EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://atencionaclientes.finsus.mx	Checks	9 pruebas
Dominio	atencionaclientes.finsus.mx	Hallazgos	49 totales
Fecha	26 de marzo de 2026 a las 13:53	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio atencionaclientes.finsus.mx arroja una puntuación de 68/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron exitosos, 2 presentaron advertencias y 2 fueron calificados como fallos críticos. Aunque el sitio posee un cifrado de transporte válido, la ausencia total de cabeceras de seguridad y la configuración incorrecta de cookies comprometen la integridad de la plataforma. Se concluye que el sitio es vulnerable y requiere medidas correctivas inmediatas para proteger los datos de los usuarios.

Resumen de Riesgos

0	6	3	3	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 62 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	CMS detectado: PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	67	AVISO	csrf_cookie_name: falta Secure; sp_session: falt...
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 62 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  62 dias restantes (expira: 2026-05-27T19:12:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-26T19:12:36.000Z
- 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 — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 307 redirige a https://atencionaclientes.finsus.mx/authentication/login
- 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

CMS detectado: PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js

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

csrf_cookie_name: falta Secure; sp_session: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: csrf_cookie_name — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: csrf_cookie_name — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: csrf_cookie_name — SameSite**
  SameSite=lax
- INFO **Cookie: sp_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: sp_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: sp_session — SameSite**
  SameSite=lax

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 **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

[ALTA] Content-Security-Policy: La falta de esta cabecera permite ataques de inyección de contenido y ejecución de scripts maliciosos (XSS).
[ALTA] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking mediante el uso de marcos.
[ALTA] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones cifradas, facilitando ataques de degradación de protocolo.
[ALTA] Cookie Secure Flag (csrf_cookie_name): La falta de este atributo permite que la cookie de seguridad se envíe por canales no cifrados.
[ALTA] Cookie Secure Flag (sp_session): Al carecer del flag Secure, la cookie de sesión puede ser interceptada en conexiones HTTP estándar.
[MEDIA] X-Content-Type-Options: La falta de esta protección permite el sniffing de tipos MIME, lo que facilita la ejecución de archivos maliciosos.
[MEDIA] Referrer-Policy: No existe una política definida, lo que provoca que se filtre información sensible de navegación a sitios externos.
[MEDIA] Permissions-Policy: No se restringe el acceso de las APIs del navegador, dejando expuestas funciones como la cámara o el micrófono.
[BAJA] Server header expuesto: El servidor revela que utiliza Apache, lo que ayuda a posibles atacantes a identificar exploits específicos para esa tecnología.
[BAJA] Archivos robots.txt y sitemap.xml faltantes: La ausencia de estos archivos indica una configuración web incompleta y dificulta la auditoría de rutas.