EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://socage.es/pick-up-con-cesta-elevadora/	Checks	9 pruebas
Dominio	socage.es	Hallazgos	48 totales
Fecha	6 de mayo de 2026 a las 06:42	Problemas	15 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio ha arrojado una puntuación de 64/100, lo que equivale a una nota de C. Se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias y 2 fallos críticos de configuración. Los hallazgos principales revelan una ausencia total de cabeceras de seguridad y la exposición de información técnica sensible sobre el servidor y el CMS. Debido a la falta de mecanismos de protección activa y la presencia de servicios de transferencia de archivos inseguros, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	6	5	4	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 81 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.7.5 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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 81 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  81 dias restantes (expira: 2026-07-26T15:07:45.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-27T15:07:46.000Z
- 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: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.25, PleskLin — Revela framework/lenguaje
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

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

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.7.5
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.1.25, PleskLin

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.7.5 expuesta

- ALTO **WordPress version**
  Version 6.7.5 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 (114 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://socage.it/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), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: El sitio no protege contra ataques de clickjacking, permitiendo que la web sea embebida en marcos externos.
[HIGH] Falta de Strict-Transport-Security: No se fuerza la conexión HTTPS a nivel de navegador, facilitando ataques de degradación de SSL (HSTS).
[HIGH] Versión de WordPress 6.7.5 expuesta: La visibilidad pública de la versión exacta permite a los atacantes identificar CVEs específicos para este software.
[HIGH] Puerto 21 (FTP) ABIERTO: Este puerto permite la transferencia de archivos sin cifrado, exponiendo credenciales y datos en texto plano.
[MEDIUM] X-Content-Type-Options faltante: El sitio es vulnerable al sniffing de tipos MIME, lo que puede llevar a la ejecución de archivos no deseados.
[MEDIUM] Referrer-Policy faltante: No existe control sobre la información de referencia enviada a otros dominios, lo que podría filtrar rutas internas.
[MEDIUM] Permissions-Policy faltante: No se restringe el acceso a APIs críticas del navegador como la cámara o el micrófono.
[MEDIUM] Puerto 22 (SSH) ABIERTO: El acceso remoto está disponible, lo que supone un vector de ataque si no se cuenta con autenticación robusta o restricción de IP.
[MEDIUM] Ruta /wp-login.php accesible: El panel de administración de WordPress está expuesto a ataques de fuerza bruta por parte de bots.
[LOW] Cabeceras de servidor expuestas: Se revela el uso de nginx, PHP/8.1.25 y PleskLin, facilitando el reconocimiento del entorno técnico.
[LOW] Meta generator expuesto: La etiqueta meta confirma el uso de WordPress 6.7.5, reforzando la información para el escaneo de vulnerabilidades.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, guiando a posibles atacantes hacia zonas restringidas.