EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://comunitariocerritos.edu.co/datosoft/	Checks	9 pruebas
Dominio	comunitariocerritos.edu.co	Hallazgos	48 totales
Fecha	24 de mayo de 2026 a las 03:45	Problemas	15 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 64/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 controles de seguridad pasivos, obteniendo como resultado 5 verificaciones correctas, 2 advertencias y 2 fallos críticos. Se han detectado deficiencias severas en la configuración de cabeceras de seguridad y la exposición de versiones de software desactualizadas. Debido a estos hallazgos técnicos y la presencia de configuraciones incompletas en el servidor, se concluye que el sitio es actualmente vulnerable ante posibles ataques dirigidos.

Resumen de Riesgos

0	5	7	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 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: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-07-13T09:21:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-14T09:21:16.000Z
- 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://comunitariocerritos.edu.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: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://mail.google.com/a/comunitariocerritos.edu.co/%20targe...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (127 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://comunitariocerritos.edu.co/wp-sitemap.xml
- 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

[HIGH] WordPress version: La versión 6.9.4 se encuentra expuesta públicamente, lo que permite a atacantes identificar y explotar vulnerabilidades conocidas (CVEs) para ese lanzamiento específico.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera deja al sitio desprotegido contra ataques de inyección de código, como Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que la interfaz sea cargada en marcos externos maliciosos.
[HIGH] Strict-Transport-Security: Falta la configuración HSTS, lo que impide que el navegador fuerce siempre una conexión segura a través de HTTPS.
[MEDIUM] Contenido Mixto: Se detectaron 2 recursos cargados mediante HTTP (gmpg.org y mail.google.com) dentro de la página protegida por SSL, comprometiendo la integridad de la sesión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido (MIME sniffing), facilitando la ejecución de scripts maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a sitios externos, lo que podría filtrar datos de navegación de los usuarios.
[MEDIUM] Permissions-Policy: No hay restricciones sobre las APIs del navegador, dejando abierta la posibilidad de uso no autorizado de funciones como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html: Este archivo de instalación es accesible y revela detalles internos del CMS que facilitan el reconocimiento para un atacante.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible para cualquier usuario de internet, aumentando el riesgo de ataques de fuerza bruta.
[LOW] Server header expuesto: El servidor revela el uso de Apache, proporcionando información tecnológica valiosa para la fase de reconocimiento de un adversario.
[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 6.9.4, facilitando el perfilado del sistema.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a rutas relacionadas con la administración, guiando involuntariamente a los atacantes hacia directorios privados.