EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.elp.edu.pe/	Checks	9 pruebas
Dominio	www.elp.edu.pe	Hallazgos	51 totales
Fecha	22 de julio de 2026 a las 20:33	Problemas	11 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación exacta de 69/100, lo que le otorga una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos relacionados con la configuración de seguridad y la gestión de cookies. Aunque el sitio posee un cifrado de transporte robusto, la falta de cabeceras de protección esenciales y la exposición de versiones de software obsoletas incrementan el riesgo de ataques dirigidos. En conclusión, el sitio web se considera vulnerable debido a fallos de configuración que podrían permitir ataques de inyección de código y suplantación de identidad.

Resumen de Riesgos

0	5	4	2	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 87 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Wix
Version CMS Expuesta	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	0	FALLO	ssr-caching: falta HttpOnly; ssr-caching: falta ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 87 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  87 dias restantes (expira: 2026-10-17T09:52:51.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-19T09:52:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Pepyaka — 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31556952
- 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://www.elp.edu.pe/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31556952
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31556952 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Wix

- 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**
  Detectado via HTML body
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Wix.com Website Builder
- INFO **Tecnologias detectadas**
  React, Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- ALTO **WordPress version**
  Version 2 expuesta publicamente — Permite a atacantes buscar CVEs conocidos

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 0/100

Estado: FALLO

ssr-caching: falta HttpOnly; ssr-caching: falta Secure; ssr-caching: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: ssr-caching — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ssr-caching — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ssr-caching — 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 (488 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.elp.edu.pe/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
  Cerrado — 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
- 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] WordPress version: Se detectó la exposición pública de la versión 2 de WordPress, lo que permite a atacantes identificar y explotar vulnerabilidades conocidas (CVEs) para tomar el control del sitio.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) y ataques de inyección de contenido malicioso.
[HIGH] X-Frame-Options: La falta de esta directiva deja al portal desprotegido frente a ataques de clickjacking, permitiendo que el sitio sea cargado en iframes maliciosos.
[HIGH] Cookie ssr-caching (HttpOnly): La cookie carece del flag HttpOnly, lo que permite que sea accesible a través de scripts de navegador, elevando el riesgo de robo de sesión mediante XSS.
[HIGH] Cookie ssr-caching (Secure): El flag Secure no está configurado, provocando que la cookie pueda ser transmitida a través de conexiones HTTP no cifradas.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia que el navegador envía a otros dominios, lo que puede filtrar datos sensibles de la estructura de la URL.
[MEDIUM] Permissions-Policy: No se han definido restricciones para las APIs del navegador, dejando activos permisos potenciales para el uso de cámara, micrófono o geolocalización.
[MEDIUM] Cookie ssr-caching (SameSite): La omisión de este atributo hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Bloqueo total robots.txt: El archivo robots.txt bloquea el acceso a todo el contenido del sitio mediante la directiva Disallow: /, lo cual puede ser un error de configuración.
[LOW] Server header expuesto: La cabecera del servidor revela el uso de la tecnología Pepyaka, facilitando la fase de reconocimiento de un atacante.
[LOW] Meta generator: Se expone públicamente el uso de la herramienta Wix.com Website Builder.