EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://chavarino.es/	Checks	9 pruebas
Dominio	chavarino.es	Hallazgos	47 totales
Fecha	26 de marzo de 2026 a las 09:39	Problemas	10 detectados

B

82/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 82/100 con una calificación de grado B. De los 9 checks pasivos ejecutados, 7 resultaron satisfactorios, se generó 1 advertencia y se registró 1 fallo crítico en la configuración de seguridad. Los resultados muestran una implementación robusta del cifrado SSL y la gestión de protocolos de transporte seguro, aunque se detectaron carencias importantes en la protección contra ataques de inyección y gestión de archivos sensibles. Se concluye que el sitio es moderadamente seguro, pero presenta vulnerabilidades específicas que podrían ser explotadas para comprometer la integridad de la sesión del usuario o facilitar el reconocimiento del servidor.

Resumen de Riesgos

0	2	8	0	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-05-28T08:56:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-27T07:57:38.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31556926
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://chavarino.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556926
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556926 (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
- INFO **Tecnologias detectadas**
  React

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 (70 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 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: Falta esta cabecera, lo que facilita la ejecución de ataques XSS y la inyección de contenido malicioso en el navegador del usuario.
[HIGH] X-Frame-Options: La ausencia de esta protección deja el sitio expuesto a ataques de clickjacking, permitiendo que sea cargado en marcos de sitios externos.
[MEDIUM] X-Content-Type-Options: No está presente, lo que permite el MIME-type sniffing y aumenta el riesgo de ejecución de scripts disfrazados de otros formatos.
[MEDIUM] Referrer-Policy: La falta de esta cabecera impide controlar la cantidad de información de referencia que se envía al navegar hacia otros enlaces.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no deseado a funciones como la cámara o el micrófono.
[MEDIUM] Archivos de documentación expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo que puede revelar detalles técnicos del sistema subyacente.
[MEDIUM] Rutas administrativas visibles: Se detectó acceso público a paneles de gestión como /wp-login.php, /administrator/ y /user/login, facilitando intentos de fuerza bruta.
[LOW] Sitemap faltante: No se ha detectado el archivo sitemap.xml en la configuración de robots.txt, lo que afecta a la visibilidad y auditoría de los recursos del sitio.