EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.terrachat.es	Checks	9 pruebas
Dominio	www.terrachat.es	Hallazgos	43 totales
Fecha	6 de julio de 2026 a las 11:35	Problemas	14 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 64/100, lo que equivale a una nota de C. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 terminaron en fallo crítico. Se ha detectado una exposición grave de la base de datos y una ausencia total de cabeceras de seguridad fundamentales. Por tanto, se concluye que el sitio es vulnerable y presenta riesgos significativos para la integridad de los datos y la privacidad de los usuarios.

Resumen de Riesgos

1	4	5	4	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 188 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	CMS detectado: Joomla
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	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 188 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  188 dias restantes (expira: 2027-01-09T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-09T00:00:00.000Z
- 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: LiteSpeed — 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://www.terrachat.es/
- 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

CMS detectado: Joomla

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  Detectado via HTML body
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Joomla! - Open Source Content Management

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

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.movilchat.net

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 3306 (MySQL)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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] Puerto 3306 (MySQL): La base de datos está abierta a conexiones externas, lo que permite intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de inyección de código como Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de Clickjacking donde se puede suplantar la interfaz.
[HIGH] Strict-Transport-Security: La falta de HSTS permite que un atacante degrade la conexión de HTTPS a HTTP mediante ataques de intermediario.
[MEDIUM] Puerto 22 (SSH): El servicio de administración remota está visible, aumentando la superficie de ataque frente a intrusiones.
[MEDIUM] Contenido Mixto: Se detectó un recurso stylesheet cargado vía HTTP desde movilchat.net, comprometiendo la integridad de la conexión cifrada.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador adivine el tipo de contenido, facilitando la ejecución de archivos maliciosos.

[MEDIUM] Referrer-Policy: No existe control sobre la información que se envía a otros sitios al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como la cámara o el micrófono, incrementando el riesgo de abuso de APIs.
[LOW] Server header expuesto: El servidor revela que utiliza LiteSpeed, facilitando la búsqueda de exploits específicos para esa tecnología.
[LOW] Meta generator: La etiqueta meta expone que el sitio utiliza Joomla, ayudando a los atacantes a identificar vectores de ataque conocidos.
[LOW] Robots.txt y Sitemap: La ausencia de estos archivos dificulta la auditoría legítima y el correcto indexado de seguridad.