EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://zoko-swap.emergent.host/	Checks	9 pruebas
Dominio	zoko-swap.emergent.host	Hallazgos	46 totales
Fecha	24 de junio de 2026 a las 20:05	Problemas	15 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha determinado una puntuación de 57/100, lo que equivale a una calificación de nota D. Se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 fallaron críticamente. El diagnóstico revela una ausencia total de cabeceras de seguridad esenciales y una gestión deficiente de las redirecciones de tráfico. Debido a estos fallos en la configuración del servidor, el sitio web se considera vulnerable y presenta riesgos significativos para la integridad de los usuarios.

Resumen de Riesgos

0	5	9	1	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 74 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	1 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-09-06T15:14:28.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-08T14:14:30.000Z
- 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: cloudflare — 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 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
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que sea embebido en marcos externos no autorizados.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, exponiendo a los usuarios a ataques de degradación de protocolo.
[HIGH] Ausencia de redirección HTTPS: El servidor responde a peticiones HTTP sin redirigirlas automáticamente a HTTPS, permitiendo comunicaciones no cifradas.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo aumenta la superficie de ataque y puede revelar servicios internos no protegidos.
[MEDIUM] Rutas administrativas expuestas: El acceso público a /wp-login.php, /administrator/ y /user/login facilita ataques de fuerza bruta contra el panel de gestión.
[MEDIUM] Archivos informativos accesibles: La disponibilidad de /readme.html y /README.txt puede revelar detalles técnicos sobre la infraestructura a posibles atacantes.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de scripts camuflados.
[MEDIUM] Referrer-Policy y Permissions-Policy: La ausencia de estas políticas compromete la privacidad del usuario y el control sobre las funciones del navegador.
[LOW] Cabecera de servidor expuesta: El campo Server revela el uso de Cloudflare, proporcionando información útil para el reconocimiento por parte de terceros.