EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.pepinapastel.es/	Checks	9 pruebas
Dominio	www.pepinapastel.es	Hallazgos	53 totales
Fecha	1 de mayo de 2026 a las 22:12	Problemas	21 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar una auditoría de ciberseguridad, el sitio web ha obtenido una puntuación de 59/100, lo que le otorga una calificación de grado D. El análisis se basó en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fallaron con severidad alta. Se han detectado debilidades críticas en la exposición de servicios de infraestructura y una gestión deficiente de las cabeceras de seguridad. Debido a la visibilidad de versiones de software desactualizadas y puertos de base de datos abiertos, se concluye que el sitio es actualmente vulnerable a ataques externos.

Resumen de Riesgos

1	6	11	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 34 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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 6.1.10 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	7 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 34 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  34 dias restantes (expira: 2026-06-04T10:24:25.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-06T10:24:26.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

- BAJO **Server header expuesto**
  Server: LiteSpeed — 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.pepinapastel.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

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: WordPress 6.1.10
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.1.10 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.1.10 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

7 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.pepinapastel.es/wp-content/uploads/2020/10/pepina...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.pepinapastel.es/wp-content/uploads/2020/10/pepina...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://www.pepinapastel.es/wp-content/uploads/2020/10/pepina...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.pepinapastel.es/cp/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.pepinapastel.es/about/
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1959 bytes)
- INFO **Reglas robots.txt**
  40 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.pepinapastel.es/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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

- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos está expuesta a internet, lo que permite intentos de conexión directa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP) abierto: El servicio de transferencia de archivos no está cifrado, lo que facilita la interceptación de credenciales de administración.
[HIGH] WordPress versión 6.1.10 expuesta: El uso de una versión obsoleta permite a potenciales atacantes explotar vulnerabilidades conocidas (CVEs) para tomar el control del sitio.
[HIGH] Content-Security-Policy (CSP) falta: La ausencia de esta directiva facilita la ejecución de ataques de XSS e inyección de contenido malicioso.
[HIGH] X-Frame-Options falta: El sitio es vulnerable a ataques de clickjacking, donde un atacante puede camuflar la interfaz para engañar al usuario.
[HIGH] Strict-Transport-Security (HSTS) falta: No se obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIUM] Contenido Mixto: Existen 7 recursos cargándose mediante HTTP inseguro dentro de la página HTTPS, comprometiendo la integridad del candado de seguridad.
[MEDIUM] X-Content-Type-Options falta: El sitio no previene que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de scripts maliciosos.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela información técnica y versiones del CMS que facilitan el reconocimiento por parte de atacantes.
[MEDIUM] Referrer-Policy falta: No se controla la información que se envía a otros sitios al hacer clic en enlaces salientes.
[MEDIUM] Bloqueo total en robots.txt: La directiva Disallow: / impide el rastreo legítimo pero no oculta la estructura del sitio a ojos malintencionados.
[LOW] Server header expuesto: El servidor revela el uso de LiteSpeed, acotando los vectores de ataque posibles para un intruso.
[LOW] Meta generator expuesto: Se confirma públicamente el uso de WordPress 6.1.10 en el código fuente de la página.