EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.servidor2.webcolegios.com/pablocorrea/	Checks	9 pruebas
Dominio	www.servidor2.webcolegios.com	Hallazgos	48 totales
Fecha	26 de mayo de 2026 a las 03:12	Problemas	19 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de ciberseguridad realizada al sitio web arroja una puntuacion de 56/100, lo que resulta en una calificacion de grado D. El analisis se baso en la ejecucion de 9 checks pasivos, de los cuales 4 fueron superados con exito, 2 presentaron advertencias y 3 resultaron en fallos criticos. Se han detectado deficiencias severas en la configuracion de las cabeceras de seguridad y una exposicion peligrosa de puertos de infraestructura. Por tanto, se concluye que el sitio es actualmente vulnerable y presenta riesgos significativos para la integridad de los datos y la privacidad de los usuarios.

Resumen de Riesgos

1	7	10	1	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

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: 2026-08-14T13:27:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-16T13:27:36.000Z
- 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 301 redirige a https://www.servidor2.webcolegios.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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — 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 — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
  Presente, 3 URLs
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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) abierto: La base de datos esta expuesta directamente a internet, permitiendo intentos de intrusion externos.
[HIGH] Content-Security-Policy falta: Ausencia de politica que previene ataques de inyeccion de codigo como XSS.
[HIGH] X-Frame-Options falta: El sitio es vulnerable a ataques de clickjacking al permitir ser cargado en marcos externos.
[HIGH] Strict-Transport-Security falta: No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles degradaciones de conexion.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: La cookie de sesion es accesible mediante scripts, aumentando el riesgo de robo de identidad.
[HIGH] Cookie PHPSESSID sin flag Secure: Los datos de sesion podrian transmitirse por canales no cifrados.
[HIGH] Puerto 21 (FTP) abierto: Servicio de transferencia de archivos activo que suele enviar credenciales en texto plano.
[MEDIUM] Puerto 22 (SSH) abierto: Interfaz de administracion remota expuesta que puede ser objeto de ataques de fuerza bruta.
[MEDIUM] X-Content-Type-Options falta: Riesgo de ataques de MIME-type sniffing al no restringir la interpretacion de archivos.
[MEDIUM] Referrer-Policy falta: El servidor no controla cuanta informacion de navegacion se envia a otros sitios.
[MEDIUM] Permissions-Policy falta: No existen restricciones sobre el uso de APIs del navegador como la camara o el microfono.
[MEDIUM] Rutas de administracion expuestas: Se detecto acceso publico a /wp-login.php, /administrator/ y /user/login.
[MEDIUM] Archivos de informacion publicos: Existencia de /readme.html y /README.txt que pueden revelar detalles tecnicos del sistema.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: La sesion es vulnerable a ataques de falsificacion de peticiones en sitios cruzados (CSRF).
[LOW] Server header expuesto: El servidor revela el uso de Apache, facilitando la busqueda de exploits especificos.