EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.clrnetsec.com	Checks	9 pruebas
Dominio	www.clrnetsec.com	Hallazgos	49 totales
Fecha	4 de mayo de 2026 a las 16:35	Problemas	16 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 60/100, lo que resulta en una calificación de nota C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 presentaron fallos críticos. Se detectaron deficiencias importantes en la configuración de cabeceras de protección y la exposición de servicios obsoletos. Actualmente, el sitio se considera vulnerable debido a la combinación de software desactualizado y protocolos de comunicación no cifrados.

Resumen de Riesgos

0	6	6	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 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
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  53 dias restantes (expira: 2026-06-27T04:12:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-29T04:12:43.000Z
- 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: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.20, PleskLin — Revela framework/lenguaje
- 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.clrnetsec.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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  PHP/8.4.20, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- 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 (src (script/img/iframe))**
  http://clrnetsec.com/wp-content/plugins/cookie-law-info/lite...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://clrnetsec.com/wp-content/plugins/cookie-law-info/lite...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (114 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://clrnetsec.com/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- 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
- 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] Puerto 21 (FTP) abierto: El servicio FTP transfiere datos y credenciales en texto plano, permitiendo la interceptación de información sensible.
[HIGH] Versión de WordPress 6.9.4 expuesta: El uso de una versión antigua permite a atacantes explotar vulnerabilidades conocidas (CVEs) para tomar el control del sitio.
[HIGH] Falta de cabecera Content-Security-Policy: La ausencia de esta política facilita ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] Falta de cabecera X-Frame-Options: El sitio es susceptible a ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas.
[HIGH] Falta de cabecera Strict-Transport-Security: No se obliga al navegador a usar conexiones HTTPS, permitiendo ataques de degradación de protocolo.
[MEDIUM] Contenido mixto detectado: Existen 2 recursos cargándose mediante HTTP, lo que debilita el cifrado SSL y permite la manipulación de scripts o imágenes.
[MEDIUM] Falta de cabecera X-Content-Type-Options: Permite que el navegador intente adivinar el tipo de contenido, facilitando la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Falta de cabecera Referrer-Policy: No se controla la información que se envía a otros sitios al hacer clic en enlaces, comprometiendo la privacidad.
[MEDIUM] Falta de cabecera Permissions-Policy: El sitio no restringe el acceso a funciones del navegador como la cámara o el micrófono.
[MEDIUM] Panel de login expuesto: La ruta /wp-login.php es accesible públicamente, facilitando ataques de fuerza bruta contra las cuentas de usuario.
[LOW] Cabeceras de servidor expuestas: Se revela el uso de nginx y versiones de PHP/Plesk, información útil para que un atacante planifique un exploit específico.
[LOW] Meta generator expuesto: La etiqueta meta confirma públicamente que se utiliza la versión 6.9.4 de WordPress.
[LOW] Rutas sensibles en robots.txt: Se hace referencia directa a directorios de administración, revelando estructuras internas del sitio.