EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cursoselite.com.mx	Checks	9 pruebas
Dominio	cursoselite.com.mx	Hallazgos	44 totales
Fecha	28 de mayo de 2026 a las 00:50	Problemas	12 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio cursoselite.com.mx arroja una puntuación técnica de 77/100, lo que otorga una nota de calificación B. Se han ejecutado 9 checks pasivos, resultando en 6 verificaciones exitosas, 1 advertencia y 2 fallos críticos en la configuración. Aunque el cifrado de datos es robusto, la infraestructura presenta carencias importantes en la implementación de cabeceras de seguridad y control de archivos públicos. Se concluye que el sitio es vulnerable a ataques de interceptación de datos y secuestro de clics (clickjacking) debido a la falta de políticas estrictas de transporte. La ausencia de un pentest activo limita la visibilidad sobre vulnerabilidades lógicas profundas, pero los hallazgos actuales demandan atención inmediata.

Resumen de Riesgos

0	3	8	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 78 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 78 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  78 dias restantes (expira: 2026-08-14T00:34:07.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-16T00:34:08.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: hcdn — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://cursoselite.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
- INFO **Tecnologias detectadas**
  React

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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)**
  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

[LOW] Server header expuesto: La cabecera revela el uso de hcdn, lo cual facilita a atacantes potenciales la búsqueda de exploits específicos para esa tecnología.
[HIGH] X-Frame-Options: La falta de esta cabecera permite que el sitio sea cargado dentro de marcos externos, haciendo al usuario vulnerable a ataques de clickjacking.

[HIGH] Strict-Transport-Security: No se implementó HSTS, lo que permite que un atacante intente degradar la conexión de HTTPS a HTTP para capturar datos.
[MEDIUM] X-Content-Type-Options: La ausencia de esta política permite el MIME-type sniffing, pudiendo ejecutar archivos maliciosos disfrazados de elementos legítimos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que podría filtrar rutas internas privadas.
[MEDIUM] Permissions-Policy: El sitio no restringe el uso de APIs del navegador como la cámara o el micrófono, aumentando la superficie de riesgo para el usuario.
[HIGH] HSTS no configurado: Aunque existe redirección a HTTPS, el navegador no está obligado a mantenerla, permitiendo ataques de intermediario (MitM).
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles públicamente y suelen contener detalles técnicos sobre la versión del sistema y su configuración.
[MEDIUM] Paneles de login expuestos: Las rutas /wp-login.php, /administrator/ y /user/login están abiertas, lo que facilita intentos de acceso no autorizado por fuerza bruta.
[FAIL] Ausencia de Robots.txt y Sitemap: No se han definido reglas de rastreo, lo que puede llevar a la indexación de directorios que deberían permanecer privados.