EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://remu-pre.rjcfactura18.com/links_rjc/buscar.aspx	Checks	9 pruebas
Dominio	remu-pre.rjcfactura18.com	Hallazgos	44 totales
Fecha	16 de abril de 2026 a las 20:25	Problemas	11 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 72/100, lo que se traduce en una calificación de grado C. El análisis consistió en 9 checks pasivos, resultando en 6 verificaciones exitosas, 1 advertencia y 2 fallos críticos de configuración. Aunque la gestión de certificados de cifrado es correcta, la ausencia total de cabeceras de seguridad básicas debilita la postura defensiva del servidor. Se concluye que el sitio es vulnerable ante ataques de interceptación y manipulación de contenido debido a estas omisiones técnicas. Es imperativo corregir las brechas de configuración para alcanzar un nivel de seguridad aceptable.

Resumen de Riesgos

0	4	3	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 200 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	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 200 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  200 dias restantes (expira: 2026-11-02T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-02T00:00:00.000Z
- 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.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://remu-pre.rjcfactura18.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

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**
  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

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 facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyecciones de código malicioso.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio permite ser cargado en marcos externos, exponiendo a los usuarios a ataques de clickjacking.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el servidor obligue al navegador a utilizar siempre conexiones cifradas, permitiendo posibles degradaciones de seguridad.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el rastreo de tipos MIME, lo que puede derivar en la ejecución de archivos con contenido inesperado.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a enlaces externos, lo que compromete la privacidad de la navegación.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el uso de APIs sensibles del navegador como la cámara o el micrófono por parte de terceros.
[LOW] Server header expuesto: Se revela la versión específica Microsoft-IIS/10.0, permitiendo que atacantes identifiquen vulnerabilidades conocidas del software del servidor.
[LOW] X-Powered-By expuesto: El encabezado revela el uso del framework ASP.NET, proporcionando detalles técnicos innecesarios sobre la infraestructura interna.
[LOW] Robots.txt y Sitemap: La falta de estos archivos dificulta la correcta indexación y gestión de permisos para los motores de búsqueda y rastreadores.