

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://fantasy.lu/.well-known/security.txt?_gl=1*n8fosg*_gcl_au*OTAwNDg1MDYxLjE9OTZlMSQ0NDY.	Alcance	190713
Dominio	fantasy.lu	Hallazgos	41 totales
Fecha	6 de octubre de 2026 a las 17:11	Problemas	10 detectados

D

59/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web ha resultado en una puntuación de 59/100, lo que otorga una nota de calificación D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 fueron exitosos, 2 generaron advertencias y 2 resultaron en fallos críticos de configuración. A pesar de contar con un certificado SSL válido, la carencia total de cabeceras de seguridad y la falta de redirección forzosa al protocolo seguro comprometen la integridad del sitio. En su estado actual, la plataforma se considera vulnerable debido a que no implementa las protecciones básicas recomendadas para mitigar ataques comunes en la web.

Resumen de Riesgos

0	5	4	1	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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 robots.txt
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
77 dias restantes (expira: 2026-12-23T02:07:25.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-24T02:07:26.000Z
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 200 — No redirige a HTTPS
- 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 robots.txt

INFO

sitemap.xml
Presente, ? URLs

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 — La ausencia de esta cabecera permite la ejecución de scripts no autorizados, aumentando el riesgo de ataques XSS e inyección de contenido.

[HIGH] X-Frame-Options: Falta — El sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la página en marcos invisibles para engañar a los usuarios.

[HIGH] Strict-Transport-Security: Falta — Al no existir una política HSTS, los navegadores no están obligados a usar conexiones cifradas, facilitando ataques de degradación de protocolo.

[HIGH] Redirección HTTP a HTTPS: Fallo — El servidor responde a peticiones inseguras por el puerto 80 sin redirigirlas automáticamente al entorno seguro, exponiendo los datos en tránsito.

[MEDIUM] X-Content-Type-Options: Falta — El navegador podría intentar interpretar archivos con tipos MIME incorrectos, lo que facilita ataques de sniffing de contenido.

[MEDIUM] Referrer-Policy: Falta — No se controla la cantidad de información de referencia que el navegador envía al navegar hacia otros sitios, pudiendo filtrar datos privados.

[MEDIUM] Permissions-Policy: Falta — No se restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono a través de políticas de origen.

[MEDIUM] Puerto 8080 (HTTP-Alt): Abierto — Se ha detectado un puerto de servidor alternativo activo que podría estar exponiendo servicios internos o interfaces administrativas de forma innecesaria.

[LOW] Server header expuesto: Cloudflare — El servidor revela información sobre su infraestructura tecnológica, lo cual ayuda a posibles atacantes en la fase de reconocimiento.

[LOW] Robots.txt: Falta — No existe un archivo de instrucciones para rastreadores, lo que impide una gestión adecuada de la indexación en motores de búsqueda.