EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Paiporta.es	Checks	9 pruebas
Dominio	paiporta.es	Hallazgos	47 totales
Fecha	19 de mayo de 2026 a las 01:19	Problemas	10 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad web realizado ha otorgado una puntuacion de 87/100 con una nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y no se detectaron fallos criticos segun el resumen de estado. El sitio web muestra una base de seguridad solida, aunque presenta deficiencias en la configuracion de cabeceras de seguridad y en la gestion de recursos internos. No se ejecuto un pentest activo, por lo que la evaluacion se basa en la configuracion expuesta y visible. Se concluye que el sitio es generalmente seguro, pero vulnerable a ataques especificos de inyeccion y navegacion insegura debido a errores de configuracion menores.

Resumen de Riesgos

1	1	4	4	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Drupal, PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000
- INFO **X-Content-Type-Options**
  Presente: nosniff, nosniff

- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: geolocation=(),sync-xhr=(),fullscreen=(self)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.paiporta.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 dias
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Drupal, PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- 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: Drupal 10 (https://www.drupal.org)
- INFO **Tecnologias detectadas**
  Next.js

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 — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.paiporta.es/va
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.paiporta.es/va
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://portalesmunicipales.dival.es/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (2027 bytes)
- INFO **Reglas robots.txt**
  34 Disallow, 18 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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

[CRITICAL] Conexion SSL: No se pudo establecer o verificar correctamente la conexion SSL/TLS durante el proceso de escaneo.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite potenciales ataques de Cross-Site Scripting (XSS) e inyeccion de contenido malicioso.
[MEDIUM] HSTS max-age: La directiva Strict-Transport-Security tiene una duracion de solo 30 dias, cuando el estandar de seguridad recomienda un minimo de 180 dias.
[MEDIUM] Contenido Mixto: Se detectaron 3 recursos cargados a traves de HTTP (inseguro) dentro de una sesion HTTPS, lo que compromete la integridad de la conexion.
[LOW] Meta generator: El sitio expone publicamente que utiliza Drupal 10, lo cual facilita a potenciales atacantes la busqueda de vulnerabilidades especificas para esa version.
[LOW] Ruta sensible en robots.txt: El archivo menciona rutas como admin y config, lo que revela la estructura interna del servidor a actores malintencionados.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la auditoria de paginas indexadas y la transparencia del sitio.