EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://www.absornsawan.ac.th	Checks	9 pruebas
Dominio	www.absornsawan.ac.th	Hallazgos	40 totales
Fecha	17 de septiembre de 2026 a las 01:12	Problemas	12 detectados

D

48/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio revela una puntuación de 48/100, lo que equivale a una calificación de grado D. Durante la auditoría se ejecutaron 9 controles pasivos, de los cuales 4 resultaron satisfactorios, 1 generó una advertencia y 3 fueron fallos críticos. La ausencia de un certificado SSL válido y la falta de implementación de cabeceras de seguridad esenciales comprometen la integridad del sitio. Se concluye que el sitio web es actualmente vulnerable y no cumple con los estándares mínimos de protección para el intercambio de información en línea.

Resumen de Riesgos

1	5	3	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-12-12T12:42:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-13T12:42:15.000Z
- 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: nginx — 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: 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

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 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

[CRITICAL] Certificado SSL no válido: El sitio no cuenta con un certificado SSL funcional, lo que significa que la comunicación entre el usuario y el servidor no está cifrada.
[HIGH] Protocolo Inseguro: El sitio opera bajo HTTP y no redirige automáticamente a HTTPS, permitiendo la interceptación de datos en tránsito.
[HIGH] Content-Security-Policy: Falta esta cabecera, lo que deja al sitio vulnerable a ataques de Cross-Site Scripting (XSS) e inyección de contenido.
[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos (iframes), facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se detectó la política HSTS, por lo que el navegador no puede forzar conexiones seguras de forma obligatoria.
[MEDIUM] X-Content-Type-Options: Falta la instrucción para prevenir el MIME-type sniffing, lo que podría permitir que archivos maliciosos sean interpretados como scripts.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que puede filtrar URLs privadas.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela el uso de la tecnología nginx, proporcionando información útil a posibles atacantes para buscar exploits específicos.
[LOW] robots.txt no encontrado: La ausencia de este archivo dificulta la gestión de la indexación por parte de motores de búsqueda.
[LOW] sitemap.xml no encontrado: No se dispone de un mapa del sitio, lo que afecta negativamente al SEO y a la estructura de navegación.