EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://autodesguacescastellar.es	Checks	9 pruebas
Dominio	autodesguacescastellar.es	Hallazgos	45 totales
Fecha	21 de mayo de 2026 a las 08:44	Problemas	15 detectados

D

49/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio autodesguacescastellar.es ha arrojado una puntuación de 49/100, lo que resulta en una calificación de grado D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 1 presentó advertencias y 4 fallaron críticamente. A pesar de contar con un certificado SSL válido, la plataforma presenta deficiencias graves en la configuración de cabeceras de seguridad y en el forzado de conexiones seguras. Por lo tanto, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación de datos y explotación de vulnerabilidades conocidas.

Resumen de Riesgos

0	6	5	4	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 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 6.8.2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-07-28T11:05:43.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-29T11:05:44.000Z
- 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 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 429

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 6.8.2
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO
WordPress 6.8.2 expuesta

- ALTO **WordPress version**
  Version 6.8.2 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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://fonts.googleapis.com/

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 429)
- 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] Redirección HTTP a HTTPS: El sitio no redirige automáticamente a conexiones seguras, permitiendo que la comunicación viaje sin cifrar.

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La falta de protección contra marcos hace que el sitio sea susceptible a ataques de secuestro de clics (clickjacking).
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador obligue al uso de HTTPS en futuras visitas.
[HIGH] WordPress Version Exposed: Se detectó públicamente la versión 6.8.2, lo que permite a posibles atacantes identificar y explotar CVEs específicos.
[MEDIUM] Contenido Mixto: Existen recursos como fuentes de Google cargados mediante el protocolo inseguro HTTP dentro de la página HTTPS.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a sitios terceros, lo que supone un riesgo para la privacidad.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador, como la cámara o la geolocalización.
[LOW] Server header expuesto: El servidor revela que utiliza Apache, facilitando el reconocimiento técnico a actores malintencionados.
[LOW] Meta generator: El sitio expone la versión exacta del gestor de contenidos en el código fuente.
[LOW] Robots.txt y Sitemap: La ausencia de estos archivos dificulta la correcta indexación y el control de acceso a rutas del sitio.