EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://data.amorosdata.org/	Checks	9 pruebas
Dominio	data.amorosdata.org	Hallazgos	46 totales
Fecha	21 de mayo de 2026 a las 22:03	Problemas	11 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado a la plataforma arroja una puntuación de 83/100, lo que corresponde a una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas y 4 advertencias, sin detectarse fallos críticos de seguridad. Aunque la infraestructura de cifrado es sólida, se identificaron omisiones importantes en las directivas de seguridad del servidor y una exposición innecesaria de rutas administrativas. Se concluye que el sitio es generalmente seguro, pero se considera vulnerable ante ataques de intermediario y técnicas de reconocimiento externo debido a estas configuraciones incompletas.

Resumen de Riesgos

0	2	8	1	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	65	AVISO	4/6 presentes. Faltan: Strict-Transport-Security...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-07-21T13:25:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-22T12:27:59.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 65/100

Estado: AVISO

4/6 presentes. Faltan: Strict-Transport-Security, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: child-src 'self'; connect-src 'self' blob: https://raw.githubusercontent.com/own...
- 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: no-referrer
- 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://data.amorosdata.org/
- 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

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 (26 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Strict-Transport-Security (HSTS): La ausencia de esta cabecera impide que el navegador fuerce conexiones HTTPS, lo que facilita ataques de degradación de protocolo (SSL Stripping).
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de servicios en puertos alternativos aumenta la superficie de ataque y permite el acceso a posibles interfaces de administración o proxys.
[MEDIUM] Rutas de administración expuestas: Se detectaron paneles de login en /wp-login.php, /administrator/ y /user/login, facilitando intentos de acceso no autorizado mediante fuerza bruta.
[MEDIUM] Archivos de información accesibles: El acceso público a /readme.html y /README.txt puede revelar detalles técnicos y versiones de la infraestructura subyacente.
[MEDIUM] Permissions-Policy: Falta de configuración de esta cabecera, lo que impide restringir el uso de APIs sensibles del navegador como la cámara, micrófono o geolocalización.
[MEDIUM] Falta de sitemap.xml: El archivo robots.txt bloquea todo el sitio y no proporciona una ruta de mapa del sitio, lo que afecta la transparencia de la estructura web.
[LOW] Cabecera de servidor expuesta: El campo Server revela el uso de Cloudflare, proporcionando información útil para que un atacante perfile la tecnología del objetivo.