EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://autorizaciones.arsrenacer.com	Checks	9 pruebas
Dominio	autorizaciones.arsrenacer.com	Hallazgos	44 totales
Fecha	23 de mayo de 2026 a las 22:01	Problemas	14 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio autorizaciones.arsrenacer.com arroja una puntuación de 69/100, lo que resulta en una calificación de grado C. De los 9 checks pasivos ejecutados, se obtuvieron 5 resultados satisfactorios, 2 advertencias y 1 fallo crítico relacionado con la configuración de red y cabeceras. El análisis detectó la exposición de servicios obsoletos y una ausencia total de políticas de seguridad en el servidor, lo que eleva el perfil de riesgo. Se concluye que el sitio es vulnerable debido a configuraciones deficientes que facilitan ataques de interceptación y suplantación de identidad.

Resumen de Riesgos

0	4	8	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

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**
  React, 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 (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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

[ALTA] Puerto 21 (FTP) ABIERTO: El protocolo FTP transmite credenciales y datos en texto plano, permitiendo la interceptación de información sensible.
[ALTA] Falta de Content-Security-Policy: Ausencia de reglas para prevenir la ejecución de scripts maliciosos (XSS) y ataques de inyección de código.
[ALTA] Falta de X-Frame-Options: El sitio permite ser cargado en marcos externos, lo que facilita ataques de clickjacking para engañar a los usuarios.
[ALTA] Falta de Strict-Transport-Security: No se obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIA] Falta de X-Content-Type-Options: El servidor no previene el MIME-sniffing, lo que puede causar que el navegador ejecute archivos con contenido malicioso.
[MEDIA] Rutas administrativas expuestas: Los paneles de acceso (/wp-login.php, /administrator/, /user/login) son accesibles públicamente, aumentando el riesgo de ataques de fuerza bruta.

[MEDIA] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles y pueden revelar detalles técnicos de la infraestructura.
[MEDIA] Falta de Referrer-Policy: No se controla la información de procedencia enviada a terceros al navegar desde el sitio.
[MEDIA] Falta de Permissions-Policy: No existen restricciones sobre el uso de hardware del usuario como cámara, micrófono o geolocalización.
[BAJA] Cabecera Server expuesta: Se revela el uso de Microsoft-IIS/10.0, proporcionando información valiosa para atacantes que busquen vulnerabilidades específicas.
[BAJA] Cabecera X-Powered-By expuesta: Se confirma el uso de ASP.NET, ayudando a los atacantes a identificar el framework de desarrollo.
[BAJA] Falta de sitemap.xml: El sitio carece de un mapa de estructura, lo que dificulta la auditoría de contenidos y el SEO.