EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://exileworld.io/shop?view=cases	Checks	9 pruebas
Dominio	exileworld.io	Hallazgos	44 totales
Fecha	14 de agosto de 2026 a las 03:24	Problemas	11 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad web realizada al sitio arroja una puntuacion exacta de 61/100, lo que equivale a una nota de C. El analisis se baso en 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se identifico 1 advertencia y se registraron 2 fallos criticos. La ausencia de cabeceras de seguridad fundamentales y la falta de una redireccion forzada a HTTPS impactan negativamente en la postura defensiva. Se concluye que el sitio es actualmente vulnerable a ataques de interceptacion de datos, clickjacking e inyeccion de contenido.

Resumen de Riesgos

0	5	5	1	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 57 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	100	OK	No se detecto contenido mixto
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 57 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  57 dias restantes (expira: 2026-10-09T20:14:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-11T20:14:52.000Z
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

- 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 — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1996 bytes)
- INFO **Reglas robots.txt**
  14 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://alderveil.org/sitemap.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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecucion de scripts maliciosos y ataques de inyeccion de contenido (XSS).
[HIGH] X-Frame-Options: Falta de proteccion que permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: Al no estar configurado, el navegador no fuerza el uso de conexiones cifradas permanentemente.
[HIGH] Redireccion HTTP a HTTPS: El servidor permite conexiones inseguras a traves del puerto 80 sin redirigir automaticamente al protocolo seguro.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detecto un puerto alternativo abierto que podria exponer servicios internos o interfaces administrativas.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el sniffing de tipos MIME, lo que puede llevar a la ejecucion de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla que informacion de origen se envia a terceros al navegar desde el sitio.
[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador como el acceso a la camara, microfono o geolocalizacion.
[MEDIUM] Bloqueo total en Robots.txt: El archivo bloquea toda la indexacion del sitio, lo que suele indicar una configuracion de desarrollo o error de visibilidad.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando informacion tecnica que un atacante puede usar para reconocimiento.