EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://edumedia.tech	Checks	9 pruebas
Dominio	edumedia.tech	Hallazgos	52 totales
Fecha	4 de julio de 2026 a las 16:28	Problemas	19 detectados

D

58/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio edumedia.tech ha arrojado una puntuación de 58/100, lo que equivale a una calificación de nota D. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 3 generaron advertencias y 3 fallaron de forma crítica. Los resultados indican deficiencias importantes en la configuración del servidor, la gestión de cookies y la exposición de servicios de infraestructura. Por tanto, se concluye que el sitio es actualmente vulnerable y requiere intervención técnica inmediata para mitigar riesgos de intrusión y robo de datos.

Resumen de Riesgos

1	6	9	3	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	33	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Same...
Contenido Mixto	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
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 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-09-19T11:50:30.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-21T11:50:31.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: 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/8.3.30 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- 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://edumedia.tech/
- 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: WordPress 7.0
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.30

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 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 — 33/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: PHPSESSID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://edumedia.tech/wp-content/uploads/2023/06/330508.png
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://edumedia.tech/wp-content/uploads/2023/06/1f1f2-1f1fd....
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://edumedia.tech/wp-content/uploads/2023/09/descargar-5....

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (171 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://edumedia.tech/sitemap_index.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), 3306 (MySQL)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- 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): Base de datos expuesta públicamente, lo que permite intentos de conexión externa y ataques de fuerza bruta directos.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y carece de cifrado, facilitando la interceptación de credenciales de administración.
[HIGH] Falta X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en iframes de terceros, facilitando ataques de clickjacking.
[HIGH] Falta Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo que las conexiones sean degradadas a HTTP inseguro.
[HIGH] Versión de WordPress 7.0 expuesta: La visibilidad pública de la versión del CMS permite a los atacantes identificar CVEs específicos para comprometer el sitio.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: Al ser accesible mediante scripts (document.cookie), la sesión del usuario es vulnerable a robos mediante ataques XSS.
[MEDIUM] Falta X-Content-Type-Options: El sitio es vulnerable a ataques de sniffing de MIME-type, lo que puede llevar a la ejecución de contenido malicioso.
[MEDIUM] Falta Referrer-Policy: No se restringe la información que se envía en las peticiones salientes, lo que puede filtrar datos de navegación sensibles.
[MEDIUM] Falta Permissions-Policy: No existen restricciones sobre las APIs del navegador, permitiendo potencialmente el uso no autorizado de periféricos.
[MEDIUM] Archivo /readme.html y ruta /wp-login.php expuestos: Estos elementos revelan información técnica y facilitan el acceso al panel administrativo para ataques de fuerza bruta.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: La ausencia de este atributo hace que las sesiones de los usuarios sean vulnerables a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto detectado: Se cargan 3 recursos a través de HTTP dentro de la página HTTPS, lo que anula la integridad del cifrado SSL para esos elementos.
[LOW] Cabeceras de servidor expuestas: Se revela el uso de LiteSpeed y PHP/8.3.30, información técnica que ayuda a los atacantes a perfilar el entorno de ejecución.
[LOW] Meta generator expuesto: El código fuente confirma explícitamente el uso de WordPress 7.0.