EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://explendersalud.sytes.net/login	Checks	9 pruebas
Dominio	explendersalud.sytes.net	Hallazgos	42 totales
Fecha	28 de abril de 2026 a las 13:02	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al portal arroja una puntuación de 68/100, lo que resulta en una calificación de grado C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, obteniendo 5 resultados satisfactorios, 2 advertencias por configuraciones riesgosas y 2 fallos críticos en la estructura de protección. A pesar de contar con un certificado SSL válido, la carencia absoluta de cabeceras de seguridad y la exposición de puertos de administración remota incrementan significativamente la superficie de ataque. Se concluye que el sitio es actualmente vulnerable y requiere medidas correctivas inmediatas para proteger la integridad de los datos y la sesión de los usuarios.

Resumen de Riesgos

1	4	4	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 81 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	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	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 3389 (RD...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 81 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  81 dias restantes (expira: 2026-07-18T06:04:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-19T06:04:15.000Z
- 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: nginx/1.22.1 — 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://explendersalud.sytes.net/
- 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 — 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)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 3389 (RDP), 8080 (HTTP-Alt)

- 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
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3389 (RDP): ABIERTO — El servicio de escritorio remoto de Windows está expuesto, permitiendo ataques de fuerza bruta directos contra el servidor.
[HIGH] Content-Security-Policy: Falta — La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de código.
[HIGH] X-Frame-Options: Falta — El sitio es vulnerable a ataques de clickjacking al permitir que el contenido sea cargado en marcos externos no autorizados.
[HIGH] Strict-Transport-Security: Falta — No se obliga al navegador a usar conexiones seguras, lo que permite ataques de degradación de SSL (Mina-in-the-middle).
[MEDIUM] Puerto 8080 (HTTP-Alt): ABIERTO — La presencia de un servidor web alternativo puede exponer paneles de administración o servicios en desarrollo no protegidos.

[MEDIUM] X-Content-Type-Options: Falta — El navegador podría intentar interpretar archivos como scripts (MIME-sniffing), aumentando el riesgo de ejecución de malware.
[MEDIUM] Referrer-Policy: Falta — No se controla la información de referencia enviada a otros dominios, lo que podría filtrar URLs internas sensibles.
[MEDIUM] Permissions-Policy: Falta — No existen restricciones sobre el acceso del navegador a funciones de hardware como cámara, micrófono o geolocalización.
[LOW] Server header expuesto: Server: nginx/1.22.1 — La divulgación de la versión exacta del servidor permite a atacantes buscar exploits específicos para esa versión.
[LOW] robots.txt: No encontrado — La ausencia de este archivo impide una gestión adecuada del rastreo por parte de motores de búsqueda.
[LOW] sitemap.xml: No encontrado — No se proporciona un mapa de la estructura del sitio, afectando la organización y visibilidad de los recursos.