EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pulso.saona.es/login	Checks	9 pruebas
Dominio	pulso.saona.es	Hallazgos	47 totales
Fecha	16 de julio de 2026 a las 16:35	Problemas	9 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web pulso.saona.es ha dado como resultado una puntuación de 88/100, lo que equivale a una calificación de grado B. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios, una advertencia por configuración de archivos y un fallo en las cabeceras de seguridad. El sitio presenta una base sólida en cuanto a cifrado de datos y redirecciones seguras, aunque expone información técnica que podría ser aprovechada por terceros. En conclusión, el sitio es mayoritariamente seguro, pero requiere ajustes en sus políticas de seguridad del lado del servidor para mitigar riesgos de inyección y exposición de datos. No se realizó un pentest activo en esta sesión.

Resumen de Riesgos

0	1	7	1	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-10-14T13:30:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-16T13:30:28.000Z
- 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: nginx/1.24.0 (Ubuntu) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://pulso.saona.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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

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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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 sitemap.xml

- INFO **robots.txt**
  Presente (160 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 5 Allow
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

2 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)**
  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] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso al navegador.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que puede provocar la fuga de información sensible en las URLs al navegar hacia sitios externos.
[MEDIUM] Permissions-Policy: La falta de esta configuración impide restringir el uso de funciones del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede revelar detalles técnicos específicos sobre la infraestructura del sitio.
[MEDIUM] Archivo /README.txt: La disponibilidad pública de este documento facilita la identificación de versiones de software y configuraciones internas.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo es visible, lo que aumenta la superficie de ataque para intentos de fuerza bruta.
[MEDIUM] Ruta /administrator/: Se detectó una interfaz de gestión accesible, representando un vector potencial para accesos no autorizados.
[MEDIUM] Ruta /user/login: El punto de entrada para usuarios está expuesto, facilitando el reconocimiento del sistema por parte de agentes externos.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.24.0 (Ubuntu), proporcionando datos precisos para buscar vulnerabilidades específicas del software.
[LOW] Falta sitemap.xml: La ausencia de este archivo de mapa del sitio genera una advertencia en la estructura técnica y de indexación.