EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://genterena-qa.arsrenacer.com	Checks	9 pruebas
Dominio	genterena-qa.arsrenacer.com	Hallazgos	42 totales
Fecha	24 de mayo de 2026 a las 12:42	Problemas	0 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web genterena-qa.arsrenacer.com ha finalizado con una puntuación de 100/100 y una calificación de grado A. El análisis consistió en la ejecución de 9 checks pasivos, de los cuales 8 resultaron satisfactorios, sin registrarse advertencias ni fallos en los parámetros evaluados. Se ha verificado una implementación robusta de cabeceras de seguridad y una gestión adecuada de certificados SSL. La ausencia de un CMS detectable reduce significativamente la superficie de exposición ante ataques automatizados. Con base en los datos obtenidos, se concluye que el sitio es seguro en su configuración actual.

Resumen de Riesgos

0	0	0	0	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 110 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 110 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  110 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 — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'nonce-+hGwboc8lHnqHDuqYI9YKQ==' 'unsafe-h...

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: geolocation=(), camera=(), microphone=(), payment=(), usb=(), fullscreen=(self)

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

- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (150 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://genterena-qa.arsrenacer.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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

No se detectaron vulnerabilidades durante el escaneo pasivo realizado. El sistema cumple con los estándares de seguridad en cuanto a cifrado, configuración de cookies y cabeceras de respuesta.