EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://service.ceos.digital	Checks	9 pruebas
Dominio	service.ceos.digital	Hallazgos	41 totales
Fecha	12 de mayo de 2026 a las 15:23	Problemas	10 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el dominio service.ceos.digital arroja una puntuación de 72/100, lo que corresponde a una nota C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas y 2 fallos críticos relacionados con la configuración del servidor. No se detectaron advertencias intermedias, pero la ausencia total de políticas de seguridad en las cabeceras eleva el perfil de riesgo. En conclusión, el sitio se considera vulnerable ante ataques de intermediación y suplantación debido a una configuración de infraestructura incompleta.

Resumen de Riesgos

0	3	3	4	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	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	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-07-30T23:51:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-01T23:51:28.000Z
- 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: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — 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.)

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
- INFO **Tecnologias detectadas**
  ASP.NET

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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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: Su ausencia permite ataques de inyección de contenido y Cross-Site Scripting (XSS) al no restringir el origen de los recursos.
[HIGH] X-Frame-Options: La falta de esta cabecera hace que el sitio sea susceptible a ataques de clickjacking, permitiendo que sea embebido en marcos maliciosos.
[HIGH] Strict-Transport-Security: No se implementa HSTS, lo que impide forzar conexiones seguras y facilita ataques de degradación de protocolo (SSL Stripping).
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido, abriendo la puerta a ataques de sniffing de MIME-type.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que podría filtrar datos de navegación privados.
[MEDIUM] Permissions-Policy: No se restringe el acceso de la aplicación a APIs sensibles del navegador como la cámara, el micrófono o la ubicación.
[LOW] Server header expuesto: El servidor revela el uso de Microsoft-IIS/10.0, proporcionando información valiosa para que un atacante busque exploits específicos de esa versión.
[LOW] X-Powered-By expuesto: Se divulga el uso del framework ASP.NET, lo que ayuda a perfilar la tecnología interna del sitio para ataques dirigidos.
[LOW] Ausencia de archivos de rastreo: No se encontraron robots.txt ni sitemap.xml, lo que dificulta la gestión de indexación y puede exponer directorios no deseados.