EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://eyesecurityforum.com/	Checks	9 pruebas
Dominio	eyesecurityforum.com	Hallazgos	43 totales
Fecha	30 de abril de 2026 a las 18:12	Problemas	15 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre eyesecurityforum.com ha arrojado una puntuacion de 53/100, lo que equivale a una nota D. El analisis se baso en 9 checks pasivos, de los cuales 5 resultaron satisfactorios y 4 presentaron fallos significativos de configuracion. A pesar de contar con un certificado SSL valido, el sitio web muestra deficiencias criticas en la proteccion de su infraestructura de red y en la implementacion de cabeceras de seguridad. La exposicion directa de servicios de base de datos y la falta de cifrado en transito obligatorio comprometen la integridad de la plataforma. En conclusion, el sitio se considera vulnerable y requiere correcciones inmediatas para mitigar riesgos de intrusión y fuga de datos.

Resumen de Riesgos

2	6	4	3	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	4 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-07-24T03:29:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-25T03:29:33.000Z
- 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: Apache — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — 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
- INFO **Tecnologias detectadas**
  React

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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

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 — 20/100

Estado: FALLO

4 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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 5432 (PostgreSQL): Base de datos PostgreSQL expuesta publicamente, lo que permite ataques directos de autenticacion y posible extraccion de informacion.
[CRITICAL] Puerto 3306 (MySQL): Base de datos MySQL abierta al exterior, representando un riesgo critico de compromiso de datos sensibles.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos activo sin cifrar, facilitando la interceptacion de credenciales en la red.
[HIGH] Falta de Strict-Transport-Security (HSTS): La ausencia de esta cabecera permite que las conexiones sean vulnerables a ataques de degradacion de protocolo.
[HIGH] Redireccion HTTP a HTTPS: El servidor no fuerza el uso de conexiones cifradas, permitiendo que los usuarios naveguen de forma insegura por el puerto 80.
[HIGH] Falta de Content-Security-Policy (CSP): No existen politicas para prevenir la ejecucion de scripts maliciosos o ataques de inyeccion de contenido.

[HIGH] Falta de X-Frame-Options: El sitio no protege contra ataques de clickjacking, permitiendo que el contenido sea embebido en sitios de terceros.
[MEDIUM] Puerto 22 (SSH): Acceso remoto seguro abierto, el cual es un objetivo constante para ataques de fuerza bruta.
[MEDIUM] Falta de X-Content-Type-Options: El navegador podria interpretar archivos de forma incorrecta, facilitando ataques de sniffing de contenido.
[MEDIUM] Falta de Referrer-Policy: No se controla la informacion de navegacion que se envia a otros sitios mediante los enlaces salientes.
[MEDIUM] Falta de Permissions-Policy: No se restringe el acceso de las APIs del navegador a funciones sensibles como la ubicacion o la camara.
[LOW] Server header expuesto: Se revela que el servidor utiliza Apache, informacion que ayuda a los atacantes a buscar vulnerabilidades especificas de esa version.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la gestion correcta del rastreo por parte de los motores de busqueda.