EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://analytics.elespacio.net/	Checks	9 pruebas
Dominio	analytics.elespacio.net	Hallazgos	45 totales
Fecha	27 de mayo de 2026 a las 10:52	Problemas	14 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio analytics.elespacio.net arroja una puntuación de 70/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 fue calificado como fallo crítico por la ausencia total de cabeceras de seguridad. El análisis confirma que, aunque el cifrado SSL es correcto, el servidor carece de las protecciones básicas necesarias para mitigar ataques modernos. Debido a la exposición de servicios de administración y la falta de políticas defensivas, se concluye que el sitio es actualmente vulnerable. No se realizó un pentest activo en esta sesión.

Resumen de Riesgos

0	4	9	1	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-08-06T11:37:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-08T11:37:24.000Z
- 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/1.31.0 — 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 302 redirige a https://analytics.elespacio.net/
- 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

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (160 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 5 Allow
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de XSS e inyección de contenido malicioso.

[HIGH] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No está configurado, por lo que el navegador no fuerza conexiones HTTPS automáticamente mediante HSTS.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría intentar interpretar archivos como un tipo MIME diferente, permitiendo la ejecución de scripts.
[MEDIUM] Referrer-Policy: No se controla la información de navegación que se envía a otros sitios al hacer clic en enlaces salientes.
[MEDIUM] Permissions-Policy: No se restringe el acceso de la web a APIs sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles y pueden revelar datos técnicos sobre la infraestructura.
[MEDIUM] Rutas de administración expuestas: Se detectaron rutas de login activas como /wp-login.php, /administrator/ y /user/login que son objetivos de fuerza bruta.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de acceso remoto está expuesto a internet, lo cual incrementa el riesgo de intentos de acceso no autorizados.
[LOW] Server header expuesto: La cabecera revela el uso de nginx/1.31.0, facilitando a un atacante la búsqueda de exploits específicos para esa versión.
[WARN] Falta de sitemap.xml: El sitio no cuenta con un mapa de estructura web, lo que dificulta la auditoría completa de sus endpoints.