EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://forum.guerrastribales.es	Checks	9 pruebas
Dominio	forum.guerrastribales.es	Hallazgos	46 totales
Fecha	14 de mayo de 2026 a las 02:02	Problemas	12 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado en forum.guerrastribales.es ha resultado en una puntuación de 72/100 con una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 2 advertencias y 1 fallo crítico en la configuración de seguridad. Aunque la implementación del certificado SSL es robusta, se detectó una ausencia total de cabeceras de protección esenciales y la presencia de contenido mixto. Debido a la carencia de políticas contra ataques de inyección y suplantación, el sitio se considera actualmente vulnerable ante amenazas comunes de la web.

Resumen de Riesgos

0	4	7	1	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 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	60	AVISO	3 recurso(s) 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 — 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 — 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://forum.guerrastribales.es/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 429

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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://help.guerrastribales.es/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.guerrastribales.es/sds_rounds.php?mode=pas
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.guerrastribales.es/sds_rounds.php?mode=present

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1810 bytes)
- INFO **Reglas robots.txt**
  50 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **sitemap.xml**
  Presente, 13355 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio queda expuesto a ataques de clickjacking donde un atacante puede camuflar la interfaz.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador obligue siempre a una conexión segura, facilitando ataques de degradación de protocolo.
[HIGH] HSTS (Strict-Transport-Security): No se ha configurado el mecanismo de transporte estricto, lo que debilita la política de redirección HTTPS.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos con contenido inesperado.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que puede comprometer la privacidad del usuario.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Contenido Mixto: Se cargan 3 recursos mediante HTTP en una página segura, lo que compromete la integridad del cifrado SSL.
[MEDIUM] Bloqueo total en Robots.txt: El archivo robots.txt prohíbe el rastreo de todo el sitio, lo que puede ser un error de configuración administrativa.
[LOW] Server header expuesto: El encabezado revela el uso del servidor nginx, proporcionando información útil para atacantes que busquen vulnerabilidades específicas de software.