

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://classic2punto0.es/wp-login.php?redirect_to=https%3A%2F%2Fclassic2punto0.es/wp-admin%2F&reauth=1	Hallazgos	100 totales
Dominio	classic2punto0.es	Problemas	46 detectados
Fecha	30 de septiembre de 2026 a las 22:51		

C

67/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 67/100 con una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fallaron críticamente. Se han identificado debilidades significativas en la configuración de cabeceras de seguridad, protección de cookies y exposición de servicios en red. Debido a la presencia de puertos críticos abiertos y la falta de directivas de cifrado estricto, se concluye que el sitio es actualmente vulnerable a ataques dirigidos.

Resumen de Riesgos

1 CRITICO	21 ALTO	22 MEDIO	2 BAJO	54 INFO
--------------	------------	-------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 76 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 520650 expuesta, WordPress 2 expuesta
Seguridad de Cookies	35	FALLO	wordpress_test_cookie: falta SameSite; wordpress...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 76 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
76 dias restantes (expira: 2026-12-16T00:42:41.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-17T00:42:42.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, X-Content-Type-Options, Permissions-Policy

- BAJO Server header expuesto
Server: LiteSpeed — Revela tecnologia del servidor

- BAJO

X-Powered-By expuesto
X-Powered-By: PHP/7.4.33, PleskLin — Revela framework/lenguaje
- INFO

Content-Security-Policy
Presente: frame-ancestors 'self';
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO

X-Content-Type-Options
Falta — Evita MIME-type sniffing
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- 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://classic2punto0.es/
- 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
- INFO

Tecnologias detectadas
PHP/7.4.33, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 520650 expuesta, WordPress 2 expuesta

- ALTO

WordPress version
Version 520650 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 — 35/100

Estado: FALLO

wordpress_test_cookie: falta SameSite; wordpress_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpress_sec_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_sec_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpress_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpress_sec_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_sec_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wp-settings-0: falta HttpOnly; wp-settings-0: falta SameSite; wp-settings-time-0: falta HttpOnly; wp-settings-time-0: falta SameSite; wordpress_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpress_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_sec_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpress_sec_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpress_sec_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpressuser_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpressuser_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpresspass_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpresspass_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wordpresspass_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wordpresspass_36982d8bf55743e597f5c99e004c6f1a: falta SameSite; wp-postpass_36982d8bf55743e597f5c99e004c6f1a: falta HttpOnly; wp-postpass_36982d8bf55743e597f5c99e004c6f1a: falta SameSite

●	INFO	Cookies detectadas 18 cookie(s) encontrada(s)
●	INFO	Cookie: wordpress_test_cookie — HttpOnly HttpOnly activo — No accesible via JavaScript
●	INFO	Cookie: wordpress_test_cookie — Secure Flag Secure activo — Solo se envia por HTTPS
●	MEDIO	Cookie: wordpress_test_cookie — SameSite Falta SameSite — Vulnerable a CSRF
●	ALTO	Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — HttpOnly Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
●	INFO	Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — Secure Flag Secure activo — Solo se envia por HTTPS
●	MEDIO	Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — SameSite Falta SameSite — Vulnerable a CSRF
●	ALTO	Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — HttpOnly Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
●	INFO	Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — Secure Flag Secure activo — Solo se envia por HTTPS
●	MEDIO	Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — SameSite Falta SameSite — Vulnerable a CSRF
●	ALTO	Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — HttpOnly Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
●	INFO	Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — Secure Flag Secure activo — Solo se envia por HTTPS
●	MEDIO	Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — SameSite Falta SameSite — Vulnerable a CSRF
●	ALTO	Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — HttpOnly Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
●	INFO	Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — Secure Flag Secure activo — Solo se envia por HTTPS
●	MEDIO	Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — SameSite Falta SameSite — Vulnerable a CSRF
●	ALTO	Cookie: wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a — HttpOnly Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
●	INFO	Cookie: wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a — Secure Flag Secure activo — Solo se envia por HTTPS
●	MEDIO	Cookie: wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a — SameSite Falta SameSite — Vulnerable a CSRF
●	ALTO	Cookie: wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a — HttpOnly Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
●	INFO	Cookie: wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a — Secure Flag Secure activo — Solo se envia por HTTPS

-  **MEDIO** **Cookie: wordpress_logged_in_36982d8bf55743e597f5c99e004c6f1a — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wp-settings-0 — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wp-settings-0 — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wp-settings-0 — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wp-settings-time-0 — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wp-settings-time-0 — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wp-settings-time-0 — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wordpress_36982d8bf55743e597f5c99e004c6f1a — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wordpress_sec_36982d8bf55743e597f5c99e004c6f1a — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wordpressuser_36982d8bf55743e597f5c99e004c6f1a — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wordpressuser_36982d8bf55743e597f5c99e004c6f1a — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wordpressuser_36982d8bf55743e597f5c99e004c6f1a — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wordpresspass_36982d8bf55743e597f5c99e004c6f1a — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wordpresspass_36982d8bf55743e597f5c99e004c6f1a — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wordpresspass_36982d8bf55743e597f5c99e004c6f1a — SameSite**
Falta SameSite — Vulnerable a CSRF
-  **ALTO** **Cookie: wordpressuser_36982d8bf55743e597f5c99e004c6f1a — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  **INFO** **Cookie: wordpressuser_36982d8bf55743e597f5c99e004c6f1a — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  **MEDIO** **Cookie: wordpressuser_36982d8bf55743e597f5c99e004c6f1a — SameSite**
Falta SameSite — Vulnerable a CSRF

- ALTO

Cookie: wordpresspass_36982d8bf55743e597f5c99e004c6f1a — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO

Cookie: wordpresspass_36982d8bf55743e597f5c99e004c6f1a — Secure
Flag Secure activo — Solo se envia por HTTPS
- MEDIO

Cookie: wordpresspass_36982d8bf55743e597f5c99e004c6f1a — SameSite
Falta SameSite — Vulnerable a CSRF
- ALTO

Cookie: wp-postpass_36982d8bf55743e597f5c99e004c6f1a — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO

Cookie: wp-postpass_36982d8bf55743e597f5c99e004c6f1a — Secure
Flag Secure activo — Solo se envia por HTTPS
- MEDIO

Cookie: wp-postpass_36982d8bf55743e597f5c99e004c6f1a — 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (175 bytes)
- INFO

Reglas robots.txt
1 Disallow, 0 Allow
- INFO

Sitemap en robots.txt
https://classic2punto0.es/sitemap_index.xml
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- 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
- 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 autentificacion por defecto
- INFO

Puerto 8080 (HTTP-Alt)
Cerrado — Servidor web alternativo / proxy



Analisis de Seguridad

VULNERABILIDADES DETECTADAS

- [CRITICAL] Puerto 3306 (MySQL): El puerto de la base de datos está abierto y expuesto, permitiendo intentos de conexión externa y ataques de fuerza bruta.
- [HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos activo sin cifrado, lo que permite la interceptación de credenciales en la red.
- [HIGH] WordPress version: La versión 520650 se encuentra expuesta públicamente, permitiendo a potenciales atacantes identificar y explotar vulnerabilidades conocidas.
- [HIGH] Strict-Transport-Security (HSTS): La ausencia de esta cabecera impide que el navegador fuerce conexiones seguras, facilitando ataques de degradación de SSL.
- [HIGH] Cookies sin atributo HttpOnly: Múltiples cookies de sesión carecen de esta protección, permitiendo que sean robadas mediante scripts maliciosos en ataques XSS.
- [MEDIUM] X-Content-Type-Options: Al faltar esta cabecera, el sitio es vulnerable a ataques de sniffing de tipos MIME para ejecutar archivos maliciosos.
- [MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, dejando abierta la posibilidad de acceso no autorizado a periféricos o funciones del usuario.
- [MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública y revela detalles técnicos sobre la instalación y versión del CMS.
- [MEDIUM] Ruta /wp-login.php: El panel de administración es visible para cualquier usuario, lo que aumenta la superficie de ataque para accesos no autorizados.
- [MEDIUM] Cookies sin atributo SameSite: La falta de esta configuración en las cookies de WordPress facilita la ejecución de ataques de falsificación de petición en sitios cruzados (CSRF).
- [LOW] Server header expuesto: El servidor revela que utiliza la tecnología LiteSpeed, proporcionando información útil para perfilar el entorno técnico.
- [LOW] X-Powered-By expuesto: Se detalla el uso de PHP/7.4.33 y Plesk, exponiendo versiones de software que podrían tener debilidades conocidas.