EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.damel.com	Checks	9 pruebas
Dominio	www.damel.com	Hallazgos	54 totales
Fecha	17 de septiembre de 2026 a las 10:14	Problemas	14 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre la plataforma ha dado como resultado una puntuación de 70/100, lo que corresponde a una calificación de grado C. Durante la auditoría se ejecutaron un total de 9 checks pasivos, identificando 4 verificaciones correctas, 3 advertencias de riesgo medio y 2 fallos de seguridad críticos. Aunque el sitio implementa correctamente el cifrado de transporte, presenta debilidades significativas en la configuración de sus cabeceras de seguridad y en la gestión de sesiones. Por tanto, se concluye que el sitio web es actualmente vulnerable ante ataques de interceptación de datos y manipulación de interfaz.

Resumen de Riesgos

0	6	4	4	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 135 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	ASP.NET_SessionId: falta Secure; Damel: falta Ht...
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 135 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  135 dias restantes (expira: 2027-01-30T06:58:25.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-29T06:58:26.000Z
- 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: Microsoft-IIS/8.5 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Addis Network SL — Revela framework/lenguaje
- 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=15768000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.damel.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15768000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=15768000 (183 dias)
- 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
- BAJO **Meta generator**
  Expone: ADDIS Commerce
- INFO **Tecnologias detectadas**
  Addis Network SL

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

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

- INFO **Cookies detectadas**
  2 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
- ALTO **Cookie: Damel — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: Damel — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: Damel — 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.addis.es

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (324 bytes)
- INFO **Reglas robots.txt**
  12 Disallow, 1 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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] Puerto 21 (FTP): Se detectó un puerto de transferencia de archivos abierto que opera habitualmente sin cifrado, permitiendo la posible interceptación de credenciales.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta política permite que el sitio sea embebido en marcos externos, exponiendo a los usuarios a ataques de Clickjacking.
[HIGH] Seguridad de Cookies (Secure/HttpOnly): Las cookies ASP.NET_SessionId y Damel carecen de atributos críticos, permitiendo que sean enviadas por canales no seguros o accedidas mediante scripts.
[MEDIUM] Cookie Damel (SameSite): Al no estar definido este atributo, la plataforma es susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se identificó la carga de un recurso mediante protocolo HTTP inseguro dentro de la página HTTPS, lo que degrada la seguridad global de la sesión.
[MEDIUM] Referrer-Policy y Permissions-Policy: La omisión de estas cabeceras impide controlar qué información de procedencia se comparte y qué funciones del navegador están permitidas.
[LOW] Exposición de tecnología (Server/X-Powered-By): Las cabeceras revelan el uso de Microsoft-IIS/8.5 y Addis Network SL, proporcionando información valiosa para atacantes sobre posibles exploits específicos.
[LOW] Meta generator: La etiqueta revela el uso de ADDIS Commerce como software de gestión, facilitando el reconocimiento de la infraestructura.
[LOW] Sitemap.xml: No se encontró el archivo de mapa del sitio, lo cual representa una falta de estandarización en la configuración web.