EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.pixels.xyz/	Checks	9 pruebas
Dominio	www.pixels.xyz	Hallazgos	44 totales
Fecha	20 de septiembre de 2026 a las 21:15	Problemas	11 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma arroja una puntuación exacta de 64/100, lo que corresponde a una nota de C. Esta evaluación se basó exclusivamente en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fallaron críticamente. A pesar de contar con una gestión de certificados adecuada, la ausencia total de cabeceras de seguridad y la exposición de puertos alternativos representan un riesgo significativo. Se concluye que el sitio es vulnerable a ataques de inyección y suplantación de identidad en su estado actual.

Resumen de Riesgos

0	4	5	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 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	1 cookies, todas con flags correctos
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 72 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  72 dias restantes (expira: 2026-12-01T13:52:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-02T12:52:24.000Z
- 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: cloudflare — 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://www.pixels.xyz/
- 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

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: _cfuvid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _cfuvid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _cfuvid — SameSite**
  SameSite=none

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://discord.gg/pixels

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — 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 esencial que previene ataques de XSS y la inyección de contenido no autorizado.
[HIGH] X-Frame-Options: La ausencia de esta directiva hace que el sitio sea susceptible a ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, lo que impide que el navegador fuerce conexiones seguras HTTPS automáticamente.
[MEDIUM] X-Content-Type-Options: La falta de esta protección permite el MIME-type sniffing, facilitando la ejecución de archivos maliciosos.

[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, funcionando como un servidor web alternativo o proxy que amplía la superficie de ataque.
[MEDIUM] Contenido Mixto: Se detectó un recurso de hoja de estilo vinculado mediante HTTP inseguro (discord.gg/pixels) dentro de la página segura.
[MEDIUM] Referrer-Policy: No hay control sobre la información de navegación que se envía a terceros al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando abierta la posibilidad de acceso no deseado a funciones como la cámara o el micrófono.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, proporcionando información técnica que ayuda a un atacante en la fase de reconocimiento.
[LOW] sitemap.xml: El archivo no fue encontrado, lo que dificulta la auditoría de rutas y la indexación correcta.