EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://idte.app	Checks	9 pruebas
Dominio	idte.app	Hallazgos	46 totales
Fecha	12 de mayo de 2026 a las 22:39	Problemas	13 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio idte.app ha arrojado una puntuación de 59/100, lo que resulta en una calificación de grado D. Durante la auditoría se ejecutaron un total de 9 comprobaciones pasivas, identificando 5 resultados satisfactorios, 2 advertencias y 2 fallos críticos en la configuración. La ausencia total de cabeceras de seguridad y la falta de redirección forzada hacia el protocolo HTTPS representan riesgos significativos para la integridad de la plataforma. Por lo tanto, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación de datos y manipulación de contenido en el navegador.

Resumen de Riesgos

0	5	5	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-06-18T17:09:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-20T16:11:35.000Z
- 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: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.19 — 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**
  React, PHP/8.4.19

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- 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] Redirección HTTPS ausente: El servidor no redirige el tráfico HTTP inseguro hacia HTTPS, permitiendo comunicaciones vulnerables a interceptación.
[HIGH] HSTS (Strict-Transport-Security) no configurado: La ausencia de esta política impide que los navegadores fuercen conexiones cifradas de forma automática.
[HIGH] Content-Security-Policy (CSP) faltante: El sitio carece de protecciones contra ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options faltante: La falta de esta cabecera permite que el sitio sea cargado en marcos externos, facilitando ataques de Clickjacking.
[MEDIUM] X-Content-Type-Options faltante: Sin esta cabecera, el navegador podría interpretar archivos de forma incorrecta, permitiendo ataques de MIME-sniffing.
[MEDIUM] Referrer-Policy faltante: No se controla la cantidad de información de referencia que se envía a otros dominios al navegar.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso a APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Puerto 8080 abierto: Se detectó el puerto HTTP-Alt accesible, lo cual aumenta la superficie de ataque y expone servicios potencialmente inseguros.
[MEDIUM] Bloqueo total en robots.txt: El archivo de rastreo prohíbe el acceso a todo el sitio, lo que podría indicar una configuración incorrecta del servidor.
[LOW] Exposición de versión de PHP: La cabecera X-Powered-By revela que el sitio utiliza PHP/8.4.19, facilitando la búsqueda de exploits específicos.
[LOW] Cabecera Server expuesta: Se identifica el uso de Cloudflare, revelando detalles sobre la infraestructura de red utilizada.
[LOW] Sitemap.xml no encontrado: La falta de este archivo dificulta la auditoría de rutas y el correcto indexado de los recursos del sitio.