

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyeccion de contenido
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **INFO** **Strict-Transport-Security**
Presente: max-age=31536000
- **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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://kikkifest.com/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000
- **BAJO** **HSTS includeSubDomains**
HSTS no cubre subdominios
- **INFO** **HSTS max-age**
max-age=31536000 (365 dias)
- **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
- **INFO** **Tecnologias detectadas**
Next.js

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)

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 (262 bytes)
- INFO **Reglas robots.txt**
1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
<https://kikkifest.com/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 autentificacion 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 la cabecera, lo cual permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] WordPress version: La versión 7.0 está expuesta públicamente, permitiendo a posibles atacantes identificar y explotar CVEs específicos conocidos.

[HIGH] X-Frame-Options: Ausencia de esta cabecera, dejando el sitio vulnerable ante ataques de clickjacking que pueden engañar a los usuarios.

[MEDIUM] X-Content-Type-Options: Falta la directiva, lo que permite el MIME-type sniffing y facilita la carga de archivos maliciosos disfrazados.

[MEDIUM] Referrer-Policy: No se controla la información enviada en el campo referer, pudiendo filtrar datos de navegación sensibles a terceros.

[MEDIUM] Permissions-Policy: Ausencia de restricciones sobre APIs del navegador, permitiendo el uso no autorizado de funciones como cámara o micrófono.

[MEDIUM] Archivo /readme.html: El archivo es accesible públicamente, lo cual revela información técnica y versiones del CMS que facilitan el reconocimiento inicial.

[LOW] Server header expuesto: El encabezado Server: nginx revela la tecnología utilizada, ayudando a los atacantes a buscar vulnerabilidades específicas del software.