EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://soporte.degenaro.eu	Checks	9 pruebas
Dominio	soporte.degenaro.eu	Hallazgos	51 totales
Fecha	4 de mayo de 2026 a las 21:56	Problemas	11 detectados

A

91/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado en soporte.degenaro.eu arroja una puntuación de 91/100 con una calificación de grado A. Se ejecutaron 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias y 3 generaron advertencias que requieren atención técnica. El sitio muestra una base sólida en cuanto a cifrado y protocolos de transferencia, aunque se identificaron vectores de exposición de información en la configuración del servidor. En conclusión, el sitio se considera seguro bajo parámetros generales, pero presenta vulnerabilidades moderadas que podrían ser explotadas para realizar reconocimiento avanzado. La ausencia de un pentest activo implica que no se han evaluado vulnerabilidades de ejecución o lógica de negocio.

Resumen de Riesgos

0	0	7	4	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 40 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 40 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  40 dias restantes (expira: 2026-06-13T11:44:57.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-15T10:46:29.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self';script-src 'self' 'unsafe-inline' https://fonts.googleapis.co...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://soporte.degenaro.eu/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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
- INFO **Tecnologias detectadas**
  Next.js

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 /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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (295861 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "\.env" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un puerto de servidor web alternativo aumenta la superficie de ataque y puede exponer servicios internos no protegidos.
[MEDIUM] Paneles de login accesibles: Las rutas /administrator/ y /user/login son accesibles públicamente, lo que facilita intentos de intrusión mediante fuerza bruta.
[MEDIUM] Exposición de archivos de documentación: Los archivos /readme.html y /README.txt están expuestos, lo cual permite a un atacante identificar versiones de software o configuraciones internas.
[MEDIUM] Rutas sensibles en robots.txt: El archivo referencia directamente carpetas críticas como admin, .env y config, sirviendo como una hoja de ruta para atacantes.
[MEDIUM] Falta de cabecera Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono, aumentando el riesgo de ataques de privacidad.
[LOW] Cabecera de servidor expuesta: El campo Server revela el uso de Cloudflare, proporcionando información sobre la infraestructura tecnológica subyacente.
[LOW] Falta de sitemap.xml: La ausencia de este archivo y un bloqueo total en robots.txt dificulta la indexación controlada y el análisis de estructura legítima.