EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://estoyalerta.org	Checks	9 pruebas
Dominio	estoyalerta.org	Hallazgos	47 totales
Fecha	18 de agosto de 2026 a las 06:39	Problemas	22 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de ciberseguridad realizada a estoyalerta.org arroja una puntuacion de 68/100, lo que corresponde a una nota de C. El analisis consistio en 9 checks pasivos, resultando en 6 satisfactorios, 1 advertencia y 2 fallos criticos que comprometen la infraestructura. Se han identificado multiples servicios internos y bases de datos expuestos directamente a internet, ademas de una carencia total de politicas de seguridad en cabeceras HTTP. En su estado actual, el sitio se clasifica como vulnerable debido a riesgos severos de acceso no autorizado y fuga de informacion.

Resumen de Riesgos

6	5	10	1	25
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	20	FALLO	9 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-11-06T11:47:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-08T11:47:27.000Z
- 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: Fly/d778e1ff4 (2026-08-17) — 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://estoyalerta.org/
- 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**
  Astro

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (69 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://estoyalerta.org/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 20/100

Estado: FALLO

9 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- CRITICO **Puerto 23 (Telnet)**
  ABIERTO — 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
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- CRITICO **Puerto 27017 (MongoDB)**
  ABIERTO — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 27017 (MongoDB): Base de datos expuesta que permite intentos de acceso externo y posible exfiltracion de datos sensibles.
[CRITICAL] Puerto 6379 (Redis): Almacenamiento en cache accesible sin autenticacion por defecto, lo que facilita la manipulacion de sesiones.
[CRITICAL] Puerto 3389 (RDP): Protocolo de escritorio remoto visible, aumentando el riesgo de ataques de fuerza bruta contra el servidor.
[CRITICAL] Puerto 5432 (PostgreSQL): Exposicion de base de datos relacional que podria ser blanco de inyecciones o ataques directos.
[CRITICAL] Puerto 3306 (MySQL): Servicio de base de datos abierto al publico, representando un vector de ataque critico para la integridad de la informacion.
[CRITICAL] Puerto 23 (Telnet): Protocolo de administracion remota sin cifrar que transmite credenciales en texto plano.
[HIGH] Content-Security-Policy: Ausencia de esta cabecera, lo que deja al sitio desprotegido contra ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Falta de proteccion contra Clickjacking, permitiendo que el sitio sea embebido en marcos maliciosos.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo posibles ataques de degradacion de conexion.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos sin cifrado activo, vulnerable a la interceptacion de datos.
[MEDIUM] Puertos 22 (SSH) y 8080 (HTTP-Alt): Servicios de gestion y servidores alternativos detectados que amplian la superficie de ataque.
[MEDIUM] Exposicion de archivos tecnicos: Los archivos /readme.html y /README.txt son accesibles y pueden revelar detalles de la infraestructura.
[MEDIUM] Rutas de administracion expuestas: Paneles de login en /wp-login.php, /administrator/ y /user/login son visibles para cualquier usuario.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME por parte del navegador.
[MEDIUM] Referrer-Policy y Permissions-Policy: Ausencia de control sobre la informacion de referencia y el uso de APIs del navegador como camara o microfono.
[LOW] Server header expuesto: La cabecera revela el uso de Fly/d778e1ff4, facilitando la identificacion de la tecnologia del servidor a atacantes.