

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://deporteselda.es/	Checks	9 pruebas
Dominio	deporteselda.es	Hallazgos	44 totales
Fecha	6 de octubre de 2026 a las 09:56	Problemas	15 detectados

D

53/100

puntos de seguridad



RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre deporteselda.es arroja una puntuacion de 53/100, lo que equivale a una nota D. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios y 4 presentaron fallos significativos. A pesar de contar con un cifrado SSL correcto, la infraestructura presenta debilidades criticas en la configuracion del servidor y la exposicion de servicios internos. Debido a la presencia de puertos abiertos de alto riesgo y la ausencia de cabeceras de proteccion, el sitio se clasifica actualmente como vulnerable.

Resumen de Riesgos

2 CRITICO	6 ALTO	3 MEDIO	4 BAJO	29 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 78 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 78 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
78 dias restantes (expira: 2026-12-23T12:49:27.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-24T12:49:28.000Z
- 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/8.3.27 — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 200 — No redirige a HTTPS
- 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
PHP/8.3.27

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 — 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 — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO

Puerto 21 (FTP)
ABIERTO — Transferencia de archivos sin cifrar
- INFO

Puerto 22 (SSH)
Cerrado — 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
- 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

[CRITICAL] Puerto 3306 (MySQL): Base de datos expuesta a internet, lo que permite ataques directos de fuerza bruta o exfiltracion de datos.
[CRITICAL] Puerto 23 (Telnet): Servicio de acceso remoto sin cifrar activo, permitiendo la interceptacion de credenciales en texto plano.
[HIGH] Puerto 21 (FTP): Protocolo de transferencia de archivos inseguro que expone el trafico a ataques de intermediario.
[HIGH] Redireccion HTTPS: El servidor no fuerza el uso de conexiones seguras, permitiendo que los usuarios naveguen por HTTP vulnerable.

[HIGH] Content-Security-Policy: Ausencia de politica de seguridad de contenido, dejando el sitio expuesto a inyecciones XSS.
[HIGH] X-Frame-Options: Falta de proteccion contra Clickjacking, permitiendo que el sitio sea embebido en marcos maliciosos.
[HIGH] Strict-Transport-Security: La cabecera HSTS no esta configurada, por lo que el navegador no obliga el uso de HTTPS.
[MEDIUM] X-Content-Type-Options: Riesgo de ataques de sniffing de contenido al no estar definida esta cabecera de seguridad.
[MEDIUM] Referrer-Policy: No se controla la informacion de procedencia enviada en las peticiones salientes.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el acceso de las APIs del navegador a funciones de hardware.
[LOW] Server header expuesto: El servidor revela que utiliza nginx, facilitando la identificacion de exploits especificos.
[LOW] X-Powered-By expuesto: Se muestra publicamente la version PHP/8.3.27, proporcionando informacion valiosa a atacantes.
[LOW] Robots.txt y Sitemap: Los archivos de indexacion y guia para rastreadores no han sido encontrados.