EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://buoh.ai/	Checks	9 pruebas
Dominio	buoh.ai	Hallazgos	47 totales
Fecha	9 de abril de 2026 a las 08:50	Problemas	15 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 77/100, lo que corresponde a una calificación de grado B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue categorizado como fallo. Aunque el cifrado de la conexión es robusto, se han detectado debilidades críticas en la configuración del servidor y la falta de cabeceras de protección. Se concluye que el sitio es vulnerable debido a la exposición de servicios de infraestructura y la carencia de políticas de endurecimiento web.

Resumen de Riesgos

1	4	8	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 54 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS 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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 54 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  54 dias restantes (expira: 2026-06-01T20:58:07.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-03T20:58:08.000Z
- 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

- 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://buoh.ai/
- 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

- 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
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 (382 bytes)
- INFO **Reglas robots.txt**
  3 Disallow, 4 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://buoh.ai/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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): El servicio de base de datos está expuesto públicamente, lo que permite ataques directos de fuerza bruta o explotación de vulnerabilidades.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y no utiliza cifrado, permitiendo la interceptación de credenciales.
[HIGH] X-Frame-Options: Esta cabecera de seguridad no está configurada, facilitando ataques de Clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: La ausencia de esta cabecera permite el olfateo de tipos MIME, lo que puede derivar en la ejecución de scripts maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de navegación enviada a otros dominios al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles y pueden revelar detalles técnicos del sistema.
[MEDIUM] Paneles de login accesibles: Se detectaron rutas como /wp-login.php y /administrator/ abiertas, facilitando intentos de acceso no autorizado.
[LOW] Server header expuesto: El servidor revela el uso de tecnología LiteSpeed, ayudando a atacantes a buscar vulnerabilidades específicas.
[LOW] Ruta sensible en robots.txt: Se hace referencia a directorios administrativos, exponiendo rutas de interés para agentes malintencionados.