EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://petitretol.es	Checks	9 pruebas
Dominio	petitretol.es	Hallazgos	51 totales
Fecha	5 de mayo de 2026 a las 14:59	Problemas	8 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a petitretol.es ha dado como resultado una puntuación de 85/100 con una calificación de grado B. De los 9 checks pasivos ejecutados, 7 finalizaron con éxito y 2 presentaron fallos críticos relacionados con la configuración de cabeceras y la seguridad de las cookies. Se ha verificado que el sitio cuenta con un cifrado SSL robusto y una correcta redirección de tráfico hacia HTTPS. No obstante, existen deficiencias técnicas en la protección contra ataques de sesión y de interfaz de usuario. En su estado actual, el sitio se considera mayoritariamente seguro pero vulnerable ante ataques dirigidos por falta de políticas de seguridad preventivas.

Resumen de Riesgos

0	2	3	3	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 dias
Cabeceras de Seguridad	60	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Ref...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	__cf_bm: falta Secure; __cf_bm: falta SameSite
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 70 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-07-14T10:57:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-15T10:57:16.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: openresty — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: HostingerWebsiteBuilder — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: frame-ancestors zyro.com *.zyro.com *.builder-preview.com *.zyro.space *.hosting...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubDomains; preload;
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://petitretol.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubDomains; preload;
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- 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
- BAJO **Meta generator**
  Expone: Hostinger Website Builder
- INFO **Tecnologias detectadas**
  Next.js, Astro, HostingerWebsiteBuilder

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 — 33/100

Estado: FALLO

__cf_bm: falta Secure; __cf_bm: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: __cf_bm — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: __cf_bm — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://petitretol.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] X-Frame-Options: Falta esta cabecera de seguridad, lo que hace al sitio vulnerable a ataques de clickjacking.
[HIGH] Cookie __cf_bm (Secure): La cookie carece del flag Secure, lo que permite que se envíe a través de conexiones HTTP no cifradas.
[MEDIUM] Referrer-Policy: No se detectó esta cabecera, necesaria para controlar cuánta información de referencia se envía a otros sitios.
[MEDIUM] Permissions-Policy: Ausencia de configuración para restringir el acceso del navegador a APIs sensibles como cámara o micrófono.
[MEDIUM] Cookie __cf_bm (SameSite): Falta el atributo SameSite, lo que expone al usuario a posibles ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] Server header expuesto: El servidor revela el uso de openresty, proporcionando información técnica útil para un atacante.
[LOW] X-Powered-By expuesto: La cabecera revela que el sitio utiliza HostingerWebsiteBuilder como framework subyacente.
[LOW] Meta generator expuesto: El código fuente del sitio confirma el uso de Hostinger Website Builder.