EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Clipo.gg	Checks	9 pruebas
Dominio	clipo.gg	Hallazgos	48 totales
Fecha	5 de mayo de 2026 a las 07:50	Problemas	15 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio Clipo.gg ha arrojado una puntuación de 72/100, lo que equivale a una calificación de nota C. La evaluación consistió en 9 checks pasivos, resultando en 6 verificaciones exitosas, 2 advertencias por configuraciones incompletas y 1 fallo crítico debido a la ausencia de protecciones esenciales. Aunque la capa de transporte está cifrada correctamente, la carencia de políticas de seguridad en las cabeceras HTTP expone a los usuarios a ataques de inyección y suplantación. En su estado actual, el sitio se considera vulnerable a ataques web comunes que podrían comprometer la integridad de la sesión del usuario.

Resumen de Riesgos

0	4	9	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 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	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	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-08-01T01:27:22.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-03T01:27:23.000Z
- 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: nginx/1.24.0 (Ubuntu) — 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://clipo.gg/
- 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
- INFO **Tecnologias detectadas**
  Next.js

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 (269 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://clipo.gg/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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 crítica que previene ataques de XSS y la inyección de contenido malicioso en el navegador.
[HIGH] X-Frame-Options: La ausencia de esta protección hace que el sitio sea susceptible a ataques de clickjacking.
[HIGH] Strict-Transport-Security: Al no estar configurado el HSTS, el servidor no obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación.
[MEDIUM] X-Content-Type-Options: No se previene el MIME-type sniffing, lo que podría permitir la ejecución de scripts camuflados como otros tipos de archivos.
[MEDIUM] Referrer-Policy: La falta de esta política impide controlar qué información de navegación se comparte con otros dominios.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el uso de APIs del navegador, como la cámara o geolocalización, por parte de terceros.
[MEDIUM] Paneles de login expuestos: Se detectó acceso público a rutas administrativas como /wp-login.php, /administrator/ y /user/login.
[MEDIUM] Archivos técnicos públicos: Los archivos /readme.html y /README.txt son accesibles, lo que puede revelar detalles internos de la infraestructura.
[MEDIUM] Puerto 22 (SSH) abierto: El puerto de acceso remoto está disponible, representando un vector de ataque si no posee autenticación robusta.
[LOW] Server header expuesto: Se detectó el valor "nginx/1.24.0 (Ubuntu)", lo que facilita a un atacante identificar vulnerabilidades específicas de esa versión.
[LOW] Ruta sensible en robots.txt: El archivo de indexación menciona "admin", exponiendo prematuramente la ubicación de áreas privadas.