EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://edifito.com	Checks	9 pruebas
Dominio	edifito.com	Hallazgos	45 totales
Fecha	21 de abril de 2026 a las 17:18	Problemas	13 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada a edifito.com arroja una puntuación de 64/100, lo que resulta en una nota C. El análisis pasivo ejecutado consistió en 9 checks, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 2 finalizaron en fallo crítico, además de un error por tiempo de espera en un módulo. El sitio presenta deficiencias estructurales en la configuración de cabeceras de seguridad y manejo de recursos internos, lo que compromete la integridad de la conexión. Debido a la falta de políticas de protección básicas en el servidor, el sitio se considera actualmente vulnerable ante ataques de interceptación y suplantación.

Resumen de Riesgos

0	4	7	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 313 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	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	5 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 313 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  313 dias restantes (expira: 2027-02-28T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-28T00:00:00.000Z
- 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/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips — 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 302 redirige a https://edifito.com/
- 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Powered by Slider Revolution 6.6.20 - responsive, Mobile-Friendly Slider Plugin for WordPress with comfortable drag and drop interface.
- INFO **Tecnologias detectadas**
  Next.js

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 — 20/100

Estado: FALLO

5 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://edifito2021.edifitolabs.com/sobre-edifito/

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://edifito2021.edifitolabs.com/rse/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://edifito2021.edifitolabs.com/medios/blog/
- MEDIO **href (link/stylesheet)**
  ...y 2 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (173 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.edifito.com/sitemap_index.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 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] Content-Security-Policy: Falta esta cabecera crítica que previene ataques de inyección de código y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta política permite ataques de clickjacking, donde el sitio puede ser cargado en marcos externos para engañar al usuario.
[HIGH] Strict-Transport-Security: HSTS no está configurado, lo que impide que el navegador obligue a realizar conexiones cifradas de forma permanente.
[MEDIUM] Contenido Mixto: Se detectaron 5 recursos cargando mediante protocolo HTTP inseguro dentro de la página HTTPS, lo que debilita el cifrado general.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros dominios, pudiendo filtrar datos de navegación.

[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones como la cámara o el micrófono ante posibles abusos.
[LOW] Server header expuesto: Se detectó la versión específica del servidor Apache/2.4.6 y el sistema operativo, facilitando la búsqueda de exploits conocidos.
[LOW] Meta generator: El sitio expone versiones técnicas de plugins como Slider Revolution 6.6.20, lo que ayuda a potenciales atacantes en la fase de reconocimiento.