EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://escolar.cobao.edu.mx/	Checks	9 pruebas
Dominio	escolar.cobao.edu.mx	Hallazgos	39 totales
Fecha	29 de abril de 2026 a las 21:17	Problemas	13 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio escolar.cobao.edu.mx arroja una puntuación de 59/100, lo que corresponde a una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 4 verificaciones satisfactorias, 1 advertencia y 2 fallos críticos en la infraestructura base. El sitio web presenta deficiencias graves en el cifrado de datos y la configuración del servidor, exponiendo información técnica sensible. En su estado actual, la plataforma se considera vulnerable debido a la falta de protocolos de comunicación segura.

Resumen de Riesgos

1	5	3	4	26
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

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/2.2.22 (Ubuntu) — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/5.3.10-1ubuntu3.48 — Revela framework/lenguaje
- 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 — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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**
  PHP/5.3.10-1ubuntu3.48

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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 500)
- BAJO **sitemap.xml**
  No encontrado (HTTP 500)
- 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

[CRITICAL] Conexión SSL: No se pudo establecer una conexión cifrada, lo que permite que cualquier dato transmitido sea interceptado fácilmente por terceros.
[HIGH] HTTP a HTTPS: El servidor no redirige automáticamente a una versión segura, manteniendo las sesiones de los usuarios en un canal de comunicación vulnerable.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La falta de esta protección permite ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.
[HIGH] Strict-Transport-Security: No se obliga al uso de conexiones seguras, permitiendo que la comunicación sea degradada a protocolos no cifrados.
[MEDIUM] X-Content-Type-Options: El sitio es vulnerable al sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No se controla el envío de información sobre el origen de la navegación a sitios externos.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones del navegador como la geolocalización o la cámara mediante políticas de seguridad.
[LOW] Server header expuesto: El servidor revela el uso de Apache/2.2.22 sobre Ubuntu, una versión antigua que facilita ataques dirigidos.
[LOW] X-Powered-By expuesto: Se expone el uso de PHP/5.3.10, una versión obsoleta que contiene múltiples vulnerabilidades conocidas.
[LOW] Archivos de gestión: No se encontraron los archivos robots.txt ni sitemap.xml, recibiendo errores internos del servidor (HTTP 500) al intentar acceder a ellos.