EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ceiber.com	Checks	9 pruebas
Dominio	ceiber.com	Hallazgos	46 totales
Fecha	22 de abril de 2026 a las 17:56	Problemas	15 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría técnica realizada al sitio web arroja una puntuación de 62/100, lo que sitúa la seguridad de la plataforma en una nota C. El análisis consistió en la ejecución de 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fallaron críticamente por la ausencia de controles esenciales. Aunque el cifrado SSL es correcto, la carencia absoluta de cabeceras de seguridad y la exposición de puertos de red sensibles comprometen la integridad del servidor. Se concluye que el sitio es vulnerable ante ataques de interceptación de datos y manipulación de contenido en el lado del cliente.

Resumen de Riesgos

0	5	8	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 33 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	20	FALLO	6 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 33 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  33 dias restantes (expira: 2026-05-25T19:31:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-24T19:31:18.000Z
- 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/1.18.0 (Ubuntu) — 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://ceiber.com/
- 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**
  Next.js

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 — 20/100

Estado: FALLO

6 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.omie.es/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.omie.es/files/flash/ResultadosMercado.html
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.omip.pt/
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, 3 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 8080 (HTTP-Alt)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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: Falta esta cabecera esencial para prevenir ataques de inyección de código y Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras y permite ataques de degradación de protocolo.
[HIGH] Puerto 21 (FTP): El servicio FTP se encuentra abierto, lo cual es peligroso por transmitir credenciales y archivos sin ningún tipo de cifrado.
[MEDIUM] Contenido Mixto: Se detectaron 6 recursos cargados mediante HTTP (como enlaces a omie.es), lo que invalida parcialmente la seguridad de la conexión HTTPS.
[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto está abierto y suele alojar servicios de administración o proxies que aumentan la superficie de exposición.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores ignoren el tipo MIME declarado, abriendo la puerta a la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de navegación que se envía a sitios externos a través de los referers.
[MEDIUM] Permissions-Policy: Falta la restricción de acceso a APIs del navegador, permitiendo potencialmente el uso no autorizado de funciones como la cámara o geolocalización.
[LOW] Server header expuesto: El servidor revela la versión exacta de software (nginx/1.18.0 en Ubuntu), facilitando a atacantes la búsqueda de vulnerabilidades específicas.
[LOW] Archivo robots.txt: No se encontró el archivo en el servidor, lo que impide una gestión adecuada del rastreo por parte de motores de búsqueda.