EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://theobservatoryschool.es	Checks	9 pruebas
Dominio	theobservatoryschool.es	Hallazgos	47 totales
Fecha	30 de marzo de 2026 a las 15:07	Problemas	15 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación de 57/100, lo que equivale a una calificación de nota D. Se han ejecutado un total de 9 checks pasivos, de los cuales 6 han sido satisfactorios y 3 han resultado en fallos críticos de configuración. El sitio presenta deficiencias importantes en la implementación de cabeceras de seguridad y en la gestión de protocolos de conexión segura. A pesar de contar con un certificado SSL vigente, la exposición de versiones del sistema y la falta de directivas de protección contra ataques comunes elevan el perfil de riesgo. En conclusión, el sitio se considera vulnerable y requiere acciones correctivas inmediatas para alcanzar un nivel de seguridad aceptable.

Resumen de Riesgos

0	6	5	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 50 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	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 9.8.5 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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 50 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  50 dias restantes (expira: 2026-05-19T09:28:55.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-18T09:28:56.000Z
- 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: LiteSpeed — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30 — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 301 — 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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.168.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.2.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 9.8.5 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 9.8.5 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

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 (281 bytes)
- INFO **Reglas robots.txt**
  4 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.theobservatoryschool.com/sitemap_index.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Redirección HTTP a HTTPS: El sitio no redirige automáticamente el tráfico no cifrado hacia la versión segura, permitiendo conexiones vulnerables.
[HIGH] HSTS (Strict-Transport-Security) ausente: El servidor no ordena al navegador el uso exclusivo de conexiones HTTPS, facilitando ataques de degradación de protocolo.
[HIGH] Content-Security-Policy ausente: La falta de esta cabecera permite la ejecución de scripts no autorizados y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options ausente: No existe protección contra ataques de clickjacking, lo que permite que el sitio sea embebido en marcos maliciosos.
[HIGH] Versión de WordPress expuesta: La visibilidad pública de la versión 9.8.5 permite a atacantes identificar vulnerabilidades específicas y CVEs conocidos.
[MEDIUM] X-Content-Type-Options ausente: El sitio no previene el sniffing de tipos MIME, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy ausente: No se controla la información de referencia enviada a terceros, comprometiendo la privacidad de los flujos de navegación.
[MEDIUM] Permissions-Policy ausente: El sitio no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara o el micrófono.
[MEDIUM] Archivo readme.html y README.txt expuestos: Estos archivos son accesibles públicamente y pueden revelar información técnica detallada sobre la instalación del CMS.
[LOW] Cabecera Server expuesta: Se revela el uso del servidor LiteSpeed, facilitando el reconocimiento de la infraestructura tecnológica.
[LOW] Cabecera X-Powered-By expuesta: Se muestra la versión exacta de PHP (8.2.30), permitiendo ataques dirigidos a vulnerabilidades de dicho framework.
[LOW] Meta generator expuesto: El código fuente revela el uso de Site Kit by Google y su versión, aportando datos innecesarios a posibles atacantes.
[LOW] Ruta sensible en robots.txt: Se menciona la ruta de administración, lo que ayuda a los atacantes a localizar puntos de acceso críticos del sistema.