EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://octapus.io/	Checks	9 pruebas
Dominio	octapus.io	Hallazgos	47 totales
Fecha	5 de junio de 2026 a las 20:31	Problemas	15 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio octapus.io arroja una puntuación de 64/100, lo que sitúa al sitio en una calificación de grado C. El análisis técnico se basó en 9 comprobaciones pasivas, resultando en 5 verificaciones exitosas, 2 advertencias y 2 fallos de seguridad críticos. A pesar de contar con un cifrado SSL sólido, la infraestructura presenta carencias graves en la protección contra ataques de inyección y una gestión de parches obsoleta. En consecuencia, el sitio se clasifica como vulnerable debido a la exposición de información técnica sensible y software desactualizado.

Resumen de Riesgos

0	5	7	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 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 3.7.1 expuesta, WordPress 2 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	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-08-05T14:04:24.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-07T14:04:25.000Z
- 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: LiteSpeed — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://octapus.io/
- 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: Elementor 4.1.1; features: additional_custom_breakpoints; settings: css_print_method-external, google_font-enabled, font_display-swap
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 3.7.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 3.7.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- 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://octapus.io/sitemap_index.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[ALTA] WordPress version: Se detectó la versión 3.7.1 expuesta públicamente, la cual es antigua y vulnerable a múltiples exploits conocidos y ataques de ejecución remota.
[ALTA] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[ALTA] X-Frame-Options: La falta de esta cabecera permite que el sitio sea cargado en iframes, exponiéndolo a ataques de clickjacking.
[ALTA] Strict-Transport-Security: No se ha configurado HSTS, lo que permite ataques de degradación de protocolo (SSL Stripping) al no forzar HTTPS de forma estricta.
[MEDIA] Puerto 8080 (HTTP-Alt): La presencia de un puerto de servidor web alternativo abierto incrementa la superficie de ataque y exposición de servicios internos.
[MEDIA] Archivo /readme.html y /README.txt: Estos archivos son accesibles y pueden revelar detalles específicos sobre la versión y configuración del CMS a un atacante.
[MEDIA] Ruta /wp-login.php: El panel de administración de WordPress es accesible globalmente, lo que facilita intentos de intrusión mediante fuerza bruta.
[MEDIA] X-Content-Type-Options: La falta de esta directiva permite que los navegadores realicen MIME-sniffing, aumentando el riesgo de ejecución de archivos maliciosos.
[MEDIA] Referrer-Policy y Permissions-Policy: La ausencia de estos controles permite la fuga de información sobre la navegación y el acceso no restringido a APIs del dispositivo.
[BAJA] Server header expuesto: El servidor responde con la cabecera LiteSpeed, facilitando la identificación de la tecnología subyacente para ataques dirigidos.
[BAJA] Meta generator: Se exponen metadatos del plugin Elementor 4.1.1, revelando configuraciones internas del diseño web.
[BAJA] Ruta sensible en robots.txt: Se menciona explícitamente la ruta "admin", indicando a los rastreadores y atacantes dónde se encuentran áreas administrativas.