EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.multiplaza.com.do/umbraco/login	Checks	9 pruebas
Dominio	www.multiplaza.com.do	Hallazgos	42 totales
Fecha	24 de julio de 2026 a las 21:07	Problemas	10 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web ha sido evaluado obteniendo una puntuacion exacta de 68/100, lo que corresponde a una nota C. El analisis consistio en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presento advertencias y 2 fallaron significativamente. Se han identificado carencias criticas en las politicas de defensa del navegador y en la configuracion de la seguridad de las cookies. Aunque el cifrado de conexion es correcto, la ausencia de capas de proteccion modernas permite diversos vectores de ataque. En conclusion, el sitio se considera vulnerable debido a configuraciones de servidor incompletas que exponen la integridad de la sesion del usuario.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 76 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	67	AVISO	.AspNetCore.Mvc.CookieTempDataProvider: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 76 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  76 dias restantes (expira: 2026-10-08T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-09T00:00:00.000Z
- 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: Kestrel — 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.)

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 — 67/100

Estado: AVISO

.AspNetCore.Mvc.CookieTempDataProvider: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: .AspNetCore.Mvc.CookieTempDataProvider — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: .AspNetCore.Mvc.CookieTempDataProvider — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: .AspNetCore.Mvc.CookieTempDataProvider — SameSite**
  SameSite=lax

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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)**
  Cerrado — 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, lo que deja al sitio vulnerable ante ataques de inyeccion de codigo y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se implementa HSTS, lo que permite que las conexiones puedan ser degradadas a protocolos HTTP no seguros.
[HIGH] Cookie .AspNetCore.Mvc.CookieTempDataProvider: Falta el flag Secure, lo cual es peligroso porque la cookie de sesion podria ser interceptada al enviarse por conexiones no cifradas.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podria intentar interpretar el contenido de forma distinta a la declarada, permitiendo la ejecucion de scripts maliciosos.
[MEDIUM] Referrer-Policy: No existe una politica que controle cuanta informacion de la URL se comparte con otros sitios al navegar por enlaces externos.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la camara, el microfono o la geolocalizacion a traves de APIs.
[LOW] Server header expuesto: Se detecto el encabezado Server: Kestrel, lo cual revela informacion tecnica sobre la infraestructura que un atacante puede usar para buscar exploits especificos.
[LOW] Ausencia de archivos de rastreo: No se encontraron robots.txt ni sitemap.xml, lo cual dificulta la indexacion correcta y el control sobre que partes del sitio deben ser rastreadas.