EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.arsrenacer.com	Checks	9 pruebas
Dominio	www.arsrenacer.com	Hallazgos	48 totales
Fecha	23 de mayo de 2026 a las 22:03	Problemas	15 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha otorgado una puntuación de 60/100 con una nota final de C. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 1 advertencia y 3 fallos críticos de seguridad. Los hallazgos principales incluyen la ausencia total de cabeceras de seguridad y la exposición pública de versiones del sistema de gestión. Debido a estas deficiencias técnicas y a la presencia de contenido mixto, se concluye que el sitio es actualmente vulnerable ante ataques de intermediarios y de inyección.

Resumen de Riesgos

0	5	8	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	9 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-07-09T01:24:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-10T01:24:47.000Z
- 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: nginx — Revela tecnologia del servidor

- 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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.arsrenacer.com/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.177.0
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 — 20/100

Estado: FALLO

9 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://arsrenacer.com/seguros-medicos/mama-tambien-necesita-...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://arsrenacer.com/seguros-medicos/salud-de-la-mujer-prev...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://services
- MEDIO **href (link/stylesheet)**
  ...y 6 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (249 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://arsrenacer.com/sitemap_index.xml
- 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

[HIGH] Content-Security-Policy: Falta esta cabecera, lo cual permite la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de protección facilita ataques de clickjacking para engañar a los usuarios finales.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, impidiendo que el navegador fuerce siempre una conexión HTTPS segura.
[HIGH] WordPress version: La versión 7 se encuentra expuesta públicamente, permitiendo a posibles atacantes identificar vulnerabilidades conocidas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos no autorizados.
[MEDIUM] Referrer-Policy: No existe una política para controlar la información de procedencia enviada a otros dominios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a las APIs del navegador, dejando expuestos componentes como la cámara o el micrófono.
[MEDIUM] Contenido Mixto: Se detectaron 9 recursos cargados mediante HTTP en una página protegida por HTTPS, rompiendo el cifrado de la sesión.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y revela información técnica sensible sobre el CMS.
[LOW] Server header expuesto: El encabezado revela el uso de tecnología nginx, facilitando la fase de reconocimiento para un atacante.
[LOW] Meta generator: Se expone la versión del plugin Site Kit by Google, revelando detalles sobre la infraestructura interna.