EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ceos.digital	Checks	9 pruebas
Dominio	ceos.digital	Hallazgos	44 totales
Fecha	12 de mayo de 2026 a las 13:01	Problemas	13 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio ceos.digital ha resultado en una puntuación de 61/100, lo que otorga al sitio una calificación de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 finalizaron correctamente y 3 presentaron fallos críticos en la configuración del servidor. El sitio web muestra una gestión adecuada de su certificado SSL, pero carece de medidas básicas de endurecimiento contra ataques web comunes. Debido a la ausencia total de cabeceras de seguridad y la falta de redirección forzada a HTTPS, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	5	4	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	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	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 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-07-30T20:51:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-01T20:51:24.000Z
- 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: 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.)

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
- 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)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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

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] Ausencia de redirección HTTP a HTTPS: El servidor permite conexiones no cifradas en el puerto 80 sin redirigir automáticamente al usuario a la versión segura.
[HIGH] Content-Security-Policy (CSP) faltante: No existe una política de seguridad de contenido, lo que facilita ataques de Cross-Site Scripting (XSS) e inyección de datos.

[HIGH] X-Frame-Options faltante: La ausencia de esta cabecera permite que el sitio sea cargado en iframes externos, exponiéndolo a ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El navegador no recibe la instrucción de conectar exclusivamente mediante HTTPS, permitiendo posibles degradaciones de conexión.
[MEDIUM] X-Content-Type-Options faltante: El servidor no previene el MIME-type sniffing, lo que podría permitir la ejecución de archivos maliciosos disfrazados de contenido legítimo.
[MEDIUM] Referrer-Policy faltante: No se controla la cantidad de información de referencia que el navegador envía al navegar desde este sitio hacia otros enlaces.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el uso de APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Archivo /README.txt accesible: El acceso público a este archivo puede revelar información técnica interna o detalles sobre la estructura del sitio.
[LOW] Cabecera Server expuesta: Se detectó el valor Microsoft-IIS/10.0, lo cual revela la tecnología y versión exacta del servidor a posibles atacantes.
[LOW] Cabecera X-Powered-By expuesta: Se revela el uso de ASP.NET, proporcionando información valiosa para ataques dirigidos al framework.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la auditoría de indexación y no proporciona guías de rastreo a los motores de búsqueda.