EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://exed.uth.hn/index.php	Checks	9 pruebas
Dominio	exed.uth.hn	Hallazgos	50 totales
Fecha	7 de mayo de 2026 a las 21:44	Problemas	14 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio exed.uth.hn arroja una puntuación técnica de 64/100, lo que resulta en una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fueron clasificados como fallos críticos. Aunque la implementación del certificado SSL es correcta, la ausencia total de cabeceras de seguridad y la exposición de puertos de administración representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable ante ataques de intermediarios, secuestro de clics y explotación de sesiones. Se requiere una remediación técnica inmediata para elevar los estándares de protección de la plataforma.

Resumen de Riesgos

0	4	6	4	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 104 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	67	AVISO	ch_sid: falta SameSite; GotoCourse: falta SameSi...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 104 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  104 dias restantes (expira: 2026-08-19T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-19T00:00:00.000Z
- 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/2.4.41 (Ubuntu) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Lab I+D+i 1 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://exed.uth.hn
- 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
- BAJO **Meta generator**
  Expone: Lab I+D+i 1
- INFO **Tecnologias detectadas**
  Next.js, Astro, Lab I+D+i 1

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 — 67/100

Estado: AVISO

ch_sid: falta SameSite; GotoCourse: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: ch_sid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ch_sid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ch_sid — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: GotoCourse — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: GotoCourse — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: GotoCourse — SameSite**
  Falta SameSite — Vulnerable a CSRF

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

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

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — 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)**
  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 esta cabecera esencial que previene ataques de XSS e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS): No está configurado, lo que impide que el navegador fuerce conexiones HTTPS de manera permanente y segura.
[MEDIUM] X-Content-Type-Options: Falta la cabecera, lo que permite que el navegador realice sniffing de tipos MIME y ejecute archivos con formatos incorrectos.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que podría exponer información sensible en las URL al navegar hacia sitios externos.
[MEDIUM] Permissions-Policy: La falta de esta cabecera impide restringir el acceso de las APIs del navegador a componentes como cámara o micrófono.
[MEDIUM] Cookie ch_sid: Carece del atributo SameSite, lo que aumenta la susceptibilidad ante ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Cookie GotoCourse: Carece del atributo SameSite, exponiendo la sesión del usuario a posibles riesgos de seguridad web comunes.
[MEDIUM] Puerto 22 (SSH) abierto: La detección de un puerto de administración expuesto facilita intentos de acceso no autorizado mediante fuerza bruta.
[LOW] Server header expuesto: Se revela la versión exacta del servidor (Apache/2.4.41 en Ubuntu), facilitando la búsqueda de exploits específicos.
[LOW] X-Powered-By expuesto: El valor Lab I+D+i 1 revela información interna sobre el entorno de desarrollo del sitio.
[LOW] Sitemap y Robots.txt: La ausencia de estos archivos genera un fallo en la estructura de indexación y visibilidad controlada del sitio.