EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://x24.com.mx	Checks	9 pruebas
Dominio	x24.com.mx	Hallazgos	42 totales
Fecha	28 de septiembre de 2026 a las 21:27	Problemas	12 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web arroja una puntuacion de 60/100, lo que corresponde a una nota de grado C. Durante la auditoria se ejecutaron 9 checks pasivos, resultando en 4 validaciones correctas, 3 advertencias y 2 fallos criticos. La ausencia total de cabeceras de seguridad y la proximidad extrema de la expiracion del certificado SSL comprometen la integridad de la plataforma. Debido a estas deficiencias tecnicas y la exposicion de informacion del servidor, el sitio se clasifica actualmente como vulnerable.

Resumen de Riesgos

0	5	4	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	50	AVISO	Certificado expira en 1 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	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 50/100

Estado: AVISO

Certificado expira en 1 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- ALTO **Dias hasta expiracion**
  1 dias restantes (expira: 2026-09-29T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-29T00:00:00.000Z
- 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/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 — 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://x24.com.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 — 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

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://x24.com.mx/proveedores/

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- INFO **Puerto 21 (FTP)**
  Cerrado — 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Dias hasta expiracion: El certificado SSL expira en 1 dia, lo que provocara el bloqueo del acceso a los usuarios de forma inminente.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyeccion de codigo y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: No hay proteccion configurada, dejando el sitio vulnerable a ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: La falta de HSTS permite que las conexiones seguras sean degradadas a HTTP mediante ataques de intermediario.
[MEDIUM] Recurso HTTP (Contenido Mixto): Se detecto un enlace stylesheet cargado por HTTP en la ruta /proveedores/, rompiendo el cifrado de la pagina.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador puede interpretar archivos de forma incorrecta facilitando la ejecucion de scripts maliciosos.
[MEDIUM] Referrer-Policy: No se controla la informacion de navegacion que se envia a sitios de terceros mediante los referers.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso del navegador a funciones sensibles como microfono, camara o geolocalizacion.
[LOW] Server header expuesto: El encabezado revela el uso de Apache/2.4.38, OpenSSL/1.0.2q y PHP/5.6.40, proporcionando vectores de ataque especificos.
[LOW] Archivos de rastreo faltantes: La ausencia de robots.txt y sitemap.xml dificulta la auditoria de indexacion y el control de acceso de bots.