EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://omi.edu/	Checks	9 pruebas
Dominio	omi.edu	Hallazgos	52 totales
Fecha	22 de junio de 2026 a las 13:02	Problemas	13 detectados

C

71/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre omi.edu arroja una puntuación de 71/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 4 resultaron satisfactorias, 3 generaron advertencias y 2 se identificaron como fallos de seguridad. Aunque el cifrado de datos es sólido, la exposición de versiones específicas del software y de puertos de administración críticos eleva el riesgo operativo. El sitio cuenta con una base de seguridad aceptable, pero se considera vulnerable debido a la visibilidad de información técnica que facilita ataques dirigidos. Es imperativo corregir las configuraciones del servidor y las cabeceras de respuesta para alcanzar un nivel de protección óptimo.

Resumen de Riesgos

0	3	7	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.8.5 expuesta, WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	lp_session_guest: falta SameSite
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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-08-29T16:30:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-31T16:30:18.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: LiteSpeed — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.1.34 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubDomains
- 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://omi.edu/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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: Site Kit by Google 1.181.0
- INFO **Tecnologias detectadas**
  PHP/8.1.34

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.8.5 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.8.5 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 67/100

Estado: AVISO

lp_session_guest: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: lp_session_guest — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: lp_session_guest — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: lp_session_guest — 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://omi.aquinas.tech/

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (165 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://omi.edu/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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] Versión de WordPress expuesta: La versión 6.8.5 es visible públicamente, lo que permite a atacantes identificar vulnerabilidades conocidas (CVEs) para dicha versión.
[HIGH] Content-Security-Policy faltante: La ausencia de esta cabecera facilita ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] Puerto 21 (FTP) ABIERTO: Este servicio transmite datos y credenciales sin cifrar, siendo un objetivo primario para la interceptación de archivos.
[MEDIUM] Archivo /readme.html accesible: Revela información sobre la instalación del CMS que debería ser privada para evitar el reconocimiento del sistema.
[MEDIUM] Ruta /wp-login.php accesible: El panel de acceso administrativo es público, permitiendo ataques de fuerza bruta contra las cuentas de usuario.
[MEDIUM] Referrer-Policy faltante: No se controla qué información de origen se envía a terceros, lo que podría filtrar datos de navegación.
[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso a funciones sensibles del navegador como el micrófono o la cámara.
[MEDIUM] Cookie lp_session_guest sin SameSite: La falta de este atributo hace que la sesión sea vulnerable a ataques de falsificación de peticiones en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto detectado: El recurso http://omi.aquinas.tech/ se carga de forma insegura, comprometiendo la integridad de la conexión HTTPS.
[MEDIUM] Puerto 22 (SSH) ABIERTO: La exposición del acceso remoto seguro aumenta el riesgo de intentos de acceso no autorizados mediante fuerza bruta.
[LOW] Cabecera Server expuesta: Indica el uso de LiteSpeed, ayudando a los atacantes a perfilar la tecnología del servidor web.
[LOW] Cabecera X-Powered-By expuesta: Revela que el sitio utiliza PHP/8.1.34, proporcionando detalles técnicos innecesarios para el usuario final.
[LOW] Meta generator expuesto: El plugin Site Kit by Google 1.181.0 expone su versión, lo que podría usarse para explotar fallos específicos del complemento.