EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.buroempresas.com	Checks	9 pruebas
Dominio	www.buroempresas.com	Hallazgos	41 totales
Fecha	3 de julio de 2026 a las 04:23	Problemas	7 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web buroempresas.com ha arrojado una puntuación de 85/100, lo que equivale a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, mientras que se detectaron una advertencia y un fallo crítico en la gestión de transporte y sesiones. A pesar de contar con una configuración robusta en sus cabeceras de seguridad, el sistema presenta deficiencias severas en la implementación de certificados SSL y en la protección de cookies de sesión. Estos hallazgos indican que la plataforma no garantiza actualmente un canal de comunicación cifrado ni una gestión de identidad blindada contra ataques externos. Por lo tanto, se concluye que el sitio es vulnerable y requiere intervenciones técnicas inmediatas para proteger la integridad de sus usuarios.

Resumen de Riesgos

1	3	2	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	17	FALLO	PHPSESSID: falta Secure; PHPSESSID: falta SameSi...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- INFO **Content-Security-Policy**
  Presente: script-src 'self' 'unsafe-inline' 'unsafe-eval' https://*.google-analytics.com ...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains

- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=(), payment=(), usb=(), fullscreen=(s...

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

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 — 17/100

Estado: FALLO

PHPSESSID: falta Secure; PHPSESSID: falta SameSite; TS01676dc9: falta HttpOnly; TS01676dc9: falta Secure; TS01676dc9: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS01676dc9 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS01676dc9 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS01676dc9 — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 robots.txt

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, 59 URLs
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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] Conexión SSL/TLS: No se pudo establecer una conexión cifrada verificable, lo que expone todo el tráfico de datos a interceptaciones.
[HIGH] Cookie PHPSESSID - Falta flag Secure: El identificador de sesión se transmite a través de conexiones no cifradas, facilitando el robo de la sesión en redes públicas o comprometidas.
[HIGH] Cookie TS01676dc9 - Falta flag Secure: Esta cookie técnica carece de la instrucción para viajar únicamente por canales seguros, aumentando el riesgo de exposición.
[HIGH] Cookie TS01676dc9 - Falta flag HttpOnly: El token es accesible mediante scripts del navegador, lo que lo hace vulnerable a ataques de robo de sesión mediante Cross-Site Scripting (XSS).
[MEDIUM] Cookie PHPSESSID - Falta atributo SameSite: La ausencia de este control permite que la cookie sea enviada en peticiones de terceros, exponiendo al usuario a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Cookie TS01676dc9 - Falta atributo SameSite: No se restringe el contexto de envío de la cookie, lo que facilita vectores de ataque para manipular la sesión del usuario desde otros dominios.
[LOW] Archivo robots.txt no encontrado: La falta de este archivo de directrices puede permitir que los motores de búsqueda indexen áreas sensibles o no deseadas del servidor.