# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://www.rutificador.live/ | Checks | 9 pruebas |
| Dominio | www.rutificador.live | Hallazgos | 44 totales |
| Fecha | 9 de mayo de 2026 a las 08:22 | Problemas | 12 detectados |

C

70/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web arroja una puntuación de 70/100, lo que corresponde a una calificación de grado C. El análisis constó de 9 checks pasivos, resultando en 5 aprobados, 3 advertencias y 1 fallo crítico relacionado con la configuración de cabeceras. Aunque el cifrado SSL es correcto y está vigente, la ausencia total de políticas de seguridad en las respuestas del servidor y la exposición de puertos críticos representan un riesgo considerable. Debido a la falta de medidas de endurecimiento y la visibilidad de servicios internos, el sitio se considera vulnerable a diversos vectores de ataque.

## Resumen de Riesgos

| 1 | 4 | 5 | 2 | 32 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 90 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 | 60 | AVISO | Falta sitemap.xml |
| Puertos Abiertos | 60 | AVISO | 2 puerto(s) potencialmente riesgoso(s): 22 (SSH)... |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-08-07T00:15:35.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-09T00:15:36.000Z
- 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: https://git.gay/gitgay/pages-server — 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.rutificador.live/
- 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

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1050 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 6379 (Redis)

- 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
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — 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 6379 (Redis) ABIERTO: Este servicio de caché suele carecer de autenticación por defecto, permitiendo el acceso no autorizado a datos sensibles almacenados en memoria.
[HIGH] Content-Security-Policy: Falta esta cabecera indispensable para prevenir ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Falta esta directiva, lo que deja al sitio desprotegido contra ataques de clickjacking que pueden engañar al usuario.
[HIGH] Strict-Transport-Security: HSTS no configurado, lo que impide que el navegador fuerce conexiones HTTPS de manera permanente y segura.
[MEDIUM] Puerto 22 (SSH) ABIERTO: El acceso remoto está expuesto a internet, lo que facilita intentos de intrusión mediante ataques de fuerza bruta.
[MEDIUM] X-Content-Type-Options: Falta esta cabecera, permitiendo que el navegador realice MIME-type sniffing y pueda ejecutar archivos con tipos de contenido incorrectos.
[MEDIUM] Referrer-Policy: Falta esta política, lo que provoca una fuga de información sobre la procedencia del tráfico al navegar hacia enlaces externos.
[MEDIUM] Permissions-Policy: Falta esta configuración para restringir el acceso del navegador a funciones sensibles como la cámara, el micrófono o la ubicación.
[MEDIUM] Bloqueo total en robots.txt: La instrucción Disallow: / impide que cualquier motor de búsqueda indexe el contenido del sitio.
[LOW] Server header expuesto: El servidor revela su tecnología exacta (git.gay/gitgay/pages-server), proporcionando información valiosa para atacantes que busquen vulnerabilidades específicas.
[LOW] sitemap.xml: No se encontró el archivo de mapa del sitio, lo cual afecta la estructura y el rastreo profesional de la web.