EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://reset.sanclemente.cl/sistemas/orden/index.php	Checks	9 pruebas
Dominio	reset.sanclemente.cl	Hallazgos	45 totales
Fecha	25 de mayo de 2026 a las 20:00	Problemas	16 detectados

F

36/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha dado como resultado una puntuación de 36/100, lo que equivale a una calificación de nota F. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 1 generó una advertencia y 4 finalizaron en fallo crítico. La ausencia de cifrado válido y la falta total de cabeceras de protección básicas representan un riesgo elevado para la integridad de los datos. Se concluye que el sitio es actualmente vulnerable y no cumple con los estándares mínimos de seguridad web profesional.

Resumen de Riesgos

1	7	4	4	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	0	FALLO	PHPSESSID: falta HttpOnly; PHPSESSID: falta Secu...
Contenido Mixto	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  52 dias restantes (expira: 2026-07-16T10:31:50.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-17T10:31:51.000Z
- 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 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/5.3.1 — Revela framework/lenguaje
- 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: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 302 — No redirige a HTTPS

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**
  PHP/5.3.1

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 — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa 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

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

[CRITICAL] Certificado SSL no válido: El certificado SSL no es funcional, lo que impide establecer conexiones cifradas seguras.

[HIGH] Fallo en redirección HTTPS: El servidor no redirige el tráfico de forma automática a una conexión segura, operando bajo el protocolo HTTP expuesto.
[HIGH] Ausencia de Content-Security-Policy: No existe una política que prevenga ataques de inyección de código o XSS.
[HIGH] Falta de X-Frame-Options: El sitio es susceptible a ataques de clickjacking al permitir ser embebido en marcos externos.
[HIGH] Ausencia de Strict-Transport-Security: No se fuerza al navegador a comunicarse exclusivamente mediante HTTPS a través de HSTS.
[HIGH] Cookie PHPSESSID sin flag HttpOnly: La cookie de sesión es accesible mediante scripts de cliente, aumentando el riesgo de robo de sesión.
[HIGH] Cookie PHPSESSID sin flag Secure: La sesión se transmite a través de conexiones no cifradas, facilitando su interceptación.
[MEDIUM] Falta de X-Content-Type-Options: El sitio no previene que el navegador adivine el tipo de contenido, lo que permite ataques de MIME-sniffing.
[MEDIUM] Ausencia de Referrer-Policy: No se controla cuánta información de referencia se envía a otros sitios web al navegar.
[MEDIUM] Falta de Permissions-Policy: No se restringen las capacidades del navegador como el acceso a la ubicación, cámara o micrófonos.
[MEDIUM] Cookie PHPSESSID sin flag SameSite: La falta de este atributo hace que el sitio sea vulnerable a ataques de falsificación de peticiones en sitios cruzados (CSRF).
[LOW] Exposición de cabecera Server: El servidor revela que utiliza Apache, información que ayuda a atacantes a buscar vulnerabilidades específicas.
[LOW] Exposición de X-Powered-By: Se revela el uso de PHP/5.3.1, una versión extremadamente obsoleta y con vulnerabilidades conocidas.
[LOW] Ausencia de archivos de control: No se encontraron los archivos robots.txt ni sitemap.xml para la gestión de indexación.