EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://antioquia-test.taxationsmart.co/ords/f?p=150000:1:::::1:F_CDGO_CLNTE:	Checks	9 pruebas
Dominio	antioquia-test.taxationsmart.co	Hallazgos	45 totales
Fecha	26 de agosto de 2026 a las 20:51	Problemas	10 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el dominio antioquia-test.taxationsmart.co arroja una puntuacion de 70/100, lo que resulta en una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 4 resultaron exitosos, 3 generaron advertencias y 2 fueron calificados como fallos criticos. Aunque el sitio cuenta con un cifrado de transporte valido, presenta carencias importantes en las configuraciones de cabeceras de seguridad y gestion de puertos. Se concluye que el sitio es actualmente vulnerable a ataques de inyeccion de contenido y suplantacion debido a una configuracion defensiva incompleta.

Resumen de Riesgos

0	3	4	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 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	ORA_WWV_APP_150000: falta SameSite
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): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-11-24T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-24T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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 301 redirige a https://antioquia-test.taxationsmart.co/
- 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

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

ORA_WWV_APP_150000: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: ORA_WWV_APP_150000 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ORA_WWV_APP_150000 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ORA_WWV_APP_150000 — 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 **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

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso al no restringir el origen de los recursos.

[HIGH] Strict-Transport-Security: Falta la configuracion HSTS, lo que impide forzar conexiones HTTPS y deja el sitio expuesto a ataques de degradacion de protocolo.
[MEDIUM] Cookie ORA_WWV_APP_150000: La falta del atributo SameSite en esta cookie de sesion la hace vulnerable a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto expone un servidor web alternativo o proxy que aumenta la superficie de ataque innecesariamente.
[MEDIUM] Referrer-Policy: La falta de esta cabecera no permite controlar que informacion de referencia se envia a otros sitios, comprometiendo la privacidad.
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, permitiendo potencialmente el acceso no autorizado a hardware como camara o microfono.
[LOW] Server header expuesto: El servidor revela que utiliza la tecnologia Cloudflare, lo cual facilita a un atacante el reconocimiento de la infraestructura tecnica.
[LOW] robots.txt no encontrado: La ausencia de este archivo impide gestionar correctamente el rastreo de los motores de busqueda sobre directorios sensibles.
[LOW] sitemap.xml no encontrado: La falta del mapa del sitio dificulta la auditoria de contenidos y la correcta indexacion de la plataforma.