EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://testprep.amhealthinstitute.com/	Checks	9 pruebas
Dominio	testprep.amhealthinstitute.com	Hallazgos	49 totales
Fecha	19 de junio de 2026 a las 17:29	Problemas	12 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha arrojado una puntuación de 76/100 con una calificación de grado B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 se marcaron como fallos críticos. Aunque el sitio cuenta con cifrado SSL vigente y redirecciones HTTPS correctas, se detectaron brechas graves relacionadas con la exposición de bases de datos y el uso de software obsoletos. Debido a la presencia de puertos críticos abiertos y una versión de WordPress vulnerable, el sitio se considera actualmente vulnerable y con un nivel de riesgo elevado.

Resumen de Riesgos

2	4	3	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 35 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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 4.5.2 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	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 35 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  35 dias restantes (expira: 2026-07-24T16:59:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-25T16:59:22.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options

- 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
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://testprep.amhealthinstitute.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 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: All in One SEO (AIOSEO) 4.9.8
- INFO **Tecnologias detectadas**
  React, Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.5.2 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 4.5.2 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 (400 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://testprep.amhealthinstitute.com/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) abierto: La base de datos está expuesta directamente a internet, permitiendo intentos de acceso no autorizados y ataques de fuerza bruta.
[CRITICAL] Puerto 5432 (PostgreSQL) abierto: Exposición de la base de datos PostgreSQL, lo que aumenta drásticamente el riesgo de exfiltración de información sensible.
[HIGH] Versión de WordPress 4.5.2 expuesta: El uso de una versión obsoleta facilita ataques dirigidos mediante vulnerabilidades conocidas (CVEs) que ya han sido parcheadas en versiones actuales.
[HIGH] Puerto 21 (FTP) abierto: Este servicio de transferencia de archivos sin cifrar es susceptible a la interceptación de credenciales y datos en tránsito.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera permite la ejecución de ataques de cross-site scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options ausente: La carencia de esta protección hace al sitio vulnerable a ataques de clickjacking para engañar a los usuarios finales.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela información técnica sobre el CMS que asiste a los atacantes en la fase de reconocimiento de la infraestructura.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de administración es accesible públicamente, lo que facilita ataques coordinados de fuerza bruta contra las cuentas de gestión.
[MEDIUM] HSTS max-age insuficiente: La política de transporte estricto está configurada por solo 30 días, incumpliendo el estándar recomendado de al menos 180 días.
[LOW] Cabecera de servidor expuesta: El servidor revela el uso de nginx, proporcionando pistas innecesarias sobre la tecnología de la infraestructura subyacente.
[LOW] Meta generator expuesto: La etiqueta meta revela versiones de plugins activos como All in One SEO 4.9.8, facilitando el perfilado del sitio.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios como "admin", orientando a posibles atacantes hacia zonas que deberían ser restringidas.