EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://oregonsv.com/?fbclid=IwRlRTSASzkX9wZG9mA2ZkaWQWC1JxEk-TWhx9DHw2GHLFBYY1ZWV4dG4DYWVtAjEwAHNydGMGYXBwX2lkCjY2Mjg1NjgzNzkAAR711dtP5GK9iYZbf3S5vU3a0XackuD5RUSUZdYxn8aBmFlXcrnitdbNSRBdfQ_aem_mUz96aZw2yNNdj83joOG5Q	Checks	9 pruebas
Dominio	oregonsv.com	Hallazgos	46 totales
Fecha	2 de julio de 2026 a las 18:50	Problemas	12 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 64/100, otorgando una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron calificados como fallos críticos. Aunque el cifrado de datos básico es correcto, la ausencia total de cabeceras de protección y la gestión deficiente de sesiones exponen vulnerabilidades importantes. Por tanto, se concluye que el sitio es actualmente vulnerable ante ataques comunes de interceptación y manipulación de datos.

Resumen de Riesgos

0	6	4	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-09-24T22:02:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-26T22:02:42.000Z
- 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: Apache/2.4.58 (Ubuntu) — 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://oregonsv.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
- INFO **Tecnologias detectadas**
  Next.js

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 — 0/100

Estado: FALLO

PHPSESSID: falta HttpOnly; PHPSESSID: falta Secure; PHPSESSID: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: PHPSESSID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: PHPSESSID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: PHPSESSID — SameSite**
  Falta SameSite — Vulnerable a CSRF

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

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **sitemap.xml**
  Presente, 676 URLs
- 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

[HIGH] Ausencia de Content-Security-Policy (CSP): No se detectó esta cabecera, lo que permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] Ausencia de X-Frame-Options: La falta de esta directiva facilita ataques de clickjacking, permitiendo que el sitio sea embebido en marcos de terceros no autorizados.
[HIGH] Ausencia de Strict-Transport-Security (HSTS): El servidor no obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de protocolo.
[HIGH] Cookie PHPSESSID insegura (HttpOnly): La cookie de sesión es accesible mediante JavaScript, lo que facilita el robo de identidad si ocurre un ataque XSS.
[HIGH] Cookie PHPSESSID insegura (Secure): El identificador de sesión puede enviarse a través de conexiones HTTP no cifradas, exponiéndolo a interceptación en la red.
[MEDIUM] Ausencia de X-Content-Type-Options: El navegador podría intentar interpretar el contenido de forma distinta a la declarada, permitiendo ataques de MIME-type sniffing.
[MEDIUM] Cookie PHPSESSID sin atributo SameSite: La ausencia de este control incrementa el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Ausencia de Referrer-Policy y Permissions-Policy: No se limita la información de origen enviada a otros sitios ni se restringen las APIs sensibles del navegador.
[LOW] Exposición de cabecera Server: El servidor revela el software Apache/2.4.58 (Ubuntu), proporcionando información técnica valiosa para un atacante potencial.
[LOW] Ausencia de robots.txt: No se encontró el archivo de directivas para buscadores, lo que puede afectar la gestión del rastreo de la web.