EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://denier.es	Checks	9 pruebas
Dominio	denier.es	Hallazgos	52 totales
Fecha	12 de mayo de 2026 a las 11:37	Problemas	21 detectados

D

47/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 47/100, lo que equivale a una calificación de grado D. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 4 verificaciones superadas, 1 advertencia y 4 fallos críticos de seguridad. La infraestructura presenta deficiencias notables en la configuración del servidor y en el mantenimiento del sistema de gestión de contenidos. Por todo ello, se concluye que el sitio es actualmente vulnerable y requiere intervenciones urgentes para mitigar riesgos de explotación.

Resumen de Riesgos

0	6	12	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 5.1.19 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	62 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-08-06T15:41:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-08T15:41:53.000Z
- 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: Apache — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 301 — No redirige a HTTPS
- 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 5.1.19
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.1.19 expuesta

- ALTO **WordPress version**
  Version 5.1.19 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- 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

62 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://denier.es/welcome/wp-content/plugins/LayerSlider/stat...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://denier.es/welcome/wp-includes/js/jquery/jquery.js?ver...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://denier.es/welcome/wp-includes/js/jquery/jquery-migrat...
- MEDIO **src (script/img/iframe)**
  ...y 19 mas del mismo tipo
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://denier.es/welcome/xmlrpc.php
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://denier.es/welcome/wp-content/uploads/2015/01/denier_i...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://denier.es/welcome/feed/
- MEDIO **href (link/stylesheet)**
  ...y 36 mas del mismo tipo
- MEDIO **Recurso HTTP (form action)**
  http://denier.es/welcome/

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, 61 URLs
- 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] Versión de WordPress expuesta: Se detectó la versión 5.1.19, lo cual permite a potenciales atacantes identificar y explotar vulnerabilidades conocidas (CVEs) asociadas a esta versión obsoleta.
[HIGH] Falta de redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, permitiendo que las conexiones se realicen por canales no cifrados.
[HIGH] HSTS (Strict-Transport-Security) no configurado: La ausencia de esta cabecera impide que el navegador fuerce conexiones seguras, facilitando ataques de interceptación de datos.
[HIGH] Content-Security-Policy (CSP) faltante: La falta de esta política de seguridad facilita ataques de inyección de contenido malicioso y scripts de sitios cruzados (XSS).
[HIGH] X-Frame-Options faltante: El sitio no bloquea su carga dentro de marcos, lo que lo hace susceptible a ataques de clickjacking.
[MEDIUM] Contenido Mixto: Se identificaron 62 recursos (imágenes, scripts y formularios) que se cargan mediante protocolo inseguro HTTP dentro de la página HTTPS.
[MEDIUM] X-Content-Type-Options faltante: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy faltante: No existe un control sobre la información de origen que el navegador envía a terceros al hacer clic en enlaces.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso a APIs del navegador como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: La cabecera revela que el servidor utiliza Apache, facilitando la fase de reconocimiento de un ciberataque.
[LOW] Meta generator visible: El código fuente expone públicamente la versión exacta del CMS, ayudando a los atacantes a perfilar el objetivo.
[LOW] Archivo robots.txt no encontrado: El servidor responde con un error 404, lo que indica una falta de instrucciones para los motores de búsqueda y posibles problemas de visibilidad.