

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Www.goal.com	Checks	9 pruebas
Dominio	www.goal.com	Hallazgos	43 totales
Fecha	26 de septiembre de 2026 a las 07:54	Problemas	2 detectados

A

92/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha otorgado una puntuación de 92/100 con una calificación final de nota A. Se han ejecutado un total de 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias y 2 generaron advertencias técnicas relacionadas con cabeceras de seguridad. No se detectaron fallos críticos ni se procedió con la ejecución de un pentest activo en esta fase del escaneo. En conclusión, el sitio web se considera seguro para la navegación, aunque presenta carencias en las políticas de transporte estricto que deben ser subsanadas.

Resumen de Riesgos

0 CRITICO	2 ALTO	0 MEDIO	0 BAJO	41 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 65 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
65 dias restantes (expira: 2026-11-29T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-15T00:00:00.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- INFO **Content-Security-Policy**
Presente: default-src https;; script-src https: 'unsafe-inline' 'unsafe-eval'; style-src h...

- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: geolocation=(), camera=(), microphone=()

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 302 redirige a https://www.goal.com/de
- 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, Astro

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 — 100/100

Estado: OK
robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (1558 bytes)
- INFO **Reglas robots.txt**
0 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
https://www.goal.com/sitemap
- 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 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

[ALTA] Falta de cabecera Strict-Transport-Security: La ausencia de esta cabecera impide que el servidor obligue a los navegadores a utilizar exclusivamente conexiones cifradas, exponiendo a los usuarios a posibles ataques de degradación de protocolo.
[ALTA] Redirección HTTPS incompleta: Aunque el tráfico HTTP se redirige a HTTPS, la falta de HSTS hace que esta transición no sea obligatoria de forma permanente en el cliente, lo que permite riesgos de interceptación en la conexión inicial.