EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.imprentareyes.es	Checks	9 pruebas
Dominio	www.imprentareyes.es	Hallazgos	43 totales
Fecha	24 de julio de 2026 a las 12:43	Problemas	8 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web ha obtenido una puntuación de 76/100, lo que equivale a una calificación de grado B. De los 9 checks pasivos ejecutados, 7 resultaron satisfactorios, mientras que se identificó una advertencia en la redirección HTTPS y un fallo crítico por la ausencia total de cabeceras de seguridad. El certificado SSL es válido y la infraestructura básica es correcta, pero la falta de protecciones contra ataques web comunes es evidente. Se concluye que el sitio es funcionalmente seguro en su transporte de datos, pero vulnerable a ataques de inyección y suplantación de interfaz debido a una configuración de servidor incompleta.

Resumen de Riesgos

0	4	3	1	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 56 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 56 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  56 dias restantes (expira: 2026-09-18T20:36:25.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-20T20:36:26.000Z
- 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.imprentareyes.es/
- 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

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (124 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.imprentareyes.es/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 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)**
  Abierto (esperado) — 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

[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a clickjacking, permitiendo que un atacante cargue la web en marcos invisibles para engañar al usuario.
[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a usar siempre HTTPS (HSTS), lo que facilita ataques de degradación de protocolo y robo de cookies.
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador realice MIME-sniffing, aumentando el riesgo de ejecución de archivos con contenido malicioso disfrazado.

[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios web, lo que puede filtrar URLs privadas.
[MEDIUM] Falta de Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la ubicación, cámara o micrófono.
[LOW] Cabecera Server expuesta: El servidor revela el uso de nginx, lo que proporciona información técnica valiosa a posibles atacantes para buscar vulnerabilidades específicas.