EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://asilodicepuebla.com/	Checks	9 pruebas
Dominio	asilodicepuebla.com	Hallazgos	48 totales
Fecha	22 de abril de 2026 a las 21:44	Problemas	17 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 56/100, lo que equivale a una calificación de grado D. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 4 verificaciones exitosas, 2 advertencias y 3 fallos críticos. Aunque el sitio posee un certificado SSL válido, la exposición de servicios internos y la ausencia total de cabeceras de seguridad representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable y requiere intervención inmediata para mitigar riesgos de intrusión y fuga de datos.

Resumen de Riesgos

1	6	9	1	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 40 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
Version CMS Expuesta	20	FALLO	WordPress 6.5.8 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	5 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 40 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  40 dias restantes (expira: 2026-06-02T03:24:44.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-04T03:24:45.000Z
- 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

- 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://asilodicepuebla.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

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.5.8
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.5.8 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.5.8 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 — 20/100

Estado: FALLO

5 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.asilodicepuebla.com
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.instagram.com/pueblapreciosa/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://puebla.gob.mx/
- MEDIO **href (link/stylesheet)**
  ...y 2 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (177 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://asilodicepuebla.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- 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
- 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): La base de datos se encuentra expuesta a internet, lo que permite intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y opera sin cifrado, permitiendo la interceptación de credenciales.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: No se detectó esta cabecera, dejando el sitio vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security: La falta de HSTS permite que los usuarios puedan ser degradados a conexiones HTTP inseguras.
[HIGH] Versión WordPress expuesta: El sistema revela públicamente la versión 6.5.8, permitiendo a atacantes identificar vulnerabilidades específicas.
[MEDIUM] Contenido Mixto: Se detectaron 5 recursos cargando vía HTTP, lo que debilita la integridad de la conexión cifrada.
[MEDIUM] Archivo /readme.html: Este archivo es accesible y revela información técnica sensible sobre la instalación del CMS.
[MEDIUM] Ruta /wp-login.php: El panel de administración es accesible globalmente, aumentando el riesgo de ataques automatizados de acceso.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de ejecución.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación enviada a otros dominios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones del navegador como cámara o micrófono desde el sitio.
[LOW] Meta generator: La etiqueta meta expone detalles del software utilizado en la creación de la página.