EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://edutech.global	Checks	9 pruebas
Dominio	edutech.global	Hallazgos	49 totales
Fecha	26 de abril de 2026 a las 21:13	Problemas	15 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre edutech.global ha resultado en una puntuación de 68/100, obteniendo una calificación de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos de configuración. A pesar de contar con un cifrado de transporte adecuado, se han detectado múltiples servicios de bases de datos expuestos y una gestión de cabeceras de seguridad prácticamente inexistente. El sitio presenta una superficie de ataque considerable debido a la visibilidad de puertos internos y versiones de software desactualizadas. Se concluye que el sitio es actualmente vulnerable y requiere intervención inmediata para proteger su infraestructura y datos.

Resumen de Riesgos

2	4	6	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	4 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-06-29T05:18:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-31T05:18:10.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.27.2 — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains;
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://edutech.global/
- 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

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 — 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 (274 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://edutech.global/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

4 puertos riesgosos abiertos

- 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
- 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 5432 (PostgreSQL) abierto: Exposición directa del motor de base de datos a internet, lo que permite ataques de fuerza bruta o explotación de fallos del servicio.
[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos principal es accesible desde el exterior, facilitando intentos de acceso no autorizado a la información almacenada.
[HIGH] Content-Security-Policy faltante: La ausencia de esta cabecera impide prevenir ataques de inyección de código como Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options faltante: El sitio puede ser cargado en marcos externos, lo que lo hace susceptible a ataques de secuestro de clics o clickjacking.
[HIGH] Versión de WordPress 6.9.4 expuesta: Revelar la versión específica del CMS permite a atacantes buscar y ejecutar exploits conocidos para dicha versión.
[HIGH] Puerto 21 (FTP) abierto: El uso de este protocolo implica la transferencia de archivos y credenciales sin cifrado, permitiendo la interceptación de datos.
[MEDIUM] X-Content-Type-Options faltante: No se previene el sniffing de tipos MIME, lo que podría permitir al navegador ejecutar archivos con contenido malicioso disfrazado.
[MEDIUM] Referrer-Policy faltante: El servidor no controla qué información de procedencia se envía a otros sitios, pudiendo filtrar rutas internas.
[MEDIUM] Permissions-Policy faltante: No se restringen las capacidades del navegador para acceder a hardware o APIs, ampliando los vectores de ataque.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administración remota es visible, invitando a intentos de intrusión mediante ataques de diccionario.
[MEDIUM] Archivo /readme.html accesible: Este archivo confirma detalles técnicos y la versión del sistema de gestión de contenidos a terceros.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso administrativo es público, permitiendo ataques directos contra las cuentas de usuario.
[LOW] Server header expuesto: El servidor responde revelando el uso de nginx/1.27.2, facilitando la fase de reconocimiento de un atacante.
[LOW] Meta generator expuesto: La etiqueta en el código fuente confirma nuevamente el uso de WordPress 6.9.4.
[LOW] Ruta sensible en robots.txt: Se listan directorios como "admin", proporcionando pistas sobre la estructura interna del sitio.