EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Zerviz.zengine.online	Checks	9 pruebas
Dominio	zerviz.zengine.online	Hallazgos	42 totales
Fecha	18 de junio de 2026 a las 05:15	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web https://Zerviz.zengine.online ha resultado en una puntuación de 72/100 con una nota de C. El análisis se basó en 9 checks pasivos ejecutados, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fallaron críticamente. Si bien el sitio cuenta con un cifrado de transporte robusto, carece por completo de cabeceras de seguridad esenciales para la protección del navegador. En su estado actual, el sitio se considera vulnerable a ataques de inyección de contenido y suplantación debido a configuraciones de servidor incompletas.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 156 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	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	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 156 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  156 dias restantes (expira: 2026-11-20T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-07T00:00:00.000Z
- 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: AmazonS3 — 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://zerviz.zengine.online/
- 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

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 504)
- BAJO **sitemap.xml**
  No encontrado (HTTP 504)
- 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] Content-Security-Policy: Falta. Esta ausencia permite la ejecución de scripts maliciosos (XSS) y ataques de inyección de datos.
[HIGH] X-Frame-Options: Falta. El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles para engañar al usuario.
[HIGH] Strict-Transport-Security: Falta. No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: Falta. El navegador podría intentar interpretar archivos como un tipo de contenido diferente al declarado, facilitando la ejecución de malware.
[MEDIUM] Referrer-Policy: Falta. No se controla la información de navegación que se envía a otros sitios al seguir enlaces externos.
[MEDIUM] Permissions-Policy: Falta. No se restringe el acceso de las APIs del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: Server: AmazonS3. Revelar la tecnología del servidor ayuda a potenciales atacantes a buscar vulnerabilidades específicas para esa infraestructura.

[LOW] robots.txt y sitemap.xml: No encontrados. La ausencia de estos archivos dificulta el control sobre el rastreo de buscadores y sugiere una configuración de servidor incompleta (error HTTP 504).