EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://eco-green.us	Checks	9 pruebas
Dominio	eco-green.us	Hallazgos	45 totales
Fecha	17 de agosto de 2026 a las 19:18	Problemas	16 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web eco-green.us presenta una puntuación de 68/100, lo que resulta en una calificación de nota C. Durante la evaluación se llevaron a cabo 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fueron fallos críticos. Aunque el cifrado de transporte inicial es correcto, la exposición de múltiples servicios internos y la falta de cabeceras de seguridad fundamentales comprometen la integridad de la plataforma. Se concluye que el sitio es vulnerable y requiere una intervención inmediata para mitigar riesgos de filtración de datos y acceso no autorizado.

Resumen de Riesgos

6	5	3	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 36 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	67	AVISO	_eco_green_session: falta Secure
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	9 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 36 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  36 dias restantes (expira: 2026-09-22T23:35:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-24T23:35:28.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Fly/40bd1ce81 (2026-08-13) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://eco-green.us/
- 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
- INFO **Tecnologias detectadas**
  Next.js

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

Seguridad de Cookies — 67/100

Estado: AVISO

_eco_green_session: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: _eco_green_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: _eco_green_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: _eco_green_session — SameSite**
  SameSite=lax

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 **sitemap.xml**
  No encontrado (HTTP 406)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

9 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- CRITICO **Puerto 23 (Telnet)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- CRITICO **Puerto 27017 (MongoDB)**
  ABIERTO — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 23 (Telnet), 3306 (MySQL), 3389 (RDP), 5432 (PostgreSQL), 6379 (Redis), 27017 (MongoDB): Servicios de administración y bases de datos expuestos directamente a internet sin protección de firewall.
[HIGH] Content-Security-Policy: Ausencia de cabecera que previene ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] Strict-Transport-Security: Falta de configuración HSTS que obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de protocolo.

[HIGH] Cookie _eco_green_session: El flag Secure no está configurado, permitiendo que la cookie de sesión se transmita por canales no cifrados.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos activo que envía credenciales y datos en texto plano.
[MEDIUM] Permissions-Policy: Falta de restricciones sobre el uso de APIs del navegador como cámara, micrófono o geolocalización.
[MEDIUM] Puerto 22 (SSH) y 8080 (HTTP-Alt): Servicios de acceso remoto y servidores alternativos visibles que aumentan la superficie de ataque.
[LOW] Server header expuesto: El servidor Fly/40bd1ce81 revela información técnica que facilita el reconocimiento para ataques dirigidos.
[LOW] sitemap.xml y robots.txt: Ausencia de archivos de estructura que indica una configuración web incompleta o errores de acceso (HTTP 406).