EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://digital.compumed.edu/	Checks	9 pruebas
Dominio	digital.compumed.edu	Hallazgos	51 totales
Fecha	19 de junio de 2026 a las 17:32	Problemas	17 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 62/100, lo que corresponde a una calificación de grado C. El análisis consistió en la ejecución de 9 comprobaciones pasivas, resultando en 4 verificaciones exitosas, 2 advertencias y 3 fallos críticos en áreas clave. Se han detectado deficiencias severas en la configuración de cabeceras de seguridad, protección de cookies y exposición de servicios en puertos de red. Debido a la visibilidad pública de la base de datos y la falta de políticas de endurecimiento, se concluye que el sitio es actualmente vulnerable. Es urgente aplicar medidas correctivas para evitar el acceso no autorizado o la explotación de vulnerabilidades conocidas.

Resumen de Riesgos

1	6	6	4	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 42 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	33	FALLO	haircki: falta HttpOnly; haircki: falta SameSite
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 42 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  42 dias restantes (expira: 2026-07-31T23:40:48.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-02T23:40:49.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://digital.compumed.edu/
- 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

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: WordPress 7.0
- INFO **Tecnologias detectadas**
  React, Next.js, Astro, PHP/8.3.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 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 — 33/100

Estado: FALLO

haircki: falta HttpOnly; haircki: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: haircki — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: haircki — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: haircki — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (448 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://digital.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), 3306 (MySQL)

- 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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

[CRÍTICO] Puerto 3306 (MySQL): El servicio de base de datos se encuentra expuesto a Internet, lo que permite intentos de conexión externa y ataques de fuerza bruta.
[ALTO] Puerto 21 (FTP): Servicio de transferencia de archivos abierto que transmite datos sin cifrado, facilitando la interceptación de credenciales.
[ALTO] Versión de WordPress expuesta: Se detectó públicamente el uso de WordPress 7.0, permitiendo a posibles atacantes identificar CVEs específicos para dicha versión.
[ALTO] Falta de Strict-Transport-Security (HSTS): El servidor no instruye al navegador para usar exclusivamente conexiones HTTPS, permitiendo posibles ataques de degradación de protocolo.
[ALTO] Falta de X-Frame-Options: La ausencia de esta cabecera hace que el sitio sea susceptible a ataques de clickjacking mediante el uso de frames.
[ALTO] Cookie haircki sin flag HttpOnly: La cookie de sesión es accesible mediante scripts de cliente, aumentando drásticamente el riesgo de robo de identidad vía XSS.
[MEDIO] Falta de X-Content-Type-Options: El sitio no previene el sniffing de tipos MIME, lo que podría llevar a la ejecución de contenido malicioso disfrazado.
[MEDIO] Falta de Referrer-Policy y Permissions-Policy: No existe control sobre la información de navegación compartida ni restricciones sobre el uso de APIs del navegador como cámara o micrófono.
[MEDIO] Archivos sensibles expuestos: El archivo /readme.html y la ruta /wp-login.php son accesibles públicamente, facilitando el reconocimiento del sistema.
[MEDIO] Cookie haircki sin flag SameSite: La falta de este atributo hace que las sesiones de los usuarios sean vulnerables a ataques de Cross-Site Request Forgery (CSRF).
[BAJO] Exposición de cabeceras tecnológicas: Los campos Server (LiteSpeed) y X-Powered-By (PHP/8.3.30) revelan versiones exactas del software del servidor.
[BAJO] Meta generator expuesto: La etiqueta meta identifica WordPress 7.0, facilitando el escaneo automatizado de vulnerabilidades por parte de bots.
[BAJO] Rutas en robots.txt: Se hace referencia directa a directorios como "admin", proporcionando pistas sobre la estructura interna a atacantes.