EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://alubang.es/Produccion	Checks	9 pruebas
Dominio	alubang.es	Hallazgos	43 totales
Fecha	18 de septiembre de 2026 a las 17:53	Problemas	10 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis de ciberseguridad, el sitio web ha obtenido una puntuación de 68/100 con una calificación de C. La auditoría consistió en 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fueron fallos críticos. Se detectó una ausencia total de cabeceras de seguridad esenciales y la exposición de archivos que sugieren el uso de software desactualizado. Por tanto, el sitio se considera vulnerable a ataques de inyección y suplantación de identidad. Es imperativo abordar las debilidades estructurales en la configuración del servidor para alcanzar un nivel de protección aceptable.

Resumen de Riesgos

0	4	4	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 193 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	No se detecto un CMS conocido
Version CMS Expuesta	20	FALLO	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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 193 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  193 dias restantes (expira: 2027-03-30T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-17T00:00:00.000Z
- 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 — 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
- 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://alubang.es/
- 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 — 20/100

Estado: FALLO

WordPress 2 expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 (111 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://alubang.es/wp-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] Content-Security-Policy: Falta esta cabecera que previene ataques de Cross-Site Scripting (XSS) e inyecciones de código malicioso.
[HIGH] X-Frame-Options: Su ausencia permite ataques de clickjacking, donde un atacante puede engañar al usuario para que realice acciones no deseadas mediante marcos invisibles.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce una conexión segura, facilitando ataques de interceptación de tráfico o degradación de protocolo.
[MEDIUM] WordPress 2 expuesta: El archivo /readme.html es accesible y revela una versión antigua del CMS, lo que facilita ataques dirigidos a vulnerabilidades conocidas de versiones obsoletas.

[MEDIUM] X-Content-Type-Options: Sin esta cabecera, el navegador puede intentar adivinar el tipo de contenido, permitiendo la ejecución de scripts camuflados como otros tipos de archivos.
[MEDIUM] Referrer-Policy: No se controla qué información de origen se envía a otros dominios, lo que puede comprometer la privacidad de la estructura interna del sitio.
[MEDIUM] Permissions-Policy: No se restringen las funciones del navegador, como el acceso a la cámara o el micrófono, a nivel de política de servidor.
[LOW] Server header expuesto: La cabecera revela que el servidor usa Apache, proporcionando información técnica valiosa para que un atacante busque exploits específicos.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a un directorio administrativo, exponiendo posibles puntos de entrada a usuarios malintencionados.