EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://buenavistahospital.com/myvue/login.html	Checks	9 pruebas
Dominio	buenavistahospital.com	Hallazgos	43 totales
Fecha	13 de abril de 2026 a las 21:09	Problemas	13 detectados

D

55/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría técnica del sitio web, se ha determinado una puntuación de seguridad de 55/100, lo que corresponde a una calificación de nota D. El análisis se fundamentó en la ejecución de 9 checks pasivos, obteniendo 5 resultados satisfactorios, 1 advertencia y 3 fallos críticos en la infraestructura y configuración. Se han identificado brechas graves de seguridad, especialmente relacionadas con la exposición de servicios de base de datos y la ausencia total de protecciones en las cabeceras HTTP. Debido a la combinación de servicios críticos abiertos a internet y la falta de cifrado forzado, se concluye que el sitio es actualmente vulnerable y presenta un riesgo elevado para la integridad de la información.

Resumen de Riesgos

1	6	4	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 70 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 70 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-06-22T13:22:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-24T13:22:52.000Z
- 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: Apache — 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.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

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 — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- 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
- 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

[CRITICAL] Puerto 3306 (MySQL) ABIERTO: La base de datos está expuesta directamente a internet, permitiendo intentos de acceso no autorizados y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP) ABIERTO: Este servicio permite la transferencia de archivos sin cifrar, lo que expone credenciales y datos a interceptaciones.
[HIGH] HTTP a HTTPS redirección FALLIDA: El sitio no obliga al uso de conexiones cifradas, permitiendo que los usuarios naveguen por canales inseguros.
[HIGH] Content-Security-Policy (CSP) FALTA: La ausencia de esta cabecera facilita ataques de inyección de código como Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options FALTA: El sitio no cuenta con protección contra ataques de clickjacking, permitiendo que la página sea embebida en sitios maliciosos.
[HIGH] Strict-Transport-Security (HSTS) FALTA: El servidor no instruye al navegador para que use exclusivamente HTTPS, aumentando el riesgo de ataques de degradación de SSL.
[MEDIUM] Puerto 22 (SSH) ABIERTO: El servicio de administración remota es visible públicamente, lo cual es una superficie de ataque para accesos no autorizados al servidor.
[MEDIUM] X-Content-Type-Options FALTA: No se previene el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados de otros formatos.
[MEDIUM] Referrer-Policy FALTA: Se carece de control sobre la información de navegación que se envía a otros sitios web externos.
[MEDIUM] Permissions-Policy FALTA: No se restringen las capacidades de hardware del navegador como el micrófono o la cámara desde las cabeceras del servidor.
[LOW] Server header expuesto (Apache): El servidor revela la tecnología exacta que utiliza, facilitando a los atacantes la búsqueda de vulnerabilidades específicas para esa versión.
[LOW] sitemap.xml no encontrado: La falta de este archivo dificulta la auditoría de la estructura del sitio y la correcta indexación de sus recursos.