EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cbtis123.edu.mx/	Checks	9 pruebas
Dominio	cbtis123.edu.mx	Hallazgos	46 totales
Fecha	27 de abril de 2026 a las 13:17	Problemas	16 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 53/100, lo que representa una calificación de grado D. Se ejecutaron un total de 9 verificaciones pasivas, de las cuales 5 resultaron satisfactorias y 4 presentaron fallos críticos que comprometen la integridad del sitio. El análisis revela deficiencias significativas en la implementación de cabeceras de seguridad y una gestión inadecuada del tráfico cifrado. Con base en estos resultados, se concluye que el sitio es actualmente vulnerable ante ataques comunes de interceptación y suplantación de identidad.

Resumen de Riesgos

0	5	8	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	20	FALLO	25 recursos 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 — 100/100

Estado: OK

Certificado valido, expira en 69 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  69 dias restantes (expira: 2026-07-05T21:22:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-06T21:22:48.000Z
- 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: LiteSpeed — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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 — 20/100

Estado: FALLO

25 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://ajax.googleapis.com/ajax/libs/jquery/1.8/jquery.min.j...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.decidetusestudios.sep.gob.mx/vista/test-vocaciona...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://guias.ceneval.edu.mx
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://acompanamiento.ingreso.cosdac.sems.gob.mx
- MEDIO **href (link/stylesheet)**
  ...y 21 mas del mismo tipo

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] Content-Security-Policy: Falta de política de seguridad de contenido, lo que permite ataques de inyección de scripts y XSS.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no obliga el uso de conexiones seguras.
[HIGH] Redirección HTTPS: El sitio no redirige automáticamente el tráfico HTTP a HTTPS, dejando las conexiones iniciales expuestas.
[MEDIUM] Contenido Mixto: Se detectaron 25 recursos (scripts y hojas de estilo) cargándose mediante HTTP dentro de una página HTTPS.
[MEDIUM] X-Content-Type-Options: Falta la protección contra el rastreo de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios web.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como el acceso a cámara, micrófono o geolocalización.
[LOW] Server header expuesto: El servidor revela la tecnología LiteSpeed, facilitando la búsqueda de vulnerabilidades específicas para dicho software.
[LOW] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos de indexación y guía, dificultando la auditoría legítima y el SEO.