

Escanear Vulnerabilidades

Informe de Seguridad Web

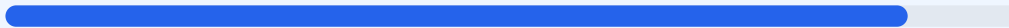
URL https://GenteRena-QA.arsrenacer.com
Dominio genterena-qa.arsrenacer.com
Fecha 23 de mayo de 2026 a las 21:58

Checks 9 pruebas
Hallazgos 44 totales
Problemas 6 detectados

B

89/100

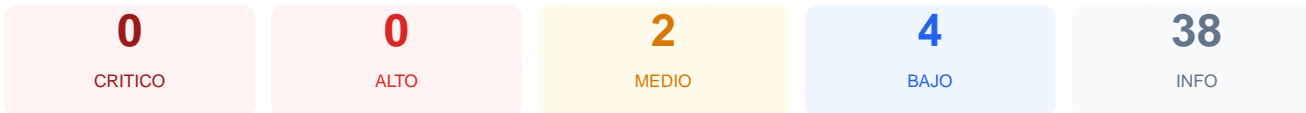
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del sitio GenteRena-QA.arsrenacer.com ha resultado en una puntuación de 89/100, lo que otorga una nota de B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 1 registró fallos críticos de configuración. El sistema demuestra una implementación sólida de cifrado SSL y gestión de cookies, pero presenta deficiencias en el endurecimiento de cabeceras y protocolos de redirección. Se concluye que el sitio es generalmente seguro, aunque vulnerable a técnicas de reconocimiento y posibles fugas de información por falta de políticas de seguridad estrictas.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 111 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
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	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y 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: 2026-09-11T23:59:00Z)
- INFO **Fecha de emision**
Emitido desde: 2025-08-13T00:00:00Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: 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: PHP/8.2.12, ASP.NET — Revela framework/lenguaje
- **INFO** **Content-Security-Policy**
Presente: default-src 'self'; script-src 'self' 'nonce-mbPFRQgWICOzgo3BlezYoA==' https://c...
- **INFO** **X-Frame-Options**
Presente: SAMEORIGIN
- **INFO** **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains
- **INFO** **X-Content-Type-Options**
Presente: nosniff
- **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**
PHP/8.2.12, ASP.NET

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

1 cookies, todas con flags correctos

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

● INFO **Cookie: PHPSESSID — SameSite**
SameSite=strict

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- **BAJO robots.txt**
No encontrado (HTTP 404)
- **BAJO sitemap.xml**
No encontrado (HTTP 404)
- **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 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

- [MEDIUM] Referrer-Policy: La ausencia de esta cabecera impide controlar qué información de origen se envía a otros sitios, comprometiendo la privacidad del usuario.
- [MEDIUM] Permissions-Policy: Falta esta configuración para restringir el uso de APIs del navegador como cámara o micrófono, aumentando la superficie de ataque.
- [LOW] Server header expuesto: Se detectó el valor Microsoft-IIS/10.0, lo que revela la tecnología exacta del servidor y facilita ataques dirigidos.
- [LOW] X-Powered-By expuesto: La presencia de PHP/8.2.12 y ASP.NET indica el framework y lenguaje utilizado, permitiendo a atacantes buscar vulnerabilidades específicas.
- [ERROR] Redirección HTTPS: No se pudo verificar que el tráfico inseguro sea forzado hacia conexiones cifradas, lo que podría exponer datos en tránsito.
- [LOW] robots.txt: El archivo no fue encontrado, lo que impide dar instrucciones claras a los rastreadores sobre áreas restringidas.

[LOW] sitemap.xml: La ausencia de este archivo dificulta la auditoría de la estructura del sitio y la indexación controlada por motores de búsqueda.