EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://redprofesional.juntadeandalucia.es/	Checks	9 pruebas
Dominio	redprofesional.juntadeandalucia.es	Hallazgos	48 totales
Fecha	23 de julio de 2026 a las 09:49	Problemas	14 detectados

C

67/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica del dominio ha dado como resultado una puntuación exacta de 67/100, lo que otorga al sitio una nota de C. Se han realizado 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron calificados como fallos críticos. A pesar de contar con un certificado SSL robusto, la carencia de cabeceras de seguridad modernas y la deficiente configuración de las cookies de sesión comprometen la integridad de la plataforma. Concluimos que el sitio es actualmente vulnerable ante ataques de secuestro de sesión e inyección de contenido debido a estas omisiones en la configuración del servidor.

Resumen de Riesgos

0	5	7	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 136 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	0	FALLO	Elgg: falta HttpOnly; Elgg: falta Secure; Elgg: ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 136 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  136 dias restantes (expira: 2026-12-06T07:55:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-21T07:55:30.000Z
- 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

- BAJO **Server header expuesto**
  Server: Apache/2.2.15 (Red Hat) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.0.33 — Revela framework/lenguaje
- 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 307 redirige a https://redprofesional.juntadeandalucia.es/
- 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**
  PHP/7.0.33

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
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 0/100

Estado: FALLO

Elgg: falta HttpOnly; Elgg: falta Secure; Elgg: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: Elgg — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: Elgg — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: Elgg — 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 sitemap.xml

- INFO **robots.txt**
  Presente (61 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de ejecución de scripts no autorizados (XSS) e inyección de datos.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce siempre una conexión cifrada, permitiendo ataques de degradación de SSL.
[HIGH] Cookie Elgg (HttpOnly): La cookie de sesión no tiene el flag HttpOnly, lo que permite que sea robada mediante scripts maliciosos en el navegador.
[HIGH] Cookie Elgg (Secure): Falta el flag Secure, lo que significa que la cookie de sesión podría transmitirse a través de conexiones HTTP no cifradas.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el servidor no evita que el navegador realice "MIME-sniffing", lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No existe una política definida para controlar cuánta información de referencia se envía a otros sitios web al navegar.
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, dejando expuestas funciones como la cámara, el micrófono o la geolocalización.
[MEDIUM] Cookie Elgg (SameSite): La ausencia de este atributo hace que el sitio sea vulnerable a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles públicamente y pueden revelar detalles técnicos o versiones del software base.
[MEDIUM] Robots.txt (Bloqueo total): El archivo robots.txt está configurado para bloquear todo el sitio (Disallow: /), lo que puede afectar la visibilidad y sugerir una configuración restrictiva mal aplicada.
[LOW] Server header expuesto: El servidor revela que utiliza Apache/2.2.15 (Red Hat), una versión antigua que facilita a los atacantes encontrar exploits específicos.
[LOW] X-Powered-By expuesto: La cabecera revela el uso de PHP/7.0.33, exponiendo el lenguaje de programación y su versión exacta.