

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://ov.arsrenacer.com
Dominio ov.arsrenacer.com
Fecha 23 de mayo de 2026 a las 22:53

Checks 9 pruebas
Hallazgos 44 totales
Problemas 13 detectados

C

74/100

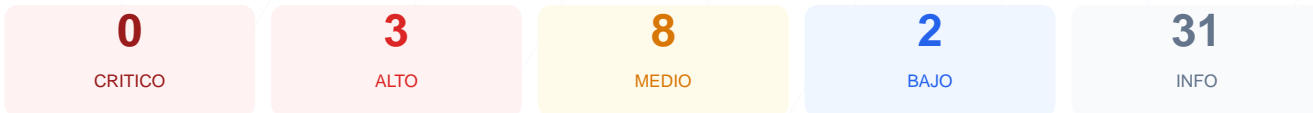
puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 74/100, lo que corresponde a una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 6 resultaron satisfactorios, uno presentó advertencias y otro fue categorizado como fallo crítico debido a la ausencia total de protecciones en el servidor. Aunque el cifrado de datos es correcto, la configuración global presenta debilidades importantes al no implementar mecanismos de defensa contra ataques de inyección y suplantación. En su estado actual, el sitio se considera vulnerable a amenazas dirigidas que exploten la falta de políticas de seguridad en el navegador.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 111 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 111 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
111 dias restantes (expira: 2026-09-11T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2025-08-13T00:00:00.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: ASP.NET — Revela framework/lenguaje
- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyeccion de contenido
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **ALTO** **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- **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.)

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**
ASP.NET

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
- **BAJO** **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
Cerrado — 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 autentificacion 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 esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en frames externos, facilitando ataques de clickjacking.

[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras, lo que permite ataques de degradación de SSL (Man-in-the-Middle).

[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría intentar interpretar archivos de forma incorrecta, permitiendo la ejecución de scripts ocultos.

[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a otros dominios, lo que podría filtrar rutas internas sensibles.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones del navegador como la cámara o el micrófono, aumentando la superficie de ataque.

[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos de la plataforma.

[MEDIUM] Paneles de login expuestos: Se detectó acceso público a rutas administrativas como /wp-login.php, /administrator/ y /user/login.

[LOW] Server header expuesto: El servidor revela la versión específica Microsoft-IIS/10.0, facilitando la búsqueda de exploits conocidos.

[LOW] X-Powered-By expuesto: Se expone el uso del framework ASP.NET, lo que ayuda a potenciales atacantes a mapear la tecnología interna.

[LOW] Falta de sitemap.xml: El sitio no cuenta con un archivo de mapa web, lo que afecta la visibilidad y estructura de indexación.