

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.deepwebthemovie.com/#land	Checks	9 pruebas
Dominio	www.deepwebthemovie.com	Hallazgos	53 totales
Fecha	7 de octubre de 2026 a las 04:09	Problemas	14 detectados

D

57/100

puntos de seguridad



RESUMEN EJECUTIVO

Tras realizar la auditoría técnica, el sitio web presenta una puntuación de seguridad de 57/100, obteniendo una calificación de nota D. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios y 4 detectaron fallos críticos en la configuración. El análisis revela deficiencias importantes en la implementación de cabeceras de protección y en la gestión de recursos cifrados. Debido a la falta de políticas contra inyección de código y la presencia de contenido mixto, se concluye que el sitio es actualmente vulnerable a diversos vectores de ataque.

Resumen de Riesgos

0	4	8	2	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: Squarespace
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	33	FALLO	crumb: falta HttpOnly; crumb: falta SameSite
Contenido Mixto	20	FALLO	31 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 60 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
60 dias restantes (expira: 2026-12-06T10:10:46.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-07T10:10:47.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: Squarespace — 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
- INFO

Strict-Transport-Security
Presente: max-age=0
- INFO

X-Content-Type-Options
Presente: nosniiff
- 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
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=0
- BAJO

HSTS includeSubDomains
HSTS no cubre subdominios
- MEDIO

HSTS max-age
max-age=0 (0 dias) — Recomendado minimo 180 dias
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Squarespace

- 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
Detectado via HTML body
- 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 — 33/100

Estado: FALLO

crumb: falta HttpOnly; crumb: falta SameSite

-  INFO **Cookies detectadas**
1 cookie(s) encontrada(s)
-  ALTO **Cookie: crumb — HttpOnly**
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
-  INFO **Cookie: crumb — Secure**
Flag Secure activo — Solo se envia por HTTPS
-  MEDIO **Cookie: crumb — SameSite**
Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

31 recursos HTTP en pagina HTTPS

-  MEDIO **Recurso HTTP (href (link/stylesheet))**
http://www.deepwebthemovie.com
-  MEDIO **Recurso HTTP (href (link/stylesheet))**
http://www.deepwebthemovie.com/welcome?format=rss
-  MEDIO **Recurso HTTP (href (link/stylesheet))**
http://alexwinter.com/
-  MEDIO **href (link/stylesheet)**
...y 28 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

-  INFO **robots.txt**
Presente (1513 bytes)
-  INFO **Reglas robots.txt**
27 Disallow, 1 Allow
-  BAJO **Ruta sensible en robots.txt**
Referencia a "config" — Puede revelar rutas sensibles a atacantes
-  INFO **Sitemap en robots.txt**
http://www.deepwebthemovie.com/sitemap.xml
-  BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 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)**
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 autentificacion 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] 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 presente, el sitio es vulnerable a ataques de clickjacking que podrían engañar a los usuarios.
- [HIGH] Redirección HTTP a HTTPS: El servidor no fuerza la conexión cifrada, permitiendo el acceso a través de canales no seguros.
- [HIGH] Seguridad de Cookies (HttpOnly): La cookie denominada crumb carece del atributo HttpOnly, lo que permite su lectura mediante scripts y aumenta el riesgo de robo de sesión.
- [MEDIUM] Contenido Mixto: Se detectaron 31 recursos cargados mediante HTTP en una página HTTPS, rompiendo la integridad de la conexión segura.
- [MEDIUM] Referrer-Policy: Falta el control sobre la información de procedencia que el navegador envía a otros dominios.
- [MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, dejando expuestas funciones como la cámara o el micrófono.
- [MEDIUM] HSTS max-age: El valor actual es 0, lo que significa que no se obliga al navegador a recordar la conexión segura en futuras visitas.
- [MEDIUM] Seguridad de Cookies (SameSite): La falta del atributo SameSite en la cookie crumb expone a los usuarios a ataques de falsificación de petición en sitios cruzados (CSRF).
- [LOW] Cabecera Server expuesta: El servidor revela que utiliza Squarespace, facilitando información técnica útil para potenciales atacantes.
- [LOW] Robots.txt: El archivo incluye una referencia a la ruta config, lo que podría orientar a un atacante hacia áreas sensibles del CMS.