EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://enterprise.cltechcloud.net:37101/	Checks	9 pruebas
Dominio	enterprise.cltechcloud.net	Hallazgos	42 totales
Fecha	15 de julio de 2026 a las 12:56	Problemas	14 detectados

D

48/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar una auditoría de seguridad sobre el activo digital, se ha obtenido una puntuación de 48/100, lo que otorga una calificación de grado D. Durante el análisis, se ejecutaron 9 checks pasivos, de los cuales únicamente 4 resultaron exitosos, identificando 1 advertencia y 3 fallos críticos en la infraestructura base. La ausencia total de un certificado SSL válido y la carencia de cabeceras de seguridad fundamentales comprometen la integridad del sitio. Debido a estas deficiencias técnicas, se concluye que el sitio es vulnerable y no cumple con los estándares mínimos de seguridad web industrial.

Resumen de Riesgos

1	4	8	1	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
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 — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-09-21T20:55:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-23T20:55:34.000Z
- 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 **X-Powered-By expuesto**
  X-Powered-By: Express — 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: ERROR

No se pudo verificar la redireccion HTTPS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 303 redirige a https://cltechecuador.com/

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**
  Express

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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[CRITICAL] Certificado SSL no válido: El sitio no cuenta con un certificado SSL/TLS funcional, lo que impide el cifrado de datos entre el servidor y el usuario.
[HIGH] Protocolo inseguro: El sitio opera bajo HTTP, permitiendo ataques de interceptación de datos (Man-in-the-Middle).
[HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options faltante: El sitio es vulnerable a ataques de clickjacking al permitir ser cargado dentro de iframes externos.
[HIGH] Strict-Transport-Security (HSTS) faltante: No se obliga al navegador a utilizar conexiones seguras, facilitando el downgrade de seguridad.
[MEDIUM] Paneles de login expuestos: Se detectaron rutas de administración accesibles públicamente en /wp-login.php, /administrator/ y /user/login.
[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt son públicos y pueden revelar metadatos técnicos sensibles.

[MEDIUM] X-Content-Type-Options faltante: El sitio es susceptible a ataques basados en MIME-type sniffing.
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: No existe control sobre la información de navegación enviada a terceros ni sobre las APIs del navegador.
[LOW] X-Powered-By expuesto: La cabecera revela el uso del framework Express, facilitando a un atacante la búsqueda de exploits específicos.
[LOW] Ausencia de archivos de rastreo: No se encontraron robots.txt ni sitemap.xml, lo que dificulta la gestión del indexado y la seguridad del contenido.