EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.graficaslar.es/	Checks	9 pruebas
Dominio	www.graficaslar.es	Hallazgos	51 totales
Fecha	16 de junio de 2026 a las 07:00	Problemas	19 detectados

D

54/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 54/100, lo que resulta en una calificación de grado D. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, obteniendo 2 resultados satisfactorios, 5 advertencias y 2 fallos críticos en la configuración. Se han identificado deficiencias severas en las cabeceras de protección y la exposición de servicios de red no cifrados que comprometen la integridad de la plataforma. Debido a la ausencia de políticas de seguridad modernas y la presencia de contenido mixto, el sitio se considera vulnerable ante ataques de interceptación y suplantación. Es urgente aplicar medidas correctivas para elevar el nivel de protección de la infraestructura actual.

Resumen de Riesgos

0	5	9	5	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Joomla
Version CMS Expuesta	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	f37d363274cb3fa0825581fc1126944a: falta SameSite
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 42 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  42 dias restantes (expira: 2026-07-28T07:43:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-29T07:43:48.000Z
- 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: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.31, PleskLin — Revela framework/lenguaje
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.graficaslar.es/
- 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

CMS detectado: Joomla

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  Detectado via HTML body
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Helix Ultimate - The Most Popular Joomla! Template Framework.
- INFO **Tecnologias detectadas**
  PHP/8.2.31, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

Seguridad de Cookies — 67/100

Estado: AVISO

f37d363274cb3fa0825581fc1126944a: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: f37d363274cb3fa0825581fc1126944a — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: f37d363274cb3fa0825581fc1126944a — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: f37d363274cb3fa0825581fc1126944a — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.libroslar.com
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.libroslar.com

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (779 bytes)
- INFO **Reglas robots.txt**
  13 Disallow, 5 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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 la cabecera CSP, lo que permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea susceptible a ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, permitiendo que las conexiones puedan ser degradadas a HTTP inseguro.
[HIGH] Puerto 21 (FTP): El puerto está abierto, lo que implica el uso de un protocolo de transferencia de archivos que envía credenciales y datos sin cifrar.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, aumentando el riesgo de ejecución de archivos no autorizados.
[MEDIUM] Referrer-Policy: No hay control sobre la información de referencia que se envía a otros sitios web al navegar.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Seguridad de Cookies: La cookie de sesión f37d363274cb3fa0825581fc1126944a no tiene el atributo SameSite, facilitando ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron recursos cargados mediante HTTP en una página HTTPS, lo que rompe la cadena de confianza del cifrado.
[MEDIUM] Ruta /administrator/: El panel de acceso administrativo de Joomla es públicamente accesible, facilitando intentos de intrusión por fuerza bruta.
[MEDIUM] Archivo /README.txt: Este archivo técnico es accesible y puede revelar información específica sobre la estructura o versiones del sistema.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto está abierto, representando un vector potencial de ataque si no está debidamente protegido.
[MEDIUM] Versión CMS Expuesta: Se ha detectado información que apunta a una versión de WordPress 2 expuesta, lo cual supone un riesgo alto por obsolescencia.
[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando información útil a posibles atacantes para buscar exploits específicos.
[LOW] X-Powered-By expuesto: Se detalla el uso de PHP/8.2.31 y PleskLin, exponiendo la tecnología subyacente del backend.
[LOW] Meta generator: El código fuente expone el uso del framework Helix Ultimate para Joomla.
[LOW] Rutas sensibles en robots.txt: Se hace referencia directa a directorios de administración, guiando a atacantes hacia rutas críticas.
[LOW] sitemap.xml: El archivo no fue encontrado, lo que dificulta la auditoría de la estructura completa del sitio.