EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://pyrenees.ad	Checks	9 pruebas
Dominio	pyrenees.ad	Hallazgos	55 totales
Fecha	24 de abril de 2026 a las 18:12	Problemas	17 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al dominio pyrenees.ad arroja una puntuación de 62/100, lo que equivale a una calificación de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fueron clasificados como fallos críticos. Los principales riesgos detectados se centran en la ausencia total de cabeceras de seguridad y en una configuración deficiente de las cookies de sesión. Se concluye que el sitio es actualmente vulnerable, ya que carece de protecciones esenciales contra ataques comunes como el secuestro de sesiones y la inyección de contenido.

Resumen de Riesgos

0	8	7	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	44	FALLO	ASP.NET_SessionId: falta Secure; ASP.NET_Session...
Contenido Mixto	60	AVISO	1 recurso(s) 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 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-07-07T03:11:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-08T02:11:21.000Z
- 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: ASP.NET — 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.pyrenees.ad/
- 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
- INFO **Tecnologias detectadas**
  ASP.NET

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 — 44/100

Estado: FALLO

ASP.NET_SessionId: falta Secure; ASP.NET_SessionId: falta Secure; PyreneesGMP_LANGUAGE: falta HttpOnly; PyreneesGMP_LANGUAGE: falta Secure; PyreneesGMP_LANGUAGE: falta SameSite

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: ASP.NET_SessionId — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=lax
- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: ASP.NET_SessionId — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=lax
- ALTO **Cookie: PyreneesGMP_LANGUAGE — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PyreneesGMP_LANGUAGE — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PyreneesGMP_LANGUAGE — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.pyrenees.ad/brands

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **sitemap.xml**
  Presente, 157 URLs
- 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 Content-Security-Policy: No se restringe el origen del contenido, lo que permite ataques de scripts maliciosos y XSS.
[HIGH] Falta de X-Frame-Options: El sitio es susceptible a ataques de clickjacking al permitir ser cargado dentro de marcos externos.
[HIGH] Falta de Strict-Transport-Security (HSTS): El servidor no instruye a los navegadores a usar únicamente conexiones cifradas, permitiendo posibles degradaciones de protocolo.
[HIGH] Cookies de sesión sin flag Secure: Las cookies ASP.NET_SessionId y PyreneesGMP_LANGUAGE pueden transmitirse en canales no cifrados, facilitando su interceptación.
[HIGH] Cookies sin flag HttpOnly: La cookie PyreneesGMP_LANGUAGE es accesible mediante scripts, lo que aumenta el riesgo de robo de identidad en caso de un ataque XSS.
[MEDIUM] Contenido Mixto detectado: Se carga una hoja de estilos mediante una URL HTTP insegura dentro del entorno HTTPS, comprometiendo la integridad de la página.
[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: La exposición de este puerto alternativo incrementa la superficie de ataque y puede revelar servicios internos no protegidos.
[MEDIUM] Falta de flag SameSite en cookies: La ausencia de este atributo en la cookie PyreneesGMP_LANGUAGE hace al usuario vulnerable a ataques de falsificación de petición en sitios cruzados.
[MEDIUM] Falta de X-Content-Type-Options: Permite que los navegadores realicen sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos camuflados.
[MEDIUM] Configuración de Robots.txt restrictiva: El archivo bloquea la indexación total del sitio mediante la directiva Disallow: /, lo cual es inusual para un sitio de producción.
[LOW] Cabecera Server expuesta: Revela el uso de Cloudflare, proporcionando información técnica inicial a posibles atacantes.
[LOW] Cabecera X-Powered-By expuesta: Indica directamente el uso del framework ASP.NET, permitiendo ataques dirigidos a vulnerabilidades específicas de esa tecnología.