EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://senadual.com/	Checks	9 pruebas
Dominio	senadual.com	Hallazgos	42 totales
Fecha	29 de abril de 2026 a las 18:34	Problemas	8 detectados

B

81/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web senadual.com arroja una puntuación de 81/100, lo que corresponde a una nota B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 5 resultaron correctos, 3 presentaron advertencias y 1 se identificó como fallo crítico. Si bien el sitio posee un cifrado de transporte sólido, la exposición de servicios internos y la falta de políticas de seguridad en cabeceras representan un riesgo significativo. En su estado actual, el sitio se considera vulnerable debido a la exposición pública de puertos críticos que podrían ser explotados por terceros.

Resumen de Riesgos

1	3	1	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	65	AVISO	4/6 presentes. Faltan: Strict-Transport-Security...
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	100	OK	No se encontraron cookies
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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-07-18T09:16:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-19T09:16:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 65/100

Estado: AVISO

4/6 presentes. Faltan: Strict-Transport-Security, Permissions-Policy

- BAJO **Server header expuesto**
  Server: openresty — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com ht...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- 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 301 redirige a https://senadual.com/
- 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 — 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 — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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] Puerto 3306 (MySQL): El puerto de la base de datos se encuentra abierto al tráfico externo, permitiendo ataques de fuerza bruta o acceso directo a la información sensible.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos sin cifrar expuesto, lo que facilita la interceptación de credenciales y datos en tránsito.
[HIGH] HSTS (Strict-Transport-Security): La ausencia de esta cabecera impide que el navegador fuerce siempre conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIUM] Permissions-Policy: Falta de restricción en las APIs del navegador, lo que permite que el sitio o scripts de terceros accedan potencialmente a la cámara o micrófono sin control estricto.
[LOW] Server header expuesto: La cabecera revela el uso de openresty, proporcionando información valiosa a atacantes sobre la tecnología del servidor para buscar exploits específicos.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos genera errores 404 y dificulta la gestión del rastreo por parte de motores de búsqueda.