EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://congresodaauga.webs.uvigo.es	Checks	9 pruebas
Dominio	congresodaauga.webs.uvigo.es	Hallazgos	49 totales
Fecha	19 de mayo de 2026 a las 09:18	Problemas	12 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio congresodaauga.webs.uvigo.es arroja una puntuación de 70/100, lo que equivale a una calificación de nota C. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 4 resultaron exitosas, 3 generaron advertencias y 2 fueron marcadas como fallos críticos. Aunque el cifrado de datos es robusto, se han detectado deficiencias importantes en las cabeceras de seguridad y la exposición de información técnica del servidor. Por estas razones, el sitio se considera vulnerable ante ataques de intermediarios y explotación de vulnerabilidades conocidas.

Resumen de Riesgos

0	3	5	4	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 182 dias
Cabeceras de Seguridad	40	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Joomla
Version CMS Expuesta	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	1ce78cd650a453f4a370cf6edb786ee9: falta SameSite
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 182 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  182 dias restantes (expira: 2026-11-17T15:24:44.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-11-17T15:24:44.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 40/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://congresodaauga.webs.uvigo.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: Joomla

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  Detectado via HTML body
- 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: Joomla! - Open Source Content Management

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

Seguridad de Cookies — 67/100

Estado: AVISO

1ce78cd650a453f4a370cf6edb786ee9: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: 1ce78cd650a453f4a370cf6edb786ee9 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: 1ce78cd650a453f4a370cf6edb786ee9 — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: 1ce78cd650a453f4a370cf6edb786ee9 — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (463 bytes)
- INFO **Reglas robots.txt**
  12 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 la ejecución de scripts no autorizados y ataques de inyección de contenido XSS.
[HIGH] Strict-Transport-Security: Al no estar configurado HSTS, el navegador no fuerza conexiones cifradas, facilitando ataques de degradación de SSL.
[MEDIUM] Versión del CMS expuesta: Los datos indican la detección de WordPress 2, lo que expone al sitio a vulnerabilidades de seguridad de versiones obsoletas.
[MEDIUM] Ruta /administrator/ expuesta: El panel de acceso administrativo es accesible de forma pública, aumentando el riesgo de ataques de fuerza bruta.
[MEDIUM] Archivo /README.txt accesible: Este archivo revela información técnica del gestor de contenidos que puede ser aprovechada por atacantes.
[MEDIUM] Cookie SameSite: La falta de este atributo en la cookie de sesión hace que el sitio sea susceptible a ataques de falsificación de solicitud en sitios cruzados o CSRF.
[MEDIUM] Permissions-Policy: La falta de esta configuración permite que el navegador acceda a APIs sensibles sin restricciones explícitas del servidor.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea el indexado completo mediante la instrucción Disallow: /, afectando la visibilidad legítima del sitio.
[LOW] Cabecera Server expuesta: El servidor revela el uso de Apache, lo que facilita la identificación de vectores de ataque específicos para ese software.
[LOW] Meta generator expuesto: La etiqueta meta confirma el uso del CMS Joomla, proporcionando datos adicionales sobre la infraestructura interna.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a la ruta admin, facilitando el descubrimiento de directorios privados.
[LOW] sitemap.xml ausente: El archivo de mapa del sitio no fue encontrado, lo que dificulta el análisis de la estructura del portal.