# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://novaipro.com/plataforma-instructor/ | Checks | 9 pruebas |
| Dominio | novaipro.com | Hallazgos | 48 totales |
| Fecha | 12 de julio de 2026 a las 12:27 | Problemas | 16 detectados |

**C**

64/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web novaipro.com arroja una puntuación de 64/100, lo que otorga una nota de C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 5 verificaciones correctas, 2 advertencias por configuraciones incompletas y 2 fallos críticos de seguridad. Aunque el cifrado básico de datos es adecuado, la ausencia total de políticas de seguridad en las cabeceras y la exposición de puertos de administración representan un riesgo latente. En conclusión, el sitio se considera vulnerable debido a que facilita información crítica a posibles atacantes y carece de protecciones modernas contra ataques de inyección.

## Resumen de Riesgos

| 0 | 6 | 6 | 4 | 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 | 70 | AVISO | HTTP redirige a HTTPS pero falta HSTS |
| Deteccion CMS | 100 | OK | CMS detectado: WordPress, PrestaShop |
| Version CMS Expuesta | 20 | FALLO | WordPress 7.0.1 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 76 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  76 dias restantes (expira: 2026-09-26T22:11:00.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-28T22:11:01.000Z
- 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/2.4.65 (Unix) OpenSSL/3.5.5 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.31 — Revela framework/lenguaje
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://novaipro.com/
- 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 7.0.1
- INFO **Tecnologias detectadas**
  PHP/8.2.31

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0.1 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 (113 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://novaipro.com/wp-sitemap.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] Content-Security-Policy faltante: El sitio carece de esta política, lo que facilita ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] X-Frame-Options faltante: La ausencia de esta cabecera permite que el sitio sea cargado en marcos externos, exponiéndolo a ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no obliga al navegador a usar conexiones HTTPS, permitiendo posibles degradaciones de seguridad.
[HIGH] Puerto 21 (FTP) abierto: Se detectó un canal de transferencia de archivos sin cifrar, lo que es altamente peligroso por el envío de credenciales en texto plano.
[HIGH] Versión de WordPress 7.0.1 expuesta: La visibilidad pública de la versión del CMS permite a los atacantes buscar exploits específicos de forma dirigida.
[MEDIUM] X-Content-Type-Options faltante: No se previene el sniffing de tipos MIME, permitiendo que archivos maliciosos sean interpretados como scripts.
[MEDIUM] Referrer-Policy faltante: El sitio no controla qué información de origen se envía a otros dominios al navegar por enlaces externos.
[MEDIUM] Permissions-Policy faltante: No existen restricciones sobre el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Acceso público a /wp-login.php y /readme.html: Estas rutas exponen el panel de administración y detalles técnicos del sistema a cualquier usuario.
[MEDIUM] Puerto 22 (SSH) abierto: Un punto de acceso remoto activo que puede ser blanco de intentos de acceso por fuerza bruta.
[LOW] Cabeceras de tecnología expuestas: El servidor revela el uso de Apache/2.4.65 y PHP/8.2.31, facilitando el reconocimiento del entorno técnico.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a directorios de administración, ayudando a los atacantes a mapear el sitio.