	8	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-11-14T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-16T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: openresty — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta esta cabecera esencial para prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido.
[HIGH] X-Frame-Options: El sitio no protege contra ataques de clickjacking al no restringir cómo se carga la página en marcos o iframes.
[HIGH] Strict-Transport-Security: No se aplica la política HSTS, lo que impide que los navegadores fuercen siempre una conexión HTTPS segura.
[HIGH] Redirección HTTP a HTTPS: El servidor permite conexiones inseguras a través del puerto 80 sin redirigir automáticamente al tráfico cifrado.

[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite que los navegadores realicen sniffing de tipos MIME, aumentando el riesgo de ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe una política que controle qué información de referencia se envía a otros sitios web al navegar desde la página.
[MEDIUM] Permissions-Policy: No se han definido restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivos informativos expuestos: El acceso público a /readme.html y /README.txt puede revelar información técnica sensible sobre la infraestructura.
[MEDIUM] Rutas de login accesibles: Se detectó acceso público a paneles de administración como /wp-login.php, /administrator/ y /user/login.
[LOW] Server header expuesto: La cabecera revela el uso de la tecnología openresty, lo cual facilita a un atacante la búsqueda de exploits específicos para ese software.
[LOW] Ausencia de robots.txt: No se encontró el archivo de control para motores de búsqueda, lo que dificulta la gestión del rastreo.