EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.forentrepreneurs.com/	Checks	9 pruebas
Dominio	www.forentrepreneurs.com	Hallazgos	59 totales
Fecha	31 de julio de 2026 a las 03:08	Problemas	19 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 53/100, lo que corresponde a una calificación de grado D. El análisis se basó en 9 comprobaciones pasivas, de las cuales 3 resultaron satisfactorias, 3 generaron advertencias y 3 fallaron debido a configuraciones críticas ausentes. Se han identificado debilidades importantes en la protección de las comunicaciones, la gestión de sesiones y la exposición de información del sistema de gestión de contenidos. Por lo tanto, se concluye que el sitio es actualmente vulnerable y requiere intervenciones inmediatas para mitigar riesgos de ataques comunes.

Resumen de Riesgos

0	7	9	3	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 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
Version CMS Expuesta	20	FALLO	WordPress 1785121712 expuesta
Seguridad de Cookies	78	AVISO	ep_session_id: falta HttpOnly; ep_session_id: fa...
Contenido Mixto	20	FALLO	6 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  61 dias restantes (expira: 2026-09-30T03:23:54.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-02T03:23:55.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: WP Engine — Revela framework/lenguaje
- 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://www.forentrepreneurs.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: WPML ver:4.9.5 stt:1,28,29,44,2;
- INFO **Tecnologias detectadas**
  Next.js, WP Engine

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1785121712 expuesta

- ALTO **WordPress version**
  Version 1785121712 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 78/100

Estado: AVISO

ep_session_id: falta HttpOnly; ep_session_id: falta HttpOnly

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: ep_session_id — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ep_session_id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ep_session_id — SameSite**
  SameSite=lax
- ALTO **Cookie: ep_session_id — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ep_session_id — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ep_session_id — SameSite**
  SameSite=lax
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

Contenido Mixto — 20/100

Estado: FALLO

6 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.matrixpartners.com/about-us/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.matrixpartners.com/team/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.matrixpartners.com/portfolio/
- MEDIO **href (link/stylesheet)**
  ...y 3 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (198 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.forentrepreneurs.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] Falta de Strict-Transport-Security: La ausencia de HSTS permite ataques de degradación de SSL y no garantiza conexiones seguras obligatorias.
[HIGH] Falta de Content-Security-Policy: El sitio carece de políticas para prevenir ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] Falta de X-Frame-Options: No se implementa protección contra ataques de clickjacking, permitiendo que la web sea cargada en marcos externos maliciosos.
[HIGH] Versión de WordPress expuesta: La visibilidad pública de la versión 1785121712 permite a atacantes buscar vulnerabilidades específicas (CVE) para dicho sistema.
[HIGH] Cookie ep_session_id sin HttpOnly: Las cookies de sesión son accesibles mediante scripts del navegador, lo que facilita el robo de sesiones en caso de un ataque XSS.
[MEDIUM] Contenido mixto detectado: Se identificaron 6 recursos cargados a través de HTTP en una página HTTPS, comprometiendo la integridad y privacidad del sitio.
[MEDIUM] Puerto 8080 abierto: La exposición de este puerto alternativo aumenta la superficie de ataque y revela servicios internos potencialmente vulnerables.
[MEDIUM] Falta de X-Content-Type-Options: La ausencia de esta cabecera permite el sniffing de tipos MIME, lo que puede derivar en la ejecución de código no deseado.
[MEDIUM] Panel de login accesible: La ruta /wp-login.php está disponible públicamente, lo que facilita intentos de acceso no autorizado mediante fuerza bruta.
[MEDIUM] Falta de Referrer-Policy y Permissions-Policy: No existe control sobre la información de navegación compartida ni sobre las funciones del navegador permitidas.
[LOW] Exposición de cabeceras de servidor: Se revela el uso de Cloudflare y WP Engine, entregando información técnica valiosa para el reconocimiento por parte de atacantes.
[LOW] Meta generator expuesto: La etiqueta meta revela detalles del plugin WPML, aportando más datos sobre la infraestructura interna.