

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://becier.ad	Checks	9 pruebas
Dominio	becier.ad	Hallazgos	47 totales
Fecha	28 de abril de 2026 a las 09:19	Problemas	11 detectados

C

70/100

puntos de seguridad



RESUMEN EJECUTIVO

El sitio web analizado ha obtenido una puntuación de 70/100, lo que resulta en una calificación de grado C. Durante la auditoría se realizaron 9 comprobaciones pasivas, de las cuales 4 resultaron exitosas, 2 generaron advertencias y 2 presentaron fallos críticos. Se han identificado debilidades importantes en la configuración de las cabeceras de seguridad y una exposición innecesaria de las versiones del software utilizado. Debido a la falta de políticas de seguridad modernas y la presencia de recursos no cifrados, el sitio se considera actualmente vulnerable ante ataques de inyección y reconocimiento. Es fundamental aplicar medidas correctivas para elevar el nivel de protección de la infraestructura web.

Resumen de Riesgos

0	3	5	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 31 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.8.5 expuesta, WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	pll_language: falta HttpOnly
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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 31 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
31 dias restantes (expira: 2026-05-28T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2025-05-28T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

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

- BAJO Server header expuesto
Server: none — Revela tecnologia del servidor

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- INFO

Strict-Transport-Security
Presente: max-age=63072000
- 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

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 6.8.5
- INFO

Tecnologias detectadas
Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.5 expuesta, WordPress 2 expuesta

- ALTO

WordPress version
Version 6.8.5 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)

Seguridad de Cookies — 67/100

Estado: AVISO

pll_language: falta HttpOnly

- INFO

Cookies detectadas
1 cookie(s) encontrada(s)
- ALTO

Cookie: pll_language — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO

Cookie: pll_language — Secure
Flag Secure activo — Solo se envia por HTTPS

● INFO **Cookie: pll_language — SameSite**
SameSite=lax

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://www.citactiva.es/becier/usuarios/acceso

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (441 bytes)
- INFO **Reglas robots.txt**
7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
https://www.becier.ad/sitemap_index.xml
- BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 puerto(s) abierto(s), todos esperados

- 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
- 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido.

[HIGH] WordPress version: La versión 6.8.5 está expuesta públicamente, permitiendo a posibles atacantes identificar vulnerabilidades específicas conocidas.

[HIGH] Cookie pll_language: Carece del atributo HttpOnly, lo que permite que la cookie sea accesible mediante scripts del navegador aumentando el riesgo de robo de sesión.

[MEDIUM] Referrer-Policy: No se detectó esta cabecera, lo que impide controlar qué información de navegación se envía a otros sitios web.

[MEDIUM] Permissions-Policy: Ausencia de restricciones sobre APIs del navegador, dejando expuestas funciones como la cámara o el micrófono.

[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y suele revelar información técnica detallada sobre la instalación del CMS.

[MEDIUM] Contenido Mixto: Se detectaron 2 recursos cargando mediante HTTP en una página protegida por HTTPS, lo que degrada la seguridad de la conexión.

[LOW] Server header expuesto: El servidor revela información sobre su tecnología mediante la cabecera Server: none.

[LOW] Meta generator: La etiqueta meta expone explícitamente el uso de WordPress 6.8.5, facilitando las tareas de reconocimiento.

[LOW] Ruta sensible en robots.txt: El archivo incluye una referencia directa al directorio admin, revelando rutas administrativas a usuarios no autorizados.