EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://lldp2.cc/	Checks	9 pruebas
Dominio	lldp2.cc	Hallazgos	45 totales
Fecha	18 de mayo de 2026 a las 20:51	Problemas	11 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras completar la auditoría técnica del sitio web, los resultados arrojan una puntuación de 65/100, lo que corresponde a una calificación de C. El análisis se basó exclusivamente en 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias y 3 presentaron fallos críticos de configuración. Se ha detectado una ausencia alarmante de cabeceras de seguridad y una gestión deficiente en la redirección forzada de tráfico cifrado. Debido a estas omisiones técnicas, se concluye que el sitio es actualmente vulnerable a ataques de intermediario e inyección de código. Es imperativo aplicar medidas correctivas para elevar el nivel de protección de la infraestructura actual.

Resumen de Riesgos

0	3	6	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 64 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 64 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  64 dias restantes (expira: 2026-07-22T03:27:53.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-23T03:27:54.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000; preload
- 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
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000; preload
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 dias
- 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

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- 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)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso en el navegador del usuario.

[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, permitiendo que terceros carguen la web en marcos invisibles para engañar a los visitantes.
[HIGH] Redirección HTTPS: El servidor no fuerza el paso de HTTP a HTTPS, permitiendo que las comunicaciones viajen sin cifrar y sean interceptadas fácilmente.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva expone a los usuarios a ataques de MIME-type sniffing, donde el navegador interpreta archivos de forma insegura.
[MEDIUM] Referrer-Policy: No existe control sobre la información de procedencia enviada a enlaces externos, lo que puede derivar en la fuga de datos de navegación.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador, como la cámara o el micrófono, aumentando la superficie de ataque.
[MEDIUM] HSTS max-age insuficiente: El tiempo de persistencia de seguridad HTTPS está configurado en solo 30 días, muy por debajo de los 180 días recomendados como estándar de industria.
[MEDIUM] Rutas administrativas expuestas: Se han localizado los puntos de acceso /administrator/ y /user/login disponibles públicamente, lo que facilita intentos de acceso no autorizado.
[LOW] Ausencia de archivos de indexación: No se encontraron los archivos robots.txt ni sitemap.xml, lo que impide un control adecuado sobre el rastreo de los motores de búsqueda.