EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pbx.arsrenacer.com	Checks	9 pruebas
Dominio	pbx.arsrenacer.com	Hallazgos	39 totales
Fecha	23 de mayo de 2026 a las 22:02	Problemas	9 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación de 72/100, lo que otorga una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron exitosos y 2 presentaron fallos críticos relacionados con la configuración del servidor. Aunque la infraestructura de cifrado SSL es sólida, la ausencia total de cabeceras de seguridad modernas representa un riesgo significativo. Se concluye que el sitio es vulnerable debido a configuraciones de endurecimiento (hardening) deficientes que exponen la plataforma a ataques conocidos. La seguridad general requiere atención inmediata en la capa de respuesta del servidor.

Resumen de Riesgos

0	3	3	3	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	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: 2026-09-11T23:59:59.000Z)
- 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-HTTPAPI/2.0 — 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.)

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

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 — 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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de XSS e inyección de contenido.
[HIGH] X-Frame-Options: Al no estar presente, el sitio puede ser cargado en iframes externos, lo que lo hace vulnerable a ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras, permitiendo ataques de degradación de protocolo y la interceptación de datos en tránsito.
[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría permitir al navegador interpretar archivos de forma malintencionada.
[MEDIUM] Referrer-Policy: Falta de control sobre la información de referencia enviada a otros sitios web, lo que puede filtrar URLs privadas o datos de navegación.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando la superficie de riesgo para el usuario.
[LOW] Server header expuesto: La cabecera Server muestra Microsoft-HTTPAPI/2.0, proporcionando información técnica valiosa a posibles atacantes para buscar exploits específicos.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 404 para estos archivos, lo que indica una gestión de indexación y visibilidad deficiente.