

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://openwebinars.net/
Dominio openwebinars.net
Fecha 5 de mayo de 2026 a las 10:56

Checks 9 pruebas
Hallazgos 47 totales
Problemas 6 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar un análisis de seguridad en el dominio, se ha obtenido una puntuación de 78/100 con una calificación de nota B. La auditoría consistió en la ejecución de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 presentó un fallo crítico de configuración. Se identificaron deficiencias importantes en la redirección de tráfico inseguro y en la gestión de cabeceras de seguridad avanzadas. Aunque el sitio muestra una base sólida en cuanto al cifrado de datos mediante SSL, la falta de redirección automática hacia HTTPS lo clasifica como parcialmente vulnerable ante ataques de interceptación. En conclusión, el estado de seguridad es aceptable pero requiere correcciones técnicas inmediatas para alcanzar un nivel de protección óptimo.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 32 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 32 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
32 dias restantes (expira: 2026-06-06T17:06:13.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-08T16:06:30.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- INFO **Content-Security-Policy**
Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https: blob:...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=2592000; includeSubDomains
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
HTTP 404 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=2592000; includeSubDomains
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- MEDIO **HSTS max-age**
max-age=2592000 (30 dias) — Recomendado minimo 180 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
- BAJO **Meta generator**
Expone: Astro v6.1.2
- INFO **Tecnologias detectadas**
Astro

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
No accesible (correcto)

- INFO **Archivo /README.txt**
No accesible (correcto)
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (598 bytes)
- INFO **Reglas robots.txt**
18 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
<https://openwebinars.net/sitemap.xml>
- **BAJO** **security.txt**
No encontrado — Recomendado para politica de divulgacion

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] HTTP a HTTPS redireccion: El servidor no redirige automáticamente el tráfico inseguro a la versión cifrada, devolviendo un error HTTP 404.

[MEDIUM] Permissions-Policy: Cabecera de seguridad ausente que permite restringir el acceso a APIs sensibles del navegador como la cámara o el micrófono.

[MEDIUM] HSTS max-age: El tiempo de persistencia de la política de seguridad estricta es de solo 30 días, cuando el estándar recomendado es de al menos 180 días.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que podría exponer servicios administrativos o proxys innecesarios.

[LOW] Server header expuesto: La cabecera del servidor revela el uso de tecnología Cloudflare, lo que facilita información técnica a posibles atacantes.

[LOW] Meta generator: El código fuente expone el uso del framework Astro v6.1.2, revelando la tecnología y versión exacta utilizada en el desarrollo.