EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.compumed.edu/	Checks	9 pruebas
Dominio	www.compumed.edu	Hallazgos	48 totales
Fecha	22 de junio de 2026 a las 12:27	Problemas	8 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio compumed.edu arroja una puntuación de 88/100, lo que equivale a una nota de grado B. De los 9 checks pasivos ejecutados, 7 resultaron satisfactorios, registrándose 1 advertencia y 1 fallo crítico de seguridad. A pesar de contar con una base sólida en cifrado y cabeceras de seguridad, la exposición de versiones antiguas del CMS representa un riesgo de intrusión. Se concluye que el sitio es actualmente vulnerable a ataques dirigidos debido a componentes desactualizados y servicios de red expuestos innecesariamente. Es fundamental corregir los fallos de configuración de red para evitar compromisos en la integridad del servidor.

Resumen de Riesgos

0	2	4	2	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 48 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 4.11.12 expuesta, WordPress 2 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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-08-09T12:27:11.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-11T12:27:12.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(), autoplay=(), camera=(), cross-origin-isolated=(), display-capt...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.compumed.edu/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.181.0
- INFO **Tecnologias detectadas**
  React, Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.11.12 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 4.11.12 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 — 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 (296 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.compumed.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: Se detectó la versión 4.11.12, la cual es obsoleta y permite a atacantes buscar y ejecutar exploits conocidos para este núcleo.
[HIGH] Puerto 21 (FTP) abierto: Este servicio permite la transferencia de archivos sin cifrado, lo que facilita la interceptación de credenciales y datos en tránsito.
[MEDIUM] Puerto 22 (SSH) abierto: El acceso remoto está disponible públicamente, aumentando el riesgo de ataques de fuerza bruta contra las cuentas del servidor.
[MEDIUM] Archivo /readme.html accesible: La visibilidad pública de este archivo revela información técnica específica sobre la instalación del CMS que debería ser privada.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de administración es accesible para cualquier usuario, lo que representa el primer paso para ataques de acceso no autorizado.
[MEDIUM] Configuración de robots.txt: El archivo bloquea la indexación de todo el sitio mediante la directiva Disallow: /, lo que podría indicar un error de configuración.
[LOW] Cabecera de servidor expuesta: Se revela el uso de LiteSpeed, proporcionando información valiosa a un atacante sobre la tecnología de base del servidor.
[LOW] Meta generator expuesto: La etiqueta Site Kit by Google 1.181.0 revela versiones de complementos instalados que pueden ser utilizados para reconocimiento.