EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://hackthissite.org	Checks	9 pruebas
Dominio	hackthissite.org	Hallazgos	52 totales
Fecha	17 de julio de 2026 a las 20:38	Problemas	12 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de seguridad en hackthissite.org, el sitio ha obtenido una puntuación de 71/100 con una calificación de grado C. El proceso consistió en la ejecución de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, uno presentó advertencias y tres fueron fallos críticos. Aunque la infraestructura de cifrado es sólida, existen debilidades importantes en la configuración de las cabeceras de seguridad y el manejo de los datos de sesión. Por consiguiente, se concluye que el sitio es vulnerable ante ataques dirigidos a los usuarios finales, como el secuestro de sesiones y el clickjacking.

Resumen de Riesgos

0	3	7	2	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, X-C...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	0	FALLO	HackThisSite: falta HttpOnly; HackThisSite: falt...
Contenido Mixto	20	FALLO	9 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

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: 2026-10-10T06:05:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-25T06:05:48.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, X-Content-Type-Options, Permissions-Policy

- BAJO **Server header expuesto**
  Server: HackThisSite — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: child-src 'self' hackthissite.org *.hackthissite.org htscdn.org *.htscdn.org dis...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: origin-when-cross-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://hackthissite.org/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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**
  Next.js

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 — 0/100

Estado: FALLO

HackThisSite: falta HttpOnly; HackThisSite: falta Secure; HackThisSite: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: HackThisSite — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: HackThisSite — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: HackThisSite — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

9 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npak...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://hts.io/x/http://creativecommons.org/licenses/by-nc/3....
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://hts.io/x/http://creativecommons.org/licenses/by-nc/3....
- MEDIO **href (link/stylesheet)**
  ...y 6 mas del mismo tipo

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (66 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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] Cookie HttpOnly: La falta de este flag en la cookie HackThisSite permite que sea accesible mediante scripts, aumentando el riesgo de robo de sesión vía XSS.
[HIGH] Cookie Secure: La ausencia de la bandera Secure permite que la cookie se transmita por conexiones no cifradas, exponiendo datos sensibles.
[HIGH] X-Frame-Options: La falta de esta cabecera de seguridad deja al dominio vulnerable a ataques de clickjacking.
[MEDIUM] Cookie SameSite: No se ha implementado este atributo, lo que hace al sitio susceptible a ataques de Cross-Site Request Forgery (CSRF).
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite que el navegador realice sniffing de tipos MIME, pudiendo ejecutar archivos maliciosos.
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, permitiendo potencialmente el uso no autorizado de hardware como cámara o micrófono.
[MEDIUM] Contenido Mixto: Se detectaron 9 recursos cargados mediante protocolo HTTP inseguro dentro de una página HTTPS, rompiendo la cadena de confianza.
[LOW] Server header expuesto: El servidor revela el nombre "HackThisSite", proporcionando información técnica que facilita el reconocimiento por parte de atacantes.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que representa una deficiencia en la organización y visibilidad de los recursos.