EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.cifprodolfoucha.es/	Checks	9 pruebas
Dominio	www.cifprodolfoucha.es	Hallazgos	46 totales
Fecha	24 de septiembre de 2026 a las 14:02	Problemas	16 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web muestra una puntuación de 59/100, lo que otorga una calificación de grado D. Se han ejecutado un total de 9 checks pasivos, de los cuales 4 resultaron correctos, se emitieron 2 advertencias y se detectaron 2 fallos críticos de configuración. Aunque el cifrado de transporte básico está presente, la ausencia total de cabeceras de seguridad y la exposición de servicios de administración suponen un riesgo elevado. Por tanto, se concluye que el sitio es actualmente vulnerable y requiere intervenciones correctivas inmediatas para mitigar posibles ataques de inyección y acceso no autorizado.

Resumen de Riesgos

0	5	8	3	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 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	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	4 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 65 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  65 dias restantes (expira: 2026-11-28T06:46:41.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-30T06:46:42.000Z
- 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: nginx — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.33, PleskLin — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.cifprodolfoucha.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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.1.2
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.33, PleskLin

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 — 20/100

Estado: FALLO

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.edu.xunta.gal/portal/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.edu.xunta.es/fp/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.edu.xunta.gal/portal/es/cfrferrol
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (180 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.cifprodolfoucha.es/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking donde un atacante puede camuflar la interfaz.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo ataques de degradación de SSL.
[HIGH] Puerto 21 (FTP): El servicio de transferencia de archivos está abierto y opera sin cifrado, exponiendo credenciales de acceso.
[MEDIUM] Contenido Mixto: Se detectaron 4 recursos cargados mediante HTTP en una página HTTPS, lo cual compromete la integridad de la sesión cifrada.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite a los navegadores realizar sniffing de tipos MIME, facilitando la ejecución de archivos maliciosos.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a terceros, lo que puede derivar en fugas de privacidad.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a funciones sensibles como cámara o geolocalización.
[MEDIUM] Puerto 22 (SSH): La exposición del puerto de acceso remoto seguro incrementa el riesgo de intentos de intrusión por fuerza bruta.
[LOW] Cabeceras de tecnología expuestas: Los encabezados Server y X-Powered-By revelan el uso de nginx, PHP/8.3.33 y PleskLin.
[LOW] Exposición de versión de CMS: El meta generator revela públicamente que el sitio utiliza WordPress 7.1.2.