EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.elportaldelalumno.com/Login/	Checks	9 pruebas
Dominio	www.elportaldelalumno.com	Hallazgos	47 totales
Fecha	22 de mayo de 2026 a las 11:17	Problemas	10 detectados

C

69/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado en el sitio web ha dado como resultado una puntuacion exacta de 69/100, lo que corresponde a una nota de C. Durante la auditoria se ejecutaron un total de 9 checks pasivos, identificando 4 puntos correctos, 3 advertencias y 2 fallos criticos en la configuracion del servidor. Aunque el cifrado de datos es adecuado, la ausencia de cabeceras de seguridad modernas y una gestion de cookies deficiente representan riesgos significativos. Debido a estas omisiones tecnicas y a la exposicion de servicios de administracion, el sitio se considera vulnerable ante ataques de interceptacion de sesiones e inyeccion de codigo. Es necesaria una correccion de las politicas de seguridad para alcanzar un nivel de proteccion aceptable.

Resumen de Riesgos

0	4	4	2	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 236 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	83	AVISO	SERVERID: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 236 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  236 dias restantes (expira: 2027-01-12T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-12T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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://www.elportaldelalumno.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

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 — 83/100

Estado: AVISO

SERVERID: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)

- INFO **Cookie: ASP.NET_SessionId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ASP.NET_SessionId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ASP.NET_SessionId — SameSite**
  SameSite=lax
- ALTO **Cookie: SERVERID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: SERVERID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SERVERID — SameSite**
  SameSite=none

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — 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: Falta — Esta cabecera es fundamental para prevenir ataques de Cross-Site Scripting (XSS) y la inyeccion de contenido no autorizado.
[HIGH] Strict-Transport-Security: Falta — Al no estar configurada, el navegador no puede forzar conexiones seguras via HSTS, permitiendo ataques de degradacion de protocolo.
[HIGH] Cookie SERVERID sin HttpOnly: La falta de este flag permite que scripts maliciosos accedan a la cookie de sesion, facilitando el robo de identidad del usuario.
[MEDIUM] X-Content-Type-Options: Falta — El servidor no impide el MIME-type sniffing, lo que podria permitir la ejecucion de archivos con contenido malicioso disfrazado.
[MEDIUM] Referrer-Policy: Falta — No existe un control sobre la informacion de procedencia que se envia a terceros cuando un usuario navega desde el sitio.
[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el uso de APIs sensibles del navegador como la camara o el microfono, aumentando la superficie de ataque.
[MEDIUM] Puerto 22 (SSH) ABIERTO: El puerto de acceso remoto para administracion esta expuesto a internet, lo que facilita intentos de intrusion por fuerza bruta.
[LOW] robots.txt no encontrado: La ausencia de este archivo impide gestionar correctamente que partes del sitio deben ser ignoradas por los motores de busqueda.
[LOW] sitemap.xml no encontrado: No se dispone de un indice estructurado del sitio, lo que dificulta el rastreo controlado y la auditoria de contenidos.