EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://wow.genoray.com/login?lang=en	Checks	9 pruebas
Dominio	wow.genoray.com	Hallazgos	47 totales
Fecha	20 de julio de 2026 a las 07:26	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha arrojado una puntuación de 68/100, obteniendo una nota final de C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, resultando en 5 verificaciones satisfactorias, 1 advertencia y 3 fallos críticos en la configuración. Aunque el cifrado de datos básico es correcto, se han detectado debilidades significativas en la protección de las cabeceras de respuesta y en la gestión de sesiones. Por tanto, se concluye que el sitio es vulnerable ante ataques de interceptación y secuestro de sesión debido a configuraciones de seguridad incompletas.

Resumen de Riesgos

0	7	3	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 251 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	33	FALLO	GOSSOcookie: falta HttpOnly; GOSSOcookie: falta ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 251 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  251 dias restantes (expira: 2027-03-27T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-12T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: sameorigin
- 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 302 redirige a https://wow.genoray.com/
- 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 — 33/100

Estado: FALLO

GOSSOcookie: falta HttpOnly; GOSSOcookie: falta Secure; GOSSOcookie: falta HttpOnly; GOSSOcookie: falta Secure

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)

- ALTO **Cookie: GOSSOcookie — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: GOSSOcookie — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: GOSSOcookie — SameSite**
  SameSite=lax
- ALTO **Cookie: GOSSOcookie — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: GOSSOcookie — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: GOSSOcookie — SameSite**
  SameSite=lax

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

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

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de contenido y ejecución de scripts maliciosos (XSS) en el navegador del usuario.
[ALTA] Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS a nivel de navegador, lo que facilita ataques de degradación de protocolo y robo de datos en tránsito.
[ALTA] Seguridad de Cookies (GOSSOcookie): La cookie carece de los atributos HttpOnly y Secure, permitiendo que sea accesible mediante scripts y enviada por conexiones no cifradas.
[MEDIA] X-Content-Type-Options: La falta de esta directiva permite el sniffing de tipos MIME, lo que podría llevar al navegador a interpretar archivos de forma incorrecta y peligrosa.
[MEDIA] Referrer-Policy: No hay control sobre la información de origen que se envía a terceros, lo que podría exponer URLs internas o sensibles.
[MEDIA] Permissions-Policy: El sitio no restringe el acceso a funciones del hardware o APIs del navegador como la cámara, el micrófono o la geolocalización.
[BAJA] Redirección HTTPS: El servidor redirige el tráfico pero la ausencia de HSTS genera una ventana de riesgo en el primer contacto del usuario con la web.
[BAJA] Archivos de Estructura: No se encontraron los archivos robots.txt ni sitemap.xml, lo que impide una gestión adecuada de la indexación por parte de motores de búsqueda.