EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://simtec-local.ct.ws/?i=1	Checks	9 pruebas
Dominio	simtec-local.ct.ws	Hallazgos	44 totales
Fecha	1 de abril de 2026 a las 09:35	Problemas	15 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web muestra una puntuación de 61/100, lo que otorga una calificación de nota C. Durante la evaluación, se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos de configuración. A pesar de contar con un cifrado SSL válido, la plataforma carece de las protecciones mínimas recomendadas en la configuración del servidor y cabeceras de seguridad. Debido a la ausencia de mecanismos de defensa contra ataques de inyección y la falta de redirección segura, se concluye que el sitio es actualmente vulnerable. Es necesario implementar medidas correctivas inmediatas para mitigar los riesgos identificados.

Resumen de Riesgos

0	5	8	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 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	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 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-06-25T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-27T00:00:00.000Z
- 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: openresty — 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques XSS y la inyección de contenido no autorizado.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es vulnerable a ataques de clickjacking donde se puede secuestrar la interfaz del usuario.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce el uso exclusivo de conexiones seguras HTTPS.
[HIGH] Redireccion HTTP a HTTPS: El servidor no redirige el tráfico inseguro de forma automática, permitiendo que la navegación ocurra sin cifrado.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a terceros, lo que puede comprometer la privacidad de los usuarios.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Acceso a rutas administrativas y de login: Se detectó que paneles como /wp-login.php, /administrator/ y /user/login son accesibles públicamente.
[MEDIUM] Archivos de información técnica accesibles: Los archivos /readme.html y /README.txt están expuestos y pueden revelar detalles internos del software.
[LOW] Server header expuesto: El encabezado revela que se utiliza la tecnología openresty, proporcionando datos útiles para un atacante.
[LOW] Ausencia de robots.txt y sitemap.xml: El sitio no define reglas de rastreo para motores de búsqueda, lo que afecta la gestión de la seguridad del contenido.