EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.escuela-vela.com/	Checks	9 pruebas
Dominio	www.escuela-vela.com	Hallazgos	49 totales
Fecha	13 de mayo de 2026 a las 11:20	Problemas	19 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web escuela-vela.com ha arrojado una puntuación de 56/100, lo que corresponde a una calificación de grado D. Durante la auditoría se ejecutaron un total de 9 checks pasivos, resultando en 4 verificaciones superadas, 2 advertencias y 3 fallos críticos en la configuración. Se han detectado deficiencias graves en la protección de la infraestructura, destacando la exposición pública de bases de datos y la falta total de cabeceras de seguridad. Debido a la combinación de servicios críticos abiertos y software desactualizado, el sitio se clasifica actualmente como vulnerable y de alto riesgo para la integridad de la información.

Resumen de Riesgos

2	6	8	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 43 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: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 43 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  43 dias restantes (expira: 2026-06-25T01:05:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-27T01:05:27.000Z
- 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://www.escuela-vela.com/
- 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: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://WWW.MALAVIDABEACH.ES
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.theworktrailer.com
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.islantilla.es/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (323 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.escuela-vela.com/wp-sitemap.xml
- 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
- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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): El servicio de base de datos está abierto al exterior, permitiendo intentos de conexión directa y ataques de fuerza bruta.
[CRITICAL] Puerto 5432 (PostgreSQL): Servicio de base de datos expuesto públicamente, lo que representa un riesgo extremo de exfiltración de datos.
[HIGH] Puerto 21 (FTP): Protocolo de transferencia de archivos activo y sin cifrar, vulnerable a la interceptación de credenciales.
[HIGH] WordPress versión 6.9.4 expuesta: El uso de una versión antigua y pública permite a los atacantes explotar vulnerabilidades conocidas (CVEs).
[HIGH] Content-Security-Policy (CSP): Ausencia de esta cabecera, lo que facilita ataques de Cross-Site Scripting (XSS) e inyección de código.
[HIGH] X-Frame-Options: La falta de esta protección hace que el sitio sea susceptible a ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS, permitiendo posibles ataques de degradación de protocolo.
[MEDIUM] Contenido Mixto: Se detectaron 3 recursos cargados mediante HTTP en una página HTTPS, afectando la integridad de la conexión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador realice MIME-sniffing, aumentando el riesgo de ejecución de scripts maliciosos.
[MEDIUM] Ruta /wp-login.php accesible: El panel de administración es visible para cualquier usuario, facilitando ataques de acceso no autorizado.
[MEDIUM] Archivo /readme.html: Este archivo está disponible públicamente y puede ser utilizado para confirmar versiones específicas del CMS.
[MEDIUM] Referrer-Policy y Permissions-Policy: Ausencia de controles sobre la información de referer y el uso de APIs del navegador.
[LOW] Server header expuesto: La cabecera revela el uso de nginx, proporcionando información útil para el reconocimiento por parte de atacantes.
[LOW] Meta generator: La etiqueta identifica explícitamente el uso de WordPress 6.9.4 en el código fuente.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a rutas de administración, guiando a posibles atacantes hacia áreas restringidas.