EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://losotrosdatos.enews.mx/index	Checks	9 pruebas
Dominio	losotrosdatos.enews.mx	Hallazgos	46 totales
Fecha	4 de abril de 2026 a las 09:12	Problemas	14 detectados

D

58/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web ha resultado en una puntuacion de 58/100, lo que equivale a una nota de D. Durante la evaluacion se ejecutaron 9 checks pasivos, de los cuales 4 resultaron correctos, 3 generaron advertencias y 2 fueron marcados como fallos criticos. El sitio web presenta deficiencias estructurales graves en la configuracion de cabeceras de seguridad y en la proteccion de las sesiones de usuario. Al no haberse ejecutado un pentest activo, el alcance se limita a la superficie visible del servidor. En su estado actual, el sitio se considera vulnerable debido a la falta de controles basicos contra ataques de inyeccion y secuestro de datos.

Resumen de Riesgos

0	7	6	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	60	AVISO	1 recurso(s) 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 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-06-14T11:34:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-16T11:34:03.000Z
- 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: Apache — 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://losotrosdatos.enews.mx/
- 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

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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://html5shim.googlecode.com/svn/trunk/html5.js

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (222 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://losotrosdatos.com.mx/sitemap.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), 22 (SSH)

- 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
- INFO **Puerto 3306 (MySQL)**
  Cerrado — 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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecucion de scripts maliciosos y ataques de inyeccion de contenido XSS.
[HIGH] X-Frame-Options: El sitio carece de proteccion contra clickjacking, permitiendo que atacantes carguen la web en marcos externos para engañar al usuario.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, facilitando ataques de degradacion de conexion y robo de cookies.
[HIGH] Cookie PHPSESSID (HttpOnly): La cookie de sesion es accesible mediante scripts, lo que permite a un atacante robar la identidad del usuario tras un XSS.
[HIGH] Cookie PHPSESSID (Secure): El identificador de sesion puede enviarse a traves de canales no cifrados, quedando expuesto en redes publicas o interceptadas.
[HIGH] Puerto 21 (FTP): El puerto de transferencia de archivos esta abierto y opera sin cifrado, lo que pone en riesgo las credenciales de administracion.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido, facilitando la ejecucion de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla que informacion de origen se envia a otros sitios, lo que puede filtrar URLs privadas o datos sensibles.
[MEDIUM] Permissions-Policy: El sitio no restringe el uso de APIs del navegador como la camara o el microfono, aumentando la superficie de ataque.
[MEDIUM] Cookie PHPSESSID (SameSite): La ausencia de esta configuracion hace que el sitio sea vulnerable a ataques de falsificacion de peticion en sitios cruzados o CSRF.
[MEDIUM] Contenido Mixto: Se detecto el recurso http://html5shim.googlecode.com/svn/trunk/html5.js cargado de forma insegura, comprometiendo la integridad de la pagina.
[MEDIUM] Puerto 22 (SSH): El puerto de acceso remoto esta abierto, representando un vector potencial para ataques de fuerza bruta si no esta debidamente restringido.
[LOW] Server Header Expuesto: La cabecera revela que el servidor utiliza Apache, informacion tecnica que ayuda a un atacante a buscar vulnerabilidades especificas.