EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://guerrastribales.es	Checks	9 pruebas
Dominio	guerrastribales.es	Hallazgos	56 totales
Fecha	14 de mayo de 2026 a las 02:04	Problemas	19 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio guerrastribales.es arroja una puntuación de 53/100, lo que equivale a una nota de D. De los 9 checks pasivos ejecutados, se han obtenido 5 resultados satisfactorios y 4 fallos críticos relacionados con la configuración del servidor y la privacidad de los datos. Se observa una ausencia casi total de cabeceras de seguridad esenciales y una gestión deficiente de las cookies de sesión, que carecen de los atributos mínimos de protección. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable frente a ataques de interceptación de datos e inyección de scripts.

Resumen de Riesgos

0	8	9	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	33	FALLO	ref: falta HttpOnly; ref: falta Secure; ref: fal...
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-06-28T11:51:21.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-30T11:51:22.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: NONE
- 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 307 — 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

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 — 33/100

Estado: FALLO

ref: falta HttpOnly; ref: falta Secure; ref: falta SameSite; cid: falta HttpOnly; cid: falta Secure; cid: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: ref — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ref — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ref — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: cid — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: cid — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: cid — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: PHPSESSID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: PHPSESSID — SameSite**
  SameSite=lax

Contenido Mixto — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://om.elvenar.com/ox/es/?ref=ds_portalbar_text
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://om.tribalwars2.com/tw2/es/?ref=ds_portalbar_text
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://om.forgeofempires.com/foe/es/?ref=ds_portalbar_text
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (162 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- 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

[LOW] Server header expuesto: El servidor revela el uso de nginx, lo que proporciona información técnica útil para atacantes que busquen vulnerabilidades específicas de esa tecnología.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) y otras inyecciones de contenido malicioso.
[HIGH] Strict-Transport-Security (HSTS) ausente: El servidor no obliga al navegador a utilizar conexiones cifradas, permitiendo posibles ataques de degradación de SSL.
[MEDIUM] X-Content-Type-Options ausente: Al no estar configurada, el sitio es vulnerable a ataques de MIME-type sniffing para ejecutar archivos con contenido malicioso.
[MEDIUM] Referrer-Policy ausente: El sitio no controla qué información de navegación se envía a otros dominios, lo que puede comprometer la privacidad del usuario.
[MEDIUM] Permissions-Policy ausente: No existen restricciones sobre el acceso del navegador a APIs sensibles como la cámara, el micrófono o la ubicación.
[HIGH] Redirección HTTP a HTTPS inexistente: El servidor responde con un código 307 pero no fuerza la navegación segura, dejando la comunicación inicial expuesta.
[HIGH] Cookie ref sin flags de seguridad: Carece de los atributos HttpOnly, Secure y SameSite, permitiendo que la cookie sea robada mediante scripts o interceptada en conexiones no cifradas.
[HIGH] Cookie cid sin flags de seguridad: Al igual que la anterior, esta cookie es accesible vía JavaScript y vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido mixto detectado: Se cargan 4 recursos (stylesheets y enlaces) mediante el protocolo inseguro HTTP dentro de la página protegida por HTTPS.
[LOW] Ruta sensible en robots.txt: El archivo de indexación hace referencia directa a una ruta admin, facilitando a posibles atacantes la localización de paneles de administración.