EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://anonimizaidor.es	Checks	9 pruebas
Dominio	anonimizaidor.es	Hallazgos	46 totales
Fecha	16 de septiembre de 2026 a las 15:32	Problemas	14 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web anonimizaidor.es ha arrojado una puntuación de 72/100, lo que resulta en una calificación de grado C. El análisis se basó en la ejecución de 9 checks pasivos, de los cuales 6 finalizaron correctamente, 2 generaron advertencias y 1 resultó en fallo crítico. Aunque el cifrado de datos mediante SSL es óptimo, el sitio presenta deficiencias graves en la implementación de cabeceras de seguridad y exposición de servicios internos. Se concluye que el sitio es vulnerable a ataques de inyección, suplantación de identidad y fuerza bruta debido a una configuración de servidor incompleta.

Resumen de Riesgos

0	4	9	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 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	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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-12-09T06:57:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-10T06:57:27.000Z
- 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

- 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://anonimizaidor.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

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (129 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://anonimizaidor.es/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — 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 (CSP) ausente: La falta de esta política facilita la ejecución de ataques Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options ausente: El sitio no protege contra ataques de clickjacking, permitiendo que atacantes embeban la web en marcos para engañar al usuario.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no instruye al navegador para usar exclusivamente conexiones HTTPS, permitiendo ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options ausente: La carencia de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos con contenido inesperado.
[MEDIUM] Referrer-Policy ausente: No se controla el flujo de información de referencia enviada a otros sitios, lo que podría comprometer la privacidad de la navegación.
[MEDIUM] Permissions-Policy ausente: El navegador no tiene restricciones sobre el uso de APIs sensibles como la cámara o el micrófono dentro del contexto del sitio.
[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo cual revela detalles técnicos innecesarios sobre la infraestructura.
[MEDIUM] Paneles de gestión accesibles: Se detectó acceso público a rutas administrativas como /wp-login.php y /administrator/, aumentando el riesgo de ataques dirigidos a credenciales.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administración remota está expuesto a internet, lo que representa un vector de ataque si no existen controles de acceso estrictos.
[LOW] Cabecera Server expuesta: El servidor revela que utiliza la tecnología nginx, proporcionando información útil para que un atacante busque vulnerabilidades específicas.