EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://desguacestito.com/	Checks	9 pruebas
Dominio	desguacestito.com	Hallazgos	49 totales
Fecha	25 de septiembre de 2026 a las 18:44	Problemas	6 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoria de ciberseguridad, el sitio presenta una puntuación exacta de 100/100 con una nota final de A. Los 9 checks pasivos ejecutados resultaron exitosos, sin registrarse advertencias ni fallos en los protocolos analizados. Se han identificado hallazgos menores relacionados con la visibilidad de rutas administrativas y archivos de informacion tecnica que no afectan la calificacion global pero requieren atencion. En conclusion, desguacestito.com se considera un sitio seguro y bien configurado bajo los parametros de este analisis superficial.

Resumen de Riesgos

0	0	4	2	43
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 69 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	100	OK	No se encontraron cookies
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 69 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  69 dias restantes (expira: 2026-12-03T08:44:08.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-04T08:44:09.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests; frame-ancestors 'self'; base-uri 'self'; object-src '...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=(), payment=(), usb=(), interest-cohort=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://desguacestito.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 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

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 — 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 (137 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://desguacestito.com/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

[LOW] Server header expuesto: El encabezado revela la tecnologia hcdn, lo cual facilita a un atacante potencial la fase de reconocimiento de la infraestructura.
[MEDIUM] Archivo /readme.html accesible: Este archivo se encuentra disponible publicamente y puede filtrar informacion sensible sobre la estructura o versiones del sistema.
[MEDIUM] Ruta /wp-login.php accesible: El panel de acceso administrativo esta expuesto a ataques de fuerza bruta por parte de bots automatizados.
[MEDIUM] Ruta /administrator/ accesible: La ubicacion estandar de administracion es visible, aumentando la superficie de ataque para accesos no autorizados.
[MEDIUM] Ruta /user/login accesible: Punto de entrada para usuarios disponible para intentos de inicio de sesion malintencionados.
[LOW] Ruta sensible en robots.txt: La mencion de la palabra admin en este archivo publico orienta a atacantes hacia directorios que deberian permanecer ocultos.