EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://thepiratebay.org	Checks	9 pruebas
Dominio	thepiratebay.org	Hallazgos	43 totales
Fecha	20 de mayo de 2026 a las 21:27	Problemas	13 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio thepiratebay.org arroja una puntuación de 66/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 4 generaron advertencias y 1 fue clasificado como fallo crítico. A pesar de contar con un cifrado de transporte válido, la configuración de seguridad de la plataforma presenta carencias importantes en la protección del lado del cliente. Debido a la ausencia de cabeceras de seguridad esenciales y la presencia de contenido mixto, se concluye que el sitio es vulnerable ante ataques de interceptación y manipulación de datos.

Resumen de Riesgos

0	4	8	1	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 36 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	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 36 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  36 dias restantes (expira: 2026-06-25T11:52:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-27T10:53:28.000Z
- 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: cloudflare — 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://thepiratebay.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

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
- 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

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://piratebayo3klnzokct3wt5yyxb2vpebbuyjl7m623iaxmqhsd52c...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://ikeanangelsaidthe.com/redirect?tid=858335

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (49 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar implementada, el sitio es vulnerable a ataques de clickjacking donde un atacante puede camuflar la interfaz.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce una conexión segura, facilitando ataques de degradación de SSL.
[MEDIUM] X-Content-Type-Options: La carencia de esta directiva permite que el navegador realice "MIME-sniffing", lo que puede derivar en la ejecución de archivos no ejecutables.
[MEDIUM] Contenido Mixto: Se detectaron 2 recursos cargados mediante HTTP (piratebayo3klnzokct3wt5yyxb2vpebbuyjl7m623iaxmqhsd52c e ikeanangelsaidthe.com) que comprometen la integridad de la página HTTPS.

[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo que podría revelar detalles técnicos sobre la infraestructura.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de un puerto de servidor web alternativo incrementa la superficie de ataque disponible para posibles intrusiones.
[MEDIUM] Referrer-Policy: No se ha configurado una política para controlar la información de navegación que se envía a sitios externos.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: El encabezado revela el uso de la tecnología Cloudflare, lo cual facilita la fase de reconocimiento de un atacante.