EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://iewdevelopment.com.co:82	Checks	9 pruebas
Dominio	iewdevelopment.com.co	Hallazgos	41 totales
Fecha	27 de mayo de 2026 a las 23:31	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de ciberseguridad realizada sobre el sitio web arroja una puntuacion de 80/100, lo que equivale a una nota B. El analisis se baso en la ejecucion de 9 checks pasivos, obteniendo 5 resultados satisfactorios, 1 advertencia y 2 fallos en configuraciones criticas. Aunque el cifrado de datos es robusto, la infraestructura presenta debilidades importantes en el endurecimiento del servidor y la exposicion de servicios administrativos. Por lo tanto, el sitio se considera vulnerable a ataques de reconocimiento y fuerza bruta debido a la visibilidad de puertos de gestion.

Resumen de Riesgos

1	1	2	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 170 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
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	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): 3389 (RD...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 170 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  170 dias restantes (expira: 2026-11-13T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-14T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https://code.jquery.com ht...
- 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.)

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
- INFO **Tecnologias detectadas**
  ASP.NET

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

1 puerto(s) potencialmente riesgoso(s): 3389 (RDP)

- 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)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — 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 3389 (RDP) ABIERTO: El servicio de Escritorio Remoto de Windows es visible desde internet, permitiendo intentos de acceso no autorizado y ataques de fuerza bruta directos al servidor.
[HIGH] Strict-Transport-Security (HSTS) faltante: El servidor no obliga al navegador a usar conexiones HTTPS, lo que facilita ataques de interceptacion de datos y degradacion de protocolo.
[MEDIUM] Referrer-Policy faltante: No se controla la informacion que el navegador envia en el encabezado referer, pudiendo filtrar rutas internas o datos sensibles a sitios externos.
[MEDIUM] Permissions-Policy faltante: La ausencia de esta cabecera impide restringir el uso de APIs del navegador como camara o microfono, aumentando la superficie de ataque.
[LOW] Cabecera Server expuesta: Se revela el uso de Microsoft-IIS/10.0, informacion que un atacante utiliza para buscar vulnerabilidades conocidas de esa version especifica.
[LOW] Cabecera X-Powered-By expuesta: Se identifica el framework ASP.NET, lo que reduce el esfuerzo de reconocimiento necesario para planificar un exploit.
[LOW] Ausencia de robots.txt y sitemap.xml: No se han configurado los archivos que guian a los motores de busqueda, afectando el control sobre el rastreo del sitio.